Groupe de travail Réseau
Request for Comments : 4949
FYI : 36
RFC rendue obsolète : 2828
Catégorie : Information

R. Shirey
août 2007

Traduction Claude Brière de L'Isle

Glossaire de la sécurité de l'Internet, version 2

Statut du présent mémoire
Le présent mémoire fournit des informations pour la communauté de l'Internet. Il ne spécifie aucune norme de l'Internet. La distribution du présent mémoire n'est soumise à aucune restriction.

Note de l'éditeur de la RFC
Le présent document est à la fois une révision et une expansion substantielle du Glossaire de la sécurité de la RFC 2828. Ce glossaire révisé est une référence majeure qui devrait aider la communauté de l'Internet à améliorer la clarté de la documentation et des discussions dans un domaine important de la technologie Internet. Cependant, les lecteurs devraient être conscients de ce qui suit :

(1) Les recommandations et certaines interprétations particulières dans les définitions sont celles de l'auteur, et non une position officielle de l'IETF. L'IETF n'a pas pris de position formelle, ni pour, ni contre les recommandations faites dans ce glossaire, et l'utilisation du langage de la [RFC2119] (par exemple, NE DEVRAIT PAS) dans le glossaire ne doit pas être entendue comme une prescription officielle. En d'autres termes, les règles d'utilisation, l'interprétation des expressions, et les autres recommandations du présent glossaire sont des opinions personnelles de l'auteur de ce glossaire. Les lecteurs devront juger par eux-mêmes s'ils doivent ou non suivre ses recommandations, sur la base de leurs propres connaissances combinées avec les raisonnements présentés dans le glossaire.

(2) Le glossaire est riche de l'histoire des premiers travaux sur la sécurité des réseaux, mais il peut être un peu incomplet sur la description des travaux récents en matière de sécurité, qui se sont développés rapidement.

Résumé
Le présent glossaire fournit des définitions, abréviations, et explications de terminologie pour les systèmes de sécurité de l'information. Les 164 pages d'entrées offrent des recommandations pour améliorer la compréhensibilité des matériaux écrits qui sont générés dans le processus de normalisation de l'Internet (RFC2026). Les recommandations suivent les principes que de telles rédactions devraient (a) utiliser le même terme ou définition chaque fois que le même concept est mentionné ; (b) utiliser les termes dans leur sens le plus ordinaire, le sens du dictionnaire ; (c) utiliser des termes qui sont déjà bien établis dans des publications accessibles ; et (d) éviter les termes qui favorisent un fabricant particulier ou favorisent une technologie ou mécanisme particulier par rapport à un autre, ou les techniques qui existent déjà ou pourraient être développées.

Table des Matières

1. Introduction

Ce glossaire *n'est pas* une norme de l'Internet, et ses recommandations représentent seulement les opinions de son auteur. Cependant, ce glossaire donne les raisons de ses recommandations – en particulier pour les NE DEVRAIT PAS – de façon que le lecteur puisse juger par lui-même de ce qu'il doit faire.

Ce glossaire fournit un ensemble de termes d'abréviations et de définitions cohérent et auto suffisant – soutenu par des explications, recommandations, et références – pour la terminologie qui concerne la sécurité des systèmes d'information. L'intention de ce glossaire est d'améliorer la compréhension des matériaux écrits qui sont générés dans le processus de normalisation de l'Internet (RFC2026) – c'est-à-dire, les RFC, les projets Internet, et les autres éléments du discours – qui sont désignés ici sous le nom de IDOC. Quelques termes de réseautage, extérieurs à la sécurité, sont inclus pour que ce glossaire soit auto suffisant, mais des glossaires plus complets de ces termes sont disponibles ailleurs [A1523], [F1037], [RFC1208], [RFC1983].

Ce glossaire soutient les objectif du processus de normalisation de l'Internet :

- Documentation claire, concise, facilement compréhensible
  Ce glossaire cherche à améliorer la compréhension du contenu en rapport avec la sécurité des IDOC. Cela exige que la formulation soit claire et compréhensible, et que l'ensemble des termes et définitions qui se rapportent à la sécurité soit cohérent et auto suffisant. La terminologie doit aussi être uniforme à travers les IDOC ; c'est-à-dire, le même terme ou définition doit être utilisé chaque fois et partout où le même concept est mentionné. L'harmonisation des IDOC existants n'a pas besoin d'être effectuée immédiatement, mais il est souhaitable de corriger et normaliser la terminologie quand de nouvelles versions sont produites dans le cours normal du développement et l'évolution des normes.

- Excellence technique
  Tout comme les protocoles normalisés de l'Internet (STD) devraient fonctionner efficacement, les IDOC devraient utiliser une terminologie adéquate, précise et sans ambiguïté pour permettre la mise en œuvre correcte des normes.

- Mise en œuvre et essais préalables
  Tout comme les protocoles standard requièrent une expérience et une stabilité démontrée avant leur adoption, les IDOC ont besoin d'utiliser un langage bien établi ; et le principe de robustesse pour les protocoles -- "soyez libéral dans ce que vous acceptez, et conservateur dans ce que vous envoyez" -- est aussi applicable au langage utilisé dans les IDOC qui décrivent les protocoles. Utiliser les termes dans leur vrai sens, celui du dictionnaire (quand c'est approprié) aide à les faire mieux comprendre des lecteurs internationaux. Les IDOC doivent éviter d'utiliser des termes privés, nouvellement inventés à la place de termes généralement acceptés, pour les publications ouvertes au public. Les IDOC doivent éviter de substituer de nouvelles définitions qui entrent en conflit avec celles qui sont établies. Les IDOC doivent éviter d'utiliser de "jolis" synonymes (par exemple, "Livre Vert"), parce que quelle que soit la popularité d'un surnom dans une communauté, il va créer de la confusion dans une autre.

  Cependant, bien que le présent glossaire se veuille en bon anglais international, ses termes et définitions ont le biais de l'anglais tel qu'il est utilisé aux États Unis d'Amérique (U.S.A). Aussi, par rapport à la terminologie utilisée par les gouvernements nationaux et dans les milieux de la défense nationale, le glossaire ne vise qu'une utilisation aux USA.

- Ouverture, impartialité et à propos
  Les IDOC doivent éviter d'utiliser des termes brevetés ou marqués par un usage commercial pour des objets autres que la référence à ces systèmes particuliers. Les IDOC doivent aussi éviter les termes qui favorisent un fabricant particulier ou une technologie de sécurité particulière, ou un mécanisme par rapport à d'autres, des techniques en concurrence qui existent déjà ou pourraient être développées à l'avenir. L'ensemble de la terminologie utilisée à travers l'ensemble des IDOC doit être souple et adaptable pour suivre l'évolution de l'art de la sécurité sur l'Internet.

À l'appui de ces objectifs, le présent glossaire propose des directives en marquant les termes et définitions comme étant recommandés ou déconseillés dans les IDOC. Les mots clés "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" sont destinés à être interprétés de la même façon que dans les normes de l'Internet (c'est-à-dire, comme spécifié dans la [RFC2119]). D'autres glossaires (par exemple, [Raym]) énumèrent des termes supplémentaires qui traitent de la sécurité de l'Internet mais n'ont pas été inclus dans le présent glossaire parce qu'ils ne sont pas appropriés pour les IDOC.

2. Format des entrées

La Section 4 présente les entrées du glossaire de la façon suivante :

2.1 Ordre des entrées

Les entrées sont triées dans l'ordre lexicographique, sans considération des majuscules. Les chiffres sont traités comme précédant les caractères alphabétiques, et les caractères spéciaux sont traités comme précédant les chiffres. Les blancs sont traités comme précédant les caractères non blancs, excepté qu'un trait d'union ou une barre oblique entre les parties d'une entrée de plusieurs mots (par exemple, séparation "ROUGE/NOIR") est traité comme un blanc.

Si une entrée a plusieurs définitions (par exemple, "domaine") elles sont numérotés en commençant par "1", et si une de ces définitions multiples est d'utilisation RECOMMANDÉE dans les IDOC, elle est présentée avant les autres définitions pour cette entrée. Si des définitions sont en rapports étroits (par exemple, "menace") elles sont notées avec l'ajout de lettres au nombre, telles que "1a" et "1b".

2.2 Majuscules et abréviations

Les entrées qui sont des noms propres sont en majuscules (par exemple, "Algorithme de chiffrement des données") comme le sont les autres mots dérivés de noms propres (par exemple, "chiffrement Caesar"). Toutes les autres entrées sont en minuscules (par exemple, "autorité de certification"). Chaque acronyme ou autre abréviation apparaissant dans ce glossaire, soit comme entrée, soit comme définition ou explication, est défini dans le glossaire, excepté les éléments d'usage courant, tels que "aussi dit", "par exemple", "etc.", "c'est-à-dire", "vol.", "pp.", et "U.S.A".

2.3 Recherche automatique

Chaque entrée est précédée d'un signe dollar ($) et d'une espace. Cela rend possible de trouver l'entrée avec la définition pour un élément "X" en cherchant la chaîne de caractères "$ X", sans s'arrêter aux autres entrées dans lesquelles "X" est utilisé dans les explications.

2.4 Type et contexte des définitions

Chaque entrée est précédée par un caractère -- I, N, O, ou D – entre parenthèses, pour indiquer le type de définition (comme expliqué à la Section 3) :

- "I" pour un terme ou définition RECOMMANDÉ d'origine Internet.
- "N" si RECOMMANDÉ mais pas d'origine Internet.
- "O" pour un terme ou définition dont l'utilisation dans les IDOC N'EST PAS recommandée mais est quelque chose que les auteurs des documents de l'Internet devraient connaître.
- "D" pour un terme ou définition qui est déconseillé et NE DEVRAIT PAS être utilisé dans les documents de l'Internet.

Si une définition n'est valide que dans un contexte spécifique (par exemple, "bagage") ce contexte est indiqué immédiatement à la suite du type de définition et est entouré d'une paire de symboles barre oblique (/). Si la définition n'est valide que pour des parties de termes spécifiques, cela est indiqué de la même façon (par exemple, "archive").

2.5 Notes explicatives

Certaines entrées ont un texte explicatif qui est introduit par un ou plusieurs des mots clés suivants :

- Abréviation déconseillée (par exemple, "AA")
- Définition déconseillée (par exemple, "certification numérique")
- Usage déconseillé (par exemple, "authentifié")
- Terme déconseillé (par exemple, "autorité de certificat")
- Prononciation (par exemple, "*-propriété")
- Dérivation (par exemple, "contrôle d'accès discrétionnaire")
- Instructions (par exemple, "accréditation")
- Exemple (par exemple, "par la porte de derrière *(back door)*")
- Usage (par exemple, "accès")

Le texte explicatif de ce glossaire PEUT être réutilisé dans les IDOC. Cependant, ce texte n'est pas destiné à se substituer autoritairement au texte d'un IDOC dans lequel l'entrée du glossaire est déjà utilisée.

2.6 Références croisées

Certaines entrées contiennent une remarque entre parenthèses de la forme "(Voir : X.)", où X est une liste d'autres termes en rapport. Certaines entrées contiennent une remarque de la forme "(Comparer : X)", où X est une liste de termes qui sont des

antonymes de l'entrée ou en diffèrent d'une autre façon digne d'être notée.

2.7 Marques commerciales

Toutes les marques de service et marques commerciales qui apparaissent dans le présent glossaire sont utilisées de façon rédactionnelle et pour le bénéfice du propriétaire de la marque, sans aucune intention de contrefaçon.

2.8 La nouvelle ponctuation

Ce glossaire utilise le "nouveau" style de ponctuation "logique" en faveur chez les programmeurs d'ordinateurs, comme décrit par Raymond [Raym] : les programmeurs utilisent des paires de guillemets de la même façon qu'ils utilisent des paires de parenthèses, c'est-à-dire, comme des délimiteurs. Par exemple, si "Alice envoie" est une phrase, ainsi que "Bill reçoit" et "Eve écoute", un programmeur écrirait les phrases suivantes : "Alice envoie", "Bill reçoit", et "Eve écoute".

Selon l'usage américain standard, la ponctuation dans cette phrase est incorrecte ; les virgules de continuation et le point final devraient aller à l'intérieur des guillemets, comme cela : "Alice envoie," "Bill reçoit," et "Eve écoute."
(Cette discussion n'a pas de sens en français où les normes typographiques en vigueur sont à l'inverse, c'est-à-dire conformes à la ponctuation "logique".)

Cependant, un programmeur n'inclura pas un caractère dans une chaîne littérale si le caractère ne lui appartient pas, parce que cela pourrait causer une erreur. Par exemple, supposons une phrase avec un projet d'instruction sur le langage d'édition vi qui ressemblerait à ceci :

> Effacer ensuite une ligne du fichier en tapant "dd".

Un éditeur qui suivrait l'usage standard pourrait transformer la phrase pour qu'elle donne ceci :

> Puis effacer une ligne du fichier en tapant "dd."

Cependant, dans le langage vi, le caractère point répète la dernière commande acceptée. De sorte que si un lecteur rentre "dd.", deux lignes seront effacées au lieu d'une.

De même, l'utilisation de la ponctuation standard américaine pourrait provoquer des malentendus dans les entrées de ce glossaire. Et donc, on utilise la nouvelle ponctuation, et nous recommandons son utilisation pour les IDOC.

3. Types d'entrées

Chaque entrée dans ce glossaire est marquée d'un type I, N, O, ou D.

3.1 Type "I" : Définitions recommandées d'origine Internet

Le marquage "I" indique deux choses :

- Origine : "I" (par opposition à "N") signifie que le processus de normalisation de l'Internet ou la communauté de l'Internet est d'autorité pour la définition *ou* que le terme est suffisamment générique pour que ce glossaire puisse librement établir une définition sans entrer en contradiction avec une autorité non Internet (par exemple, "attaque").
- Recommandation : "I" (par opposition à "O") signifie que l'utilisation du terme et de la définition est RECOMMANDÉE dans les IDOC. Cependant, certaines entrées "I" peuvent être accompagnées d'une note "Usage" qui établit une limitation (par exemple, "certification") et les IDOC NE DEVRAIENT PAS utiliser le terme défini en dehors de ce contexte limité.

De nombreuses entrées "I" sont des noms propres (par exemple, "protocole Internet") pour lesquels la définition est destinée à fournir seulement une information de base ; c'est-à-dire que la définition d'autorité pour de tels termes se trouve ailleurs. Pour un nom propre décrit comme un "protocole Internet", prière de se référer à l'édition la plus récente des "Normes officielles des protocoles de l'Internet" (STD 1) pour voir l'état de la normalisation du protocole.

3.2 Type "N" : Définitions recommandées d'origine non Internet

Le marquage "N" indique deux choses :

- Origine : "N" (par opposition à "I") signifie que l'entrée a une base ou origine non Internet.
- Recommandation : "N" (par opposition à "O") signifie que l'utilisation du terme et de la définition est RECOMMANDÉE dans les IDOC, pour autant qu'ils y soient nécessaires. Beaucoup de ces entrées sont accompagnées d'une étiquette qui établit un contexte (par exemple, "paquetage") ou une note qui établit une limitation (par exemple, "intégrité des données") et les IDOC NE DEVRAIENT PAS utiliser le terme défini en dehors de ce contexte ou limite. On s'attend à ce que certains contextes ne soient que rarement, sinon jamais, évoqués dans un IDOC (par exemple,

"bagage"). Dans ces cas, ils sont cités pour avertir les auteurs de l'Internet de la non utilisation Internet de façon qu'ils puissent éviter des conflits avec les documents non Internet.

3.3 Type "O": Autres termes et définitions à noter

Le marquage "O" signifie que la définition est d'origine non Internet et NE DEVRAIT PAS être utilisée dans les IDOC *excepté* dans les cas où le terme est spécifiquement identifié comme non Internet.

Par exemple, un IDOC pourrait mentionner "BCA" (voir : autorité de certification de marque) ou "bagage" comme exemple d'un concept ; dans ce cas, le document devrait dire spécifiquement "SET(marque commerciale) BCA" ou "SET(marque commerciale) bagage" et inclure la définition du terme.

3.4 Type "D": Termes et définitions déconseillés

Si le présent glossaire recommande qu'un terme ou définition NE DEVRAIT PAS être utilisé dans les IDOC, l'entrée est alors marquée comme type "D", et une note explicative -- "Terme déconseillé", "Abréviation déconseillée", "Définition déconseillée", ou "Utilisation déconseillée" -- est fournie.

3.5 Substitutions de définition

Certains termes ont une définition publiée par une autorité non Internet -- un gouvernement (par exemple, "Réutilisation d'objet") une industrie (par exemple, "Échange de données sécurisé") une autorité nationale (par exemple, "Norme de chiffrement des données") ou une organisation internationale (par exemple, "Confidentialité des données") – qu'il convient d'utiliser dans les IDOC. Dans ces cas, le présent glossaire marque la définition avec "N", recommandant son utilisation dans les documents de l'Internet.

D'autres de ces termes ont des définitions qui sont inadéquates ou inappropriées pour les IDOC. Par exemple, une définition peut être désuète ou trop restrictive, ou elle pourrait avoir besoin d'être précisée en substituant une formulation plus précise (par exemple, "Échange d'authentification") ou des explications, en utilisant d'autres termes qui sont définis dans le présent glossaire. Dans ces cas, le glossaire marque l'entrée avec "O", et fournit une entrée "I" ou "N" qui précède, et est destinée à se substituer à l'entrée "O".

Dans certains cas où le présent glossaire fournit une définition pour remplacer une définition "O", le substitut est destiné à se substituer à la signification de l'entrée "O" et non pas d'entrer en conflit avec elle. Pour le terme "Service de sécurité", par exemple, la définition "O" ne traite qu'étroitement des services de communication fournis par des couches dans l'OSIRM et est inadéquate pour la gamme complète d'utilisation des IDOC, alors que la nouvelle définition "I" fournie par ce glossaire peut être utilisée dans des situations et des sortes de services plus nombreuses. Cependant, la définition "O" figure aussi dans la liste, de sorte que les auteurs de IDOC seront avertis du contexte dans lequel le terme est utilisé dans son sens le plus étroit.

Lorsque il fait des substitutions, le présent glossaire essaye d'éviter de contredire toute autorité non Internet. Il reste cependant que la terminologie diffère entre des autorités telles que l'American Bar Association, l'OSI, SET, le U.S. DoD, et d'autres autorités, et le présent glossaire n'est probablement exactement en ligne avec aucune d'entre elles.

4. Définitions

$ propriété * *(*-property)*
(N) Synonyme de "propriété de confinement" dans le contexte du modèle Bell-LaPadula. Prononcer propriété étoile.

$ 3DES (N) Voir : Triple algorithme de chiffrement de données.

$ système informatique A1 *(A1 computer system)*
(O) /TCSEC/ Voir : Instructions sous "Critères d'évaluation de système informatique de confiance ". (Comparer à au-delà de A1.)

$ AA (D) Voir : Utilisation déconseillée sous "autorité d'attribut".

$ Lignes directrices ABA *(ABA Guidelines)*
(N) "Lignes directrices pour les signatures numériques de l'American Bar Association (ABA)" [DSG], un cadre de principes juridiques pour l'utilisation des signatures numériques et des certificats numériques dans le commerce électronique.

$ Notation de syntaxe abstraite n° 1 (ASN.1, *Abstract Syntax Notation One*)

(N) Norme pour la description des objets de données. [Larm], [X680] (Voir : CMS.)
Usage : les IDOC DEVRAIENT utiliser le terme "ASN.1" de façon étroite pour décrire la notation ou langage appelé "Notation de syntaxe abstraite n° 1". Les IDOC PEUVENT utiliser le terme de façon plus large pour renfermer la notation, ses règles de codage associées (voir BER) et les outils logiciels qui aident à son utilisation, lorsque le contexte rend cette signification claire.
Instructions : l'OSIRM définit les fonctions de réseau informatique en couches. Les protocoles et les objets de données aux couches supérieures sont définis abstraitement pour être mis en œuvre en utilisant les protocoles et les objets de données à partir des couches inférieures. Une couche supérieure peut définir des transferts d'objets abstraits entre ordinateurs, et une couche inférieure peut définir ces transferts concrètement comme des chaînes de bits. Une syntaxe est nécessaire pour spécifier les formats de données des objets abstraits, et des règles de codage sont nécessaires pour transformer les objets abstraits en chaînes binaires aux couches inférieures. Les normes OSI utilisent l'ASN.1 pour ces spécifications et utilisent diverses règles de codage pour ces transformations. (Voir : BER.)
En ASN.1, les noms formels sont écrits sans espaces, et les mots séparés d'un nom sont indiqués en mettant en majuscule la première lettre de chaque mot, sauf du premier mot. Par exemple, le nom d'une CRL est "certificateRevocationList".

$ risque acceptable *(acceptable risk)*
(I) Risque qui est compris et toléré par l'utilisateur, l'opérateur, le propriétaire, ou le certificateur d'un système, usuellement parce que le coût ou la difficulté de mettre en œuvre une contre-mesure efficace de la vulnérabilité associée excède les évaluations de pertes. (Voir : sécurité adéquate, risque, "seconde loi" sous "Lois de Courtney".)

$ accès *(access)*
1a. (I) Capacité et moyens pour communiquer avec, ou autrement interagir avec, un système pour utiliser les ressources du système pour traiter des informations ou pour obtenir connaissance des informations que le système contient. (Comparer à : bride.)
Usage : La définition est destinée à inclure tous les types de communication avec un système, y compris la communication unidirectionnelle dans l'une ou l'autre direction. En pratique cependant, les utilisateurs passifs peuvent être traités comme n'ayant pas "accès" et donc, être exempts de la plupart des exigences de la politique de sécurité du système. (Voir : "utilisateur passif" sous "utilisateur".)
1b. (O) "Opportunité de faire usage des ressources d'un système d'informations (IS)." [C4009]
2. (O) /modèle formel/ "Un type spécifique d'interaction entre un sujet et un objet qui résulte en un flux d'informations de l'un à l'autre." [NCS04]

$ Certificat d'accès pour services électroniques (ACES, *Access Certificate for Electronic Services*)
(O) PKI gérée par l'administration des services généraux du gouvernement américain en coopération avec des partenaires industriels. (Voir : CAM.)

$ contrôle d'accès *(access control)*
1. (I) Protection des ressources système contre l'accès non autorisé.
2. (I) Processus par lequel l'utilisation de ressources système est régulée conformément à une politique de sécurité et n'est permise que par les entités autorisées (usagers, programmes, processus, ou autres systèmes) conformément à cette politique. (Voir : accès, service de contrôle d'accès, sécurité informatique, contrôle d'accès discrétionnaire, contrôle d'accès obligatoire, contrôle d'accès fondé sur le rôle.)
3. (I) Modèle formel/ limitations aux interactions entre sujets et objets dans un système d'information.
4. (O) "Prévention de l'usage non autorisé d'une ressource, y compris la prévention de l'utilisation d'une ressource d'une manière non autorisée." [I7498-2]
5. (O) /Gouvernement US/ Système qui utilise des contrôles physiques, électroniques, ou humains pour identifier ou admettre des personnels munis d'un accès proprement autorisé à une SCIF.

$ centre de contrôle d'accès (ACC, *access control center*)
(I) Ordinateur qui tient une base de données (éventuellement sous la forme d'une matrice de contrôle d'accès) qui définit la politique de sécurité pour un service de contrôle d'accès, et qui agit comme un serveur pour les clients qui demandent des décisions de contrôle d'accès.
Instructions : Un ACC est parfois utilisé en conjonction avec un centre de clés pour mettre en œuvre un contrôle d'accès dans un système de distribution de clés pour une cryptographie symétrique. (Voir : BLACKER, Kerberos.)

$ liste de contrôle d'accès (ACL, *access control list*)
(I) /système d'information/ Mécanisme qui met en œuvre le contrôle d'accès pour une ressource système en énumérant les entités du système auxquelles il est permis d'accéder à la ressource et en déclarant, implicitement ou explicitement, les modes d'accès accordés à chaque entité. (Comparer : matrice de contrôle d'accès, liste d'accès, profil d'accès, liste de capacités.)

$ matrice de contrôle d'accès *(access control matrix)*
(I) Dispositif rectangulaire de cellules, avec une rangée par sujet et une colonne par objet. L'entrée dans une cellule – c'est-à-dire, l'entrée pour une paire sujet-objet particulière – indique les modes d'accès qu'il est permis au sujet d'exercer sur l'objet. Chaque colonne est équivalente à une "liste de contrôle d'accès" pour l'objet; et chaque rangée est équivalente à un "profil d'accès" pour le sujet.

$ service de contrôle d'accès *(access control service)*
(I) C'est un service de sécurité qui protège contre une entité système utilisant une ressource système d'une façon non autorisée par la politique de sécurité du système. (Voir : contrôle d'accès, contrôle d'accès discrétionnaire, politique de sécurité fondée sur l'identité, contrôle d'accès obligatoire, politique de sécurité fondée sur des règles.)
Instructions : Ce service inclut la protection contre l'utilisation d'une ressource d'une façon non autorisée par une entité (c'est-à-dire, un principal) qui est autorisée à utiliser la ressource d'une autre manière. (Voir : initié.) Les deux mécanismes de base pour la mise en œuvre de ce service sont les ACL et les tickets.

$ niveau d'accès *(access level)*
1. (D) Synonyme de "niveau de classification" hiérarchique dans un niveau de sécurité. [C4009] (Voir : niveau de sécurité.)
2. (D) Synonyme de "niveau d'habilitation".
Définitions déconseillées : Les IDOC NE DEVRAIENT PAS utiliser ce terme avec ces définitions parce qu'elles dupliquent la signification de termes plus spécifiques. Tout IDOC qui utilise ce terme DEVRAIT en fournir une définition spécifique parce que le contrôle d'accès peut être fondé sur de nombreux attributs autres qu'un niveau de classification et un niveau d'habilitation.

$ liste d'accès *(access list)*
(I) /sécurité physique/ Liste de personnes qui sont autorisées à entrer dans une enceinte contrôlée. (Comparer : liste de contrôle d'accès.)

$ mode d'accès *(access mode)*
(I) Type distinct d'opération de traitement de données (par exemple, lire, écrire, ajouter, ou exécuter, ou une combinaison d'opérations) qu'un sujet peut effectuer sur un objet dans un système d'informations. [Huff] (Voir : lire, écrire.)

$ politique d'accès *(access policy)*
(I) C'est une sorte de "politique de sécurité". (Voir : accès, contrôle d'accès.)

$ profil d'accès *(access profile)* (O) Synonyme de "liste de capacités".
Usage : Les IDOC qui utilisent ce terme DEVRAIENT en donner une définition parce que la définition n'est pas très connue.

$ droit d'accès *(access right)*
(I) Synonyme de "autorisation" ; met l'accent sur la possession de l'autorisation par une entité d'un système.

$ traçabilité *(accountability)*
(I) Propriété d'un système ou d'une ressource d'un système qui assure que les actions d'une entité système peuvent être retracées de façon univoque jusqu'à cette entité, qui peut donc être tenue pour responsable de ses actions. [Huff] (Voir : service d'audit.)
Instructions : La traçabilité (autrement dit, la responsabilité individuelle) exige normalement d'un système la capacité à associer positivement l'identité d'un utilisateur avec le moment, la méthode, et le mode de l'accès de l'utilisateur au système. Cette capacité prend en charge la détection et l'investigation ultérieure sur ceux qui enfreignent la sécurité. Les individus qui sont des utilisateurs d'un système sont tenus pour responsables de leurs actions après que leur ont été notifiées les règles de comportement pour l'utilisation du système et les pénalités associées à la violation de ces règles.

$ comptabilité *(accounting)* Voir : comptabilité COMSEC.

$ code de légende comptable (ACL, *accounting legend code*)
(O) / Gouvernement des USA/ Système numérique utilisé pour indiquer les contrôles comptables minimum exigés pour les éléments du matériel de COMSEC au sein du CMCS. [C4009] (Voir : comptabilité COMSEC.)

$ accréditation *(accreditation)*
(N) Action administrative par laquelle une autorité désignée déclare qu'un système d'informations est approuvé pour fonctionner dans une configuration de sécurité particulière avec un ensemble prescrit de sauvegardes. [FP102], [SP37] (Voir certification.)

Instructions : Une accréditation est usuellement fondée sur une certification technique des mécanismes de sécurité du système. Pour accréditer un système, l'autorité qui approuve doit déterminer que tout risque résiduel est un risque acceptable. Bien que les termes de "certification" et "accréditation" soient plus utilisés par le Ministère U.S. de la Défense et les autres agences gouvernementales que dans les organisations commerciales, le concept s'applique en tout endroit où des gestionnaires sont obligés de prendre et accepter la responsabilité de risques pour la sécurité. Par exemple, l'American Bar Association développe des critères d'accréditation pour les CA.

$ limite d'accréditation *(accreditation boundary)* (O) Synonyme de "périmètre de sécurité". [C4009]

$ accréditeur *(accreditor)*
(N) Gestionnaire officiel qui a été désigné pour avoir l'autorité formelle pour "accréditer" un système d'information, c'est-à-dire, pour autoriser le fonctionnement et le traitement de données sensibles dans le système et pour accepter les risques résiduels associés au système. (Voir : accréditation, risque résiduel.)

$ organisme de crédit *(acquirer)*
1. (O) /SET/ "C'est l'institution financière qui établit un compte avec un commerçant et traite les autorisations de carte de payement et les payements." [SET1]
2. (O) /SET/ "C'est l'institution (ou son agent) qui acquiert du détenteur de la carte les données financières qui se rapportent à la transaction et qui introduit les données dans un système d'échange." [SET2]

$ données d'activation *(activation data)*
(N) Données secrètes, autre que les clés, qui sont requises pour accéder à un module de chiffrement. (Voir : CIK. Comparer : valeur d'initialisation.)

$ attaque active *(active attack)* (I) Voir : définition secondaire sous "attaque".

$ contenu actif *(active content)*
1a. (I) Logiciel exécutable qui est lié à un document ou autre fichier de données et qui s'exécute automatiquement lorsque un usager accède au fichier, sans initiation explicite par l'usager. (Comparer : code mobile.)
Instructions : un contenu actif peut être un code mobile lorsque son fichier associé est transféré à travers un réseau.
1b. (O) "Document électronique qui peut porter ou déclencher des actions automatiques sur une plate-forme d'ordinateur sans l'intervention d'un usager. [Cette technologie permet au] code mobile associé à un document de s'exécuter lorsque le document est produit." [SP28]

$ utilisateur actif *(active user)* (I) Voir : définition secondaire sous "utilisateur système".

$ mise sur écoute active *(active wiretapping)*
(I) Attaque de mise sur écoute qui tente aussi d'altérer les données communiquées ou d'affecter de toute autre façon le flux des données. (Voir : mise sur écoute. À comparer à : attaque active, mise sur écoute passive.)

$ sécurité améliorée *(add-on security)*
(N) Mise à niveau des mécanismes de protection mis en œuvre par un matériel ou logiciel dans un système d'information après que le système a été mis en fonctionnement. [FP039] (À comparer à : sécurité incorporée.)

$ sécurité adéquate *(adequate security)*
(O) /U.S. DoD/ "Sécurité commensurable avec le risque et l'étendue des dégâts résultant de la perte, du mauvais usage, ou de l'accès non autorisé aux informations ou de leur modification." (Voir : risque acceptable, risque résiduel .)

$ sécurité administrative *(administrative security)*
1. (I) Procédures de gestion et contraintes pour empêcher un accès non autorisé à un système. (Voir : "troisième loi" sous "Lois de Courtney", gestionnaire, sécurité opérationnelle, sécurité procédurale, architecture de sécurité. À comparer à : sécurité technique.)
Exemples : Claire délimitation et séparation des tâches ; contrôle de configuration.
Usage: La sécurité administrative est généralement comprise comme consistant en méthodes et mécanismes qui sont mis en œuvre et exécutés principalement par des personnes, plutôt que par des systèmes automatiques.
2. (O) "Contraintes de gestion, procédures de fonctionnement, procédures comptables, et contrôles supplémentaires établis pour fournir un niveau de protection acceptable pour les données sensibles". [FP039]

$ administrateur *(administrator)*

1. (O) /Critère courant/ Personne qui est responsable de la configuration, de la maintenance, et de l'administration de la cible d'évaluation d'une manière correcte pour la sécurité maximale. (Voir : sécurité administrative.)
2. (O) /ITSEC/ Personne en contact avec la cible d'évaluation, qui est responsable du maintien de sa capacité de fonctionnement.

$ norme de chiffrement évoluée (AES, *Advanced Encryption Standard*)
(N) Norme du gouvernement américain [FP197] (successeur du DES) qui (a) spécifie "l'algorithme AES", qui est un chiffrement de bloc symétrique qui se fonde sur Rijndael et utilise des tailles de clé de 128, 192, ou 256 bits pour opérer sur un bloc de 128 bits, et (b) déclare des politiques d'utilisation de cet algorithme pour protéger des données sensibles non classées secret défense.
Instructions : Rijndael a été conçu pour traiter des tailles de bloc supplémentaires et des longueurs de clé qui n'avaient pas été adoptées dans l'AES. Rijndael a été choisi par le NIST au moyen d'une compétition publique qui s'est déroulée pour trouver un successeur au DEA ; les autres finalistes étaient MARS, RC6, Serpent, et Twofish.

$ adversaire *(adversary)*
1. (I) Entité qui attaque un système. (À comparer à : casseur, intrus, pirate.)
2. (I) Entité qui est une menace pour un système.

$ Affirm
(O) Méthodologie formelle, langage, et ensemble intégré d'outils logiciels développée à l'Institut des sciences de l'information de l'Université de Californie du Sud pour spécifier, coder, et vérifier les logiciels pour produire des programmes corrects et fiables. [Cheh]

$ agrégation *(aggregation)*
(I) Circonstance dans laquelle il est exigé d'une collection d'éléments d'information qu'elle soit classée à un niveau de sécurité supérieur à celui d'aucun des éléments individuels. (Voir : classification.)

$ Trou d'air d'en-tête d'authentification *(Authentication Header air gap)*
(I) Interface entre deux systèmes à laquelle (a) ils ne sont pas connectés physiquement et (b) aucune connexion logique n'est automatisée (c'est-à-dire, les données sont transférées seulement manuellement à travers l'interface sous contrôle humain). (Voir : sneaker net. À comparer à : passerelle.)
Exemple : L'ordinateur A et l'ordinateur B sont sur des côtés opposés d'une pièce. Pour déplacer des données de A à B, une personne porte un disque à travers la pièce. Si A et B fonctionnent dans des domaines de sécurité différents, le déplacement des données à travers l'espace *(air gap)* peut impliquer une opération de mise à niveau.

$ algorithme *(algorithm)*
(I) Ensemble fini d'instructions étape par étape pour une procédure de résolution de problème ou de calcul, en particulier ceux qui peuvent être mis en œuvre par un ordinateur. (Voir : algorithme cryptographique.)

$ alias
(I) Nom qu'utilise une entité à la place de son vrai nom, usuellement pour des besoins d'anonymat ou pour se dissimuler.

$ Alice et Bob
(I) Parties qui sont le plus souvent invoquées pour illustrer le fonctionnement de protocoles de sécurité bipartites. Ces personnages et d'autres auteurs de ce drame sont citées par Schneier [Schn].

$ Institut américain de normalisation (ANSI, *American National Standards Institute*)
(N) Association privée à but non lucratif qui administre les normes volontaires du secteur privé des U.S.A.
Instructions : ANSI a approximativement 1 000 organisations membres, incluant des utilisateurs d'équipements, des fabricants, et autres. Cela inclut des firmes commerciales, des agences gouvernementales, et d'autres institutions et entités internationales.
ANSI est le seul représentant des U.S.A (a) à l'ISO et (b) (via le comité national U.S.) à la commission électrotechnique internationale (CEI), qui sont les deux organisations internationales de normalisation non gouvernementales majeures.
ANSI constitue un forum pour les groupes de développement des normes accrédités par l'ANSI. Parmi ces groupes, les suivants sont particulièrement concernés par la sécurité de l'Internet :
- le comité international pour la normalisation des technologies de l'information (INCITS, *International Committee for Information Technology Standardization*) (anciennement X3). Principal centre U.S. de normalisation dans les technologies de l'information et de la communication, englobant la mémorisation, le traitement, le transfert, l'affichage, la gestion, l'organisation, et la restitution de l'information. Exemple : [A3092].
- Comité de normalisation accrédité X9 : développe, établit, entretient, et promeut les normes pour l'industrie des services financiers. Exemple : [A9009].

- Alliance pour les solutions de l'industrie des télécommunications (ATIS) : développe les normes, spécifications, lignes directrices, exigences, rapports techniques, processus industriels, et essais de vérification d'interopérabilité et de fiabilité des réseaux, équipements et logiciels de télécommunications. Exemple : [A1523].

$ Norme américaine de code pour les échanges d'information (ASCII, *American Standard Code for Information Interchange*)
(N) Schéma de codage de 128 caractères spécifiés – les chiffres de 0 à 9, les lettres a à z et A à Z, certains symboles de ponctuation de base, certains codes de contrôle dont l'origine est liée aux machines de télétype, et une espace blanche – dans les entiers binaires à 7 bits. Forme la base des représentations de jeux de caractères utilisés dans la plupart des ordinateurs et de nombreuses normes de l'Internet. [FP001] (Voir : code.)

$ Rapport Anderson *(Anderson report)*
(O) Étude de 1972 de sécurité informatique qui a été écrite par James P. Anderson pour l'U.S. Air Force [Ande].
Instructions : Anderson a collaboré avec un groupe d'experts pour étudier les exigences de l'armée de l'air pour une sécurité à plusieurs niveaux. L'étude recommandait des recherches et des développements qui étaient nécessaires et urgents pour fournir un traitement sécurisé de l'information pour les systèmes de commande et de contrôle et les systèmes de soutien. Le rapport introduisait le concept de moniteur de référence et fournissait l'élan du développement de la technologie de la sécurité de l'informatique et des réseaux. Cependant, beaucoup des problèmes de sécurité que le rapport de 1972 disait "en cours" sont toujours une plaie pour les systèmes d'information d'aujourd'hui.

$ détection d'anomalie *(anomaly detection)*
(I) Méthode de détection d'intrusion qui recherche des activités qui sont différentes du comportement normal des entités système et des ressources système. (Voir : IDS. À comparer à : détection de mauvaise utilisation.)

$ anonymat *(anonymity)*
(I) Condition d'une identité inconnue ou dissimulée. (Voir : alias, anonymiseur, accréditif anonyme, connexion anonyme, identité, acheminement en oignon, certificat de personne. À comparer à : intimité.)
Instructions : une application peut exiger des services de sécurité qui conservent l'anonymat des utilisateurs ou autres entités systèmes, peut-être pour préserver leur intimité ou les mettre à l'abri d'une attaque. Pour cacher le nom réel d'une entité, un alias peut être utilisé ; par exemple, une institution financière peut allouer des numéros de compte. Les parties à des transactions peuvent ainsi rester relativement anonymes, mais peuvent aussi accepter les transactions légitimes. Les noms réels des parties ne peuvent pas être facilement déterminés par les observateurs de la transaction, mais un tiers autorisé peut être capable de transposer un alias en un nom réel, comme en présentant à l'institution une injonction des tribunaux. Dans d'autres applications, des entités anonymes peuvent être complètement intraçables.

$ anonymiseur *(anonymizer)*
(I) Service inter réseaux, usuellement fourni via un serveur mandataire, qui fournit l'anonymat et la confidentialité aux clients. C'est à dire que le service permet à un client d'accéder aux serveurs (a) sans permettre à quiconque de collecter des informations sur les serveurs auxquels le client accède et (b) sans permettre aux serveurs joints de collecter des informations sur le client, comme son adresse IP.

$ accréditif anonyme *(anonymous credential)*
(D) /Gouvernement U.S./ C'est un accréditif qui (a) peut être utilisé pour authentifier une personne comme ayant un attribut spécifique ou comme étant un membre d'un groupe spécifique (par exemple, vétérans de l'armée ou citoyens U.S.) mais (b) ne révèle pas l'identité individuelle de la personne qui présente l'accréditif. [M0404] (Voir : anonymat.)
Terme déconseillé : les IDOC NE DEVRAIENT PAS utiliser ce terme ; il mélange les concepts d'une façon potentiellement trompeuse. Par exemple, lorsque l'accréditif est un certificat X.509, le terme pourrait être interprété comme signifiant que le certificat a été signé par une CA qui a un certificat de personne. À la place, utiliser "certificat d'attribut", "certificat d'organisation", ou "certificat de personne" selon ce qu'on veut dire, et fournir en tant que de besoin des explications supplémentaires.

$ connexion anonyme *(anonymous login)*
(I) Dispositif de contrôle d'accès (en fait, une vulnérabilité du contrôle d'accès) dans de nombreux hôtes Internet qui permet aux usagers d'obtenir l'accès à des services ou ressources générales ou publiques d'un hôte (comme de permettre à tout usager de transférer des données en utilisant FTP) sans avoir de compte préétabli, spécifique d'une identité (c'est-à-dire, un nom d'utilisateur et un mot de passe). (Voir : anonymat.)
Instructions : ce dispositif expose un système à plus de menaces que lorsque tous les utilisateurs sont des entités connues, préenregistrées qui peuvent individuellement rendre compte de leurs actions. Un usager se connecte en utilisant un nom d'utilisateur spécial, publiquement connu (par exemple, "anonymous", "guest", ou "ftp"). Pour utiliser le nom de connexion public, l'usager n'est pas obligé de connaître un mot de passe secret et peut n'être pas obligé de rentrer quoi que ce soit d'autre que le nom. Dans d'autres cas, pour terminer la séquence normale des étapes d'un protocole de connexion, le système peut exiger que l'usager entre un mot de passe publiquement connu (comme "anonymous") ou peut demander à

l'usager une adresse de messagerie électronique ou quelque autre chaîne de caractères arbitraire.

$ anti-brouillage *(anti-jam)*
(N) "Mesures qui assurent que les informations transmises peuvent être reçues en dépit de tentatives délibérées de brouillage". [C4009] (Voir : sécurité électronique, saut de fréquence, brouillage, étalement de spectre.)

$ ancre de confiance supérieure *(apex trust anchor)*
(N) L'ancre de confiance qui est supérieure à toutes les autres ancres de confiance dans un système ou contexte particulier. (Voir : ancre de confiance, CA supérieure.)

$ couche d'application *(Application Layer)* Voir : Suite de protocoles Internet, OSIRM.

$ programme d'application *(application program)*
(I) Programme informatique qui effectue une fonction spécifique directement pour un utilisateur (par opposition à un programme qui fait partie du système d'exploitation d'un ordinateur et existe pour effectuer des fonctions en soutien des programmes d'application).

$ architecture (I) Voir : architecture de sécurité, architecture système.

$ archive, archiver
1a. (I) /nom/ Collection de données mémorisée pour une durée relativement longue pour des raisons d'historique et autres, comme de servir de support à un service d'audit, un service de mise à disposition, ou un service de protection d'intégrité du système. (À comparer à : sauvegarde, référentiel.)
1b. (I) /verbe/ Mémoriser des données de façon à créer une archive. (À comparer à : sauvegarder.)
Instructions : une signature numérique peut devoir être vérifiée de nombreuses années après la signature. La CA – celle qui a produit le certificat qui contenait la clé publique nécessaire à la vérification de cette signature – peut n'avoir pas pu rester en fonctionnement aussi longtemps. Chaque CA doit donc assurer une mémorisation à long terme des informations nécessaires pour vérifier les signatures de ceux à qui elle a fourni les certificats.

$ ARPANET
(I) Réseau de l'agence pour les projets de recherches avancées (ARPA, *Advanced Research Projects Agency*) qui a été un pionnier de la commutation par paquets et (a) a été conçu, mis en œuvre, et entretenu par BBN de janvier 1969 jusqu'à juillet 1975 sous contrat du gouvernement américain ; (b) a conduit au développement de l'Internet d'aujourd'hui ; et (c) a été résilié en juin 1990. [B4799], [Hafn]

$ bien *(asset)*
(I) Ressource système (a) dont il est requis qu'elle soit protégée par la politique de sécurité d'un système d'information, (b) qui est destinée à être protégée par des contre-mesures, ou (c) requise pour la mission d'un système.

$ association
(I) Relation coopérative entre des entités systèmes, usuellement dans le but de transférer des informations entre elles. (Voir : association de sécurité.)

$ assurance Voir : assurance de sécurité.

$ niveau d'assurance *(assurance level)*
(N) Rang sur une échelle hiérarchique qui juge de la confiance que quelqu'un peut avoir qu'une cible d'évaluation (TOE, *Target Of Evaluation*) remplit adéquatement les exigences de sécurité déclarées. (Voir : assurance, politique de certificat, EAL, TCSEC.)
Exemple : Les directives du gouvernement américain [M0404] décrivent quatre niveaux d'assurance pour l'authentification d'identité, où chaque niveau "décrit le degré de certitude de l'agence [du gouvernement fédéral américain] que l'usager a présenté [un accréditif] qui se réfère à l'identité [de l'usager]". Dans cette directive, assurance est défini comme (a) "le degré de confiance dans le processus d'examen utilisé pour établir l'identité de l'individu à qui l'accréditif a été remis" et (b) "le degré de confiance que l'individu qui utilise l'accréditif est l'individu à qui l'accréditif a été remis"
Les quatre niveaux sont décrits comme suit :
- niveau 1 : peu ou pas de confiance dans l'identité affirmée.
- niveau 2 : une certaine confiance dans l'identité affirmée .
- niveau 3 : grande confiance dans l'identité affirmée.
- niveau 4 : très grande confiance dans l'identité affirmée.

Les règles pour déterminer ces niveaux sont données dans une publication du NIST [SP12]. Cependant, comme il y est

noté, un niveau d'assurance est un "degré de confiance, pas une vraie mesure de la sécurité réelle du système. Cette distinction est nécessaire parce qu'il est extrêmement difficile – et dans de nombreux cas, virtuellement impossible – de savoir exactement quelle est la sécurité d'un système".

$ cryptographie asymétrique *(asymmetric cryptography)*
(I) Branche moderne de la cryptographie (plus connue sous le nom de "cryptographie à clé publique") dans laquelle les algorithmes utilisent une paire de clés (une clé publique et une clé privée) et utilisent un composant différent de la paire pour chacune des deux parties des opérations de chiffrement (par exemple, chiffrement et déchiffrement, ou création de signature et vérification de signature). (Voir : paire de clés, cryptographie symétrique.)
Instructions : les algorithmes asymétriques présentent des avantages en matière de gestion de clés sur les chiffrements symétriques de force équivalente. D'abord, une clé de la paire n'a besoin d'être connue de personne d'autre que de son possesseur ; elle peut ainsi être plus facilement gardée secrète. Ensuite, bien que l'autre clé soit partagée par toutes les entités qui utilisent l'algorithme, cette clé n'a pas besoin de rester secrète pour les autres entités non utilisatrices ; donc, la partie distribution de la gestion de clé peut être faite plus facilement.
La cryptographie asymétrique peut être utilisée pour créer des algorithmes de chiffrement, de signature numérique, et d'accord de clés :
- Dans un algorithme de chiffrement asymétrique (par exemple, "RSA"), lorsque Alice veut s'assurer de la confidentialité des données qu'elle envoie à Bob, elle chiffre les données avec une clé publique fournie par Bob. Seul Bob a la clé privée correspondante qui est nécessaire pour déchiffrer les données. (À comparer à : sceller.)
- Dans un algorithme de signature numérique asymétrique (par exemple, "DSA") lorsque Alice veut s'assurer de l'intégrité des données ou fournir l'authentification des données qu'elle envoie à Bob, elle utilise sa clé privée pour signer les données (c'est-à-dire, créer une signature numérique fondée sur les données). Pour vérifier la signature, Bob utilise la clé publique correspondante que Alice a fourni.
- Dans un algorithme d'accord de clé asymétrique (par exemple, "Diffie-Hellman-Merkle") Alice et Bob envoient chacun leur propre clé publique à l'autre partie. Puis chacun utilise sa propre clé privée et la clé publique de l'autre pour calculer la nouvelle valeur de clé.

$ clé asymétrique *(asymmetric key)*
(I) Clé de chiffrement qui est utilisée dans un algorithme de chiffrement asymétrique. (Voir : cryptographie asymétrique, clé privée, clé publique.)

$ ATIS (N) Voir : "Alliance for Telecommunications Industry Solutions" sous "ANSI".

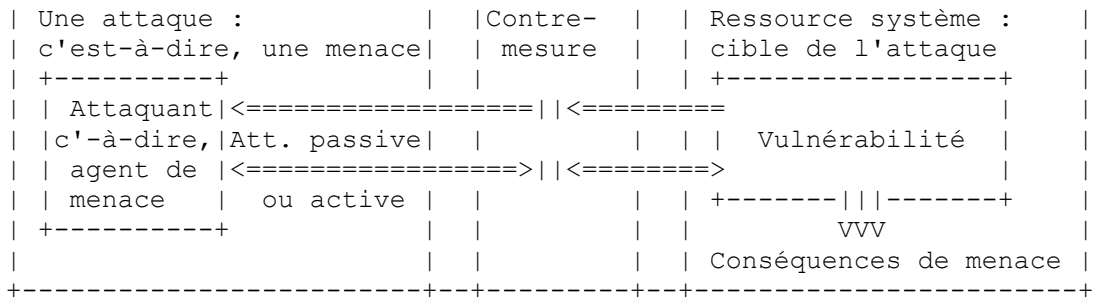
$ attaque *(attack)*
1. (I) Acte intentionnel par lequel une entité tente d'éviter les services de sécurité et de violer la politique de sécurité d'un système. C'est-à-dire, un assaut réel contre la sécurité d'un système qui découle d'une menace intelligente. (Voir : pénétration, violation, vulnérabilité.)
2. (I) Méthode ou technique utilisée dans un assaut (par exemple, déguisement). (Voir : attaque aveugle, attaque répartie.)

Instructions : Les attaques peuvent être caractérisées selon leur intention :
- Une "attaque active" tente d'altérer les ressources d'un système ou d'affecter leur fonctionnement.
- Une "attaque passive" tente d'apprendre ou utiliser des informations de la part d'un système mais n'affecte pas les ressources système de ce système. (Voir : enregistrement.) L'objet d'une attaque passive peut être d'obtenir des données qui sont nécessaires pour une attaque hors ligne.
- Dans une "attaque hors ligne", l'attaquant obtient des données du système cible et analyse ensuite ces données sur un système différent choisi par lui, éventuellement pour préparer une seconde étape d'attaque sur la cible.

Les attaques peuvent être caractérisées selon le point d'initiation :
- Une "attaque de l'intérieur" est celle qui est initiée par une entité située à l'intérieur du périmètre de sécurité (de l'intérieur") c'est-à-dire, une entité qui est autorisée à accéder aux ressources du système mais les utilise d'une façon qui n'est pas approuvée par l'entité qui a accordé l'autorisation.
- Une "attaque de l'extérieur" est initiée de l'extérieur du périmètre de sécurité, par un utilisateur non autorisé ou illégitime du système (un "externe"). Dans l'Internet, les attaquants de l'extérieur potentiels vont du bricoleur amateur au criminel organisé, au terroriste international et au gouvernement hostile.

Les attaques peuvent être caractérisées selon la méthode d'application :
- Dans une "attaque directe", l'attaquant adresse les paquets d'attaque à la ou aux victimes visées.
- Dans une "attaque indirecte", l'attaquant adresse les paquets à un tiers, et les paquets ont soit l'adresse de la victime visée comme adresse de source, soit indique la victime visée de quelque autre façon. Le tiers répond en envoyant un ou plusieurs paquets d'attaque à la ou aux victimes visées. L'attaquant peut utiliser des tiers comme amplificateurs d'attaque en fournissant une adresse de diffusion comme adresse de victime (par exemple, "attaque par surcharge"). (Voir : attaque par réflecteur. À comparer à : attaque par réflexion, attaque en répétition.)

Le terme "attaque" se rapporte à d'autres termes de base de la sécurité comme le montre le diagramme suivant :



$ potentiel d'attaque *(attack potential)*
(I) La probabilité perçue de succès si une attaque devait être lancée, exprimée en termes de capacité de l'attaquant (c'est-à-dire, expertise et ressources) et de motivation. (À comparer à : menace, risque.)

$ détection, avertissement et réponse d'attaque *(attack sensing, warning, and response)*
(I) Ensemble de services de sécurité qui coopèrent avec un service d'audit pour détecter et réagir aux indications d'actions de menace, incluant les deux types d'attaques de l'intérieur et de l'extérieur . (Voir : indicateur.)

$ arborescence d'attaque *(attack tree)*
(I) Structure hiérarchique d'embranchements de données qui représente un ensemble d'approches potentielles pour réaliser un événement dans lequel un système de sécurité est pénétré ou compromis d'une façon déterminée. [Moor]
Instructions : les arborescences d'attaques sont des cas particuliers d'arborescences de fautes. L'incident de sécurité qui est le but de l'attaque est représenté comme nœud racine de l'arborescence, et les façons dont un attaquant pourrait atteindre ce but sont représentées de façon itérative et incrémentaire comme les branches et sous nœuds de l'arborescence. Chaque sous nœud définit un sous objectif, et chaque sous objectif peut avoir son propre ensemble de sous objectifs, etc. Le nœud final sur les chemins qui partent de la racine, c'est-à-dire, les nœuds feuilles, représentent les différentes façons d'initier une attaque. Chaque nœud autre qu'une feuille est soit un nœud ET, soit un nœud OU. Pour atteindre l'objectif représenté par un nœud ET, les sous objectifs, représentés par tous les sous nœuds de ce nœud doivent être réalisés, et pour l'objectif représenté par un nœud OU, le sous objectif représenté par au moins un des sous nœuds doit être réalisé. Les branches peuvent être étiquetées avec des valeurs représentant la difficulté, le coût, ou autres attributs d'une attaque, de sorte que les autres attaques puissent être comparées.

$ attribut *(attribute)*
(N) Information d'un type particulier concernant une entité ou objet identifiable d'un système. Un "type d'attribut" est le composant d'un attribut qui indique la classe d'informations données par l'attribut ; et une "valeur d'attribut" est une instance particulière de la classe d'informations indiquée par un type d'attribut. (Voir : certificat d'attribut.)

$ autorité d'attribut *(AA, attribute authority)*
1. (N) Une CA qui produit des certificats d'attribut.
2. (O) "Une autorité [qui] alloue des privilèges en produisant des certificats d'attribut." [X509]

Utilisation déconseillée : l'abréviation "AA" NE DEVRAIT PAS être utilisée dans un IDOC à moins d'y être préalablement définie.

$ certificat d'attribut *(attribute certificate)*
1. (I) Un certificat numérique qui lie un ensemble d'éléments de données descriptives, autres qu'une clé publique, soit directement à un nom de sujet, soit à l'identifiant d'un autre certificat qui est un certificat de clé publique. (Voir : jeton de capacité.)
2. (O) "Une structure de données, signée numériquement par une autorité d'attribut, qui lie des valeurs d'attribut à des informations d'identification sur son détenteur." [X509]

Instructions : Un certificat de clé publique lie un nom de sujet à une valeur de clé publique, avec les informations nécessaires pour effectuer certaines fonctions cryptographiques qui utilisent cette clé. D'autres attributs d'un sujet, comme un niveau d'habilitation *(security clearance)* peuvent être certifiés dans une différente sorte de certificat numérique, appelé un certificat d'attribut. Un sujet peut avoir de multiples certificats d'attribut associés à son nom ou à chacun de ses certificats de clé publique.
Un certificat d'attribut peut être produit à un sujet dans les situations suivantes :
- Durées de vie différentes : lorsque la durée de vie d'un lien d'attribut est plus courte que celle du certificat de clé publique qui s'y rapporte, ou lorsque il est souhaitable de ne pas avoir besoin de révoquer la clé publique d'un sujet juste pour révoquer un attribut.
- Autorités différentes : lorsque l'autorité responsable des attributs est différente de celle qui produit le certificat de clé publique pour le sujet. (Il n'est pas exigé qu'un certificat d'attribut soit produit par la même CA que celle qui produit le certificat de clé publique associé.)

$ audit Voir : audit de sécurité.

$ journal d'audit *(audit log)*
(I) Synonyme de "chemin d'audit de sécurité".

$ service d'audit *(audit service)*
(I) Service de sécurité qui enregistre les informations nécessaires pour établir la comptabilité des événements systèmes et des actions des entités systèmes qui les causent. (Voir : audit de sécurité.)

$ chemin d'audit *(audit trail)* (I) Voir : chemin d'audit de sécurité.

$ authentifier *(autheticate)*
(I) Vérifier (c'est-à-dire, établir la vérité de) une valeur d'attribut revendiquée par ou pour une entité système ou une ressource système. (Voir : authentification, valider par rapport à vérifier, "relations entre service d'intégrité des données et services d'authentification" sous "service d'intégrité des données".)
Utilisation déconseillée : dans l'usage français courant, ce terme est utilisé avec la signification de "prouver authentique" (par exemple, un expert en art authentifie une peinture de Michel-Ange) ; mais les IDOC devraient en restreindre l'utilisation comme suit :
- Les IDOC NE DEVRAIENT PAS utiliser ce terme pour se référer à prouver ou vérifier que des données n'ont pas été changées, détruites, ou perdues d'une manière non autorisée ou accidentelle. Utiliser plutôt "vérifier".
- Les IDOC NE DEVRAIENT PAS utiliser ce terme pour se référer à prouver la véracité ou la précision d'un facteur ou valeur tel qu'une signature numérique. Utiliser plutôt "vérifier".
- Les IDOC NE DEVRAIENT PAS utiliser ce terme pour se référer à l'établissement de l'exactitude et correction d'une construction, telle qu'un certificat numérique. Utiliser plutôt "valider".

$ authentification *(authentication)*
(I) Processus de vérification de l'assertion qu'une entité ou ressource système a une certaine valeur d'attribut. (Voir : attribut, authentifier, échange d'authentification, informations d'authentification, accréditif, authentification d'origine des données, authentification d'entité homologue, "relations entre service d'intégrité des données et services d'authentification" sous "service d'intégrité des données", authentification simple, authentification forte, vérification, X.509.)
Instructions : les services de sécurité dépendent fréquemment de l'authentification de l'identité des usagers, mais l'authentification peut impliquer tout type d'attribut qui est reconnu par un système. Une assertion peut être faite par un sujet sur lui-même (par exemple, au moment de la connexion, un usager entre normalement son identité) ou une assertion peut être faite au nom d'un sujet ou objet par une autre entité système (par exemple, un usager peut prétendre qu'un objet de données provient d'une source spécifique, ou qu'un objet de données est classé à un certain niveau de sécurité).
Un processus d'authentification comporte deux étapes de base :
- Étape d'identification : Présenter la valeur d'attribut revendiquée (par exemple, un identifiant d'utilisateur) au sous-système d'authentification.
- Étape de vérification : Présenter ou générer des informations d'authentification (par exemple, une valeur signée avec une clé privée) qui agissent comme preuves pour démontrer le lien entre l'attribut et ce pour quoi il est affirmé. (Voir : vérification.)

$ code d'authentification *(authentication code)*
(D) Synonyme d'une somme de contrôle fondée sur le chiffrement. (À comparer à : code d'authentification de données, code d'authentification de message.)
Terme déconseillé : les IDOC NE DEVRAIENT PAS utiliser ce terme ; utiliser ce terme sans majuscule comme synonyme d'une sorte de somme de contrôle, sans considération de son caractère cryptographique ou non. Utiliser plutôt "somme de contrôle", "code d'authentification des données", "code de détection d'erreur", "hachage", "hachage chiffré", "code d'authentification de message", "somme de contrôle protégée", ou quelque autre terme recommandé, selon ce qu'on veut dire.
Le terme mélange les concepts d'une façon qui peut être trompeuse. Le mot "authentification" est trompeur car la somme de contrôle peut être utilisée pour effectuer une fonction d'intégrité des données plutôt qu'une fonction d'authentification d'origine des données.

$ échange d'authentification *(authentication exchange)*
1. (I) Mécanisme pour vérifier l'identité d'une entité au moyen d'un échange d'informations.
2. (O) "Mécanisme destiné à s'assurer de l'identité d'une entité au moyen d'un échange d'informations." [I7498-2]

$ en-tête d'authentification (AH, *Authentication Header*)
(I) Protocole Internet [RFC2402], [RFC4302] conçu pour fournir des services d'intégrité de données et d'authentification

d'origine des données sans connexion pour les datagrammes IP, et (facultativement) de fournir la protection partielle de l'intégrité de séquence et contre les attaques en répétition. (Voir : IPsec. À comparer à : ESP.)
Instructions : la protection contre la répétition peut être choisie par le receveur lorsque une association de sécurité est établie. AH authentifie la PDU de couche supérieure qui est portée comme une SDU IP, et authentifie aussi autant de PCI IP (c'est-à-dire, l'en-tête IP) que possible. Cependant, certains champs d'en-tête IP peuvent changer dans le transit, et la valeur de ces champs, lorsque le paquet arrive chez le receveur, ne peut pas être prévue par l'envoyeur. Donc, les valeurs de tels champs ne peuvent pas être protégées de bout en bout par AH ; la protection de l'en-tête IP par AH est seulement partielle lorsque de tels champs sont présents.
AH peut être utilisé seul, ou combiné avec ESP, ou incorporé avec le tunnelage. Des services de sécurité peuvent être fournis entre une paire d'hôtes communicants, entre une paire de passerelles de sécurité communicantes, ou entre un hôte et une passerelle. ESP peut fournir presque les mêmes services de sécurité que AH, et ESP peut aussi fournir le service de confidentialité des données. La principale différence entre les services d'authentification fournis par ESP et AH est l'étendue de la couverture ; ESP ne protège pas les champs d'en-tête IP sauf si ils sont encapsulés par AH.

$ informations d'authentification *(authentication information)*
(I) Informations utilisées pour vérifier une identité revendiquée par ou pour une entité. (Voir : authentification, accréditif, usager. À comparer à : informations d'identification.)
Instructions : les informations d'authentification peuvent exister comme, ou être déduites de, un des suivants : (a) quelque chose que l'entité sait (voir : mot de passe) ; (b) quelque chose que l'entité possède (voir : jeton) ; (c) quelque chose que l'entité est (voir : authentification biométrique).

$ service d'authentification *(authentication service)*
(I) Un service de sécurité qui vérifie une identité revendiquée par ou pour une entité. (Voir : authentification.)
Instructions : dans un réseau, il y a deux formes générales de service d'authentification : le service d'authentification d'origine des données et le service d'authentification de l'entité homologue.

$ authenticité *(authenticity)*
(I) Propriété d'être authentique et capable d'être vérifié et de confiance. (Voir : authentifier, authentification, valider, par opposition à : vérifier.)

$ autorité *(authority)*
(D) /PKI/ "Entité [qui est] responsable de la délivrance des certificats." [X509]
Utilisation déconseillée : Les IDOC NE DEVRAIENT PAS utiliser ce terme comme un synonyme de autorité d'attribut, autorité de certification, autorité d'enregistrement, ou termes similaire ; la forme abrégée peut créer une confusion. Utiliser plutôt le terme complet à la première instance d'usage et ensuite, si il est nécessaire d'abréger le texte, utiliser AA, CA, RA, et les autres abréviations définies dans le présent glossaire.

$ certificat d'autorité *(authority certificate)*
(D) "Certificat produit par une autorité (par exemple, soit une autorité de certification, soit à une autorité d'attribut)." [X509] (Voir : autorité.)
Terme déconseillé : Les IDOC NE DEVRAIENT PAS utiliser ce terme parce qu'il est ambigu. Utiliser plutôt le terme complet de "certificat d'autorité de certification", "certificat d'autorité d'attribut", "certificat d'autorité d'enregistrement", etc. à la première instance d'usage et ensuite, si nécessaire pour abréger le texte, utiliser AA, CA, RA, et les autres abréviations définies dans le présent glossaire.

$ extension d'accès aux informations d'autorité *(Authority Information Access extension)*
(I) Extension privée définie par PKIX pour les certificats X.509 pour indiquer "comment accéder aux informations et services de CA pour le producteur du certificat dans lequel l'extension apparaît. Les informations et services peuvent inclure des services de validation en ligne et des données de politique de CA." [RFC3280] (Voir : extension privée.)

$ autorisation *(authorization)*
1a. (I) Approbation accordée à une entité système d'accéder à une ressource système. (À comparer à : permission, privilège.)
Usage : Certains synonymes sont "permission" et "privilège". Des termes spécifiques sont préférés dans certains contextes :
- /PKI/ "autorisation" DEVRAIT être utilisé, pour être en cohérence avec "autorité de certification" dans [X509].
- /contrôle d'accès fondé sur le rôle/ "permission" DEVRAIT être utilisé pour être cohérent avec la norme [ANSI].
- /systèmes d'exploitation informatiques/ "privilège" DEVRAIT être utilisé, pour s'aligner sur la littérature. (Voir : processus privilégié, utilisateur privilégié.)

Instructions : la sémantique et la granularité des autorisations dépendent de l'application et de la mise en œuvre (voir : "première loi" sous "Lois de Courtney"). Une autorisation peut spécifier un mode d'accès particulier – tel que lecture, écriture, ou exécution -- pour une ou plusieurs ressources système.

1b. (I) Processus pour accorder l'approbation à une entité système d'accéder à une ressource système.
2. (O) /SET/ "Processus par lequel une ou des personnes convenablement désignées se voient accorder la permission d'effectuer une action au nom d'une organisation. Ce processus vérifie les risques de la transaction, confirme qu'une certaine transaction ne fait pas passer le débit du compte du détenteur au dessus de la limite de crédit du compte, et préserve la quantité de crédit spécifiée. (Lorsque un commerçant obtient une autorisation, le payement de la quantité autorisée est garanti – à condition, bien sûr, que le commerçant ait suivi les règles associées au processus d'autorisation.)" [SET2]

$ accréditif d'autorisation *(authorization credential)* (I) Voir : /contrôle d'accès/ sous "accréditif".

$ autoriser *(authorize)* (I) Accorder une autorisation à une entité système.

$ utilisateur autorisé *(authorized user)*
(I) /contrôle d'accès/ Entité système qui accède à une ressource système pour laquelle l'entité a reçu une autorisation. (À comparer à : interne, externe, utilisateur non autorisé.)
Utilisation déconseillée : les IDOC qui utilisent ce terme DEVRAIENT l'assortir d'une définition parce que le terme est utilisé dans de nombreux sens et pourrait facilement être mal compris.

$ système d'informations automatisé. Voir : système d'informations.

$ disponibilité *(availability)*
1. (I) Propriété d'un système ou d'une ressource système d'être accessible, ou utilisable ou fonctionnel à la demande, par une entité système autorisée, conformément aux spécifications de fonctionnement pour le système ; c'est-à-dire qu'un système est disponible si il fournit des services conformément à la conception du système chaque fois que les utilisateurs les demandent. (Voir : critique, déni de service. À comparer à : préséance, fiabilité, capacité de survie.)
2. (O) "Propriété d'être accessible et utilisable à la demande par une entité autorisée." [I7498-2]
3. (D) "Accès fiable en temps voulu aux services de données et d'informations par les utilisateurs autorisés." [C4009]

Définition déconseillée : les IDOC NE DEVRAIENT PAS utiliser ce terme avec la définition 3 ; celle-ci mélange "disponibilité" et "fiabilité", qui sont des propriétés différentes. (Voir : fiabilité.)
Instructions : les exigences de disponibilité peuvent être spécifiées par des métriques quantitatives, mais sont parfois déclarées qualitativement, comme dans ce qui suit :
- "tolérance souple aux retards" peut signifier que de brèves pannes du système ne mettent pas en danger l'accomplissement de la mission, mais des pannes prolongées peuvent mettre la mission en danger.
- "tolérance minimum aux retards" peut signifier que l'accomplissement de la mission exige que le système fournisse les services demandés à bref délai.

$ service de disponibilité *(availability service)*
(I) Service de sécurité qui protège un système pour assurer sa disponibilité.
Instructions : ce service s'adresse aux soucis de sécurité soulevés par les attaques de déni de service. Il dépend de la gestion et du contrôle appropriés des ressources système, et dépend donc du service de contrôle d'accès et des autres services de sécurité.

$ évitement *(avoidance)* (I) Voir : définition secondaire sous "sécurité".

$ système informatique B1, B2, ou B3 *(B1, B2, or B3 computer system)*
(O) /TCSEC/ Voir : Instructions sous "critères d'évaluation de système informatique de confiance".

$ porte de derrière *(back door)*
1. (I) /COMPUSEC/ Dispositif d'un système informatique – qui peut être (a) une faute involontaire, (b) un mécanisme délibérément installé par le créateur du système, ou (c) un mécanisme installé subrepticement par un intrus – qui donne accès à une ressource système par des procédures autres que les procédures usuelles et est généralement caché ou peu connu. (Voir : crochet de maintenance. À comparer à : Cheval de Troie.)

Exemple : un moyen d'accéder à un ordinateur autrement que par une connexion normale. Un tel chemin d'accès n'est pas nécessairement conçu dans une intention malveillante ; les systèmes d'exploitation sont parfois chargés par le fabricant avec des comptes cachés destinés à être utilisés par les techniciens de service ou les programmeurs d'entretien du fabricant.

2. (I) /cryptographie/ Dispositif d'un système cryptographique qui rend facilement possible de casser ou circonvenir la protection que le système est conçu pour fournir.

Exemple : un dispositif qui rend possible de déchiffrer le texte chiffré plus rapidement que par une cryptanalyse en force, sans avoir une connaissance préalable de la clé de déchiffrement.

$ sauvegarder *(back up)*
(I) /verbe/ Créer une copie de réserve de données, ou, plus généralement, fournir des moyens de remplacement pour effectuer des fonctions système en dépit de la perte de la ressources système. (Voir : plan de contingence. À comparer à : archive.)

$ sauvegarde *(backup)*
(I) /nom ou adjectif/ Se réfère à des moyens de remplacement pour effectuer des fonctions système en dépit de la perte des ressources système. (Voir : plan de contingence).
Exemple : Une copie de réserve de données, qui est, de préférence, mémorisée séparément de l'original, pour l'utiliser si l'original est perdu ou endommagé. (À comparer à : archive.)

$ bagbiter *(bouffeur de sac ?)*
(D) /argot/ "Entité, comme un programme ou un ordinateur, qui ne réussit pas à fonctionner ou qui fonctionne d'une façon remarquablement maladroite. Une personne qui a causé un problème, par inadvertance ou autrement, normalement en ne réussissant pas à programmer correctement l'ordinateur." [NCSSG] (Voir : faute.)
Terme déconseillé : Il est vraisemblable que d'autres cultures utilisent des métaphores différentes pour ces concepts. Donc, pour éviter des mauvaises interprétations en international, les IDOC NE DEVRAIENT PAS utiliser ce terme. (Voir : Utilisation déconseillée sous "Livre Vert".)

$ bagage *(baggage)*
(O) /SET/ Un "tuplet chiffré opaque, qui est inclus dans un message SET mais ajouté comme données externes aux données PKCS encapsulées. Cela évite un super chiffrement du tuplet précédemment chiffré, mais garantit la liaison avec la portion PKCS du message." [SET2]
Utilisation déconseillée : les IDOC NE DEVRAIENT PAS utiliser ce terme pour décrire un élément de données, sauf sous la forme "bagage SET(marque déposée)" avec la signification donnée ci-dessus.

$ sécurité incorporée *(baked-in security)*
(D) Inclusion de mécanismes de sécurité dans un système d'informations commençant tôt dans la durée de vie du système, c'est-à-dire, durant la phase de conception, ou au moins au début de la phase de mise en œuvre. (À comparer à : sécurité ajoutée.)
Terme déconseillé : il est vraisemblable que d'autres cultures utilisent des métaphores différentes pour ces concepts. Donc, pour éviter des mauvaises interprétations en international, les IDOC NE DEVRAIENT PAS utiliser ce terme (sauf à produire aussi une définition comme celle-ci). (Voir : Utilisation déconseillée sous "Livre Vert".)

$ bande passante *(bandwidth)*
(I) Largeur totale de la bande de fréquences qui est disponible ou est utilisée par un canal de communication ; usuellement exprimée en Hertz (Hz). (RFC3753) (À comparer à : capacité de canal.)

$ Numéro d'identification bancaire (BIN, *bank identification number*)
1. (O) Chiffres d'un numéro de carte de crédit qui identifient la banque émettrice. (Voir : numéro de compte principal.)
2. (O) /SET/ Les six premiers chiffres d'un numéro de compte principal.

$ Règles de codage de base (BER, *Basic Encoding Rules*)
(I) Norme de représentation des types de données ASN.1 comme des chaînes d'octets. [X690] (Voir : Règles de codage distinctives.)
Utilisation déconseillée : parfois traitées incorrectement au titre de l'ASN.1. Cependant, l'ASN.1 ne se réfère de façon appropriée qu'à un langage de description de syntaxe, et non aux règles de codage du langage.

$ Option de sécurité de base *(Basic Security Option)* (I) Voir : définition secondaire sous "IPSO".

$ hôte forteresse *(bastion host)*
(I) Ordinateur fortement protégé qui est dans un réseau protégé par un pare-feu (ou fait partie d'un pare-feu) et est le seul hôte (ou un des quelques hôtes) dans le réseau qui peut être directement accédé à partir de réseaux de l'autre côté du pare-feu. (Voir : pare-feu.)
Instructions : les routeurs filtrants dans un pare-feu interdisent normalement au trafic provenant de l'extérieur du réseau d'atteindre juste un hôte, l'hôte forteresse, qui fait normalement partie du pare-feu. Comme ce seul hôte peut être attaqué directement, ce seul hôte a besoin d'être très fortement protégé, de façon que la sécurité puisse être assurée plus facilement et à moindre coût. Cependant, pour permettre aux utilisateurs légitimes internes et externes d'accéder aux ressources d'application à travers le pare-feu, des protocoles et services de couche supérieure doivent être relayés et transmis par l'hôte forteresse. Certains services (par exemple, DNS et SMTP) ont la transmission incorporée ; d'autres services (par exemple, TELNET et FTP) exigent un serveur mandataire sur l'hôte forteresse.

$ BBN Technologies Corp. (BBN)
(O) Société de recherche et développement (appelée à l'origine Bolt Baranek and Newman, Inc.) qui a construit l'ARPANET.

$ Modèle de Bell-LaPadula *(Bell-LaPadula model)*
(N) Modèle mathématique formel de transition d'état de politique de confidentialité pour systèmes d'ordinateurs à plusieurs niveaux de sécurité [Bell]. (À comparer à : modèle Biba, modèle Brewer-Nash.)
Instructions : le modèle, conçu par David Bell et Léonard LaPadula de la société MITRE en 1973, caractérise les éléments de systèmes informatiques comme des sujets et des objets. Pour déterminer si un sujet est ou non autorisé à un mode d'accès particulier sur un objet, les autorisations du sujet sont comparées à la classification de l'objet. Le modèle définit la notion de "état sûr", dans lequel les seuls modes d'accès permis des sujets aux objets sont en conformité à une politique de sécurité spécifiée. Il est prouvé que chaque transition d'état préserve la sécurité en passant d'un état sûr à un état sûr, prouvant par là que le système est sûr. Dans ce modèle, un système sûr multi niveaux satisfait à plusieurs règles, incluant la "propriété de confinement" (autrement dite, la "propriété-*"), la "propriété de simple sécurité", et la "propriété de tranquillité".

$ bénin *(benign)*
1. (N) /COMSEC/ "Condition de données cryptographiques [telles] que [les données] ne peuvent pas être compromises par un accès humain [aux données]." [C4009]
2. (O) /COMPUSEC/ Voir : définition secondaire sous "confiance".

$ remplissage bénin *(benign fill)*
(N) Processus par lequel le matériel de clé est généré, distribué, et placé dans une unité cryptographique terminale (ECU) sans exposition à un humain ou autre entité système, excepté le module cryptographique qui consomme et utilise le matériel. (Voir : bénin.)

$ au-delà de A1 *(beyond A1)*
1. (O) /formel/ Niveau d'assurance de sécurité qui est au-delà du niveau le plus élevé (niveau A1) des critères spécifiés par TCSEC. (Voir les Instructions sous "Critères d'évaluation de système informatique de confiance".)
2. (O) /informel/ Niveau de confiance si élevé qu'il est au-delà de la technologie de l'état de l'art ; c'est-à-dire qu'il ne peut pas être fourni ou vérifié par les méthodes d'assurance actuellement disponibles, et en particulier pas par les méthodes formelles actuellement disponibles.

$ Intégrité Biba *(Biba integrity)* (N) Synonyme de "intégrité de source".

$ modèle Biba *(Biba model)*
(N) Modèle mathématique formel à transition d'état de politique d'intégrité pour système d'ordinateur à plusieurs niveaux de sécurité [Biba]. (Voir : intégrité de source. À comparer à : modèle Bell-LaPadula.)
Instructions : ce modèle pour le contrôle d'intégrité est analogue au modèle Bell-LaPadula pour le contrôle de confidentialité. Chaque sujet et objet reçoit un niveau d'intégrité et, pour déterminer si un sujet est autorisé ou non à un mode d'accès particulier sur un objet, le niveau d'intégrité du sujet est comparé à celui de cet objet. Le modèle interdit de changer les informations d'un objet par un sujet qui a un niveau inférieur, ou non comparable. Les règles du modèle Biba sont identiques aux règles correspondantes du modèle Bell-LaPadula.

$ billet
(N) "Position ou allocation personnelle qui peut être remplie par une personne". [JCP1] (À comparer à : principal, rôle, utilisateur.)
Instructions : dans une organisation, un "billet" est une position de population, dont il y a exactement une instance ; mais un "rôle" est une position fonctionnelle, dont il peut y avoir plusieurs instances. Les entités système sont dans une relation biunivoque avec leurs billets, mais peuvent être dans des relations de plusieurs à un et de un à plusieurs avec leurs rôles.

$ lier *(bind)*
(I) Associer de façon inséparable en appliquant un mécanisme de sécurité.
Exemple : Une CA crée un certificat de clé publique en utilisant une signature numérique pour lier ensemble (a) un nom de sujet, (b) une clé publique, et habituellement (c) des éléments de données supplémentaires (par exemple, "une certification de clé publique X.509").

$ authentification biométrique *(biometric authentication)*
(I) Méthode de génération d'informations d'authentification d'une personne par des mesures numériques de caractéristiques physiques ou comportementales, telles que les empreintes digitales, la forme de la main, le schéma rétinien, le style

d'écriture, ou le visage.

$ attaque de l'anniversaire *(birthday attack)*
(I) Classe d'attaques contre des fonctions cryptographiques, incluant aussi bien des fonctions de chiffrement que de hachage. Les attaques tirent parti d'une propriété statistique : étant donnée une fonction cryptographique qui a un résultat de N bits, la probabilité est supérieure à 1/2 que pour 2**(N/2) résultats choisis au hasard, la fonction produise au moins deux résultats identiques. (Voir : Instructions sous "fonction de hachage".)
Déduction : Du fait un peu surprenant (souvent appelé le "paradoxe de l'anniversaire") que bien qu'il y ait 365 jours dans une année, la probabilité est supérieure à 1/2 que deux personnes ou plus aient la même date d'anniversaire dans tout groupe choisi au hasard de 23 personnes. Les attaques de l'anniversaire permettent à un adversaire de trouver deux entrées pour lesquelles une fonction cryptographique produit le même texte chiffré (ou de trouver deux entrées pour lesquelles une fonction de hachage produit le même résultat de hachage) beaucoup plus rapidement que ne le peut une attaque en force brute ; et un adversaire habile peut utiliser une telle capacité pour créer des méfaits considérables. Cependant, aucune attaque de l'anniversaire ne peut permettre à un adversaire de déchiffrer un certain texte chiffré (ou de trouver une entrée de hachage qui résulte en un certain résultat de hachage) plus rapidement qu'avec une attaque en force brute.

$ bit
(I) Contraction du terme "binary digit" *(chiffre binaire)* ; la plus petite unité de mémorisation d'information, qui a deux états ou valeurs possibles. Les valeurs sont habituellement représentées par les symboles "0" (zéro) et "1" (un). (Voir : bloc, octet, quartet, mot.)

$ chaîne binaire *(bit string)*
(I) Suite de bits, dont chacun est un "0" ou un "1".

$ NOIR *(BLACK)*
1. (N) Désignation pour des données qui consistent seulement en texte chiffré, et pour des éléments ou facilités d'équipements de systèmes d'information qui ne traitent que du texte chiffré. Exemple : "clé BLACK". (Voir : BCR, changement de couleur, séparation RED/BLACK. À comparer à : RED.)
2. (O) /Gouvernement des USA/ "Désignation appliquée aux systèmes d'information, et aux domaines associés, circuits, composants, et équipements, dans lesquels les informations de sécurité nationale sont chiffrées ou ne sont pas traitées". [C4009]
3. (D) Toutes données qui peuvent être divulguées sans dommage.

Définition déconseillée : les IDOC NE DEVRAIENT PAS utiliser ce terme avec la définition 3 parce que cette définition est ambiguë sur le fait que les données sont ou non protégées.

$ chiffrement NOIR/ROUGE (BCR, *BLACK/Crypto/RED*)
(N) Système expérimental de chiffrement de paquet de bout en bout du réseau développé dans un prototype par BBN et la division radio Collins de Rockwell Corporation dans les années 1975-1980 pour le ministère de la défense U.S.. BCR était le premier système de sécurité à prendre en charge le trafic TCP/IP, et il incorporait les premières puces DES qui ont été validées par le Bureau national des normes (maintenant appelé NIST). BCR était aussi le premier à utiliser un KDC et un ACC pour gérer les connexions.

$ clé NOIRE *(BLACK key)*
(N) Clé qui est protégée par une clé de chiffrement de clé et qui doit être déchiffrée avant utilisation. (Voir : NOIR. À comparer à : clé ROUGE.)

$ BLACKER
(O) Système de chiffrement de bout en bout pour réseaux de données informatiques qui a été développé par le ministère de la défense U.S. dans les années 1980 pour assurer un service de confidentialité de données d'hôte à hôte pour les datagrammes à la couche 3 OSIRM. [Weis] (À comparer à : CANEWARE, IPsec.)
Instructions : chaque hôte utilisateur se connecte à son appareil de chiffrement d'envoi sur le réseau appelé un frontal BLACKER (BFE, *BLACKER Front End*) (TSEC/KI-111) au travers duquel l'hôte se connecte au sous-réseau. Le système comporte aussi deux types d'appareils centralisés : un ou plusieurs KDC se connectent au sous-réseau et communiquent avec les ensembles alloués de BFE, et un ou plusieurs ACC se connectent au sous-réseau et communiquent avec les KDC alloués. BLACKER utilise seulement le chiffrement symétrique. Un KDC distribue les clés de session aux paires de BFE autorisées par un ACC. Chaque ACC tient une base de données pour un ensemble de BFE, et la base de données détermine quelles paires de cet ensemble (c'est-à-dire, quelles paires d'hôtes utilisateurs derrière les BFE) sont autorisées à communiquer et à quels niveaux de sécurité.
Le système BLACKER est à plusieurs niveaux de sécurité (MLS, *MultiLevel Secure*) de trois façons : (a) les BFE forment un paramètre de sécurité autour d'un sous-réseau, séparant les hôtes utilisateurs du sous-réseau, afin que le sous-réseau puisse opérer à un niveau de sécurité différent (éventuellement inférieur, moins coûteux) que les hôtes. (b) Les composants

BLACKER sont de confiance pour séparer les datagrammes de différents niveaux de sécurité, afin que chaque datagramme d'un certain niveau de sécurité ne puisse être reçu que par un hôte autorisé pour ce niveau de sécurité ; et donc, BLACKER peut séparer des communautés qui opèrent à des niveaux de sécurité différents. (c) Le côté hôte d'un BFE est lui-même MLS et peut reconnaître une étiquette de sécurité sur chaque paquet, afin qu'un hôte utilisateur MLS puisse être autorisé à transmettre avec succès des datagrammes qui ont des étiquettes de niveau de sécurité différentes.

$ attaque aveugle *(blind attack)*
(I) Type de méthode d'attaque fondée sur le réseau qui n'exige pas que l'entité attaquante reçoive le trafic de données de l'entité attaquée ; c'est-à-dire que l'attaquant n'a pas besoin de "voir" les paquets de données envoyées par la victime. Exemple : inondation SYN.
Instructions : Si une méthode d'attaque est aveugle, les paquets de l'attaquant peuvent porter (a) une fausse adresse IP de source (rendant difficile à la victime de trouver l'attaquant) et (b) une adresse différente sur chaque paquet (rendant difficile à la victime de bloquer l'attaque). Si l'attaquant a besoin de recevoir le trafic de la victime, l'attaquant doit soit (c) révéler sa propre adresse IP à la victime (ce qui permet à la victime de trouver l'attaquant ou de bloquer l'attaque par filtrage) soit (d) de fournir une fausse adresse et aussi de subvertir les mécanismes d'acheminement du réseau pour dérouter les paquets en retour vers l'attaquant (ce qui rend l'attaque plus complexe, plus difficile, ou plus coûteuse). [RFC3552]

$ bloc *(block)*
(I) Chaîne binaire ou vecteur binaire de longueur finie. (Voir : bit, chiffrement de bloc. À comparer à : octet, mot.)
Usage : Un "bloc de N bits" contient N bits, qui sont habituellement numérotés de gauche à droite 1, 2, 3, ..., N.

$ chiffrement de bloc *(block cipher)*
(I) Algorithme de chiffrement qui coupe le texte source en segments de taille fixe et utilise la même clé pour transformer chaque segment de texte source en un segment de texte chiffré de taille fixe. Exemples : AES, Blowfish, DEA, IDEA, RC2, et SKIPJACK. (Voir : bloc, mode. À comparer à : chiffrement de flux.)
Instructions : un chiffrement de bloc peut être adapté pour avoir une interface externe différente, comme celle d'un chiffrement de flux, en utilisant un mode de chiffrement cryptographique pour aménager l'algorithme de base. (Voir : CBC, CCM, CFB, CMAC, CTR, DEA, ECB, OFB.)

$ Blowfish
(N) Chiffrement de blocs symétriques avec clés de longueur variable (32 à 448 bits) conçu en 1993 par Bruce Schneier comme remplacement non breveté, sans licence, ni redevance, de DES ou IDEA. [Schn] (Voir : Twofish.)

$ endommagé du cerveau *(brain-damaged)*
(D) /argot/ "Évidemment faux ; d'une conception extrêmement déficiente. Dire de quelque chose qu'il est endommagé du cerveau est outrancier. Le terme implique que la chose est complètement inutilisable, et que son incapacité à fonctionner est due à sa conception, et non à un accident." [NCSSG] (Voir : faute.)
Terme déconseillé : il est vraisemblable que d'autres cultures utilisent des métaphores différentes pour ce concept. Donc, pour éviter l'incompréhension entre les nations, les IDOC NE DEVRAIENT PAS utiliser ce terme. (Voir : Utilisation déconseillée sous "Livre Vert".)

$ marque *(brand)*
1. (I) Marque ou nom distinctif qui identifie un produit ou entité commerciale.
2. (O) /SET/ Nom d'une carte de payement. (Voir : BCA.)
Instructions : les institutions financières et autres compagnies ont fondé des marques de cartes de payement, protègent et font connaître les marques, établissent et mettent en application des règles d'utilisation et d'acceptation de leurs cartes de payement, et fournissent des réseaux pour interconnecter les institutions financières. Ces marques combinent les rôles de producteur et d'acquéreur dans les interactions entre les détenteurs de cartes et les commerçants. [SET1]

$ autorité de certification de marque (BCA, *brand certification authority)*
(O) /SET/ Autorité de certification (CA) détenue par une marque de carte de payement, telle que MasterCard, Visa, ou American Express. [SET2] (Voir : hiérarchie de certification, SET.)

$ identifiant de CRL de marque (BCI, *brand CRL identifier*)
(O) /SET/ Liste à signature numérique, produite par une BCA, des noms des CA pour lesquels les CRL doivent être traitées lors de la vérification des signatures dans les messages SET. [SET2]

$ casser *(break)*
(I) /cryptographie/ Réussir à effectuer une analyse cryptographique et ainsi réussir à déchiffrer des données ou à effectuer quelque autre fonction cryptographique, sans avoir initialement la connaissance de la clé que la fonction requiert. (Voir : pénétrer, force, facteur de travail.)

Usage : ce terme s'applique aux données chiffrées ou, plus généralement, à un algorithme cryptographique ou un système cryptographique. Aussi, alors que l'usage le plus courant se réfère au cassage complet d'un algorithme, le terme est aussi utilisé lorsque on trouve une méthode qui réduit substantiellement le facteur de travail.

$ modèle Brewer-Nash *(Brewer-Nash model)*

(N) Modèle de sécurité [BN89] pour mettre en application la politique de la muraille de Chine. (À comparer à : modèle Bell-LaPadula, modèle Clark-Wilson.)

Instructions : toutes les informations protégées dans l'ensemble des firmes commerciales F(1), F(2), ..., F(N) sont catégorisées dans des classes I(1), I(2), ..., I(M) mutuellement exclusives de conflit d'intérêt qui s'appliquent entre toutes les firmes. Chaque firme appartient à exactement une classe. Le modèle Brewer-Nash a les règles obligatoires suivantes :

- Règle de lecture Brewer-Nash : le sujet S peut lire l'objet d'information O de la firme F(i) seulement si soit (a) O est de la même firme qu'un certain objet lu précédemment par S *soit* (b) O appartient à une classe I(i) de laquelle S n'a pas lu d'objet précédemment. (Voir : objet, sujet.)
- Règle d'écriture Brewer-Nash : le sujet S peut écrire l'objet d'information O à la firme F(i) seulement si (a) S peut lire O selon la règle de lecture Brewer-Nash *et* (b) aucun objet d'une firme différente F(j) ne peut être lu par S, que F(j) appartienne à la même classe que F(i) ou à une classe différente.

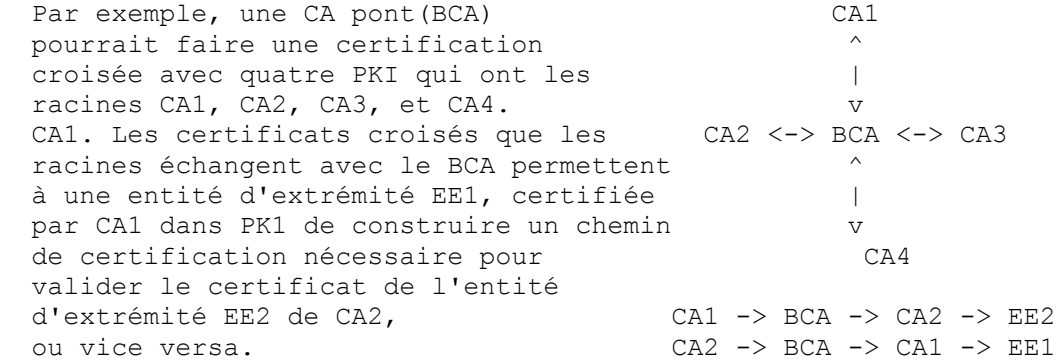
$ pont *(bridge)*

(I) Passerelle pour le trafic qui s'écoule à la couche 2 OSIRM entre deux réseaux (usuellement deux LAN). (À comparer à : CA pont, routeur.)

$ CA pont *(bridge CA)*

(I) PKI consistant en une seule CA qui fait une certification croisée avec des CA d'autres PKI. (Voir : certification croisée. À comparer à : pont.)

Instructions : une CA pont fonctionne comme une plate-forme qui active un utilisateur de certificat dans toutes les PKI qui se rattachent au pont, pour valider les certificats produits dans les autres PKI rattachées.



$ British Standard 7799

(N) La partie 1 de cette norme est un code de bonne conduite pour sécuriser un système d'information. La partie 2 spécifie le cadre de gestion, les objectifs, et les exigences de contrôle des systèmes de gestion de la sécurité des informations. [BS7799] (Voir : ISO 17799.)

$ navigateur *(browser)*

(I) Programme informatique client qui peut restituer et afficher des informations provenant de serveurs sur la Toile mondiale. Exemples : Netscape Navigator et Microsoft Internet Explorer.

$ force brute *(brute force)*

(I) Technique d'analyse cryptologique ou autre sorte de méthode d'attaque impliquant une procédure exhaustive qui essaye un grand nombre de solutions possibles au problème. (Voir : impossible, force, facteur de travail.)

Instructions : dans certains cas, la force brute implique d'essayer toutes les possibilités. Par exemple, pour du texte chiffré dont l'analyste connaît déjà l'algorithme de déchiffrement, une technique de force brute pour trouver le texte source correspondant est de déchiffrer le message avec toutes les clés possibles. Dans d'autres cas, la force brute implique d'essayer un grand nombre de possibilités mais substantiellement moins que toutes. Par exemple, étant donnée une fonction de hachage qui produit comme résultat un hachage de N bits, la probabilité que l'analyste trouve deux entrées qui ont le même résultat de hachage après avoir essayé seulement 2**(N/2) entrées choisies au hasard est supérieure à 1/2. (Voir : attaque de l'anniversaire.)

$ débordement de mémoire tampon *(buffer overflow)*

(I) Toute technique d'attaque qui exploite une vulnérabilité résultant d'un logiciel ou matériel informatique qui ne vérifie pas les dépassements de limite de la zone de mémorisation lorsque des données sont écrites dans une séquence de localisations de mémorisation commençant dans cette zone.
Instructions : en faisant qu'une opération d'un système normal écrive des données au delà des limites d'une zone de mémorisation, l'attaquant cherche soit à interrompre le fonctionnement du système, soit à causer l'exécution par le système d'un logiciel malveillant inséré par l'attaquant

$ zone tampon *(buffer zone)*
(I) Segment neutre inter réseaux utilisé pour connecter d'autres segments qui fonctionnent chacun sous une politique de sécurité différente.
Instructions : pour connecter un réseau privé à l'Internet ou quelque autre réseau relativement public, on peut construire un petit LAN séparé et isolé et le connecter à la fois au réseau privé et au réseau public ; une des connexions ou les deux vont mettre en œuvre un pare-feu pour limiter le trafic qui peut passer à travers la zone tampon.

$ chiffrement en gros *(bulk encryption)*
1. (I) Chiffrement de plusieurs canaux en les agrégeant en un seul chemin de transfert et en chiffrant ensuite ce chemin. (Voir : canal.)
2. (O) "Chiffrement simultané de tous les canaux d'une liaison de télécommunications multi canal." [C4009] (À comparer à : matériel de chiffrement en vrac .)

Usage : L'utilisation de "simultané" dans la définition 2 pourrait être interprétée comme signifiant que plusieurs canaux sont chiffrés séparément mais au même moment. Cependant, la signification courante du terme est que plusieurs flux de données sont combinés en un seul flux et qu'ensuite ce flux est chiffré comme un tout.

$ clé de gros *(bulk key)*
(D) Dans quelques descriptions publiées de chiffrement hybride pour SSH, Windows 2000, et autres applications, ce terme se réfère à une clé symétrique qui (a) est utilisée pour chiffrer une quantité relativement importante de données, et (b) est elle-même chiffrée avec une clé publique. (À comparer à : matériel de chiffrement en gros, clé de session.)
Exemple : Pour envoyer un gros fichier à Bob, Alice (a) génère une clé symétrique et l'utilise pour chiffrer le fichier (c'est-à-dire, chiffrer les informations en gros qui sont à envoyer) et ensuite (b) chiffre cette clé symétrique (la "clé de gros") avec la clé publique de Bob.
Terme déconseillé : les IDOC NE DEVRAIENT PAS utiliser ce terme ou définition ; le terme n'est pas bien établi et pourrait être confondu avec le terme établi "matériel de chiffrement en gros". À la place, utiliser "clé symétrique" et expliquer soigneusement comment la clé est appliquée.

$ matériel de chiffrement en gros *(bulk keying material)*
(N) Se réfère au traitement de matériel de chiffrement en grandes quantités, par exemple, comme un ensemble de données qui contient de nombreux éléments de matériel de chiffrement. (Voir : type 0. À comparer à : clé de gros, chiffrement en gros.)

$ dans la pile *(bump-in-the-stack)*
(I) Approche selon la mise en œuvre qui place un mécanisme de sécurité réseau à l'intérieur du système à protéger. (À comparer à : dans le réseau.)
Exemple : IPsec peut être incorporé, dans la pile de protocole d'un système existant ou dans la conception de systèmes existants, en plaçant une nouvelle couche entre les pilotes de la couche IP et de la couche OSIRM 3 existantes. L'accès au code de source n'est pas exigé pour la pile existante, mais le système qui contient la pile n'a pas besoin d'être modifié [RFC4301].

$ dans le réseau *(bump-in-the-wire)*
(I) Approche de mise en œuvre qui place un mécanisme de sécurité réseau en dehors du système à protéger. (À comparer à : dans la pile.)
Exemple : IPsec peut être mis en œuvre en externe, dans un appareil physiquement séparé, afin que le système qui reçoit la protection IPsec n'ait pas du tout besoin d'être modifié [RFC4301]. Le chiffrement de liaison de qualité militaire a principalement été mis en œuvre par des appareils dans le réseau.

$ analyse de cas d'affaires *(business-case analysis)*
(N) Forme étendue d'analyse coût-bénéfice qui prend en compte des facteurs au delà de la métrique financière, incluant les facteurs de sécurité comme les exigences de services de sécurité, leur faisabilité technique et programmatique, leurs bénéfices qualitatifs, et les risques associés. (Voir : analyse de risque.)

$ octet *(byte)*
(I) Unité fondamentale de mémorisation informatique ; plus petite unité adressable dans l'architecture d'un ordinateur.

Contient habituellement un caractère d'information et signifie habituellement aujourd'hui huit bits.
Usage : compris comme plus grand qu'un "bit", mais plus petit qu'un "mot". Bien que "octet" veuille presque toujours dire "huit bits" aujourd'hui, certaines architectures d'ordinateur ont eu des octets d'autres tailles (par exemple, six bits, neuf bits). Donc, un STD DEVRAIT déclarer le nombre de bits d'un octet lorsque le terme est utilisé pour la première fois dans le STD.

$ champ C. *(C field)* (D) Voir : champ Compartiments.

$ système informatique C1 ou C2 *(C1 or C2 computer system)*
(O) /TCSEC/ Voir : Instructions sous "Critères d'évaluation d'un système informatique de confiance".

$ certificat de CA *(CA certificate)*
(D) "Certificat [numérique] pour une CA produit par une autre CA." [X509]
Définition déconseillée : les IDOC NE DEVRAIENT PAS utiliser ce terme avec cette définition ; la définition est ambiguë à l'égard de la façon dont le certificat est construit et comment il est destiné à être utilisé. Les IDOC qui utilisent ce terme DEVRAIENT en fournir une définition technique. (Voir : profil de certificat.)
Instructions : il n'y a pas de choix évident et sans ambiguïté pour une définition technique de ce terme. Des PKI différentes peuvent utiliser des profils de certificat différents, et la Recommandation UIT-T X.509 fournit plusieurs choix de production des certificats aux CA. Par exemple, une définition possible est la suivante : un certificat de clé publique X.509 v3 qui a une extension "basicConstraints" contenant une valeur "cA" de "VRAI". Cela indiquerait spécifiquement que la "clé publique certifiée peut être utilisée pour vérifier les signatures de certificat", c'est-à-dire, que la clé privée peut être utilisée par une CA.
Cependant, il y a aussi d'autres façons d'indiquer un tel usage. Le certificat peut avoir une extension "Usage de clé" qui indique l'objet pour lequel la clé publique peut être utilisée, et une des valeurs que définit X.509 pour cette extension est "keyCertSign", pour indiquer que le certificat peut être utilisé pour vérifier une signature de CA sur les certificats. Si "keyCertSign" est présent dans un certificat qui a aussi une extension "basicConstraints", alors "cA" est réglé à "VRAI" dans cette extension. Autrement, on pourrait produire à une CA un certificat dans lequel "keyCertSign" est affirmé sans que "basicConstraints" soit présent ; et une entité qui agit comme CA pourrait recevoir un certificat avec "keyUsage" réglé à d'autres valeurs, avec ou sans "keyCertSign".

$ domaine de CA *(CA domain)*
(N) /PKI/ Domaine de politique de sécurité qui "consiste en une CA et ses sujets [c'est-à-dire, les entités désignées dans les certificats produits par la CA]. On s'y réfère parfois sous le nom de domaine de PKI." [PAG] (Voir : domaine.)

$ chiffrement César *(Caesar cipher)*
(I) Chiffrement qui est défini pour un alphabet de N caractères, A(1), A(2), ..., A(N), et crée du texte chiffré en remplaçant chaque caractère A(i) de texte en clair par A(i+K, mod N) pour 0<K<N+1. [Schn]
Exemples : (a) Durant la guerre des Gaules, Jules César utilisait un chiffrement avec K=3. Dans un chiffrement César avec K=3 pour l'alphabet français, A est remplacé par D, B par E, C par F, ..., W par Z, X par A, Y par B, Z par C. (b) Les systèmes UNIX incluent parfois un logiciel "ROT13" qui met en œuvre un chiffrement César avec K=13 (c'est-à-dire, une ROTation de 13).

$ rappel *(call back)*
(I) Technique d'authentification pour les terminaux qui accèdent à distance à un ordinateur via des lignes téléphoniques ; le système hôte déconnecte l'appelant et se reconnecte ensuite sur un numéro de téléphone qui a été préalablement autorisé pour ce terminal.

$ CANEWARE
(O) Système de chiffrement de bout en bout pour les réseaux de données informatiques qui ont été développés par le ministère U.S. de la Défense dans les années 1980 pour assurer un service de confidentialité des données d'hôte à hôte pour les datagrammes dans la couche OSIRM 3. [Roge] (À comparer à : BLACKER, IPsec.)
Instructions : chaque hôte utilisateur se connecte à son propre appareil de chiffrement sur le réseau qui est appelé un frontal CANEWARE (CFE, *CANEWARE Front End*) à travers lequel l'hôte se connecte au sous-réseau. CANEWARE utilise le chiffrement symétrique pour le trafic de CFE à CFE, mais utilise aussi FIREFLY pour établir ces clés de session. Les certificats de clé publique produits par le système FIREFLY incluent des accréditifs pour le contrôle d'accès obligatoire. Pour un contrôle d'accès discrétionnaire, le système comporte aussi un ou plusieurs processeurs de contrôle CANEWARE CCP, *CANEWARE Control Processor*) centralisés qui se connectent au sous-réseau, tiennent une base de données des autorisations de contrôle d'accès discrétionnaire, et communiquent ces autorisations aux ensembles de CFE affectés.
Le système CANEWARE n'est MLS que de deux des trois façons dont BLACKER l'est : (a) comme les BFE BLACKER, les CFE forment un périmètre de sécurité autour d'un sous-réseau, séparant les hôtes utilisateurs du sous-réseau, afin que le sous-réseau puisse fonctionner à un niveau de sécurité différent de celui des hôtes. (b) Comme BLACKER, les composants

CANEWARE sont de confiance pour séparer les datagrammes de différents niveaux de sécurité, afin que chaque datagramme d'un certain niveau de sécurité ne puisse être reçu que par un hôte qui est autorisé pour ce niveau de sécurité ; et donc, CANEWARE peut séparer des communautés d'hôtes qui opèrent à des niveaux de sécurité différents. (c) À la différence du BFE, le côté hôte d'un CFE n'est pas MLS, et traite tous les paquets reçus d'un hôte utilisateur comme étant au même niveau de sécurité obligatoire.

$ liste de capacités *(capability list)*
(I) /système d'informations/ Mécanisme qui met en œuvre le contrôle d'accès pour une entité système en énumérant les ressources système auxquelles il est permis à l'entité d'accéder, et, implicitement ou explicitement, les modes d'accès accordés pour chaque ressource. (À comparer à : liste de contrôle d'accès, matrice de contrôle d'accès, profil d'accès, jeton de capacité.)

$ jeton de capacité *(capability token)*
(I) Jeton (usuellement un objet de données inimitable) qui donne au porteur ou détenteur le droit d'accès à une ressource système. La possession du jeton est acceptée par un système comme preuve que le détenteur a été autorisé à accéder à la ressource indiquée par le jeton. (Voir : certificat d'attribut, liste de capacité, accréditif, certificat numérique, ticket, jeton.)

$ modèle de maturité de capacité (CMM, *Capability Maturity Model*)
(N) Méthode pour juger de la maturité de processus logiciels dans une organisation et pour identifier les pratiques cruciales nécessaires pour augmenter la maturité du processus. [Chris] (À comparer à : critères courants.)
Instructions : Le CMM ne spécifie pas de critères d'évaluation de la sécurité (voir : niveau d'assurance) mais son utilisation peut améliorer l'assurance de sécurité. Le CMM décrit des principes et pratiques qui peuvent améliorer les processus logiciels en termes d'évolution de processus ad hoc à des processus disciplinés. Le CMM a cinq niveaux :
- Initial : les processus sont ad hoc ou chaotiques, et peu sont bien définis. Le succès dépend d'efforts individuels héroïques.
- Répétable : des processus de gestion de projet de base sont établis pour suivre les coûts, les programmes et les fonctions. La discipline de procédure nécessaire est en place pour répéter les succès sur les projets ayant des applications similaires.
- Défini : le processus logiciel pour les activités aussi bien de gestion que d'ingénierie est documenté, normalisé, et intégré dans un processus logiciel standard pour l'organisation. Chaque projet utilise une version approuvée, sur mesure, du processus standard de l'organisation pour développer et maintenir le logiciel.
- Géré : on collecte des mesures détaillées du processus logiciel et de la qualité des produits. Le processus logiciel et les produits sont compris et contrôlés quantitativement.
- Optimisé : l'amélioration continue du processus est permise par des retours quantitatifs du procès et du pilotage d'idées et technologies innovantes.

$ CAPSTONE
(N) Microcircuit intégré (dans la série MYK-8x fabriquée par Mykotronx, Inc.) qui met en œuvre SKIPJACK, KEA, DSA, SHA, et les fonctions mathématiques de base nécessaires pour prendre en charge le chiffrement asymétrique ; il a un générateur non déterministe de nombres aléatoires ; il prend en charge le tiers de confiance. (Voir : FORTEZZA. À comparer à : CLIPPER.)

$ carte *(card)* Voir : carte cryptographique, FORTEZZA, carte de payement, carte PC, carte à mémoire, jeton.

$ sauvegarde de carte *(card backup)*. Voir : sauvegarde de jeton.

$ copie de carte *(card copy)*. Voir : copie de jeton.

$ restauration de carte *(card restore)*. Voir : restauration de jeton.

$ détenteur de carte *(cardholder)*
1. (I) Entité à laquelle une carte a été fournie.
Usage : se réfère usuellement à une personne vivante, mais peut se référer (a) à une position (voir : billet, rôle) dans une organisation ou (b) à un processus automatique. (À comparer à : utilisateur.)
2. (O) /SET/ "Détenteur d'un compte valide de carte de payement et utilisateur d'un logiciel qui prend en charge le commerce électronique" [SET2]. Une carte de payement est délivrée à un détenteur de carte par un producteur de carte. SET s'assure que dans les interactions du détenteur de carte avec les commerçants, les informations du compte de la carte de payement restent confidentielles. [SET1]

$ certificat de détenteur de carte *(cardholder certificate)*
(O) /SET/ Certificat numérique qui est produit à un détenteur de carte lors de l'approbation par l'institution financière

productrice du détenteur de carte, et qui est transmis aux commerçants avec les demandes d'achat et les instructions de payement chiffrées, qui porte l'assurance que le numéro de compte a bien été validé par l'institution financière productrice et ne peut être altéré par un tiers. [SET1]

$ autorité de certification de détenteur de carte (CCA, *cardholder certification authority*)
(O) /SET/ Une CA responsable de la production de certificats numériques pour les détenteurs de cartes et peut opérer au nom d'une marque de carte de payement, d'un producteur de carte, ou d'une autre partie conformément aux règles de la marque. Une CCA entretient des relations avec les producteurs de cartes pour permettre la vérification des comptes des détenteurs de carte. Une CCA ne produit pas une CRL mais distribue les CRL produites par les CA racines, les CA de marque, les CA géopolitiques, et les CA de passerelle de payement. [SET2]

$ CAST
(N) Procédure de conception d'algorithmes de chiffrement symétriques, et d'une famille résultante d'algorithmes, inventée par Carlisle Adams (C.A.) et Stafford Tavares (S.T.) [RFC2144], [RFC2612].

$ catégorie *(category)*
(I) Groupement d'éléments d'informations sensibles auquel une étiquette restrictive non hiérarchique est appliquée pour augmenter la protection des données. (Voir : approbation formelle d'accès. À comparer à : compartiment, classification.)

$ CCITT. (N) Acronyme de Comité Consultatif International du Téléphone et du Télégraphe. Rebaptisé UIT-T.

$ CCM. (N) Voir : Compteur avec code d'authentification de message à chaînage de bloc de chiffrement.

$ CERIAS
(O) Centre pour l'éducation et la recherche en assurance et sécurité de la Purdue University, qui inclut des facultés de nombreuses écoles et départements et a une approche pluridisciplinaire des problèmes de sécurité allant du technique à l'éthique, juridique, éducatif, la communication, la linguistique, et l'économie.

$ certificat *(certificate)*
1. (I) /langage général/ Document qui atteste de la véracité de quelque chose ou de la propriété de quelque chose.
2. (I) /sécurité générale/ Voir : jeton de capacité, certificat numérique.
3. (I) /PKI/ Voir : certificat d'attribut, certificat de clé publique.

$ module d'arbitrage de certificat (CAM, *Certificate Arbitrator Module*)
(O) Module de logiciel libre qui est conçu pour être intégré avec une application d'acheminement, la réponse, et la gestion ainsi que la médiation de la validation de certificats entre cette application et les CA dans le PKI ACES.

$ autorité de certificat *(certificate authority)*
(D) Synonyme de "autorité de certification".
Terme déconseillé : les IDOC NE DEVRAIENT PAS utiliser ce terme ; il suggère une utilisation négligente du terme "autorité de certification", qui est préférée dans les normes PKI (par exemple, [X509], [RFC3280]).

$ chaîne de certificat *(certificate chain)*
(D) Synonyme de "chemin de certification". (Voir : chaîne de confiance.)
Terme déconseillé : les IDOC NE DEVRAIENT PAS utiliser ce terme ; il fait double emploi avec la signification d'un terme normalisé. À la place, utiliser "chemin de certification".

$ validation de chaîne de certificat *(certificate chain validation)*
(D) Synonyme de "validation de certificat " ou "validation de chemin".
Terme déconseillé : les IDOC NE DEVRAIENT PAS utiliser ce terme ; il fait double emploi avec la signification de termes normalisés et mélange les concepts d'une façon potentiellement trompeuse. À la place, utiliser "validation de certificat" ou "validation de chemin", selon ce que l'on veut dire. (Voir : valider vs. vérifier.)

$ création de certificat *(certificate creation)*
(I) Acte ou processus par lequel une CA règle les valeurs des champs de données d'un certificat numérique et le signe. (Voir : produire.)

$ expiration de certificat *(certificate expiration)*
(I) Événement qui survient lorsque un certificat cesse d'être valide parce que sa durée de vie allouée a été dépassée. (Voir : révocation de certificat, expiration.)

Instructions : la durée de vie allouée à un certificat X.509 est déclarée dans le certificat lui-même. (Voir : période de validité.)

$ extension de certificat *(certificate extension)*. (I) Voir : extension.

$ détenteur de certificat *(certificate holder)*
(D) Synonyme du "sujet" d'un certificat numérique. (À comparer à : propriétaire de certificat, utilisateur de certificat.)
Définition déconseillée : les IDOC NE DEVRAIENT PAS utiliser ce terme comme synonyme du sujet d'un certificat numérique ; le terme est potentiellement ambigu. Par exemple, le terme pourrait être mal compris comme se référant à une entité système ou un composant, comme un dépositaire, qui a simplement la possession d'une copie du certificat.

$ gestion de certificat *(certificate management)*
(I) Fonctions qu'une CA peut effectuer durant le cycle de vie d'un certificat numérique, incluant ce qui suit :
- Acquérir et vérifier les éléments de données à lier dans le certificat.
- Coder et signer le certificat.
- Mémoriser le certificat dans un répertoire ou chez un dépositaire.
- Renouveler, changer les clés, et mettre à jour le certificat.
- Révoquer le certificat et produire une CRL.

(Voir : gestion d'archive, gestion de certificat, gestion de clés, architecture de sécurité, gestion de jetons.)

$ autorité de gestion de certificat (CMA, *certificate management authority*)
(D) /U.S. DoD/ Utilisé aussi bien pour une CA qu'une RA. [DoD7], [SP32]
Terme déconseillé : les IDOC NE DEVRAIENT PAS utiliser ce terme parce qu'il est potentiellement ambigu, comme dans un contexte impliquant des ICRL. À la place, utiliser CA, RA, ou les deux, selon ce que l'on veut dire.

$ propriétaire de certificat *(certificate owner)*
(D) Synonyme de "sujet" d'un certificat numérique. (À comparer à : détenteur de certificat, utilisateur de certificat.)
Définition déconseillée : les IDOC NE DEVRAIENT PAS utiliser ce terme comme synonyme de sujet d'un certificat numérique ; le terme est potentiellement ambigu. Par exemple, le terme pourrait se référer à une entité système, comme une corporation, qui a acheté un certificat pour faire fonctionner un équipement, comme un serveur de la Toile.

$ chemin de certificat *(certificate path)*
(D) Synonyme de "chemin de certification".
Terme déconseillé : les IDOC NE DEVRAIENT PAS utiliser ce terme ; il suggère une utilisation négligente de "chemin de certification", qui est préféré dans les normes de PKI (par exemple, [X509], [RFC3280]).

$ politique de certificat *(certificate policy)*
(I) "Ensemble désigné de règles qui indiquent l'applicabilité d'un certificat à une communauté et/ou classe d'application particulière avec des exigences de sécurité communes" [X509]. (À comparer à : CPS, politique de sécurité.)
Exemple : La politique de sécurité du Ministère de la Défense U.S. [DoD7] définissait quatre classes (c'est-à-dire, niveaux d'assurance) pour les certificats de clé publique X.509 et définit l'applicabilité de ces classes. (Voir : classe 2.)
Instructions : une politique de certificat peut aider un utilisateur de certificat à décider si un certificat devrait être de confiance dans une certaine application. "Par exemple, une certaine politique de certificat pourrait indiquer l'applicabilité d'un type de certificat pour l'authentification de transactions d'échange de données électroniques pour le commerce de biens dans une certaine gamme de prix" [RFC3647].
Un certificat de clé publique X.509 v3 peut avoir une extension "certificatePolicies" qui fait la liste des politiques de certificat, reconnues par la CA productrice, qui s'appliquent au certificat et gouvernent son utilisation. Chaque politique est notée par un identifiant d'objet et peut facultativement avoir des qualificatifs de politique de certificat. (Voir : profil de certificat.)
Chaque certificat SET spécifie au moins une politique de certificat, celle de la CA racine SET. SET utilise des qualificatifs de politique de certificat pour pointer sur la déclaration de politique réelle et pour ajouter des politiques qualifiantes à la politique racine. (Voir : qualificatif SET.)

$ qualificatif de politique de certificat *(certificate policy qualifier)*
(I) Informations qui relèvent d'une politique de certificat et sont incluses dans une extension "certificatePolicies" dans un certificat de clé publique X.509 v3.

$ profil de certificat *(certificate profile)*
(I) Spécification (par exemple, [DoD7], [RFC3280]) du format et de la sémantique des certificats de clé publique ou des certificats d'attribut, construits pour être utilisés dans un contexte d'application spécifique en choisissant parmi les options offertes par un standard plus large. (À comparer à : profil de protection.)

$ réactivation de certificat *(certificate reactivation)*
(I) Acte ou processus par lequel un certificat numérique qu'une CA a désigné pour la révocation mais ne figure pas encore sur une CRL, retourne à l'état valide.

$ changement de clé de certificat *(certificate rekey)*
1. (I) Acte ou processus par lequel un certificat de clé publique existant a sa valeur de clé changée par la production d'un nouveau certificat avec une clé publique différente (ordinairement nouvelle). (Voir : renouvellement de certificat, mise à jour de certificat, changement de clé.)

Instructions : Pour un certificat de clé publique X.509, l'essence du changement de clé est que le sujet reste le même et qu'une nouvelle clé publique soit liée à ce sujet. D'autres changements sont faits, et le vieux certificat n'est révoqué que si c'est exigé par la PKI et la CPS à l'appui du changement de clé. Si les changements vont au delà, le processus est une "mise à jour de certificat".

2. (O) /MISSI/ Acte ou processus par lequel une CA MISSI crée un nouveau certificat de clé publique X.509 qui est identique à l'ancien, excepté que le nouveau a (a) une nouvelle clé KEA différente, ou (b) une nouvelle clé DSS différente, ou (c) de nouvelles clés KEA et DSS différentes. Le nouveau certificat a aussi un numéro de série différent et peut avoir une période de validité différente. Une nouvelle date de création et une période de durée de vie de clé maximum sont allouées à chaque clé nouvellement générée. Si une nouvelle clé KEA est générée, on lui alloue une nouvelle KMID. Le vieux certificat reste valide jusqu'à ce qu'il arrive à expiration, mais ne peut plus être renouvelé, changé de clé, ou mis à jour.

$ renouvellement de certificat *(certificate renewal)*
(I) Acte ou processus par lequel la validité du lien affirmé par un certificat de clé publique existant est étendue en temps par la production d'un nouveau certificat. (Voir : changement de clé de certificat, mise à jour de certificat.)
Instructions : pour un certificat de clé publique X.509, ce terme signifie que la période de validité est étendue (et, bien sûr, qu'un nouveau numéro de série est alloué) mais le lien de la clé publique avec le sujet et les autres éléments de données restent les mêmes. Les autres éléments de données sont changés, et le vieux certificat n'est révoqué que si la PKI et la CPS l'exigent pour la prise en charge du renouvellement. Si les changements vont au-delà, le processus est un "changement de clé de certificat" ou une "mise à jour de certificat".

$ demande de certificat *(certificate request)*
(D) Synonyme de "demande de certification".
Terme déconseillé : les IDOC NE DEVRAIENT PAS utiliser ce terme ; il suggère l'utilisation négligente du terme "demande de certification", qui est préférée dans les normes de PKI (voir par exemple PKCS n° 10).

$ révocation de certificat *(certificate revocation)*
(I) Événement qui survient lorsque une CA déclare qu'un certificat numérique jusqu'alors valide produit par cette CA est devenu invalide ; c'est usuellement déclaré avec une date effective.
Instructions : dans X.509, une révocation est annoncée aux utilisateurs potentiels de certificat en produisant une CRL qui mentionne le certificat. La révocation et l'inscription sur une CRL ne sont nécessaires qu'avant l'arrivée à expiration programmée du certificat.

$ liste de révocation de certificat (CRL, *certificate revocation list*)
1. (I) Structure de données qui énumère les certificats numériques qui ont été invalidés par leur producteur avant le moment programmé pour leur expiration. (Voir : expiration de certificat, CRL delta, liste de révocation de certificat X.509.)
2. (O) "Liste signée qui indique un ensemble de certificats qui ne sont plus considérés comme valides par le producteur du certificat. En plus du terme générique de CRL, certains types spécifiques de CRL sont définis pour les CRL qui couvrent des domaines particuliers." [X509]

$ arborescence de révocation de certificat *(certificate revocation tree)*
(N) Mécanisme pour distribuer les notices de révocation de certificat ; utilise une arborescence de résultats hachés qui est signée par le producteur de l'arborescence. Offre une solution de remplacement à la production d'une CRL, mais n'est pas pris en charge dans X.509. (Voir : répondant d'état de certificat.)

$ numéro de série de certificat *(certificate serial number)*
1. (I) Valeur d'entier qui (a) est associée à, et peut être portée dans, un certificat numérique ; (b) est allouée au certificat par le producteur du certificat ; et (c) est unique parmi tous les certificats produits par ce producteur.
2. (O) "Valeur d'entier, unique au sein de la CA productrice, [qui] est associée sans ambiguïté à un certificat produit par cette CA." [X509]

$ autorité d'état de certificat *(certificate status authority)*
(D) /U.S. DoD/ "Entité de confiance qui fournit une vérification en ligne à un consommateur d'assertion de ce qu'un certificat de sujet est digne de confiance [on devrait plutôt parler de 'validité'], et peut aussi fournir des informations d'attribut supplémentaires sur le certificat de sujet." [DoD7]
Terme déconseillé : les IDOC NE DEVRAIENT PAS utiliser ce terme parce qu'il n'est pas largement accepté ; utiliser plutôt "répondant d'état de certificat" ou "serveur OCSP", ou autrement, expliquer ce qu'il signifie.

$ répondant d'état de certificat *(certificate status responder)*
(N) /FPKI/ Serveur de confiance en ligne qui agit pour une CA pour fournir des informations d'état de certificat authentifiées pour les utilisateurs de certificat [FPKI]. Offre une solution de remplacement à la production d'un CR. (Voir : arborescence de révocation de certificat, OCSP.)

$ mise à jour de certificat *(certificate update)*
(I) Acte ou processus par lequel des éléments de données non clés qui lient un certificat de clé publique existant, en particulier les autorisations accordées au sujet, sont changés par la production d'un nouveau certificat. (Voir : changement de clés de certificat, renouvellement de certificat.)
Usage : pour un certificat de clé publique X.509, l'essence de ce processus est que des changements fondamentaux sont faits aux données qui sont liées à la clé publique, comme celles qui sont nécessaires pour révoquer le vieux certificat. (Autrement, le processus est seulement un "changement de clés de certificat" ou "renouvellement de certificat".)

$ utilisateur de certificat *(certificate user)*
1. (I) Entité système qui dépend de la validité des informations (comme la valeur de clé publique d'une autre entité) fournies par un certificat numérique. (Voir : consommateur d'assertion. À comparer à : /certificat numérique/ sujet.)

Usage : l'entité dépendante peut être un être humain ou une organisation, ou un appareil ou processus contrôlé par un humain ou une organisation. (Voir : usager.)
2. (O) "Une entité qui a besoin de savoir, avec certitude, la clé publique d'une autre entité." [X509]
3. (D) Synonyme de "sujet" d'un certificat numérique.

Définition déconseillée : Les IDOC NE DEVRAIENT PAS utiliser ce terme avec la définition 3 ; le terme pourrait être confondu avec une des deux autres définitions données ci-dessus.

$ validation de certificat *(certificate validation)*
1. (I) Acte ou processus par lequel un utilisateur de certificat établit que les assertions faites par un certificat numérique peuvent être de confiance. (Voir : certificat valide, valider vs. vérifier.)
2. (O) "Processus de s'assurer qu'un certificat était valide à un instant donné, incluant éventuellement la construction et le traitement d'un chemin de certification [RFC4158], et de s'assurer que tous les certificats dans ce chemin étaient valides (c'est-à-dire n'étaient ni expirés ni révoqués) à cet instant donné." [X509]

Instructions : Pour valider un certificat, un utilisateur de certificat vérifie que le certificat est correctement formé et signé et est actuellement en vigueur :
- Vérifie la syntaxe et la sémantique : analyse la syntaxe du certificat et interprète sa sémantique, en appliquant les règles spécifiées pour et par ses champs de données, comme pour les extensions critiques dans un certificat X.509.
- Vérifie la signature : utilise la clé publique du producteur pour vérifier la signature numérique de la CA qui a produit le certificat en question. Si le vérificateur obtient la clé publique du producteur à partir du propre certificat de clé publique du producteur, ce certificat devrait être aussi validé. Cette validation peut conduire à valider encore un autre certificat, et ainsi de suite. Donc, en général, la validation de certificat implique de découvrir et de valider un chemin de certification.
- Vérifie l'actualité et la révocation : vérifie que le certificat est actuellement en vigueur en vérifiant que la date et l'heure courantes du certificat sont dans la période de validité (si elle est spécifiée dans le certificat) et que le certificat ne figure pas sur la liste d'une CRL ou est autrement annoncé comme invalide. (Les CRL doivent aussi être vérifiées par un processus de validation similaire.)

$ certification
1. (I) /Système d'information/ Évaluation complète (usuellement faite à l'appui d'une action d'accréditation) des caractéristiques techniques de sécurité d'un système d'informations et d'autres sauvegardes pour établir la mesure dans laquelle la conception et la mise en œuvre du système satisfont un ensemble d'exigences de sécurité spécifiées. [C4009], [FP102], [SP37] (Voir : accréditation. À comparer à : évaluation.)
2. (I) /certificat numérique/ Action ou processus de vérification de la confiance et de la pertinence du lien entre les éléments de données dans un certificat. (Voir : certifier.)
3. (I) /PKI/ Action ou processus de garantie de la propriété d'une clé publique par la production d'un certificat de clé publique qui lie la clé au nom de l'entité qui possède la clé privée correspondante. En plus de lier une clé à un nom, un certificat de clé publique peut lier ces éléments avec d'autres éléments de données restrictifs ou explicatifs. (Voir : certificat de clé publique X.509.)
4. (O) /SET/ "Processus qui rend certain qu'un ensemble d'exigences ou critères ont été remplis et qui atteste de ce fait à

l'égard des tiers, usuellement avec un instrument écrit. Un système qui a été inspecté et évalué comme pleinement conforme au protocole SET par des parties et processus dûment autorisés serait dit avoir été certifié conforme." [SET2]

$ autorité de certification (CA, *certification authority*)

1. (I) Une entité qui produit des certificats numériques (en particulier des certificats X.509) et garantit le lien entre les éléments de données dans un certificat.
2. (O) "Une autorité de confiance pour un ou plusieurs utilisateurs pour créer et allouer des certificats. Facultativement, l'autorité de certification peut créer les clés de l'usager." [X509]

Instructions : les utilisateurs de certificats dépendent de la validité des informations fournies par un certificat. Donc, une CA devrait être quelqu'un à qui les utilisateurs de certificats font confiance et qui détient habituellement une position officielle créée et investie par un gouvernement, une corporation, ou quelque autre organisation. Une CA est chargée de gérer la durée de vie des certificats (voir : gestion de certificat) et, selon le type de certificat et la CPS qui s'appliquent, peut être responsable du cycle de vie des paires de clés associées aux certificats (voir : gestion de clé).

$ station de travail d'autorité de certification (CAW, *certification authority workstation*)

(N) Système informatique qui permet à une CA de produire des certificats numériques et prend en charge d'autres fonctions de gestion de certificat en tant que de besoin.

$ hiérarchie de certification *(certification hierarchy)*

1. (I) Topologie de relations structurées en arborescence (sans boucle) entre des CA et les entités auxquelles les CA fournissent des certificats de clés publiques. (Voir : PKI hiérarchique, gestion hiérarchisée.)

Instructions : dans cette structure, une CA est la CA supérieure, le plus haut niveau de la hiérarchie. (Voir : racine, CA supérieure.) La CA supérieure peut produire des certificats de clé publique à une ou plusieurs CA supplémentaires qui forment le second plus haut niveau. Chacune de ces CA peut produire des certificats à plus de CA au troisième plus haut niveau, et ainsi de suite. Les CA au second niveau ne produisent des certificats qu'aux entités non CA qui forment le plus bas niveau (voir : entité d'extrémité). Donc, tous les chemins de certification commencent à la CA supérieure et descendent jusqu'au niveau zéro ou plus des autres CA. Tous les utilisateurs de certificat fondent les validations de chemin sur la clé publique de la CA supérieure.

2. (I) /PEM/ Une hiérarchie de certification pour PEM a trois niveaux de CA [RFC1422] :
- Le plus haut niveau est "l'autorité d'enregistrement des politiques de l'Internet".
- Une CA au second plus haut niveau est une "autorité de certification de politique".
- Une CA au troisième plus haut niveau est une "autorité de certification".

3. (O) /MISSI/ Une hiérarchie de certification pour MISSI a trois ou quatre niveaux de CA :
- Une CA au plus haut niveau, la CA supérieure, est une "autorité d'approbation de politique".
- Une CA au second plus haut niveau est une "autorité de création de politique".
- Une CA au troisième plus haut niveau est une autorité locale appelée une "autorité de certification".
- Une CA au quatrième plus haut niveau (facultatif) est une "autorité de certification subordonnée".

4. (O) /SET/ Une hiérarchie de certification pour SET a trois ou quatre niveaux de CA :
- Le plus haut niveau est une "CA SET racine".
- Une CA au second plus haut niveau est une "autorité de certification de marque".
- Une CA au troisième niveau (facultatif) est une "autorité de certification géopolitique".
- Une CA au quatrième plus haut niveau est une "CA de détenteur de carte", une CA commerciale", ou une "CA de passerelle de payement".

$ chemin de certification *(certification path)*

1. (I) Séquence liée d'un ou plusieurs certificats de clé publique, ou un ou plusieurs certificats de clé publique et un certificat d'attribut, qui permet à un utilisateur de certificat de vérifier la signature sur le dernier certificat du chemin, et donc permet à l'utilisateur d'obtenir (à partir du dernier certificat) une clé publique certifiée, ou des attributs certifiés, de l'entité système qui est le sujet de ce dernier certificat. (Voir : ancre de confiance, validation de certificat, certificat valide.)
2. (O) "Une séquence ordonnée de certificats d'objets dans l'arborescence d'informations de répertoire [X.500] qui, avec la clé publique de l'objet initial dans le chemin, peut être traitée pour obtenir celle de l'objet final dans le chemin." [RFC3647], [X.509]

Instructions : la liste est "liée" dans le sens où la signature numérique de chaque certificat (sauf éventuellement le premier) est vérifiée par la clé publique contenue dans le certificat précédent ; c'est-à-dire, la clé privée utilisée pour signer un certificat et la clé publique contenue dans le certificat précédent forment une paire de clés qui a été précédemment liée à l'autorité qui a signé.

Le chemin est la "liste des certificats nécessaire pour [permettre] à un utilisateur particulier d'obtenir la clé publique [ou les attributs] d'un autre [utilisateur]." [X.509] Ici, le mot "particulier" pointe sur un chemin de certification qui peut être validé par un utilisateur de certificat qui pourrait n'être pas capable d'être validé par un autre. C'est parce que soit le premier certificat a besoin d'être un certificat de confiance, soit que la signature sur le premier certificat a besoin d'être vérifiable par une clé de confiance (par exemple, une clé racine) mais une telle confiance n'est établie que par rapport à un usager

"particulier" (c'est-à-dire, spécifique) et absolument pas pour tous les usagers.

$ politique de certification *(certification policy)*
(D) Synonyme soit de "politique de certificat" soit de "déclaration de pratique de certification".
Terme déconseillé : les IDOC NE DEVRAIENT PAS utiliser ce terme comme synonyme pour l'un de ces termes ; cela ferait double emploi et mélangerait les concepts d'une façon potentiellement trompeuse. À la place, utiliser soit "politique de certificat" soit "déclaration de pratique de certification", selon ce qu'on veut dire.

$ déclaration de pratique de certification (CPS, *certification practice statement*)
(I) "Une déclaration des pratiques qu'emploient une autorité de certification pour produire les certificats." [DSG], [RFC3647] (Voir : politique de certificat.)
Instructions : une CPS est une politique de sécurité publiée qui peut aider un utilisateur de certificat à décider si un certificat produit par une CA particulière peut être assez de confiance pour l'utiliser dans une certaine application. Une CPS peut être (a) une déclaration par une CA des détails du système et des pratiques qu'elle utilise dans ses opérations de gestion des certificats, (b) une partie d'un contrat entre la CA et une entité à laquelle un certificat est produit, (c) un statut ou une réglementation applicable à la CA, ou (d) une combinaison de ces types impliquant plusieurs documents. [DSG]
Une CPS est usuellement plus détaillée et plus orientée vers la procédure qu'une politique de certificat. Une CPS s'applique à une CA ou une communauté de CA particulière, tandis qu'une politique de certificat s'applique à travers les CA ou communautés de CA. Une CA avec une seule CPS peut prendre en charge plusieurs politiques de certificat, qui peuvent être utilisées pour différentes applications ou par différentes communautés d'utilisateurs. D'un autre côté, plusieurs CA, chacune avec une CPS différente, peuvent prendre en charge la même politique de certificat. [RFC3647]

$ demande de certification *(certification request)*
(I) Format de transaction indépendant de l'algorithme (par exemple, PKCS n° 10, RFC4211) qui contient un DN, et une clé publique ou, facultativement, un ensemble d'attributs, collectivement signés par l'entité qui demande la certification, et envoyé à une CA, qui transforme la demande en un certificat de clé publique X.509 ou un autre type de certificat.

$ certifier *(certify)*
1. (I) Produire un certificat numérique et donc attester de la vérité, de l'exactitude, et du lien entre les éléments de données dans le certificat (par exemple, "certificat de clé publique X.509") comme l'identité du sujet du certificat et la possession d'une clé publique. (Voir : certification.)

Usage : "certifier une clé publique" signifie produire un certificat de clé publique qui assure le lien entre le sujet du certificat et la clé.

2. (I) Acte par lequel une CA utilise des mesures pour vérifier la vérité, l'exactitude, et le lien entre des éléments de données et un certificat numérique.

Instructions : Une description des mesures utilisées pour la vérification devrait être incluse dans la CPS de la CA.

$ chaîne *(chain)*. (D) Voir : chaîne de confiance.

$ protocole d'authentification par mise au défi de prise de contact (CHAP, *Challenge Handshake Authentication Protocol*)
(I) Méthode d'authentification d'entités homologues (employée par PPP et d'autres protocoles, par exemple, la RFC3720) qui utilise un défi généré de façon aléatoire et exige une réponse correspondante qui dépend d'un hachage cryptographique d'une certaine combinaison du défi et d'une clé secrète. [RFC1994] (Voir : défi-réponse, PAP.)

$ mise au défi-réponse *(challenge-response)*
(I) Processus d'authentification qui vérifie une identité en exigeant que des informations d'authentification correctes soient fournies en réponse à un défi. Dans un système informatique, les informations d'authentification sont usuellement une valeur dont le calcul est exigé en réponse à une valeur de défi non prévisible, mais elles peuvent être juste un mot de passe.

$ mécanisme d'authentification par mise au défi-réponse (CRAM, *Challenge-Response Authentication Mechanism*)
(I) /IMAP4/ Mécanisme de la [RFC2195], destiné à être utilisé avec IMAP4 AUTHENTICATE, par lequel un client IMAP4 utilise un hachage à clé [RRC2104] pour s'authentifier auprès d'un serveur IMAP4. (Voir : POP3 APOP.)
Instructions : le serveur comporte un unique horodatage dans sa réponse pour indiquer au client qu'il est prêt. Le client répond par le nom du client et le résultat haché de l'application de MD5 à une chaîne formée de l'enchaînement de l'horodatage et d'un secret partagé qui n'est connu que du client et du serveur.

$ canal *(channel)*
1. (I) Chemin de transfert d'informations au sein d'un système. (Voir : canal couvert.)
2. (O) "Une subdivision du support physique permettant des utilisations indépendantes éventuellement partagées du support." (RFC3753)

$ capacité de canal *(channel capacity)*
(I) Capacité totale d'une liaison à porter des informations ; usuellement exprimée en bits par seconde. (RFC3753) (À comparer à : bande passante.)
Instructions : dans une certaine bande passante, la capacité théorique maximum de canal est donnée par la Loi de Shannon. La capacité réelle de canal est déterminée par la bande passante, le système de codage utilisé, et le ratio signal sur bruit.

$ somme de contrôle *(checksum)*
(I) Une valeur qui (a) est calculée par une fonction qui dépend du contenu d'un objet de données et (b) est mémorisée ou transmise avec l'objet, pour détecter les changements des données. (Voir : contrôle de redondance cyclique, service d'intégrité des données, code de détection d'erreur, hachage, hachage à clé, bit de parité, somme de contrôle protégée.)
Instructions : pour avoir l'assurance qu'un objet de données n'a pas été changé, une entité qui utilise ultérieurement les données peut recalculer la valeur de la somme de contrôle indépendamment et comparer le résultat et la valeur qui a été mémorisée ou transmise avec l'objet.
Les systèmes et réseaux informatiques utilisent des sommes de contrôle (et autres mécanismes) pour détecter des changements accidentels des données. Cependant, une interception active qui change les données pourrait aussi changer une somme de contrôle qui les accompagne pour qu'elle corresponde aux données changées. Donc, certaines fonctions de somme de contrôle ne sont pas par elles-mêmes de bonnes contre-mesures aux attaques actives. Pour protéger contre les attaques actives, la fonction de somme de contrôle doit être bien choisie (voir : hachage cryptographique) et le résultat de la somme de contrôle doit être cryptographiquement protégé (voir : signature numérique, hachage à clé).

$ politique de la muraille de Chine *(Chinese wall policy)*
(I) Politique de sécurité pour empêcher un conflit d'intérêt causé par une entité (par exemple, un consultant) qui interagit avec des entreprises concurrentes. (Voir : modèle de Brewer-Nash.)
Instructions : toutes les informations sont rangées dans des catégories dont les classes excluent mutuellement les conflits d'intérêt I(1), I(2), ..., I(M), et chaque firme F(1), F(2), ..., F(N) appartient exactement à une classe. La politique déclare que si un consultant a accès aux informations de classe I(i) d'une firme dans cette classe, le consultant ne peut pas être admis à accéder aux informations provenant d'une autre firme dans cette même classe, mais peut accéder aux informations provenant d'une autre firme qui est dans une classe différente. Donc, la politique crée une barrière à la communication entre des firmes qui sont dans la même classe de conflit d'intérêt. Brewer et Nash ont modélisé la mise en application de cette politique [BN89], incluant le traitement des violations de politique qui pourraient survenir parce que deux consultants ou plus travaillent pour la même firme.

$ attaque du texte chiffré choisi *(chosen-ciphertext)*
(I) Technique d'analyse cryptographique dans laquelle l'analyste essaye de déterminer la clé à partir de la connaissance du texte source qui correspond au texte chiffré choisi (c'est-à-dire, dicté) par l'analyste.

$ attaque du texte source choisi *(chosen-plaintext)*
(I) Technique d'analyse cryptographique dans laquelle l'analyste essaye de déterminer la clé à partir de la connaissance du texte chiffré qui correspond au texte source choisi (c'est-à-dire, dicté) par l'analyste.

$ chiffrement *(cipher)*. (I) Algorithme cryptographique pour le chiffrement et le déchiffrement.

$ chaînage de bloc de chiffrement (CBC, *cipher block chaining*)
(N) Mode de chiffrement de bloc qui améliore le mode ECB en enchaînant ensemble les blocs de texte chiffré qu'il produit. [FP081] (Voir : chiffrement de bloc, [RFC1829], [RFC2405], [RFC2451], [SP38A].)
Instructions : Ce mode fonctionne en combinant (OU exclusif) le bloc de résultat du texte chiffré de l'algorithme avec le prochain bloc de texte source pour former le bloc d'entrée suivant pour l'algorithme.

$ chiffrement à rétroaction (CFB, *cipher feedback*)
(N) Mode de chiffrement de bloc qui améliore le mode ECB en enchaînant ensemble les blocs de texte chiffré qu'il produit et en opérant sur des segments de texte source de longueur variable inférieure ou égale à la longueur de bloc. [FP081] (Voir : chiffrement de bloc, [SP38A].)
Instructions : ce mode fonctionne en utilisant le segment de texte chiffré généré précédemment comme entrée de l'algorithme (c'est-à-dire, en "ré ingurgitant" le texte chiffré) pour générer un bloc de sortie, et ensuite en combinant (OU exclusif) ce bloc de sortie avec le prochain segment de texte source (de la longueur du bloc ou moins) pour former le prochain segment de texte chiffré.

$ texte chiffré *(cipher text)*
1. (I) /nom/ Données qui ont été transformées par chiffrement de sorte que leur contenu d'informations sémantiques (c'est-à-dire, leur signification) n'est plus intelligible ni directement disponible. (Voir : texte chiffré. À comparer à : texte en clair, texte source.)

2. (O) "Données produites à l'aide du chiffrement. Le contenu sémantique des données résultantes n'est pas disponible." [I7498-2]

$ texte chiffré *(ciphertext)*
1. (O) /nom/ Synonyme de "texte chiffré" [I7498-2].
2. (I) /adjectif/ Se référant à du texte chiffré. Usage : Couramment utilisé à la place de "texte chiffré". (À comparer à : texte en clair, texte source.)

$ texte auto chiffré (CTAK, *ciphertext auto-key*)
(D) "Logique cryptographique qui utilise le texte chiffré précédent pour générer un flux de clés." [C4009], [A1523] (Voir : KAK.)
Terme déconseillé : les IDOC NE DEVRAIENT PAS utiliser ce terme ; il n'est ni bien connu ni précisément défini. À la place, utiliser les termes associés aux modes qui sont définis dans les normes, comme CBC, CFB, et OFB.

$ attaque du seul texte chiffré *(ciphertext-only attack)*
(I) Technique d'analyse cryptographique dans laquelle l'analyste essaye de déterminer la clé à partir de la seule connaissance du texte chiffré intercepté (bien que l'analyste puisse aussi avoir d'autres indices, comme l'algorithme cryptographique, le langage dans lequel le texte source a été écrit, le sujet du texte en clair, et certains mots probables du texte source.)

$ ciphonie *(ciphony).* (O) Le processus de chiffrement d'informations audio.

$ modèle de Clark-Wilson *(Clark-Wilson model)*
(N) Modèle de sécurité [Clark] pour protéger l'intégrité des données dans le monde du commerce. (À comparer à : Modèle de Bell-LaPadula.)

$ classe 2, 3, 4, 5 *(class 2, 3, 4, 5)*
(O) /U.S. DoD/ Niveaux d'assurance pour les PKI, et pour les certificats de clé publique X.509 produits par une PKI. [DoD7] (Voir : "première loi" sous les "Lois de Courtney".)
- "Classe 2" : Destinée aux applications traitant des données non classifiées, de faible valeur dans des environnements à protection minimale ou modérée.
- "Classe 3" : Destinée aux applications traitant des données non classifiées, de valeur moyenne dans des environnements modérément protégés, ou traitant des données non classifiées ou des données de grande valeur dans des environnements très protégés, et pour le contrôle d'accès discrétionnaire de données classifiées dans des environnements très protégés.
- "Classe 4" : Destinée aux applications traitant des données non classifiées, de grande valeur dans des environnements à protection minimale.
- "Classe 5" : Destinée aux applications traitant des données classifiées dans des environnements à protection minimale, et pour l'authentification de matériel qui affecterait la sécurité de systèmes classifiés.

Les environnements sont définis comme suit :
- "Environnement très protégé" : Des réseaux qui sont protégés soit par des appareils de chiffrement approuvés par la NSA pour la protection de donnés classifiées ou via un isolement physique, et qui sont certifiés pour traiter des données classifiées au niveau système, où l'exposition des données non chiffrées est limitée aux citoyens U.S. disposant des accréditations de sécurité appropriées.
- "Environnement modérément protégé" :
  -- Réseaux non chiffrés non classifiés physiquement isolés, dans lesquels l'accès est restreint sur la base de besoins légitimes.
  -- Réseaux protégés par un chiffrement de type 1 approuvé par la NSA, accessible à des nationaux étrangers autorisés par les autorités U.S.
- "Environnements à protection minimale" : Réseaux non chiffrés connectés à l'Internet ou NIPRNET, soit directement soit via un pare-feu.

$ système informatique de classe A1, B3, B2, B1, C2, ou C1 *(Class A1, B3, B2, B1, C2, or C1 computer system)*
(O) /TCSEC/ Voir : Instructions sous "Critères d'évaluation de système informatique de confiance".

$ classification
1. (I) Un groupement d'informations classifiées auquel est appliquée une étiquette de sécurité restrictive hiérarchique, pour augmenter la protection des données contre la divulgation non autorisée. (Voir : agrégation, classifié, service de confidentialité des données. À comparer à : catégorie, compartiment.)
2. (I) Processus autorisé par lequel des informations sont déterminées comme étant à classifier et affectées à un niveau de sécurité. (À comparer à : déclassification.)

Usage : compris généralement comme impliquant la confidentialité des données, mais les IDOC DEVRAIENT préciser

quand des données sont sensibles par d'autres moyens et DEVRAIENT utiliser d'autres termes pour ces autres concepts de sensibilité. (Voir : informations sensibles, intégrité des données.)

$ étiquette de classification *(classification label)*
(I) Étiquette de sécurité qui indique le degré de dommage qui résultera d'une divulgation non autorisée des données étiquetées, et peut aussi indiquer de quelles contre-mesures l'application est requise pour protéger les données contre une divulgation non autorisée. Exemple : IPSO. (Voir : classifié, service de confidentialité des données. À comparer à : étiquette d'intégrité.)
Usage : compris généralement comme impliquant la confidentialité des données, mais les IDOC DEVRAIENT préciser cela quand les données sont aussi sensibles d'autres façons et DEVRAIENT utiliser d'autres termes pour ces autres concepts de sensibilité. (Voir : informations sensibles, intégrité des données.)

$ niveau de classification *(classification level)*
(I) Niveau hiérarchique de protection (contre la divulgation non autorisée) dont l'application est requise pour certaines données classifiées. (Voir : classifié. À comparer à : niveau de sécurité.)
Usage : compris généralement comme impliquant la confidentialité des données, mais les IDOC DEVRAIENT préciser quand des données sont aussi sensibles d'autres façons et DEVRAIENT utiliser d'autres termes pour ces autres concepts de sensibilité. (Voir : informations sensibles, intégrité des données.)

$ classifié *(classified)*
1. (I) Se réfère à des informations (mémorisées ou convoyées, sous toute forme) qui sont formellement exigées par une politique de sécurité pour recevoir un service de confidentialité de données et à marquer avec une étiquettes de sécurité (qui, dans certains cas, peut être implicite) pour indiquer son état de protection. (Voir : classifier, informations collatérales, SAP, niveau de sécurité. À comparer à : non classifié.)

Usage : Compris généralement comme impliquant la confidentialité des données, mais les IDOC DEVRAIENT préciser cela quand les données sont aussi sensibles d'autres façons et DEVRAIENT utiliser d'autres termes pour ces autres concepts de sensibilité. (Voir : informations sensibles, intégrité des données.)
Principalement utilisé par les gouvernements, spécialement les militaires, mais le concept sous-jacent s'applique aussi en dehors des gouvernements.

2. (O) /Gouvernement des USA/ "Informations qui ont été déterminées conformément au Executive Order 12958 ou à tout décret précédent, ou par le Atomic Energy Act de 1954, et ses amendements, comme exigeant une protection contre la divulgation non autorisée et sont marquées comme indiquant leur statut classifié." [C4009]

$ classificateur *(classify)*
(I) Pour désigner officiellement un élément d'information ou un type d'informations comme étant classifié et affecté à un niveau de sécurité spécifique. (Voir : classifié, déclassifié, niveau de sécurité.)

$ système propre *(clean system)*
(I) Système informatique dans lequel le système d'exploitation et le logiciel et les fichiers de système d'application ont été récemment installés depuis un support de distribution de logiciels de confiance. (À comparer à : état sûr.)

$ éliminer *(clear)* (D) /verbe/ Synonyme de "écraser". [C4009]

$ texte en clair *(clear text)*
1. (I) /nom/ Données dans lesquelles le contenu sémantique des informations (c'est-à-dire, la signification) est intelligible ou est directement disponible, c'est-à-dire, non chiffré. (Voir : texte, en clair. À comparer à : texte chiffré.)
2. (O) /nom/ "Données intelligibles, dont le contenu sémantique est disponible." [I7498-2]
3. (D) /nom/ Synonyme de "texte source".

Définition déconseillée : les IDOC NE DEVRAIENT PAS utiliser ce terme comme synonyme de "texte source", parce que le "plain text" qui est l'entrée d'une opération de chiffrement peut être lui-même du texte chiffré qui a été produit par une opération de chiffrement antérieure. (Voir : super chiffrement.)

$ accréditation *(clearance).* Voir : niveau d'habilitation,

$ niveau d'accréditation *(clearance level)*
(I) Le niveau de sécurité des informations auquel un niveau d'habilitation autorise une personne à avoir accès.

$ client
(I) Entité système qui exige et utilise un service fourni par une autre entité système, appelée un "serveur". (Voir : serveur.)
Instructions : usuellement, on comprend que le client et le serveur sont les composants automatiques du système, et le client fait la demande au nom d'un utilisateur humain. Dans certains cas, le serveur peut lui-même être un client de quelque autre

serveur.

$ système client-serveur *(client-server system)*
(I) Système réparti dans lequel une ou plusieurs entités, appelées clients, demandent un service spécifique à une ou plusieurs autres entités, appelées serveurs, qui fournissent le service aux clients.
Exemple : La Toile mondiale *(World Wide Web)* dans laquelle les serveurs composants fournissent des informations qui sont demandées par les composants clients appelés "navigateurs".

$ CLIPPER
(N) Microcircuit intégré (dans la série MYK-7x fabriquée par Mykotronx, Inc.) qui met en œuvre SKIPJACK, qui a un générateur de nombres aléatoires non déterministe, et prend en charge le tiers de confiance. (Voir : Norme de chiffrement à tiers de confiance. À comparer à : CLIPPER.)
Instructions : la puce était principalement destinée à la protection des télécommunications sur le réseau public commuté. Le schéma de tiers de confiance pour la puce implique une clé SKIPJACK qui est commune à toutes les puces et qui protège le numéro de série unique de la puce, et une seconde clé SKIPJACK unique pour la puce qui protège toutes les données chiffrées par la puce. La seconde clé est confiée à un tiers comme composant de clé partagée détenue par le NIST et le Département du Trésor US.

$ environnement de sécurité clos *(closed security environment)*
(O) /U.S. DoD/ Environnement de système qui satisfait aux deux conditions suivantes : (a) les développeurs d'application (incluant ceux qui font la maintenance) ont des accréditations et autorisations suffisantes pour fournir une présomption acceptable qu'ils n'ont pas introduit de logique malveillante. (b) Le contrôle de configuration donne une assurance suffisante que les applications système et l'équipement sur lequel elles fonctionnent sont protégées contre l'introduction de logiciels malveillants avant et durant le fonctionnement des applications. [NCS04] (Voir : "première loi" sous "Lois de Courtney". À comparer à : environnement de sécurité ouvert.)

$ CMAC
(N) Code d'authentification de message [SP38B] qui se fonde sur un chiffrement de bloc symétrique. (Voir : chiffrement de bloc.)
Dérivation : MAC fondé sur le chiffrement. (À comparer à : HMAC.)
Instructions : Comme CMAC se fonde sur des chiffrements de bloc de clé symétrique approuvés, tels que AES, CMAC peut être considéré comme un mode de fonctionnement pour ces chiffrements de bloc. (Voir : mode de fonctionnement.)

$ code
1. (I) Système de symboles utilisé pour représenter des informations, qui peuvent à l'origine avoir d'autres représentations. Exemples : ASCII, BER, code de pays, code Morse. (Voir : codage, code d'objet, code source.)

Abréviation déconseillée : pour éviter la confusion avec la définition 1, les IDOC NE DEVRAIENT PAS utiliser "code" comme abréviation de "code de pays", "code de redondance cyclique", "code d'authentification de données", "code de détection d'erreur", ou "code d'authentification de message". Pour éviter l'incompréhension, utiliser le terme pleinement qualifié de ces autres cas, au moins à la première utilisation.

2. (I) /cryptographie/ Algorithme de chiffrement fondé sur la substitution, c'est-à-dire, un système pour assurer la confidentialité des données en utilisant des groupes arbitraires (appelés des "groupes de code") de lettres, nombres, ou symboles pour représenter des unités de texte en clair de longueur variable. (Voir : livre de code, cryptographie.)
   Utilisation déconseillée : pour éviter la confusion avec la définition 1, les IDOC NE DEVRAIENT PAS utiliser "code" comme synonyme d'aucun des termes suivants : (a) "chiffrement", "hachage", ou autres mots qui signifient "un algorithme cryptographique" ; (b) "texte chiffré"; ou (c) "chiffrement", "hachage", ou autres mots qui se réfèrent à l'application d'un algorithme de chiffrement.
3. (I) Un algorithme fondé sur la substitution, mais utilisé pour raccourcir les messages plutôt que pour dissimuler leur contenu.
4. (I) /programmation informatique/ Écrire un logiciel informatique. (Voir : code objet, code source.)

Abréviation déconseillée : pour éviter la confusion avec la définition 1, les IDOC NE DEVRAIENT PAS utiliser "code" comme abréviation de "code objet" ou "code source". Pour éviter l'incompréhension, utiliser le terme pleinement qualifié dans les autres cas, au moins à la première utilisation.

$ livre de code *(code book)*
1. (I) Document contenant une liste systématique des unités de texte en clair et de leurs équivalents en langage chiffré. [C4009]
2. (I) Algorithme de chiffrement qui utilise une technique de substitution. [C4009] (Voir : code, ECB.)

$ signature de code *(code signing)*
(I) Mécanisme de sécurité qui utilise une signature numérique pour protéger l'intégrité des données et l'authentification de

l'origine des données pour un logiciel d'utilisation répartie. (Voir : code mobile, distribution de confiance.)
Instructions : dans certains cas, la signature sur un module logiciel peut impliquer des assertions que le signataire fait sur le logiciel. Par exemple, une signature peut impliquer que le logiciel a été conçu, développé ou vérifié conformément à certains critères.

$ mot de code *(code word)*
(O) /Gouvernement des USA/ Un seul mot qui est utilisé comme étiquette de sécurité (usuellement appliqué pour des informations classifiées) mais qui a lui-même une signification classifiée. (Voir : classifié, /étiquette de sécurité du gouvernement des USA/ étiquette de sécurité.)

$ démarrage à froid *(cold start)*
(N) /Module cryptographique/ Procédure pour le chiffrement initial d'un équipement cryptographique. [C4009]

$ informations collatérales *(collateral information)*
(O) /Gouvernement des USA/ Informations qui sont classifiées mais dont il n'est pas exigé qu'elles soient protégées par un SAP. (Voir : /Gouvernement des USA/ classifié.)

$ changement de couleur *(color change)*
(I) Dans un système qui fonctionne en mode de traitement périodique, l'acte de purger toutes les informations provenant d'une période de traitement puis de les changer pour la prochaine période de traitement. (Voir : NOIR, ROUGE.)

$ programme d'évaluation COMSEC commercial (CCEP, *Commercial COMSEC Evaluation Program*)
(O) "Relations entre la NSA et l'industrie dans lequel la NSA fournit l'expertise COMSEC (c'est-à-dire, les standards, les algorithmes, les évaluations, et des conseils) et l'industrie fournit les capacités de conception, de développement, et de production pour arriver à un produit de type 1 ou de type 2." [C4009]

$ facilité d'évaluation commercialement brevetée (CLEF, *commercially licensed evaluation facility*)
(N) Une organisation qui est officiellement approuvée pour évaluer la sécurité des produits et des systèmes par rapport aux critères communs, ITSEC, ou quelque autre norme. (À comparer à : KLIF.)

$ Comité des systèmes de sécurité nationaux (CNSS, *Committee on National Security Systems*)
(O) /Gouvernement des USA/ Comité permanent inter agences gouvernementales, du Bureau de protection des infrastructure critiques de la Présidence. Le CNSS est présidé par le Secrétaire à la Défense et fournit un forum de discussion des questions de politique, il définit la politique nationale, et promulgue des directives, des procédures de fonctionnement, et des instructions pour la sécurité des systèmes de sécurité nationaux. Le Secrétaire à la Défense et le Directeur des renseignements centraux sont chargés du développement et de la supervision de la mise en œuvre des politiques du gouvernement, des principes, des standards, et des lignes directrices pour la sécurité des systèmes qui gèrent les informations touchant à la sécurité nationale .

$ critères communs pour la sécurité des technologies de l'information *(Critères communs for Information Technology Security)*
(N) Norme pour évaluer les produits et systèmes de technologie de l'information (IT). Il établit les exigences pour les fonctions de sécurité et les mesures d'assurance. [CCIB] (Voir : CLEF, EAL, paquetages, profil de protection, cible de sécurité, TOE. À comparer à : CMM.)
Instructions : Canada, France, Allemagne, Pays-Bas, Royaume Uni, et États Unis (NIST et NSA) ont commencé à développer cette norme en 1993, sur la base de l'ITSEC européen, des critères d'évaluation des produits informatiques du Canada (CTCPEC, *Canadian Trusted Computer Product Evaluation Criteria*), et pour les U.S.A, les "critères fédéraux pour la sécurité des technologies de l'information" et son précurseur, le TCSEC. Des travaux ont été menés en coopération avec le groupe de travail 3 (critères de sécurité) du sous comité 27 *(*techniques de sécurité) du comité conjoint n° 1 pour les technologies de l'information de l'ISO/CEI (JTC1). La version 2.0 des critères a été produite dans la norme internationale ISO 15408. Le Gouvernement des USA a l'intention de substituer cette norme à la fois à TCSEC et à FIPS PUB 140. (Voir : NIAP.)
La norme traite de la confidentialité des données, de l'intégrité des données, et de la disponibilité des données et peut s'appliquer aux autres aspects de la sécurité. Elle se concentre sur les menaces qui pèsent sur les informations et qui proviennent des activités humaines, malveillantes ou non, mais peut s'appliquer aux menaces non humaines. Elle s'applique aux mesures de sécurité mises en œuvre dans les matériels, les progiciels ou les logiciels. Elle ne s'applique pas (a) à la sécurité administrative sans relation directe avec la sécurité technique, (b) aux aspects techniques physiques de la sécurité tels que le contrôle des émanations magnétiques électroniques, (c) à la méthodologie d'évaluation ou au cadre administratif et réglementaire sous lequel elles peuvent être appliquées, (d) aux procédures d'utilisation des résultats d'évaluation, ou (e) à la certification des qualités inhérentes des algorithmes de chiffrement.
La partie 1, Introduction et modèle général, définit les concepts et principes généraux de l'évaluation de la sécurité des IT,

présente un modèle d'évaluation général, et définit les constructions pour exprimer les objectif de la sécurité des IT, pour choisir et définir les exigences de sécurité des IT, et pour écrire des spécifications de haut niveau pour les produits et systèmes.
La partie 2, Exigences fonctionnelles de la sécurité, contient un catalogue de déclarations d'exigences fonctionnelles bien définies et bien comprises qui sont destinées à être utilisées comme une façon standard d'exprimer les exigences de sécurité pour les produits et systèmes de technologies de l'information.
La partie 3, Exigences de l'assurance de sécurité, contient un catalogue des composants de l'assurance à utiliser comme moyen standard d'exprimer de telles exigences pour les produits et systèmes d'IT, et définit les critères d'évaluation des profils de protection et des cibles de sécurité.

$ option commune de sécurité IP (CIPSO, *Common IP Security Option*). (I) Voir : définition secondaire sous "IPSO".

$ nom courant *(common name)*
(N) Une chaîne de caractères qui (a) peut faire partie du nom distinctif X.500 d'un objet de répertoire (attribut "commonName"), (b) est un nom (éventuellement ambigu) par lequel l'objet est couramment connu dans une certaine portée limitée (comme une organisation) et (c) se conforme aux conventions de désignation du pays ou de la culture auquel il est associé. [X520] (Voir : "sujet" et "producteur" sous "certificat de clé publique X.509".)
Exemples : "Dr. Albert Einstein", "Les Nations Unies", et "l'imprimante du 12ème étage".

$ communications couvertes *(communications cover)*
(N) "Dissimulation ou altération des schémas de caractéristiques des communications pour cacher les informations qui pourraient être précieuses pour un adversaire." [C4009] (Voir : sécurité de fonctionnement, confidentialité de flux de trafic, TRANSEC.)

$ sécurité de communication (COMSEC, *communication security*)
(I) Mesures qui mettent en œuvre et assurent des services de sécurité dans un système de communications, en particulier ceux qui fournissent la confidentialité et l'intégrité des données et qui authentifient les entités communicantes.
Usage : COMSEC est généralement compris comme incluant (a) le chiffrement et ses algorithmes et les méthodes et processus de gestion de clés, les appareils qui mettent en œuvre ces algorithmes et processus, et la gestion des cycles de vie des matériels et du matériel de chiffrement. COMSEC est aussi parfois compris plus largement comme incluant aussi (b) la confidentialité des flux de trafic, (c) TRANSEC, et (d) la stéganographie [Kahn]. (Voir : cryptologie, sécurité du signal.)

$ communauté d'intérêts (COI, *community of interest*)
1. (I) Ensemble d'entités qui opèrent sous une politique de sécurité commune. (À comparer à : domaine.)
2. (I) Ensemble d'entités qui échangent des informations de façon collaborative à certaines fins.

$ risque communautaire *(community risk)*
(N) Probabilité qu'une faiblesse particulière soit exploitée au sein d'une population interagissante et affecte de façon négative certains membres de cette population. [C4009] (Voir : ver de Morris, risque.)

$ chaîne de communauté *(community string)*
(I) Nom d'une communauté sous la forme d'une chaîne d'octets qui sert de mot de passe en clair dans SNMP version 1 (RFC1157) et version 2 (RFC1901). (Voir : mot de passe, protocole simple de gestion de réseau.)
Instructions : les protocoles SNMPv1 et SNMPv2 ont été déclarés "historiques" et ont été remplacés par la norme plus sûre SNMPv3 (RFC 3410 à 3418), qui n'utilisent pas de mots de passe en clair.

$ compartiment *(compartment)*
1. (I) Groupement d'éléments d'informations qui exigent des contrôles d'accès spéciaux au-delà de ceux normalement fournis pour le niveau de classification de base de l'information. (Voir : mode de sécurité par compartiment. À comparer à : catégorie, classification.)

Usage : le terme est habituellement compris comme incluant des procédures de traitement spéciales à utiliser pour les informations.
2. (I) Synonyme de "catégorie".
Utilisation déconseillée : le présent glossaire définit "catégorie" avec une signification légèrement plus restrictive que "compartiment". C'est-à-dire qu'une étiquette de sécurité est allouée à une catégorie parce que le propriétaire des données a besoin de traiter les données comme un compartiment. Cependant, un compartiment pourrait recevoir une protection particulière dans un système sans qu'il lui soit alloué une étiquette de catégorie.

$ mode de sécurité compartimentée *(compartmented security mode)*
(N) Mode de fonctionnement d'un système dans lequel tous les utilisateurs qui ont accès au système ont les accréditifs de sécurité nécessaires pour le seul niveau de classification hiérarchisé de toutes les données traitées par le système, mais certains utilisateurs n'ont pas les accréditifs pour une catégorie non hiérarchique de certaines données traitées par le système. (Voir : catégorie, /fonctionnement de système/ sous "mode", niveau de protection, accréditif de sécurité.)
Usage : usuellement abrégé en "mode compartimenté". Ce terme a été défini dans la politique du gouvernement des USA sur l'accréditation de systèmes. Dans ce mode, un système peut traiter (a) un seul niveau de classification hiérarchique, et (b) plusieurs catégories non hiérarchiques au sein de ce niveau.

$ champ Compartiments *(Compartments field)*
(I) Champ de 16 bits (le "champ C") qui spécifie les valeurs de compartiment dans l'option sécurité (type d'option 130) de la version 4 du format d'en-tête de datagramme IP. Les valeurs de champ valides sont allouées par le gouvernement des USA, comme spécifié dans la RFC0791.
Abréviation déconseillée : les IDOC NE DEVRAIENT PAS utiliser l'abréviation "champ C" ; l'abréviation est potentiellement ambiguë. À la place, utiliser "champ Compartiments".

$ composant *(component)*. Voir : composant système.

$ compression
(I) Processus qui code les informations d'une façon qui minimise le nombre de symboles de code résultant et réduit donc l'espace de mémorisation ou le temps de transmission.
Instructions : un algorithme de compression de données peut être "sans perte", c'est-à-dire, conserver toutes les informations qui ont été codées dans les données, de sorte que la décompression peut récupérer toutes les informations ; ou un algorithme peut être "à pertes". Le texte doit habituellement être compressé sans perte, mais les images sont souvent compressées avec des schémas à pertes.
Tous les schémas qui codent les informations sans perte pour le traitement machine ne sont pas efficaces en termes de minimisation du nombre de bits de sortie. Par exemple, le codage ASCII est sans perte, mais les données ASCII peuvent souvent être recodées sans perte en moins de bits avec d'autres schémas. Ces schémas plus efficaces tirent parti de certaines sortes de déséquilibrage inhérent, redondances, ou répétitions dans les données, comme de remplacer une chaîne de caractères dans laquelle tous les caractères sont les mêmes par une chaîne plus courte consistant en un seul caractère et un compte de caractères.
Les schémas de compression sans perte ne peuvent pas réduire effectivement le nombre de bits dans le texte chiffré produit par un algorithme de chiffrement fort, parce que le texte chiffré est essentiellement une chaîne binaire pseudo aléatoire qui ne contient pas de schéma susceptible de recodage. Donc, les protocoles qui offrent des services à la fois de chiffrement et de compression (par exemple, SSL) ont besoin d'effectuer l'opération de compression avant l'opération de chiffrement.

$ compromission *(compromise)*. Voir : données compromises, compromission de la sécurité.

$ récupération de compromission *(compromise recovery)*
(I) Processus pour retrouver un état sûr pour un système après détection que le système a subi une compromission de sa sécurité.

$ liste de clé compromises (CKL, *compromised key list*)
(N) /MISSI/ Liste qui identifie les clés pour lesquelles une divulgation ou une altération non autorisée peut s'être produite. (Voir : compromission.)
Instructions : une CKL est produite par une CA, comme est produite une CRL. Mais une CKL fait seulement la liste des KMID, et non des sujets qui détiennent les clés, ni des certificats dans lesquels les clés sont liées.

$ COMPUSEC. (I) Voir : sécurité informatique.

$ équipe de réponse aux urgences informatiques (CERT, *computer emergency response team*)
(I) Organisation qui étudie la sécurité informatique des ordinateurs et des réseaux afin de fournir un service de réponse aux incidents aux victimes d'attaques, qui publie des alertes concernant les vulnérabilités et les menaces, et offre d'autres informations pour aider à améliorer la sécurité des ordinateurs et des réseaux. (Voir : CSIRT, incident de sécurité.)
Exemples : Centre de coordination CERT de Carnegie Mellon University (parfois appelé "Le" CERT) ; CIAC.

$ Capacité de conseil sur les incidents informatiques (CIAC, *Computer Incident Advisory Capability*)
(O) CSIRT centralisé du Ministère de l'Énergie des U.S.A ; membre de FIRST.

$ réseau informatique *(computer network)*
(I) Collection d'ordinateurs hôtes ainsi que le sous réseau ou l'inter réseau à travers lequel ils peuvent échanger des

données.
Usage : cette définition est destinée à couvrir les systèmes de toutes tailles et types, allant du complexe Internet au simple système composé d'un ordinateur personnel qui se connecte comme terminal distant d'un autre ordinateur.

$ plateforme informatique *(computer platform)*
(I) Combinaison d'un matériel informatique et d'un système d'exploitation (qui peut consister en logiciel, progiciel, ou les deux) pour ce matériel. (À comparer à : système informatique.)

$ sécurité informatique (COMPUSEC, *computer security*)
1. (I) Mesures pour mettre en œuvre et assurer des services de sécurité dans un système informatique, en particulier, ceux qui assurent le service de contrôle d'accès.
Usage : se réfère usuellement aux contrôles internes (fonctions, dispositifs, et caractéristiques techniques) qui sont mis en œuvre dans le logiciel (en particulier dans les systèmes d'exploitation) ; parfois, se réfère aux contrôles internes mis en œuvre dans le matériel ; se réfère rarement aux contrôles externes.
2. (O) "Protection accordée à un système d'informations automatisé afin d'atteindre les objectifs applicables de préservation de l'intégrité, de disponibilité et de confidentialité des ressources du système d'informations (inclut le matériel, le logiciel, le progiciel, les informations/données, et les télécommunications)." [SP12]

$ équipe de réponse aux incidents de sécurité informatique (CSIRT, *computer security incident response team*)
(I) Organisation "qui coordonne et prend en charge la réponse aux incidents de sécurité qui impliquent des sites au sein d'une circonscription définie." [RFC2350] (Voir : CERT, FIRST, incident de sécurité.)
Instructions : pour être considérée comme une CSIRT, une organisation doit faire comme suit : (a) fournir un canal (sécurisé) pour recevoir les rapports sur les incidents de sécurité suspectés, (b) fournir assistance aux membres de sa circonscription en traitant les incidents, (c) disséminer les informations relatives aux incidents dans sa circonscription et aux autres parties impliquées.

$ objet de sécurité informatique *(computer security object)*
(I) Définition ou représentation d'une ressource, outil, ou mécanisme utilisé pour maintenir une condition de sécurité dans des environnements informatisés. Inclut de nombreux éléments auxquels on se réfère dans les normes, qui sont soit choisis, soit définis par différentes communautés d'utilisateurs. [CSOR] (Voir : identifiant d'objet, registre des objets de sécurité informatique.)

$ registre des objets de sécurité informatique (CSOR, *Computer Security Objects Register*)
(N) Service géré par le NIST qui établit un catalogue des objets de sécurité informatique pour fournir des définitions d'objet stables identifiées par des noms univoques. L'utilisation de ce registre va permettre une spécification sans ambiguïté des paramètres et algorithmes de sécurité dans les échanges de données sécurisés. (Voir : identifiant d'objet.)
Instructions : le CSOR suit les lignes directrices de l'enregistrement établies par la communauté internationale de la normalisation et l'ANSI. Ces lignes directrices établissent des responsabilités minimales pour les autorités d'enregistrement et investissent les branches supérieures d'une hiérarchie d'enregistrement internationale. Sous cette hiérarchie d'enregistrement internationale, le CSOR est chargé de l'allocation d'identifiants univoques sous la branche : {joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) csor(3)}.

$ système informatique *(computer system)*
(I) Synonyme de "système d'informations", ou un de ses composants. (À comparer à : plate-forme informatique.)

$ Risques informatiques *(Computers At Risk)*
(O) Rapport 1991 [NRC91] du comité d'étude de la sécurité des systèmes, parrainé par l'Académie Nationale des Sciences des U.S.A et soutenu par l'Agence des projets de recherches avancées de Défense du Ministère de la Défense des U.S.A. Il a fait de nombreuses recommandations pour que l'industrie et les gouvernements améliorent la sécurité et la fiabilité informatique. Certaines des plus importantes recommandations (par exemple, établir une Fondation de la sécurité informatique mandatée par le gouvernement des USA) n'ont pas été mises en œuvre du tout, et d'autres (par exemple, codifier des principes généralement acceptés de la sécurité des systèmes similaires aux principes de comptabilité) ont été mis en œuvre mais pas largement adoptés [SP14], [SP27].

$ compte COMSEC *(COMSEC account)*
(O) /Gouvernement des USA/ "Entité administrative, identifiée par un numéro de compte, utilisée pour tenir la comptabilité, assurer la garde et le contrôle du matériel de COMSEC." [C4009] (Voir : gardien COMSEC.)

$ comptabilité COMSEC *(COMSEC accounting)*
(O) /Gouvernement des USA/ Processus de création, collecte et maintenance des enregistrements de données qui décrivent l'état et la garde d'éléments désignés du matériel COMSEC. (Voir : code de légende de comptabilité.)

Instructions : presque tout système d'informations sécurisé a besoin d'enregistrer un chemin d'audit de sécurité, mais un système qui gère le matériel COMSEC a besoin d'enregistrer des données supplémentaires sur l'état et la garde des éléments COMSEC.

- Suivi COMSEC : processus de collecte automatique, d'enregistrement, et de gestion des informations qui décrivent l'état des éléments désignés du matériel COMSEC à tout instant de la durée de vie de chaque produit.
- Contrôle COMSEC : processus d'augmentation des données de suivi par des données de garde, qui consistent en accusés de réception explicites des entités du système qu'elles ont (a) reçu des éléments spécifiques COMSEC et (b) sont responsables de la prévention de l'exposition de ces éléments.

Par exemple, un système de gestion de clés qui dessert un grand nombre de consommateurs a besoin d'enregistrer les données de suivi pour les mêmes raisons qu'un système national de livraison de paquets, c'est-à-dire, répondre à la question "Où est actuellement cette chose ?". Si les clés sont chiffrées immédiatement lorsque elles sont générées et traitées seulement en forme BLACK entre le point de création et le point d'utilisation, le suivi peut être tout ce qui est nécessaire. Cependant, dans les cas où les clés sont traitées au moins partiellement en forme RED et sont potentiellement sujettes à exposition, le suivi doit être complété par le contrôle.

Les données qui sont utilisées pour le seul suivi ne doivent être conservées que temporairement, jusqu'à ce que l'état d'un élément change. Les données qui sont utilisées pour le contrôle sont conservées indéfiniment pour assurer la comptabilité et prendre en charge la récupération d'une situation de compromission.

$ limite COMSEC *(COMSEC boundary)*

(N) "Périmètre définissable qui englobe tout le matériel, le progiciel, et les composants logiciels qui effectuent des fonctions COMSEC critiques, comme la génération de clé et le traitement et la mémorisation des clés." [C4009] (À comparer à : frontière cryptographique.)

$ gardien COMSEC *(COMSEC custodian)*

(O) /Gouvernement des USA/ "Individu désigné par l'autorité appropriée comme responsable de la réception, du transfert, de la comptabilité, de la sauvegarde, et de la destruction du matériel COMSEC alloué à un compte COMSEC." [C4009]

$ matériel COMSEC *(COMSEC material)*

(N) /Gouvernement des USA/ Éléments désignés pour sécuriser ou authentifier des communications ou informations en général ; ces éléments incluent (mais ne s'y limitent pas) les clés, équipements, appareils, documents, progiciels, et logiciels qui incorporent ou décrivent la logique cryptographique ; et d'autres éléments qui effectuent des fonctions COMSEC. [C4009] (À comparer à : matériel de chiffrement.)

$ système de contrôle de matériel COMSEC (CMCS, *COMSEC Material Control System*)

(O) /Gouvernement des USA/ "Système logistique et de comptabilité à travers lequel le matériel COMSEC marqué 'CRYPTO' est distribué, contrôlé, et sauvegardé." [C4009] (Voir : compte COMSEC, gardien COMSEC.)

$ confidentialité *(confidentiality)*. Voir : confidentialité des données.

$ système de dissimulation *(concealment system)*

(O) "Méthode pour assurer la confidentialité pour cacher des informations sensibles en les incorporant dans des données non pertinentes." [NCS04] (À comparer à : stéganographie.)

$ contrôle de configuration *(configuration control)*

(I) Processus de régulation des changements de matériel, progiciels, logiciels et de la documentation tout au long du développement et de la vie opérationnelle d'un système. (Voir : sécurité administrative, durcir, distribution de confiance.)

Instructions : le contrôle de configuration aide à protéger contre les altérations non autorisées ou malveillantes d'un système et fournit donc l'assurance de l'intégrité du système. (Voir : logique malveillante.)

$ propriété de confinement *(confinement property)*

(N) /modèle formel/ Propriété d'un système par laquelle un sujet n'a un accès en écriture à un objet que si la classification de l'objet est d'une valeur supérieure à celle des accréditifs du sujet. (Voir : propriété-*, modèle de Bell-LaPadula.)

$ contrainte *(constraint)*

(I) /contrôle d'accès/ Une limitation à la fonction d'une identité, rôle, ou privilège. (Voir : contrôle d'accès fondé sur la règle.)

Instructions : en fait, une contrainte est une forme de politique de sécurité et peut être statique ou dynamique :

- "Contrainte statique" : contrainte qui doit être satisfaite au moment où la politique est définie, et continue ensuite d'être satisfaite jusqu'à la suppression de la contrainte.
- "Contrainte dynamique" : contrainte qui peut être définie pour s'appliquer à des instants divers où l'identité, rôle, ou autre objet de la contrainte est active dans le système.

$ filtre de contenu *(content filter)*
(I) /Toile mondiale/ Logiciel d'application utilisée pour empêcher l'accès à certains serveurs de la Toile, comme ceux par lesquels les parents empêchent l'accès de leurs enfants à des sites pornographiques. (Voir : filtre, garde.)
Instructions : le filtre est généralement fondé sur le navigateur, mais il pourrait faire partie d'un serveur d'antémémoire intermédiaire. Les deux techniques de base de filtre de contenu sont (a) de bloquer une liste spécifiée d'URL et (b) de bloquer le matériel qui contient des mots ou phrases spécifiés.

$ plan de contingence *(plan de contingence)*
(I) Plan de réponse d'urgence, opérations de sauvegarde, et récupération après désastre dans un système au titre d'un programme de sécurité pour assurer la disponibilité de ressources systèmes critiques et faciliter la continuité du fonctionnement dans une crise. [NCS04] (Voir : disponibilité.)

$ zone de contrôle *(control zone)*
(O) "Espace, exprimé en terme de rayon, entourant un équipement qui traite des informations sensibles, qui est sous un contrôle physique et technique suffisant pour empêcher une entrée non autorisée ou la compromission." [NCSSG] (À comparer à : espace inspectable, zone de tempête.)

$ protection d'accès contrôlé *(controlled access protection)*
(O) /TCSEC/ Critère de niveau d'évaluation pour un système informatique C2.
Instructions : les caractéristiques majeures du niveau C2 sont la comptabilité individuelle, l'audit, le contrôle d'accès, et la réutilisation d'objet.

$ élément cryptographique contrôlé (CCI, *controlled cryptographic item*)
(O) /Gouvernement des USA/ "Équipement sécurisé de télécommunications ou de traitement de l'information, ou composant cryptographique associé, qui n'est pas classifié mais gouverné par un ensemble spécial d'exigences de contrôle." [C4009] (À comparer à : EUCI.)
Instructions : cette catégorie d'équipements a été établie en 1985 pour promouvoir une large utilisation d'équipements sécurisés pour protéger les informations classifiées et non classifiées dans l'intérêt national. L'équipement CCI utilise une logique cryptographique classifiée, mais le matériel ou logiciel incorporant cette logique n'est pas classifié. Des dessins, des mises en œuvre de logiciels, et d'autres descriptions de cette logique restent classifiés. [N4001]

$ interface contrôlée *(controlled interface)*
(I) Mécanisme qui facilite l'adjudication des différentes politiques de sécurité de systèmes interconnectés. (Voir : domaine, garde.)

$ mode de sécurité contrôlée *(controlled security mode)*
(D) /U.S. DoD/ Mode de fonctionnement de système dans lequel (a) il est permis à deux niveaux de sécurité des informations ou plus d'être traités concurremment au sein du même système lorsque certains utilisateurs qui ont accès au système n'ont ni accréditif de sécurité ni besoin de connaître certaines des données traitées par le système, mais (b) la séparation des utilisateurs et du matériel classifié sur la base, respectivement, des accréditifs et du niveau de classification ne dépend que du contrôle du système d'exploitation (comme c'est le cas dans le mode de sécurité multi niveau). (Voir : /fonctionnement de système/ sous "mode", niveau de protection.)
Terme déconseillé : les IDOC NE DEVRAIENT PAS utiliser ce terme. Il a été défini dans une politique du gouvernement des USA concernant l'accréditation de système et a été remplacé par "mode de sécurité partagé" dans une politique ultérieure. Ces deux termes ont été abandonnés dans des politiques encore ultérieures.
Instructions : le mode contrôlé été destiné à encourager l'ingéniosité à satisfaire aux exigences de confidentialité des données dans des façons moins restrictives que le "mode de sécurité dédiée" et le "mode de sécurité de hauteur système", mais à un niveau de risque plus faible que celui généralement associé au vrai "mode de sécurité multi niveau". Cela était destiné à être réalisé par la mise en œuvre de mesures d'augmentation explicites pour réduire ou supprimer une quantité substantielle de faiblesses du logiciel système ainsi que la limite spécifique des niveaux d'habilitation de sécurité des utilisateurs qui ont des accès concurrents au système.

$ autorité de contrôle *(controlling authority)*
(O) /Gouvernement des USA/ "Officiel responsable de la direction du fonctionnement d'un réseau chiffré et de la gestion de l'utilisation opérationnelle et du contrôle du matériel de clés alloué au réseau chiffré." [C4009], [N4006]

$ mouchard *(cookie)*
1. (I) /HTTP/ Données échangées entre un serveur HTTP et un navigateur (un client du serveur) pour mémoriser des informations d'état sur le côté client et les restituer ultérieurement pour l'usage du serveur.

Instructions : un serveur HTTP, lorsque il envoie des données à un client, peut envoyer avec elles un mouchard, que le

client conserve après la clôture de la connexion HTTP. Un serveur peut utiliser ce mécanisme pour conserver des informations d'état persistantes du côté client pour des application fondées sur HTTP, restituant les informations d'état dans des connexions ultérieures. Un mouchard peut inclure une description de la gamme des URL pour lesquels l'état est valide. Les demandes futures faites par le client dans cette gamme vont aussi envoyer la valeur actuelle du mouchard au serveur. Les mouchards peuvent être utilisés pour générer des profils des habitudes d'utilisation de la Toile, et peuvent donc empiéter sur le droit à la protection de la vie privée.

2. (I) /IPsec/ Objets de données échangés par ISAKMP pour prévenir certaines attaques de déni de service durant l'établissement d'une association de sécurité.

3. (D) /Contrôle d'accès / Synonyme pour "jeton de capacité" ou "ticket".

Définition déconseillée : les IDOC NE DEVRAIENT PAS utiliser ce terme avec la définition 3 ; cela dupliquerait la signification de termes mieux établis et mélangerait des concepts d'une façon potentiellement trompeuse.

$ temps universel coordonné (UTC, *Universal Time Coordinated*)

(N) UTC est dérivé du temps atomique international (TAI, *International Atomic Time*) en ajoutant un certain nombre de sauts de secondes. Le Bureau International des Poids et Mesures calcule le TAI une fois par mois en faisant la moyenne des données de nombreux laboratoires. (Voir : Temps généralisé, temps UTC.)

$ correction

(I) /sécurité/ Changement de système fait pour éliminer ou réduire le risque de réapparition d'une violation de la sécurité ou des conséquences d'une menace. (Voir : définition secondaire sous "sécurité".)

$ rectitude *(correctness)*

(I) "Propriété d'un système qui est garantie comme résultat d'une activité de vérification formelle." [Huff] (Voir : preuve de rectitude, vérification.)

$ intégrité correcte *(correctness integrity)*

(I) Propriété que les informations représentées par les données sont précises et cohérentes. (À comparer à : intégrité des données, intégrité de source.)

Instructions : les IDOC NE DEVRAIENT PAS utiliser ce terme sans fournir une définition ; le terme n'est ni bien connu ni défini avec précision. Intégrité des données se réfère à la constance des valeurs des données, et l'intégrité de source se réfère à la confiance dans les valeurs des données. Cependant, intégrité correcte se réfère à la confiance dans les informations sous jacentes que représentent les valeurs des données, et cette propriété est en rapport étroit avec les questions de comptabilité et de traitement d'erreur.

$ preuve de rectitude *(correctness proof)*

(I) Preuve mathématique de cohérence entre une spécification pour la sécurité d'un système et la mise en œuvre de cette spécification. (Voir : rectitude, spécification formelle.)

$ corruption

(I) Un type d'action de menace qui altère de façon indésirable le fonctionnement d'un système en modifiant de façon malveillante des fonctions ou données du système. (Voir : interruption.)

Usage : ce type d'action de menace inclut les sous-types suivants :

- "Altération" : /corruption/ altération délibérée de la logique d'un système, de données, ou d'informations de commande pour interrompre ou empêcher le fonctionnement correct des fonctions d'un système. (Voir : mauvaise utilisation, principale entrée pour "altération".)
- "Logique malveillante" : /corruption/ tout matériel, progiciel, ou logiciel (par exemple, un virus informatique) intentionnellement introduit dans un système pour modifier les fonctions ou données du système. (Voir : incapacitation, principale entrée pour "logique malveillante", usurpation d'identité, mauvaise utilisation.)
- "Erreur humaine" : /corruption/ action ou inaction humaine qui résulte involontairement en l'altération des données ou fonctions du système.
- "Erreur de matériel ou de logiciel" : /corruption/ erreur qui résulte en l'altération des fonctions ou données du système.
- "Désastre naturel" : /corruption/ Tout "acte de force majeure" (par exemple, coupure d'électricité due à la foudre) qui altère les fonctions ou données du système. [FP031 Section 2]

$ compteur *(counter)* (N) /nom/ Voir : mode compteur.

$ contre contre-mesure *(counter- countermeasure)*

(I) Action, appareil, procédure, ou technique utilisé par un attaquant pour contrer une contre mesure défensive.

Instructions : pour toute contre-mesure imaginée pour protéger les ordinateurs et les réseaux, un casseur sera probablement capable d'imaginer une contre contre-mesure. Donc, les systèmes doivent utiliser la "défense en profondeur".

$ mode compteur (CTR, *counter mode*)
(N) Mode de chiffrement de bloc qui améliore le mode ECB en assurant que chaque bloc chiffré est différent de chacun des autres blocs chiffrés sous la même clé. [SP38A] (Voir : chiffrement de bloc.)
Instructions : ce mode fonctionne en chiffrant d'abord une séquence de blocs générés, appelée "compteurs", qui sont séparés de la séquence d'entrée des blocs de texte source que le mode est destiné à protéger. La séquence résultante de compteurs chiffrés est traitée avec l'opérateur OU exclusif avec la séquence de blocs de texte source pour produire les blocs de résultat final de texte chiffré. La séquence de compteurs doit avoir la propriété que chaque compteur est différent de tous les autres compteurs pour tout le texte source qui est chiffré sous la même clé.

$ Compteur avec code d'authentification d'enchaînement de message de bloc de chiffrement (CCM, *Counter with Cipher Block Chaining-Message Authentication Code*)
(N) Mode de chiffrement de bloc [SP38C] qui assure à la fois la confidentialité et l'authentification de l'origine des données, en combinant les techniques de CTR et du code d'authentification de message fondé sur CBC. (Voir : chiffrement de bloc.)

$ contre-mesure *(countermeasure)*
(I) Action, appareil, procédure, ou technique qui satisfait ou s'oppose (c'est-à-dire, qui contre) une menace, une faiblesse, ou une attaque en l'éliminant ou l'empêchant, en minimisant le dommage qu'elle peut causer, ou en la découvrant et en en faisant rapport de façon qu'une action corrective puisse être prise.
Instructions : dans un protocole Internet, une contre-mesure peut prendre la forme d'un dispositif du protocole, d'une fonction composante, ou d'une contrainte d'usage.

$ code de pays *(country code)*
(I) Identifiant qui est défini pour une nation par la norme ISO [I3166].
Instructions : pour chaque nation, la norme ISO 3166 définit un code alphabétique univoque de deux caractères, un code univoque de trois caractères, et un code à trois chiffres. Parmi les nombreuses utilisations de ces codes, les codes à deux caractères sont utilisés comme noms de domaines de niveau supérieur.

$ Lois de Courtney *(Courtney's laws)*
(N) Principes de gestion de la sécurité des systèmes qui ont été établis par Robert H. Courtney, Jr.
Instructions : Bill Murray a codifié les Lois de Courtney comme suit : [Murr]
- Première Loi de Courtney : On ne peut rien dire d'intéressant (c'est-à-dire, de significatif) sur la sécurité d'un système sauf dans le contexte d'une application et d'un environnement particuliers.
- Seconde Loi de Courtney : Ne jamais dépenser plus d'argent à éliminer une exposition de la sécurité que ce qu'on tolère qu'elle nous coûte. (Voir : risque acceptable, analyse de risque.)
  - Premier corollaire : La sécurité parfaite a un coût infini.
  - Second corollaire : Le risque zéro n'existe pas.
- Troisième Loi de Courtney : Il n'y a pas de solution technique aux problèmes de gestion, mais il y a des solutions de gestion aux problèmes techniques.

$ action à couvert *(covert action)*
(I) Opération qui est programmée et exécutée d'une façon qui dissimule l'identité de l'opérateur.

$ canal couvert *(covert channel)*
1. (I) Canal intra-système imprévu ou non autorisé qui permet à deux entités coopérantes de transférer des informations d'une façon qui viole la politique de sécurité du système mais n'excède pas les autorisations d'accès des entités. (Voir : canal de mémorisation couvert, canal à temporisation couverte, hors bande, tunnel.)
2. (O) "Canal de communications qui permet à deux processus coopérants de transférer des informations d'une manière qui viole la politique de sécurité du système." [NCS04]

Instructions : les entités coopérantes peuvent être deux acteurs internes ou un interne et un externe. Bien sûr, un externe n'a pas d'autorisation d'accès du tout. Un canal couvert est une caractéristique d'un système que les architectes du système n'ont ni conçue ni destinée aux transferts d'informations.

$ canal de mémorisation couvert *(covert storage channel)*
(I) Dispositif d'un système qui permet à une entité système de signaler des informations à une autre entité en écrivant directement ou indirectement une localisation de mémorisation qui est ensuite directement ou indirectement lue par la seconde entité. (Voir : canal couvert.)

$ canal à temporisation couverte *(covert timing channel)*
(I) Dispositif d'un système qui permet à une entité système de signaler des informations à une autre en modulant son propre usage d'une ressource système d'une façon telle que cela affecte le temps de réponse du système observé par la seconde

entité. (Voir : canal couvert.)

$ craqueur *(cracker)*
(I) Quelqu'un qui essaye de casser la sécurité du système de quelqu'un d'autre, et d'en obtenir un accès non autorisé, souvent avec des intentions malveillantes. (Voir : adversaire, intrus, paquet de singe, script kiddy. À comparer à : hacker.)
Usage : a parfois été épelé "krackeur". [NCSSG]

$ accréditif *(credential)*
1. (I) /authentification/ "accréditif identifiant" : Objet de données qui est une représentation portable de l'association entre un identifiant et une unité d'informations d'authentification, et qui peut être présenté pour être utilisé à vérifier une identité revendiquée par une entité qui tente d'accéder à un système. Exemple : certificat de clé publique X.509. (Voir : accréditif anonyme.)
2. (I) /contrôle d'accès / "accréditif d'autorisation" : Objet de données qui est une représentation portable de l'association entre un identifiant et une ou plusieurs autorisations d'accès, et qui peut être présenté pour être utilisé à vérifier ces autorisations pour une entité qui tente un tel accès. Exemple : certificat d'attribut X.509. (Voir : jeton de capacité, ticket.)
3. (D) /OSIRM/ "Données qui sont transférée pour établir l'identité revendiquée par une entité." [I7498-2]
   Définition déconseillée : les IDOC NE DEVRAIENT PAS utiliser ce terme avec la définition 3. Comme expliqué dans les instructions ci-dessous, un processus d'authentification peut impliquer le transfert de plusieurs objets de données, et tous ne sont pas des accréditifs.
4. (D) /Gouvernement des USA/ "Objet qui est vérifié lorsque présenté au vérificateur dans une transaction d'authentification." [M0404]
   Définition déconseillée : les IDOC NE DEVRAIENT PAS utiliser ce terme avec la définition 4 ; elle mélange des concepts d'une façon potentiellement trompeuse. Par exemple, dans un processus d'authentification, c'est l'identité qui est "vérifiée", et non l'accréditif ; l'accréditif est "validé". (Voir : valider vs. vérifier.)

Instructions : En français courant , des "accréditifs" sont des preuves ou des témoignages qui (a) prennent en charge une revendication d'identité ou d'autorisation et (b) sont généralement destinés à être utilisés plus d'une fois (c'est-à-dire que la durée d'un accréditif est longue comparée au temps nécessaire pour une utilisation). Des exemples sont une plaque de police, le permis de conduire, et un passeport national. Un processus d'authentification ou d'accès qui utilise une plaque, un permis ou un passeport est extrêmement simple : le détenteur montre juste la chose.
Le problème de l'adoption de ce terme dans la sécurité de l'Internet est qu'un processus automatisé pour l'authentification ou le contrôle d'accès exige de nombreuses étapes qui utilisent plusieurs objets de données, et il peut n'être pas immédiatement évident de savoir lequel de ces objets devrait recevoir le nom de "accréditif".
Par exemple, si l'étape de vérification dans un processus d'authentification d'usager emploie la technologie de la clé publique, le processus implique alors au moins trois éléments de données : (a) la clé privée de l'usager, (b) une valeur signée – signée avec cette clé privée et passée au système, peut-être en réponse à un défi du système -- et (c) le certificat de clé publique de l'usager, qui est validé par le système et fournit la clé publique nécessaire pour vérifier la signature.
- Clé privée : la clé privée *n'est pas* un accréditif, parce que elle n'est jamais transférée ni présentée. À la place, la clé privée est une "information d'authentification", qui est associée à l'identifiant de l'usager pour une période spécifiée et peut être utilisée à plusieurs authentifications durant cette période.
- Valeur signée : la valeur signée *n'est pas* un accréditif ; la valeur signée est seulement éphémère, et non à longue durée. La définition de OSIRM pourrait être interprétée comme appelant la valeur signée un accréditif mais cela serait en conflit avec le français courant.
- Certificat : le certificat de l'usager *est* un accréditif. Il peut être "transféré" ou "présenté" à toute personne ou processus qui en a besoin à tout moment. Un certificat de clé publique peut être utilisé comme un "accréditif d'identité", et un certificat d'attribut peut être utilisé comme un "accréditif d'autorisation".

$ critique *(critical)*
1. (I) /ressource système/ Condition d'une ressource système telle que le refus d'accès, ou l'indisponibilité, de cette ressource compromettrait la capacité d'un utilisateur du système d'effectuer une fonction principale ou résulterait en d'autres conséquences sérieuses, comme des dommages aux personnes ou la perte de la vie. (Voir : disponibilité, préséance. À comparer à : sensible.)
2. (N) /extension/ Indication qu'il n'est pas permis à une application d'ignorer une extension. [X.509]

Instructions : chaque extension d'un certificat X.509 ou d'une CRL est munie d'un fanion qui la marque comme "critique" ou "non critique". Dans un certificat, si un programme informatique ne reconnaît pas un type d'extension (c'est-à-dire, ne met pas en œuvre sa sémantique) si l'extension est critique, le programme est obligé de traiter le certificat comme invalide ; mais si l'extension n'est pas critique, il est permis au programme d'ignorer l'extension.
Dans une CRL, si un programme ne reconnaît pas une extension critique qui est associée à un certificat spécifique, le programme est obligé de supposer que le certificat cité a été révoqué et n'est plus valide, et d'entreprendre ensuite toute action requise par la politique locale.
Lorsque un programme ne reconnaît pas une extension critique qui est associée à la CRL comme un tout, le programme est obligé de supposer que tous les certificats mentionnés ont été révoqués et ne sont plus valides. Cependant, comme manquer

à traiter l'extension peut signifier que la liste n'a pas été achevée, le programme ne peut pas supposer que les autres certificats sont valides, et le programme doit donc prendre toute mesure exigée par la politique locale.

$ infrastructure d'informations critiques *(critical information infrastructure)*
(I) Systèmes qui sont si vitaux pour une nation que leur incapacité ou destruction aurait un effet débilitant sur la sécurité nationale, sur l'économie, ou la santé et la sécurité publique.

$ point de distribution de CRL *(CRL distribution point)*. (I) Voir : point de distribution

$ extension de CRL *(CRL extension)*. (I) Voir : extension.

$ certificat croisé *(cross-certificate)*
(I) Certificat de clé publique produit par une CA dans une PKI à une CA dans une autre PKI. (Voir : certification croisée.)

$ certification croisée *(cross-certification)*
(I) Acte ou processus par lequel une CA dans une PKI produit un certificat de clé publique à une CA dans une autre PKI. [X509] (Voir : CA pont.)
Instructions : X.509 dit qu'une CA (disons, CA1) peut produire un "certificat croisé" dans lequel le sujet est une autre CA (disons, CA2). X.509 appelle CA2 la "CA sujet" et CA1 une "CA intermédiaire", mais ce glossaire déconseille ces termes. (Voir : CA intermédiaire, CA sujet).
La certification croisée de CA2 par CA1 apparaît similaire à la certification d'une CA subordonnée par une CA supérieure, mais la certification croisée implique un concept différent. Le concept de "CA subordonnée" s'applique lorsque les deux CA sont dans la même PKI, c'est-à-dire, lorsque soit (a) CA1 et CA2 sont sous la même racine, soit (b) CA1 est elle-même une racine. Le concept de "certification croisée" s'applique dans d'autres cas :
D'abord, la certification croisée s'applique lorsque deux CA sont dans des PKI différentes, c'est-à-dire, lorsque CA1 et CA2 sont sous des racines différentes, ou peut-être sont elles-mêmes deux racines. Produire le certificat croisé permet aux entités d'extrémité certifiées sous CA1 dans PK1 de construire les chemins de certification nécessaires pour valider les certificats des entités d'extrémité certifiées sous CA2 dans PKI2. Parfois, une paire de certificats croisés est produite – par CA1 pour CA2, et par CA2 pour CA1 – de sorte qu'une entité d'extrémité dans l'une ou l'autre PKI puisse valider les certificats produits dans l'autre PKI.
Ensuite, X.509 dit que deux CA, dans une PKI complexe multi-CA, peuvent se certifier mutuellement pour raccourcir les chemins de certification construits par les entités d'extrémité. C'est une politique de certificat et un CPS local qui diront si une CA peut ou non effectuer cette forme de certification croisée ou une autre, et comment de tels certificats peuvent être utilisés par les entités d'extrémité.

$ solution inter domaines *(cross-domain solution)*
1. (D) Synonyme de "garde".
Terme déconseillé : les IDOC NE DEVRAIENT PAS utiliser ce terme comme synonyme de "garde" ; ce terme duplique sans nécessité (et de façon verbeuse) la signification bien établie depuis longtemps de "garde".
2. (O) /Gouvernement des USA/ Processus ou sous système qui fournit une capacité (qui pourrait être soit manuelle, soit automatisée) d'accéder à deux domaines de sécurité différents ou plus dans un système, ou de transfert d'informations entre deux de ces domaines. (Voir : domaine, garde.)

$ cryptanalyse *(cryptanalysis)*
1. (I) Science mathématique qui traite de l'analyse d'un système cryptographique pour obtenir les connaissances nécessaires pour casser ou circonvenir la protection que le système est conçu pour fournir. (Voir : cryptologie, définition secondaire sous "intrusion".)
2. (O) "Analyse d'un système cryptographique et/ou de ses entrées et résultats pour déduire les variables confidentielles et /ou les données sensibles y compris le texte en clair." [I7498-2]

Instructions : La définition 2 établit le but traditionnel de la cryptanalyse, c'est-à-dire, convertir le texte chiffré en texte source (qui est habituellement du texte en clair) sans connaître la clé ; mais cette définition ne s'applique qu'aux systèmes de chiffrement. Aujourd'hui, le terme est utilisé en référence à toutes sortes d'algorithmes de chiffrement et de gestion de clés, et la définition 1 reflète cela. Dans tous les cas, cependant, un cryptanalyste essaye de découvrir ou de reproduire les données sensibles de quelqu'un d'autre, comme du texte en clair, une clé, ou un algorithme. Les attaques de cryptanalyse de base sur les systèmes de chiffrement sont seulement sur le texte chiffré, du texte en clair connu, du texte en clair choisi, et du texte chiffré choisi, et elles se généralisent aux autres sortes de cryptographie.

$ crypto, CRYPTO
1. (N) Un préfixe ("crypto-") qui signifie "cryptographique".
Usage : les IDOC PEUVENT utiliser ce préfixe lorsque il fait partie d'un terme mentionné dans ce glossaire. Autrement, les IDOC NE DEVRAIENT PAS utiliser ce préfixe ; à la place, utiliser l'adjectif non abrégé "cryptographique".

2. (D) En minuscules, "crypto" est une abréviation pour l'adjectif "cryptographique", ou pour les noms "cryptographie" ou "composant cryptographique".
Abréviation déconseillée : les IDOC NE DEVRAIENT PAS utiliser cette abréviation parce que elle pourrait facilement être comprise à tort dans un sens technique.
3. (O) /Gouvernement des USA/ En majuscules, "CRYPTO" est un marquage ou une désignation qui identifie "le matériel de chiffrement COMSEC utilisé pour sécuriser ou authentifier les télécommunications qui portent des informations classifiées ou sensibles du gouvernement des USA ou dérivées du gouvernement des USA". [C4009] (Voir : étiquette de sécurité, marquage de sécurité.)

$ cryptographique *(cryptographic)* (I) Adjectif qui se réfère à la cryptographie.

$ algorithme cryptographique *(cryptographic algorithm)*
(I) Algorithme qui utilise la science de la cryptographie, incluant (a) des algorithmes de chiffrement, (b) des algorithmes de hachage cryptographique, (c) des algorithmes de signature numérique, et (d) des algorithmes d'accord de clés.

$ interface de programmation d'application cryptographique (CAPI, *cryptographic application programming interface*)
(I) Formats et procédures de code source par lesquels un programme d'application accède à des services cryptographiques, qui sont définis de façon abstraite par rapport à leur mise en œuvre réelle. Exemple, voir : PKCS n° 11, [RFC2628].

$ association cryptographique *(cryptographic association)*
(I) Association de sécurité qui implique l'utilisation de la cryptographie pour fournir des services de sécurité pour les données échangées par les entités associées. (Voir : ISAKMP.)

$ frontière cryptographique *(cryptographic boundary)*
(I) Voir : définition secondaire sous "module cryptographique".

$ carte cryptographique *(cryptographic card)*
(I) Jeton cryptographique de la forme d'une carte à mémoire ou d'une carte de PC.

$ composant cryptographique *(cryptographic component)*
(I) Terme générique pour tout composant de système qui implique de la cryptographie. (Voir : module cryptographique.)

$ hachage cryptographique *(cryptographic hash)*
(I) Voir : définition secondaire sous "fonction de hachage".

$ clé d'allumage cryptographique (CIK, *cryptographic ignition key*)
1. (N) Jeton physique (usuellement électronique) utilisé pour mémoriser, transporter, et protéger les clés cryptographiques et les données d'activation. (À comparer à : boîtier de protection, appareil de remplissage.)
Instructions : une clé de chiffrement de clé pourrait être divisée (voir : clé éclatée) entre une CIK et un module cryptographique, de sorte qu'il serait nécessaire de combiner les deux pour régénérer la clé, l'utiliser pour déchiffrer d'autres clés et les données contenues dans le module, et donc activer le module.
2. (O) "Appareil ou clé électronique utilisé pour déverrouiller le mode sécurisé d'un équipement cryptographique." [C4009]
Usage : Abrégé en "clé de crypto-allumage".

$ clé cryptographique *(clé de chiffrement)*
(I) Voir : clé . Usage : Usuellement abrégé juste en "clé".

$ Syntaxe de message cryptographique (CMS, *Cryptographic Message Syntax*)
(I) Syntaxe d'encapsulation (RFC3852) pour les signatures numériques, les hachages, et le chiffrement de messages arbitraires.
Instructions : la CMS dérive de PKCS n° 7. Les valeurs de CMS sont spécifiées en ASN.1 et utilisent le codage BER. La syntaxe permet plusieurs encapsulations avec incorporation, permet que des attributs arbitraires soient signés avec le contenu du message, et prend en charge une variété d'architectures pour la gestion de clés numériques fondées sur des certificats.

$ module cryptographique *(cryptographic module)*
(I) Ensemble de matériels, progiciels ou logiciels, ou de leurs combinaisons, qui met en œuvre la logique ou les processus cryptographiques, incluant les algorithmes cryptographiques, et est contenu dans la "frontière cryptographique" du module, qui est un périmètre contigu explicitement défini qui établit les limites physiques du module. [FP140]

$ système cryptographique *(cryptographic system)*

1. (I) Ensemble d'algorithmes cryptographiques incluant les processus de gestion de clés qui prennent en charge l'utilisation des algorithmes dans un certain contexte d'application.

Usage : les IDOC DEVRAIENT utiliser la définition 1 parce qu'elle couvre une plus large gamme d'algorithmes que la définition 2.

2. (O) "Une collection de transformations du texte source en texte chiffré et vice versa [qui exclurait les algorithmes de signature numérique, de hachage cryptographique, et d'accord de clés], la ou les transformations particulières à utiliser étant choisie par les clés. Les transformations sont normalement définies par un algorithme mathématique." [X.509]

$ jeton cryptographique *(cryptographic token)*

1. (I) Appareil physique portable, sous le contrôle de l'utilisateur (par exemple, une carte à mémoire ou une carte PCMCIA) utilisée pour mémoriser des informations cryptographiques et éventuellement effectuer aussi des fonctions cryptographiques. (Voir : carte cryptographique, jeton.)

Instructions : un jeton intelligent peut mettre en œuvre un certain ensemble d'algorithmes cryptographiques et peut incorporer les fonctions de gestion de clés qui s'y rapportent, comme un générateur de nombres aléatoires. Un jeton cryptographique intelligent peut contenir un module cryptographique ou peut n'être pas explicitement conçu de cette façon.

$ cryptographie *(cryptography)*

1. (I) La science mathématique qui traite de la transformation des données pour rendre leur signification inintelligible (c'est-à-dire, pour cacher leur contenu sémantique) empêcher leur altération subreptice, ou empêcher leur utilisation non autorisée. Si la transformation est réversible, la cryptographie traite aussi de la restauration des données chiffrées en forme intelligible. (Voir : cryptologie, stéganographie.)
2. (O) "Discipline qui incorpore les principes, moyens, et méthodes pour la transformation des données afin de cacher leur contenu d'informations, empêcher leur modification non détectée et/ou empêcher leur utilisation non autorisée.... La cryptographie détermine les méthodes utilisées dans le chiffrement et le déchiffrement." [I7498-2]

Instructions : la couverture complète des protocoles et algorithmes de cryptographie appliquée est fournie par Schneier [Schn]. Les affaires et les gouvernements utilisent la cryptographie pour rendre les données incompréhensibles aux personnes externes ; pour rendre les données incompréhensibles aussi bien en interne qu'en externe, les données sont passées à des juristes pour réécriture.

$ Cryptoki

(N) CAPI défini dans PKCS n° 11. Prononciation : "CRYPTO-ki". Dérivation : Abréviation de "interface de jeton cryptographique".

$ cryptologie *(cryptology)*

(I) Science de la communication secrète, qui inclut la cryptographie et la cryptanalyse.

Instructions : Le terme est parfois utilisé dans un sens plus large pour noter une activité qui inclut à la fois la sécurisation des signaux (voir : sécurité du signal) et l'extraction des informations des signaux (voir : intelligence du signal) [Kahn].

$ réseau crypté *(cryptonet)*

(I) Un réseau (c'est-à-dire, un ensemble communicant) d'entités systèmes qui partagent une clé cryptographique secrète pour un algorithme symétrique. (Voir : autorité de contrôle.)

(O) "Stations qui détiennent une clé commune." [C4009]

$ période de cryptage *(cryptoperiod)*

(I) Espace de temps pendant lequel l'utilisation de la valeur d'une certaine clé est autorisée dans un système cryptographique. (Voir : gestion de clé.)

Usage : l'usage de ce terme est depuis longtemps établi dans COMPUSEC. Dans le contexte des certificats et clés publics, "durée de vie de clé" et "période de validité" sont souvent utilisés à la place.

Instructions : une période de cryptage est usuellement déclarée en termes de calendrier ou d'heure, mais est parfois déclarée sous la forme de la quantité maximum de données dont le traitement est permis par un algorithme cryptographique qui utilise la clé. Spécifier une période de cryptage implique un compromis entre le coût du changement de clés et le risque de réussite d'une analyse cryptographique.

$ crypto système (I) Contraction de "système cryptographique".

$ crypto variable (D) Synonyme de "clé".

Utilisation déconseillée : dans l'usage contemporain de COMSEC, le terme de "clé" a remplacé le terme "crypto variable".

$ attaque de couper-coller *(cut-and-paste attack)*

(I) Attaque active contre l'intégrité des données d'un texte chiffré, effectuée en remplaçant des sections de texte chiffré par

un autre texte chiffré, de telle sorte que le résultat paraisse se déchiffrer correctement mais se déchiffre en fait en un texte en clair qui est falsifié pour la satisfaction de l'attaquant.

$ contrôle de redondance cyclique (CRC, *cyclic redundancy check*)
(I) Type d'algorithme de somme de contrôle qui n'est pas un hachage cryptographique mais est utilisé pour mettre en œuvre un service d'intégrité des données où des changements accidentels des données sont prévisibles. Parfois appelé "code de redondance cyclique".

$ code d'authentification des données (DAC, *Data Authentication Code*)
(N) Voir : code d'authentification des données, contrôle d'accès discrétionnaire.
Utilisation déconseillée : les IDOC qui utilisent ce terme DEVRAIENT en donner une définition parce que cette abréviation est ambiguë.

$ démon *(daemon)*
(I) Programme informatique qui n'est pas invoqué explicitement mais attend qu'une condition spécifiée survienne, et fonctionne alors sans utilisateur (principal) associé, généralement dans un but administratif. (Voir : zombie.)

$ menace vaine *(dangling threat)*
(O) Menace sur un système pour lequel il n'y a pas de vulnérabilité correspondante, et donc qui n'implique pas de risque.

$ vulnérabilité apparente *(dangling vulnerability)*
(O) Vulnérabilité d'un système pour laquelle il n'y a pas de menace correspondante et donc, pas de risque impliqué.

$ données *(data)*
(I) Informations dans une représentation spécifique, usuellement comme séquence de symboles qui ont une signification.
Usage : se réfère (a) aux représentations qui peuvent être reconnues, traitées, ou produites par un ordinateur ou autre type de machine, et (b) aux représentations qui peuvent être traitées par un humain.

$ algorithme d'authentification de données *(Data Authentication Algorithm)*
1. (N) /Avec majuscules/ Norme ANSI pour une fonction de hachage chiffrée qui est équivalente du chaînage de bloc de chiffrement DES avec IV = 0. [A9009]
2. (D) /En minuscules/ Synonyme d'une sorte de "somme de contrôle".

Terme déconseillé : les IDOC NE DEVRAIENT PAS utiliser ce terme ; utiliser la forme en minuscules de "algorithme d'authentification de données" comme synonyme de toute sorte de somme de contrôle, sans considérer si la somme de contrôle se fonde ou non sur un hachage. À la place, utiliser "somme de contrôle", "code d'authentification de données", "code de détection d'erreur", "hachage", "hachage chiffré", "code d'authentification de message", "somme de contrôle protégée", ou quelque autre terme spécifique, selon ce que l'on veut dire.
Le terme en minuscules peut être confondu avec le code d'authentification de données et mélange aussi des concepts d'une façon potentiellement trompeuse. Le mot "authentification" est trompeur parce que la somme de contrôle peut être utilisée pour effectuer une fonction de vérification d'intégrité des données plutôt qu'une fonction d'authentification d'origine des données.

$ code d'authentification de données *(Data Authentication Code)*
1. (N) /en majuscules/ Norme spécifique du gouvernement des USA [FP113] pour une somme de contrôle qui est calculée sur l'algorithme d'authentification des données.

Usage : autrement dit, un code d'authentification de message [A9009].) (Voir : DAC.)
2. (D) /en minuscules/ Synonyme pour une sorte de "somme de contrôle".

Terme déconseillé : les IDOC NE DEVRAIENT PAS utiliser ce terme ; utiliser la forme en minuscules de "code d'authentification de données" comme synonyme de toute forme de somme de contrôle, sans considération du fait que la somme de contrôle est ou non fondée sur l'algorithme d'authentification de données. Le terme en minuscules peut être confondu avec le code d'authentification de données et mélange aussi des concepts d'une façon qui peut être trompeuse (voir : code d'authentification).

$ compromission de données *(data compromise)*
1. (I) Incident de sécurité dans lequel des informations sont exposées à un potentiel accès non autorisé, comme une divulgation non autorisée, une altération, ou une utilisation des informations qui aurait pu se produire. (À comparer à : compromission de sécurité, incident de sécurité.)
2. (O) /U.S. DoD/ Une "compromission" est une "communication ou transfert physique des informations à un receveur non autorisé." [DoD5]
3. (O) /Gouvernement des USA/ "Type d'incident [de sécurité] où des informations sont divulguées à des individus non autorisés ou une violation de la politique de sécurité d'un système dans lequel la divulgation, la modification, la

destruction ou la perte non autorisée intentionnelle ou non intentionnelle d'un objet peut s'être produite." [C4009]

$ confidentialité des données *(data confidentiality)*

1. (I) Propriété que les données ne soient pas divulguées aux entités systèmes tant qu'elles n'ont pas été autorisées à connaître les données. (Voir : modèle de Bell-LaPadula, classification, service de confidentialité des données, secret. À comparer à : vie privée.)
2. (D) "Propriété que des informations ne soient pas rendues disponibles ou divulguées à des individus, entités, ou processus non autorisés [c'est-à-dire, à toute entité système non autorisée]." [I7498-2].

Définition déconseillée : la phrase "rendues disponibles" pourrait être interprétée comme signifiant que les données pourraient être altérées, et pourrait faire confondre ce terme avec le concept de "intégrité des données".

$ service de confidentialité des données *(data confidentiality service)*

(I) Service de sécurité qui protège les données contre la divulgation non autorisée. (Voir : contrôle d'accès, confidentialité des données, service de confidentialité de datagramme, contrôle, contrôle d'inférence.)
Utilisation déconseillée : les IDOC NE DEVRAIENT PAS utiliser ce terme comme synonyme de "confidentialité", qui est un concept différent.

$ algorithme de chiffrement de données (DEA, *Data Encryption Algorithm*)

(N) Chiffrement de bloc symétrique, défini dans le DES du gouvernement des USA. DEA utilise une clé de 64 bits, dont 56 bits sont choisis indépendamment et 8 sont des bits de parité, et transpose un bloc de 64 bits en un autre bloc de 64 bits. [FP046] (Voir : AES, cryptographie symétrique.)
Usage : on appelle généralement cet algorithme "DES". L'algorithme a aussi été adopté dans des normes non gouvernementales (par exemple, [A3092]).

$ clé de chiffrement de données (DEK, *data encryption key*)

(I) Clé de chiffrement qui est utilisée pour chiffrer les données d'application. (À comparer à : clé de chiffrement de clé.)

$ norme de chiffrement des données (DES, *Data Encryption Standard*)

(N) Norme du gouvernement des USA [FP046] qui spécifie le DEA et déclare une politique d'utilisation de l'algorithme pour protéger les données sensibles, non classifiées. (Voir : AES.)

$ intégrité des données *()*

1. (I) Propriété que des données n'aient pas été changées, détruites, ou perdues de façon non autorisée ou accidentelle. (Voir : service d'intégrité des données. À comparer à : intégrité correcte, intégrité de source.)
2. (O) "Propriété que des informations n'aient pas été modifiées ou détruites d'une façon non autorisée." [I7498-2]

Usage : A à voir avec (a) la constance et la confiance en les valeurs des données, et pas avec (b) les informations que les valeurs représentent (voir : intégrité correcte) ou (c) le caractère digne de confiance de la source des valeurs (voir : intégrité de source).

$ service d'intégrité des données *(data integrity service)*

(I) Service de sécurité qui protège contre le changement non autorisé des données, incluant à la fois le changement ou la destruction intentionnels et le changement ou perte accidentels, en s'assurant que les changements des données sont détectables. (Voir : intégrité des données, somme de contrôle, service d'intégrité des datagrammes.)
Instructions : un service d'intégrité des données peut seulement détecter un changement et en faire rapport à une entité système appropriée ; les changements ne peuvent être empêchés que si le système est parfait (sans erreur) et si aucun utilisateur malveillant n'y a accès. Cependant, un système qui offre un service d'intégrité des données peut aussi tenter de corriger et récupérer de ces changements.
La capacité de ce service à détecter les changements est limitée par la technologie des mécanismes utilisés pour mettre en œuvre le service. Par exemple, si le mécanisme est une vérification de parité sur un bit à travers chaque SDU entière, un changement d'un nombre impair de bits dans une SDU sera détecté, mais le changement d'un nombre pair de bits ne le serait pas.
Relations entre le service d'intégrité des données et les services d' authentification : bien que les services d'intégrité des données soient définis séparément du service d'authentification d'origine des données et du service d'authentification de l'entité homologue, ils sont en relation étroite avec eux. Les services d'authentification dépendent, par définition, des services compagnons d'intégrité des données. Le service d'authentification de l'origine des données assure la vérification que l'identité de la source originale d'une unité de données reçue est bien celle prétendue ; une telle vérification ne peut avoir lieu si l'unité de données a été altérée. Le service d'authentification de l'entité homologue vérifie que l'identité d'une entité homologue est actuellement associée comme prétendu ; une telle vérification ne peut avoir lieu si l'identité prétendue a été altérée.

$ authentification de l'origine des données *(data origin authentication)*

(I) "Corroboration que la source des données reçues est celle prétendue." [I7498-2] (Voir : authentification.)

$ service d'authentification de l'origine des données *(data origin authentification service)*
(I) Service de sécurité qui vérifie l'identité d'une entité système qui est prétendue être la source originale des données reçues. (Voir : authentification, service d'authentification.)
Instructions : ce service est fourni à toute entité système qui reçoit ou détient les données. À la différence du service d'authentification de l'entité homologue, ce service est indépendant de toute association entre le générateur et le receveur, et les données en question peuvent avoir été générées à tout moment dans le passé.
Un mécanisme de signature numérique peut être utilisé pour fournir ce service, parce que quelqu'un qui ne connaît pas la clé privée peut falsifier la signature correcte. Cependant, en utilisant la clé publique du signataire, tout le monde peut vérifier l'origine de données correctement signées.
Ce service est habituellement groupé avec le service d'"intégrité des données sans connexion. (Voir : "relations entre service d'intégrité des données et services d'authentification" sous "service d'intégrité des données".

$ propriétaire des données *(data owner)*
(N) Organisation qui a l'autorité finale statutaire et opérationnelle pour les informations spécifiées.

$ privauté des données *(data privacy)*
(D) Synonyme de "confidentialité des données".
Terme déconseillé : les IDOC NE DEVRAIENT PAS utiliser ce terme ; il mélange les concepts d'une façon potentiellement trompeuse. À la place, utiliser soit "confidentialité des données" soit "privauté" soit les deux, selon ce que l'on veut dire.

$ récupération des données *(data recovery)*
1. (I) /cryptanalyse/ Processus pour apprendre, à partir d'un texte chiffré, le texte source qui a été précédemment chiffré pour produire le texte chiffré. (Voir : récupération.)
2. (I) /intégrité système/ Processus de restauration des informations suite à dommage ou destruction.

$ sécurité des données *(data security)*
(I) Protection des données contre la divulgation, l'altération, la destruction, ou la perte, qui est soit accidentelle, soit intentionnelle mais non autorisée.
Instructions : les deux services de confidentialité et d'intégrité des données sont nécessaires pour réaliser la sécurité des données.

$ datagramme *(datagram)*
(I) "Entité de données auto contenue indépendante [c'est-à-dire, un paquet] portant des informations suffisantes pour être acheminées de la source [ordinateur] à l'ordinateur de destination sans s'appuyer sur les échanges précédents entre ces ordinateurs de source et de destination et le réseau de transport." [RFC1983] Exemple : une PDU de IP.

$ service de confidentialité de datagramme *(datagram confidentiality service)*
(I) Service de confidentialité de données qui préserve la confidentialité des données dans un seul paquet indépendant ; c'est-à-dire, le service s'applique à un datagramme à la fois. Exemple : ESP. (Voir : confidentialité des données.)
Usage : lorsque un protocole est dit fournir un service de confidentialité des données, ceci est généralement compris comme signifiant que seule la SDU est protégée dans chaque paquet. Les IDOC qui utilisent le terme pour signifier que la PDU entière est protégée devraient inclure une définition précise.
Instructions : cette forme de base de service de confidentialité réseau suffit pour la protection des données dans le flux de paquets dans les protocoles en mode sans connexion aussi bien qu'en mode connexion. Sauf peut-être pour la confidentialité du flux de trafic, rien de plus n'est nécessaire pour protéger la confidentialité des données portées par un flux de paquets. L'OSIRM distingue la confidentialité de connexion et la confidentialité sans connexion. La suite des protocoles de l'Internet (IPS, *Internet Protocol Suite*) n'a pas besoin de faire cette distinction, parce que ces services sont juste des instances du même service (c'est-à-dire, la confidentialité de datagramme) qui sont offertes dans le contexte de deux protocoles différents. (Cependant pour le service d'intégrité des données, un effort supplémentaire est nécessaire pour protéger un flux, et l'IPS n'a pas besoin de distinguer entre le "service d'intégrité de datagramme" et le "service d'intégrité de flux".)

$ service d'intégrité de datagramme *(datagram integrity service)*
(I) Service d'intégrité des données qui préserve l'intégrité des données dans un seul paquet indépendant ; c'est-à-dire, le service s'applique à un datagramme à la fois. (Voir : intégrité des données. À comparer à : service d'intégrité de flux.)
Instructions : la capacité de fournir une intégrité des données appropriée est importante dans de nombreuses situations de sécurité de l'Internet, et il y a donc différentes sortes de services d'intégrité des données adaptés à différentes applications. Ce service est de la plus simple sorte ; il convient pour les transferts de données sans connexion.
Le service d'intégrité de datagramme est usuellement conçu pour seulement tenter de détecter des changements de la SDU

dans chaque paquet, mais il peut aussi tenter de détecter des changements à certaines ou toutes les informations de contrôle de protocole (PCI, *protocol information control*) dans chaque paquet (voir : intégrité de champ sélective). À l'opposé de ce service simple, à utilisation unique, certaines situations de sécurité exigent un service plus complexe qui tente aussi de détecter des datagrammes supprimés, insérés, ou réordonnés au sein d'un flux de datagrammes (voir : service d'intégrité de flux).

$ tromperie *(deception)*
(I) Circonstance ou événement qui peut résulter en ce qu'une entité autorisée reçoive de fausses données et qu'elle les croie vraies. (Voir : authentification.)
Instructions : c'est un type de conséquence de menace, et il peut être causé par les types d'actions de menace suivants : mascarade, falsification, et répudiation.

$ décrypter *(decipher)*
(D) Synonyme de "déchiffrer".
Définition déconseillée : les IDOC NE DEVRAIENT PAS utiliser ce terme comme synonyme de "déchiffrer". Cependant, voir la note d'usage sous "chiffrement".

$ décryptage *(decipherment)*
(D) Synonyme de "déchiffrement".
Définition déconseillée : les IDOC NE DEVRAIENT PAS utiliser ce terme comme synonyme de "déchiffrement". Cependant, voir la note d'usage sous "chiffrement".

$ déclassification *(declassification)*
(I) Processus autorisé par lequel des informations sont déclassifiées. (À comparer à : classification.)

$ déclassifier *(declassify)*
(I) Retirer officiellement la désignation du niveau de sécurité d'un élément d'information ou type d'information classifié, tel que l'information n'est plus classifiée (c'est-à-dire, devient non classifiée). (Voir : classifié, classifier, niveau de sécurité. À comparer à : dégrader.)

$ décoder *(decode)*
1. (I) Convertir des données codées en leur forme de représentation originelle. (À comparer à : décrypter.)
2. (D) Synonyme de "déchiffrer".
Définition déconseillée : le codage n'est normalement pas destiné à dissimuler la signification. Donc, les IDOC NE DEVRAIENT PAS utiliser ce terme comme synonyme de "déchiffrer", parce que cela mélangerait des concepts d'une façon potentiellement trompeuse.

$ déchiffrer *(decrypt)*
(I) Restaurer cryptographiquement du texte chiffré en la forme du texte source qu'il avait avant le chiffrement.

$ déchiffrement *(decryption)* (I) Voir : définition secondaire sous "chiffrement".

$ mode de sécurité dédié *(dedicated security mode)*
(I) Mode de fonctionnement d'un système par lequel tous les usagers qui ont accès au système possèdent, pour toutes les données traitées par le système, à la fois (a) toutes les autorisations nécessaires (c'est-à-dire, niveau d'habilitation et d'approbation formelle d'accès) et (b) un besoin de savoir. (Voir : /fonctionnement de système/ sous "mode", approbation formelle d'accès, besoin de savoir, niveau de protection, niveau d'habilitation.)
Usage : généralement abrégé en "mode dédié". Ce mode a été défini dans la politique du gouvernement des USA sur l'accréditation de système, mais le terme est aussi utilisé en dehors du gouvernement. Dans ce mode, le système peut traiter soit (a) un seul niveau de classification ou catégorie d'informations, soit (b) une gamme de niveaux et de catégories.

$ compte par défaut *(default account)*
(I) Compte de connexion à un système (auquel on accède généralement avec un identifiant d'utilisateur et un mot de passe) qui a été prédéfini dans un système manufacturé pour permettre l'accès initial quand le système est mis en service pour la première fois. (Voir : durcir.)
Instructions : un compte par défaut devient une faiblesse sérieuse si il n'est pas géré de façon appropriée. Parfois, l'identifiant par défaut et le mot de passe sont bien connus parce que ils sont les mêmes dans chaque copie du système. Dans tous les cas, lorsque un système est mis en service, tout mot de passe par défaut devrait être immédiatement changé ou le compte par défaut devrait être désactivé.

$ défense en profondeur *(defense in depth)*
(N) "Disposition de positions de défense qui se soutiennent mutuellement pour absorber et affaiblir progressivement l'attaque, empêcher les observations préalables de l'ensemble de la position par l'ennemi, et [permettre] au commandant de manœuvrer la réserve." [JP1]
Instructions : dans les systèmes d'information, la défense en profondeur signifie de construire une architecture de sécurité du système avec des mécanismes et contre-mesures de sécurité en couches et complémentaires, afin que si un des mécanismes de sécurité est vaincu, un ou plusieurs autres mécanismes (qui sont "derrière" ou "dessous" le premier mécanisme) assurent encore la protection.
Ce concept architectural est intéressant parce qu'il fait appel aux principes traditionnels de l'art de la guerre, qui applique la défense en profondeur aux structures physiques géospatiales ; mais appliquer le concept aux structures logiques du cyber-espace des réseaux informatiques est plus difficile. Le concept suppose que les réseaux ont une représentation spatiale ou topologique. Il suppose aussi que peuvent être mise en œuvre – à partir d'un "périmètre externe" d'un réseau, à travers ses diverses "couches" de composants, jusqu'à son "centre" (c'est-à-dire, aux systèmes d'application de l'abonné pris en charge par le réseau) – une série de diverses contre-mesures qui ensemble assurent une protection adéquate. Cependant, il est plus difficile de transposer la topologie des réseaux et de s'assurer qu'il n'existe pas de chemin par lequel un attaquant puisse outrepasser toutes les couches de défense.

$ Infrastructure d'informations de défense (DII, *Defense Information Infrastructure*)
(O) /U.S. DoD/ Système partagé interconnecté de structures d'ordinateurs, de communications, de données, d'applications, de sécurité, de personnels, de formations et de soutien du Ministère Américain de la Défense, qui sert les besoins d'information dans l'ensemble du monde. (Voir : DISN.) Usage : a évolué pour s'appeler le GIG.
Instructions : le DII connecte les ordinateurs de support de missions, de commandement et de contrôle, et de renseignement et les utilisateurs par des services vocaux, de données, d'imagerie, de vidéo, et multimédia, et fournit des traitements d'informations et des services à valeur ajoutée aux abonnés sur le DISN. Les données d'utilisateur et les logiciels d'application ne font pas partie du DII.

$ Réseau de systèmes d'information de la Défense (DISN, *Defense Information Systems Network*)
(O) /U.S. DoD/ Infrastructure de télécommunications mondiales au niveau entreprise du Ministère Américain de la Défense consolidé, qui fournit le transfert d'informations de bout en bout pour la prise en charge des opérations militaires ; c'est une partie de la DII. (À comparer à : GIG.)

$ dégausser *(degauss)*
1a. (N) Appliquer un champ magnétique pour supprimer de façon permanente des données d'un support de stockage magnétique, comme une bande ou un disque [NCS25]. (À comparer à : écraser, purger, épurer.)
1b. (N) Réduire la densité de flux magnétique à zéro en appliquant un champ magnétique inverse. (Voir : rémanence magnétique.)

$ dégausseur *(degausser)*
(N) Appareil électrique qui peut dégausser les supports de stockage magnétiques.

$ retard *(delay)* (I) /paquet/ Voir : définition secondaire sous "service d'intégrité de flux".

$ suppression *(deletion)*
(I) /paquet/ Voir : définition secondaire sous "service d'intégrité de flux".

$ exposition délibérée *(deliberate exposure)*
(I) /action de menace/ Voir : définition secondaire sous "exposition".

$ CRL delta *(delta CRL)*
(I) CRL partielle qui ne contient des entrées que pour les certificats qui ont été révoqués depuis la production de la CRL de base précédente [X.509]. Cette méthode peut être utilisée pour partager les CRL qui deviennent trop grandes et peu maniables. (À comparer à : point de distribution de CRL.)

$ zone démilitarisée (DMZ, *demilitarized zone*)
(D) Synonyme de "zone tampon".
Terme déconseillé : les IDOC NE DEVRAIENT PAS utiliser ce terme parce qu'il mélange les concepts d'une façon potentiellement trompeuse. (Voir : Utilisation déconseillée sous "Livre Vert".)

$ déni de service *(denial of service)*
(I) Empêcher l'accès autorisé à une ressource système ou retarder les opérations et fonctions d'un système. (Voir : disponibilité, critique, inondation.)

Instructions : une attaque de déni de service peut empêcher la conduite normale des affaires sur l'Internet. Il y a quatre types de solutions à ce problème de sécurité :
- Vigilance : rester attentif aux menaces et faiblesses de la sécurité. (Voir : CERT.)
- Détection : trouver les attaques sur les système d'extrémité et les sous-réseaux. (Voir : détection d'intrusion.)
- Prévention : suivre les pratiques défensives des systèmes connectés aux réseaux. (Voir : [RFC2827].)
- Réponse : réagir efficacement lorsque les attaques surviennent. (Voir : CSIRT, plan de contingence.)

$ autorité d'approbation désignée (DAA, *designated approving authority*)
(O) /Gouvernement des USA/ Synonyme de "accréditeur".

$ détection *(detection)* (I) Voir : définition secondaire sous "sécurité".

$ dissuasion *(deterrence)* (I) Voir : définition secondaire sous "sécurité".

$ attaque de dictionnaire *(dictionary attack)*
(I) Attaque qui utilise la technique de force brute d'essayer successivement tous les mots d'une grande liste exhaustive.
Exemples : Attaque d'un service d'authentification par l'essai de tous les mots de passe possibles. Attaque d'un service de chiffrement en chiffrant une certaine phrase de texte en clair avec toutes les clés possibles afin d'obtenir la clé pour un message chiffré qui contient cette phrase.

$ Diffie-Hellman
$ Diffie-Hellman-Merkle
(N) Algorithme d'accord de clés publié en 1976 par Whitfield Diffie et Martin Hellman [DH76], [RFC2631].
Usage : l'algorithme est le plus souvent appelé "Diffie-Hellman". Cependant, dans la livraison de novembre 1978 de "IEEE Communications Magazine", Hellman écrivait que l'algorithme "est un système de distribution de clé publique, concept développé par [Ralph C.] Merkle, et qui devrait donc être appelé 'Diffie-Hellman-Merkle' ... pour reconnaître l'égale contribution de Merkle à l'invention de la cryptographie à clé publique".
Instructions : Diffie-Hellman-Merkle effectue l'établissement de clés, pas le chiffrement. Cependant, la clé qui est produite peut être utilisée pour le chiffrement, pour d'autres opérations de gestion de clés, ou pour toute autre cryptographie.
L'algorithme est décrit dans la [RFC2631] et dans [Schn]. En bref, Alice et Bob prennent de grands entiers qui satisfont à certaines conditions mathématiques, et utilisent les entiers pour calculer chacun séparément une paire de clés publique/privée. Ils envoient chacun à l'autre leur clé publique. Chaque personne utilise sa propre clé privée et la clé publique de l'autre personne pour calculer une clé, k, qui, à cause des mathématiques de l'algorithme, est la même pour chacun d'eux. L'espionnage passif ne peut pas divulguer la clé partagée k, parce que k n'est pas transmise, pas plus que les clés privées nécessaires pour calculer k.
La difficulté de casser Diffie-Hellman-Merkle est considérée comme égale à celle de calculer des logarithmes discrets modulo un grand nombre premier. Cependant, sans mécanismes supplémentaires pour authentifier chaque partie auprès de l'autre, un protocole fondé sur l'algorithme peut être vulnérable à une attaque par interposition.

$ résumé *(digest)* Voir : résumé de message.

$ certificat numérique *(certificat numérique)*
(I) Document de certificat sous la forme d'un objet de données numérique (un objet de données utilisé par un ordinateur) auquel est ajouté une valeur de signature numérique calculée qui dépend de l'objet de données. (Voir : certificat d'attribut, certificat de clé publique.)
Utilisation déconseillée : les IDOC NE DEVRAIENT PAS utiliser ce terme pour se référer à une CRL ou CKL signée. Bien que la définition recommandée puisse être interprétée de façon à inclure d'autres éléments signés, la communauté de la sécurité n'utilise pas le terme avec cette signification.

$ certification numérique *(digital certification)*
(D) Synonyme de "certification".
Définition déconseillée : les IDOC NE DEVRAIENT PAS utiliser cette définition sauf si le contexte n'est pas suffisant pour distinguer entre certification numérique et une autre sorte de certification, auquel cas il vaudrait mieux utiliser "certification à clé publique" ou une autre phrase qui indique ce qui est en train d'être certifié.

$ document numérique *(digital document)*
(I) Objet de données électroniques qui représente des informations écrites à l'origine sur un support non électronique, non magnétique (usuellement de l'encre sur du papier) ou est analogue à un document de ce type.

$ enveloppe numérique *(digital envelope)*
(I) Combinaison de (a) données de contenu chiffré (de toutes sortes) destinées à un receveur, et (b) la clé de chiffrement de

contenu sous forme chiffrée qui a été préparée pour l'usage du receveur.
Usage : dans les IDOC, le terme DEVRAIT être défini au point de première utilisation parce que, bien que le terme soit défini dans PKCS n° 7 et utilisé dans S/MIME, il n'est pas très connu.
Instructions : l'enveloppage numérique n'est pas simplement un synonyme de la mise en œuvre de la confidentialité des données avec un chiffrement ; l'"enveloppage numérique est un schéma de chiffrement hybride pour "sceller" un message ou d'autres données, en chiffrant les données et en les envoyant avec une forme protégée de la clé au receveur prévu, afin que personne d'autre que le receveur prévu ne puisse "ouvrir" le message. Dans PKCS n° 7, il signifie de chiffrer d'abord les données en utilisant un algorithme de chiffrement symétrique et une clé secrète, et ensuite de chiffrer la clé secrète en utilisant un algorithme de chiffrement asymétrique et la clé publique du receveur prévu. Dans S/MIME, des méthodes supplémentaires sont définies pour chiffrer la clé de chiffrement du contenu.

$ Digital ID(marque déposée)
(D) Synonyme de "certificat numérique".
Terme déconseillé : les IDOC NE DEVRAIENT PAS utiliser ce terme. C'est une marque de service d'une entreprise commerciale, et il duplique inutilement la signification d'un terme mieux établi. (Voir : accréditif.)

$ clé numérique *(digital key)*
(D) Synonyme de paramètre d'entrée d'un algorithme de chiffrement ou autre processus. (Voir : clé.)
Utilisation déconseillée : l'adjectif "numérique" n'a pas besoin d'être utilisé avec "clé" ou "clé de chiffrement", sauf si le contexte est insuffisant pour distinguer la clé numérique d'une autre sorte de clé, comme une clé métallique pour la serrure d'une porte.

$ notaire numérique *(digital notary)*
(I) Fonctionnalité électronique analogue à un notaire public. Fournit un horodatage de confiance pour un document numérique, afin que quelqu'un puisse ultérieurement prouver que le document existait à un instant donné ; vérifie les signatures sur un document signé avant d'appliquer le timbre. (Voir : notarisation.)

$ signature numérique *(digital signature)*
1. (I) Valeur calculée avec un algorithme de chiffrement et associée à un objet de données d'une façon telle que tout receveur des données puisse utiliser la signature pour vérifier l'origine et l'intégrité des données. (Voir : service d'authentification de l'origine des données, service d'intégrité des données, signataire. À comparer à : signature numérisée, signature électronique.)
2. (O) "Données, ou leur transformation cryptographique, ajoutées à une unité de données qui permet à un receveur de l'unité de données de prouver la source et l'intégrité de l'unité de données et de les protéger contre la falsification, par exemple par le receveur." [I7498-2]

Instructions : une signature numérique devrait avoir ces propriétés :
- être capable d'être vérifiée. (Voir : valider vs. vérifier.)
- être lié à l'objet de données signé d'une façon telle que si les données ont changé, lorsque on tente de vérifier la signature, elle sera vue comme non authentique. (Dans certains schémas, la signature est ajoutée à l'objet signé comme déclaré par la définition 2, mais dans d'autres schémas, elle ne l'est pas.)
- identifier de façon univoque une entité système comme étant le signataire.
- être sous le contrôle du seul signataire, de sorte qu'elle ne puisse pas être créée par une autre entité.

Pour réaliser ces propriétés, l'objet de données est d'abord entré dans une fonction de hachage, puis le résultat du hachage est transformé cryptographiquement en utilisant une clé privée du signataire. La valeur finale résultante est appelée la signature numérique de l'objet de données. La valeur de signature est une somme de contrôle protégée, parce que les propriétés d'un hachage cryptographique assurent que si l'objet de données est changé, la signature numérique ne lui correspondra plus. La signature numérique est infalsifiable parce que on ne peut pas être certain de créer correctement ou de changer la signature sans connaître la clé privée du signataire supposé.
Certains schémas de signature numérique utilisent un algorithme de chiffrement asymétrique (par exemple, "RSA") pour transformer le résultat du hachage. Donc, lorsque Alice a besoin de signer un message à envoyer à Bob, elle peut utiliser sa clé privée pour chiffrer le résultat du hachage. Bob reçoit à la fois le message et la signature numérique. Bob peut utiliser la clé publique d'Alice pour déchiffrer la signature, et comparer le résultat du texte en clair au résultat du hachage qu'il a calculé en hachant le message lui-même. Si les valeurs sont égales, Bob accepte le message parce qu'il est certain qu'il vient d'Alice et est arrivé inchangé. Si les valeurs ne sont pas égales, Bob rejette le message parce que, soit le message, soit la signature, a été altérée dans le transit.
D'autres schémas de signature numérique (par exemple, "DSS") transforment le résultat du hachage avec un algorithme (par exemple, "DSA", "El Gamal") qui ne peut pas être directement utilisé pour chiffrer les données. Un tel schéma crée une valeur de signature à partir du hachage et donne un moyen pour vérifier la valeur de la signature, mais ne donne pas de moyen pour récupérer le résultat du hachage à partir de la valeur de la signature. Dans certains pays, un tel schéma peut améliorer l'exportabilité et éviter d'autres contraintes légales sur l'utilisation. Alice envoie la valeur de la signature à Bob avec à la fois le message et son hachage résultant. L'algorithme permet à Bob d'utiliser la clé publique de signature d'Alice et la valeur de la signature pour vérifier le résultat du hachage qu'il reçoit. Puis, comme précédemment, il compare ce

résultat de hachage qu'elle a envoyé à celui qu'il calcule en hachant le message lui-même.

$ Algorithme de signature numérique (DSA, *Digital Signature Algorithm*)
(N) Algorithme de chiffrement asymétrique pour une signature numérique sous la forme d'une paire de grands nombres. La signature est calculée en utilisant des règles et paramètres tels que l'identité du signataire et l'intégrité des données signées puissent être vérifiées. (Voir : DSS.)

$ Norme de signature numérique (DSS, *Digital Signature Standard*)
(N) Norme du gouvernement des USA [FP186] qui spécifie le DSA.

$ marquage numérique effaçable *(digital watermarking)*
(I) Techniques de calcul pour incorporer de façon inséparable des marques ou étiquettes non obstructives comme bits dans des données numériques -- texte, graphiques, images, vidéo, ou audio -- et pour détecter ou extraire ultérieurement les marques.
Instructions : une "marque numérique effaçable", c'est-à-dire, l'ensemble de bits incorporés, est parfois cachée, usuellement imperceptible, et toujours destinée à être non obstructive. Selon la technique particulière utilisée, le marquage numérique effaçable peut aider à prouver la propriété, à contrôler la duplication, à retracer la distribution, à assurer l'intégrité des données, et à effectuer d'autres fonctions pour protéger les droits de propriété intellectuelle. [ACM]

$ signature numérisée *(digitized signature)*
(D) Note diverses formes d'images numérisées de signatures manuelles. (À comparer à : signature numérique).
Terme déconseillé : les IDOC NE DEVRAIENT PAS utiliser ce terme sans inclure cette définition. Ce terme suggère une utilisation négligente de "signature numérique", qui est le terme normalisé par [I7498-2]. (Voir : signature électronique.)

$ attaque directe *(direct attack)*
(I) Voir : définition secondaire sous "attaque". (À comparer à : attaque indirecte.)

$ répertoire, Annuaire *(directory, Directory)*
1. (I) /en minuscules/ Se réfère de façon générique à un serveur de base de données ou autre système qui mémorise et fournit accès à des valeurs d'éléments de données descriptives ou opérationnelles qui sont associés aux composants d'un système. (À comparer à : dépôt.)
2. (N) /en majuscules/ Se réfère spécifiquement à l'Annuaire X.500. (Voir : DN, X.500.)

$ protocole d'accès à un répertoire (DAP, *Directory Access Protocol*)
(N) Protocole OSI [X519] pour la communication entre un agent d'utilisateur de répertoire (un type de client X.500) et un agent système de répertoire (un type de serveur X.500). (Voir : LDAP.)

$ plan de catastrophe *(disaster plan)*
(O) Synonyme de "plan de contingence".
Terme déconseillé : les IDOC NE DEVRAIENT PAS utiliser ce terme ; à la place, par cohérence et pour la neutralité du langage, les IDOC DEVRAIENT utiliser "plan de contingence".

$ divulgation *(disclosure)* Voir : divulgation non autorisée. À comparer à : exposition.

$ contrôle d'accès discrétionnaire *(discretionary access control)*
1a. (I) Service de contrôle d'accès qui (a) applique une politique de sécurité fondée sur l'identité des entités systèmes et les autorisations associées aux identités et (b) incorpore un concept de propriété dans lequel les droits d'accès pour une ressource système peuvent être accordés et révoqués par l'entité qui possède la ressource. (Voir : liste de contrôle d'accès, DAC, politique de sécurité fondée sur l'identité, contrôle d'accès obligatoire.)
Dérivation : ce service est appelé "discrétionnaire" parce qu'une entité peut se voir accorder des droits d'accès à une ressource tels que l'entité puisse par sa seule volonté permettre à d'autres entités d'accéder à la ressource.
1b. (O) /modèle formel/ "Moyen de restreindre l'accès à des objets sur la base de l'identité de sujets et/ou groupes auxquels ils appartiennent. Les contrôles sont discrétionnaires en ce sens qu'un sujet avec une certaine permission d'accès est capable de passer cette permission (peut-être indirectement) à tout autre sujet". [DoD1]

$ interruption *(disruption)*
(I) Circonstance ou événement qui interrompt ou empêche le fonctionnement correct de services et fonctions systèmes. (Voir : disponibilité, critique, intégrité système, conséquence de menace.)
Instructions : l'interruption est un type de conséquence de menace ; elle peut être causée par les types suivants d'actions de menace : incapacitation, corruption, et obstruction.

$ règles de codage distinctives (DER, *Distinguished Encoding Rules*)
(N) Sous ensemble des règles de codage de base qui ne fournit jamais qu'un seul moyen de coder une structure de données définie par ASN.1. [X690].
Instructions : pour une structure de données définie abstraitement en ASN.1, les BER fournissent souvent le codage de la structure dans une chaîne d'octets de plus d'une façon, de sorte que deux mises en œuvre distinctes de BER peuvent légitimement produire des chaînes d'octets différentes pour la même définition ASN.1. Cependant, certaines applications exigent que tous les codages d'une structure soient les mêmes, afin que les codages puissent être comparés en égalité. Donc, les DER sont utilisées dans des applications dans lesquelles un codage unique est nécessaire, comme lorsque une signature numérique est calculée sur une structure définie par l'ASN.1.

$ nom distinctif (DN, *distinguished name*)
(N) Identifiant qui représente de façon univoque un objet dans l'arborescence d'information de répertoire (DIT, *Directory Information Tree*) X.500 [X501]. (À comparer à : nom de domaine, identité, autorité de désignation.)
Instructions : un DN est un ensemble de valeurs d'attributs qui identifie le chemin conduisant de la base du DIT à l'objet qui est désigné. Un certificat de clé publique X.509 ou une CRL contient un DN qui identifie son producteur, et un certificat d'attribut X.509 contient un DN ou une autre forme de nom qui identifie son sujet.

$ attaque répartie *(distributed attack)*
1a. (I) Attaque qui est mise en œuvre avec une puissance de calcul répartie. (Voir : zombie.)
1b. (I) Attaque qui utilise de nombreux agents de menace.

$ service de sécurité par authentification répartie (DASS, *Distributed Authentication Security Service*)
(I) Protocole Internet expérimental [RFC1507] qui utilise des mécanismes cryptographiques pour fournir des services d'authentification mutuelle forts dans un environnement réparti.

$ puissance de calcul répartie *(distributed computing)*
(I) Technique qui disperse un seul ensemble de tâches logiquement en rapport parmi un groupe d'ordinateurs séparés géographiquement mais coopérants. (Voir : attaque répartie.)

$ point de distribution *(distribution point)*
(I) Entrée de répertoire X.500 ou d'autre source d'informations qui est désignée dans une extension de certificat de clé publique X.509 v3 comme localisation à partir de laquelle obtenir une CRL qui puisse énumérer les certificats.
Instructions : un certificat de clé publique X.509 v3 peut avoir une extension "cRLDistributionPoints" qui désigne les endroits où obtenir des CRL sur lesquelles le certificat peut être mentionné. (Voir : profil de certificat.) Une CRL obtenue d'un point de distribution peut (a) couvrir toutes les raisons pour lesquelles un certificat pourrait être révoqué ou seulement certaines des raisons, (b) être produit par l'autorité qui a signé le certificat ou par quelque autre autorité, et (c) contient des entrées de révocation pour seulement un sous ensemble de tous les certificats produits par une CA ou (d) contient des entrées de révocation pour plusieurs CA.

$ DoD (N) *(Department of Defense)* Ministère de la Défense
Usage : pour éviter l'incompréhension entrer les nations, les IDOC DEVRAIENT n'utiliser cette abréviation qu'avec un qualificatif national (par exemple, U.S. DoD).

$ domaine *(domain)*
1a. (I) /Sécurité générale/ Environnement ou contexte qui (a) inclut un ensemble de ressources systèmes et un ensemble d'entités systèmes qui ont le droit d'accéder aux ressources et (b) est usuellement défini par une politique de sécurité, un modèle de sécurité, ou une architecture de sécurité. (Voir : domaine de CA, domaine d'interprétation, périmètre de sécurité. À comparer à : COI, enclave.)
Instructions : une "interface contrôlée" ou "garde" est nécessaire pour transférer les informations entre les domaines réseau qui fonctionnent sous différentes politiques de sécurité.
1b. (O) /politique de sécurité/ Un ensemble d'utilisateurs, leurs objets d'informations, et une politique de sécurité commune. [DoD6], [SP33]
1c. (O) /politique de sécurité/ Un système ou collection de systèmes qui (a) appartient à une communauté d'intérêt qui met en œuvre une politique de sécurité cohérente et (b) est administré par une seule autorité.
2. (O) /COMPUSEC/ Un état de fonctionnement ou un mode d'un ensemble de matériels informatique.
Instructions : la plupart des ordinateurs ont au moins deux modes de fonctionnement du matériel [Gass] :
- Mode "privilégié : autrement dit, mode "exécutif", "maître", "système", "noyau", ou "superviseur". Dans ce mode, le logiciel peut exécuter toutes les instructions machine et accéder à toutes les localisations de mémorisation.
- Mode "non privilégié" : autrement dit mode "usager", "application", ou "problème". Dans ce mode, le logiciel est restreint à un sous ensemble des instructions et à un sous ensemble des localisations de mémorisation.

3. (O) "Une portée distincte au sein de certaines caractéristiques communes est exhibée et des règles communes sont observées." [CORBA]
4. (O) /MISSI/ Le domaine d'une CA MISSI est l'ensemble d'utilisateurs MISSI dont les certificats sont signés par la CA.
5. (I) /Internet/ Partie de l'espace de noms structuré en arborescence du DNS qui est en dessous du nom qui spécifie le domaine. Un domaine est un sous domaine d'un autre domaine si il est contenu dans ce domaine. Par exemple, D.C.B.A est un sous domaine de C.B.A
6. (O) /OSI/ Partition administrative d'un système OSI réparti complexe.

$ Messagerie à domaine identifié par des clés (DKIM, *Domain Keys Identified Mail*)
(I) Protocole, qui est spécifié par le groupe de travail de même nom de l'IETF, pour assurer l'intégrité des données et l'authentification d'origine des données au niveau domaine (voir : DNS, nom de domaine) pour les messages de la messagerie Internet . (À comparer à : PEM.)
Instructions : DKIM emploie une cryptographie asymétrique pour créer une signature numérique pour un corps de message de messagerie Internet et des en-têtes choisis (voir la RFC1822) et la signature est ensuite portée dans un en-tête du message. Un receveur du message peut vérifier la signature et par là, authentifier l'identité du domaine d'origine et l'intégrité du contenu signé, en utilisant une clé publique appartenant au domaine. La clé peut être obtenue du DNS.

$ nom de domaine *(domain name)*
(I) Style d'identifiant qui est défini pour des sous arborescences dans le DNS Internet -- c'est-à-dire, une séquence d'étiquettes ASCII insensibles à la casse séparées par des points (par exemple, "bbn.com") – et qui est aussi utilisé dans d'autres types d'identifiants Internet, tels que des noms d'hôte (par exemple, "rosslyn.bbn.com"), des noms de boîtes aux lettres (par exemple, "rshirey@bbn.com") et des URL (par exemple, "http://www.rosslyn.bbn.com/foo"). (Voir : domaine. À comparer à : DN.)
Instructions : l'espace de noms du DNS est une structure arborescente dans laquelle chaque nœud et feuille détient des enregistrements qui décrivent une ressource. Chaque nœud a une étiquette. Le nom de domaine d'un nœud est la liste des étiquettes sur le chemin du nœud à la racine de l'arborescence. Les étiquettes dans un nom de domaine sont imprimées ou lues de gauche à droite, du plus spécifique (le plus bas, le plus éloigné de la racine) au moins spécifique (le plus haut, plus proche de la racine) mais l'étiquette de la racine est la chaîne nulle. (Voir : code de pays.)

$ système des noms de domaine (DNS, *Domain Name System*)
(I) Principale base de données des opérations de l'Internet, qui est répartie dans une collection de serveurs et utilisée par les logiciels clients pour des besoins tels que (a) de traduire un nom d'hôte de style nom de domaine en une adresse IP (par exemple, "rosslyn.bbn.com" se traduit en "192.1.7.10") et (b) de localiser un hôte qui accepte des messages pour une certaine adresse de boîte aux lettres. [RFC1034] (Voir : nom de domaine.)
Instructions : Le DNS a trois composants majeurs :
- Espace de noms de domaines et enregistrements de ressource : spécifications de l'espace de noms de domaines structuré en arborescence, et les données associées aux noms.
- Serveurs de noms : programmes qui détiennent les informations sur un sous ensemble de la structure de l'arborescence et détiennent des données, et détiennent aussi des pointeurs sur d'autres serveurs de noms qui peuvent fournir des informations provenant de toute partie de l'arborescence.
- Résolveurs : programmes qui extraient les informations des serveurs de noms en réponse aux demandes des clients ; normalement, des sous programmes système directement accessibles aux programmes utilisateurs.

Les extensions au DNS [RFC4033], [RFC4034], [RFC4035] prennent en charge (a) la distribution de clé pour les clés publiques nécessaires pour le DNS et pour d'autres protocoles, (b) le service d'authentification d'origine des données et le service d'intégrité des données pour les enregistrements de ressource, (c) le service d'authentification d'origine des données pour les transactions entre résolveurs et serveurs, et (d) le contrôle d'accès des enregistrements.

$ domaine d'interprétation (DOI, *domain of interpretation*)
(I) /IPsec/ Un DOI pour ISAKMP ou IKE définit des formats de charge utile, des types d'échange, et des conventions pour désigner des informations en rapport avec la sécurité, telles que les politiques de sécurité ou les algorithmes et modes de chiffrement . Exemple : voir la [RFC2407].
Dérivation : le concept de DOI se fonde sur les travaux du groupe de travail CIPSO de TSIG.

$ dominer *(dominate)*
(I) Le niveau de sécurité A est dit "dominer" le niveau de sécurité B si le niveau de classification (hiérarchique) de A est supérieur (plus haut) à, ou égal à celui de B, et si les catégories de A (non hiérarchiques) incluent (comme sous ensemble) toutes les catégories de B. (Voir : treillis, modèle en treillis.)

$ boîtier de protection *(dongle)*
(I) Appareil usuellement électronique, portable, physique, qui doit être rattaché à un ordinateur pour permettre le fonctionnement d'un logiciel particulier. (Voir : jeton.)

Instructions : un boîtier de protection est essentiellement une clé physique utilisée pour la protection de logiciels contre la copie ; c'est-à-dire que le programme ne va pas fonctionner si le boîtier de protection correspondant n'est pas rattaché. Lorsque le logiciel fonctionne, il interroge périodiquement le boîtier de protection et s'arrête si le boîtier ne répond pas avec les informations d'authentification appropriées. Les boîtiers de protection ont été à l'origine construits comme une mémoire programmable en lecture seule écrasable (EPROM, *erasable programmable read-only memory*) à connecter à un accès entrée/sortie en série d'un ordinateur personnel.

$ dégrader *(downgrade)*
(I) /sécurité des données/ Réduire le niveau de sécurité de données (en particulier le niveau de classification) sans changer le contenu d'information des données. (À comparer à : mettre à niveau.)

$ attaque en dégradation *(downgrade attack)*
(I) Type d'attaque par interposition dans laquelle l'attaquant peut causer l'accord de deux parties, au moment où elles négocient une association de sécurité, sur un niveau de protection inférieur au niveau le plus élevé qui aurait pu avoir été pris en charge par l'une et l'autre. (À comparer à : dégrader.)

$ projet de RFC *(draft RFC)*
(D) Version préliminaire, temporaire d'un document qui est destiné à devenir une RFC. (À comparer à : projet Internet.)
Terme déconseillé : les IDOC NE DEVRAIENT PAS utiliser ce terme. La série des RFC est archivée par nature et consiste seulement en documents de forme permanente. Un document qui est destiné à devenir une RFC a normalement besoin d'être d'abord publié comme projet Internet (RFC2026). (Voir : "projet de normes" sous "Norme Internet".)

$ projet de norme *(Draft Standard)* (I) Voir : définition secondaire sous "Norme Internet".

$ contrôle duel *(dual control)*
(I) Procédure qui utilise deux entités (généralement des personnes) ou plus, fonctionnant de concert pour protéger une ressource système, telle qu'une entité agissant seule ne puisse pas accéder à la ressource. (Voir : zone d'accompagnement obligatoire, séparation des tâches, savoir partagé.)

$ signature duelle *(dual signature)*
(O) /SET/ Signature numérique unique qui protège deux messages distincts en incluant le résultat haché pour les deux ensembles dans une seule valeur chiffrée. [SET2]
Utilisation déconseillée : les IDOC NE DEVRAIENT PAS utiliser ce terme sauf lorsque qualifié comme "signature duelle SET(marque déposée)" avec cette définition.
Instructions : généré par le hachage séparé de chaque message, enchaînement des deux résultats de hachage, puis hachage de la valeur obtenue et chiffrement du résulta avec la clé privée du signataire. Fait pour réduire le nombre d'opérations de chiffrement pour permettre la vérification de l'intégrité des données sans divulgation complète des données.

$ certificat à double utilisation *(dual-use certificate)*
(O) Certificat qui est destiné à être utilisé à la fois avec une signature numérique et des services de chiffrement des données. [SP32]
Usage : les IDOC qui utilisent ce terme DEVRAIENT en déclarer une définition en identifiant les utilisations prévues du certificat, parce qu'il y a plus que juste ces deux utilisations mentionnées dans la publication du NIST. Un certificat de clé publique X.509 v3 peut avoir une extension "usage de clé", qui indique les objets pour lesquels la clé publique peut être utilisée. (Voir : profil de certificat.)

$ service *(duty)*
(I) Attribut d'un rôle qui oblige une entité qui joue le rôle à effectuer une ou plusieurs tâches, qui sont habituellement essentielles pour le fonctionnement du système. [Sand] (Comparer à autorisation, privilège. Voir : rôle, billet.)

$ monnaie électronique *(e-cash)*
(O) Monnaie électronique ; monnaie qui est sous la forme de données et peut être utilisée comme mécanisme de payement sur l'Internet. (Voir : IOTP.)
Usage : les IDOC qui utilisent ce terme DEVRAIENT en déclarer une définition parce que de nombreux types différents de monnaie électronique peuvent avoir été conçus avec une grande variété de mécanismes de sécurité.

$ œuf de Paques *(Easter egg)*
(O) "Fonctionnalité cachée au sein d'un programme d'application, qui est activée lorsque sont entrées un ensemble de commandes et de touches non documentées, et souvent cachées. Les œufs de Paques sont normalement utilisés pour afficher les crédits pour l'équipe de développement et sont destinés à être non menaçants" [SP28], mais les œufs de Paques peuvent contenir du code malveillant.

Utilisation déconseillée : il est vraisemblable que d'autres cultures utilisent des métaphores différentes pour ce concept. Donc, pour éviter l'incompréhension entre les nations, les IDOC NE DEVRAIENT PAS utiliser ce terme. (Voir : Usage déconseillé sous "Livre Vert".)

$ espionnage *(eavesdropping)*
(I) Écoute passive faite secrètement, c'est-à-dire, à l'insu de l'origine ou des receveurs prévus de la communication.

$ économie d'alternatives *(economy of alternatives)*
(I) Principe qu'un mécanisme de sécurité devrait être conçu pour minimiser le nombre des façons alternatives de réaliser un service. (À comparer à : économie de mécanisme.)

$ économie de mécanisme *(economy of mechanism)*
(I) Principe qu'un mécanisme de sécurité devrait être conçu pour être aussi simple que possible, afin que (a) le mécanisme puisse être correctement mis en œuvre et (b) il puisse être vérifié que le fonctionnement du mécanisme applique la politique de sécurité du système. (À comparer à : économie d'alternatives, moindre privilège.)

$ EDIFACT (N) Voir : définition secondaire sous "échange de données électroniques".

$ EE
(D) Abréviation de "entité d'extrémité *(end entity)*" et d'autres termes.
Abréviation déconseillée : les IDOC NE DEVRAIENT PAS utiliser cette abréviation ; il pourrait y avoir confusion entre "entité d'extrémité", "chiffrement de bout en bout", "norme de récupération de chiffrement", et d'autres termes.

$ longueur effective de clé *(effective key length)*
(O) "Mesure de la force d'un algorithme de chiffrement, sans considération de la longueur réelle de la clé." [IATF] (Voir : facteur de travail.)

$ efficacité *(effectiveness)*
(O) /ITSEC/ Propriété d'un TOE représentant comment il fournit la sécurité dans le contexte de son utilisation opérationnelle réelle ou proposée.

$ Algorithme de El Gamal *(El Gamal algorithm)*
(N) Algorithme de chiffrement asymétrique, inventé en 1985 par Taher El Gamal, qui se fonde sur la difficulté de calculer des logarithmes discrets et peut être utilisé aussi bien pour le chiffrement que les signatures numériques. [ElGa]

$ livre de code électronique (ECB, *electronic codebook*)
(N) Mode de chiffrement de bloc dans lequel un bloc de texte source est utilisé directement comme entrées dans l'algorithme de chiffrement et où le bloc de sortie résultant est utilisé directement comme texte chiffré [FP081]. (Voir : chiffrement de bloc, [SP38A].)

$ commerce électronique *(electronic commerce)*
1. (I) Affaires menées par des échanges d'informations sans papier, utilisant un échange de données électronique, un transfert de fonds électronique (EFT, *electronic funds transfer*), la messagerie électronique, des babillards électroniques d'ordinateur *(computer bulletin board)*, la télécopie, et d'autres technologies sans papier.
2. (O) /SET/ "Les échange de biens et de services pour un payement entre le détenteur de carte et le marchand lorsque tout ou partie de la transaction est effectué via une communication électronique." [SET2]

$ échange de données électroniques (EDI, *electronic data interchange*)
(I) Échange d'ordinateur à ordinateur, entre des partenaires commerciaux, de données d'affaires sous des formats de document normalisés.
Instructions : les formats d'EDI ont été normalisés principalement par la norme ANSI X12 et par EDIFACT (EDI pour l'administration, le commerce, et le transport), qui est une norme internationale sous le patronage des Nations Unies, principalement utilisée en Europe et en Asie. X12 et EDIFACT se sont alignées pour créer une seule norme d'EDI mondiale.

$ système de gestion de clé électronique (EKMS, *Electronic Key Management System*)
(O) "Collection interopérable de systèmes développée par ... le gouvernement des USA pour automatiser la planification, le rangement, la génération, la distribution, le stockage, le remplissage, l'utilisation, et la destruction des matériaux de clé électronique et la gestion des autres types de matériel COMSEC." [C4009]

$ signature électronique *(electronic signature)*
(D) Synonyme de "signature numérique" ou "signature numérisée".
Terme déconseillé : les IDOC NE DEVRAIENT PAS utiliser ce terme ; il n'y a actuellement pas de consensus sur sa définition. À la place, utiliser "signature numérique", si c'est ce dont il s'agit.

$ mallette électronique *(electronic wallet)*
(D) Conteneur sécurisé pour détenir, sous forme numérisée, des objets de données sensibles qui appartiennent au propriétaire, comme de la monnaie électronique, du matériel d'authentification, et divers types d'informations personnelles. (Voir : IOTP.)
Terme déconseillé : les IDOC NE DEVRAIENT PAS utiliser ce terme. Il n'y a actuellement pas de consensus sur sa définition ; et certaines utilisations et définitions peuvent être protégées. Les significations vont de mallettes virtuelles mises en œuvre par des structures de données à des mallettes physiques mises en œuvre par des jetons cryptographiques. (Voir : Utilisation déconseillée sous "Livre Vert".)

$ cryptographie à courbe elliptique (ECC, *elliptic curve cryptography*)
(I) Type de cryptographie asymétrique fondée sur la mathématique des groupes qui sont définis par les points d'une courbe, où la courbe est définie par une équation quadratique dans un champ fini. [Schn]
Instructions : ECC se fonde sur des mathématiques différentes de celles utilisées à l'origine pour définir l'algorithme de Diffie-Hellman-Merkle et le DSA, mais ECC peut être utilisé pour définir un algorithme pour l'accord de clés qui est analogue du Diffie-Hellman-Merkle [A9063] et un algorithme pour la signature numérique qui est analogue au DSA [A9062]. Le problème mathématique sur lequel se fonde ECC est estimé être plus difficile que le problème sur lequel est fondé Diffie-Hellman-Merkle, et donc que les clés pour ECC peuvent être plus courtes pour un niveau de sécurité comparable. (Voir : ECDSA.)

$ algorithme de signature numérique à courbe elliptique (ECDSA, *Elliptic Curve Digital Signature Algorithm*)
(N) Norme [A9062] qui est analogue, dans la cryptographie à courbe elliptique, à l'algorithme de signature numérique.

$ émanation *(emanation)*
(I) Signal (par exemple, électromagnétique ou acoustique) qui est émis par un système (par exemple, par radiation ou conductivité) comme conséquence (c'est-à-dire, sous produit) du fonctionnement du système, et qui peut contenir des informations. (Voir : sécurité des émanations.)

$ analyse des émanations *(emanations analysis)*
(I) /action de menace/ Voir : définition secondaire sous "interception".

$ sécurité des émanations (EMSEC, *emanations security*)
(I) Menaces de sécurité physique pour protéger contre la compromission des données qui pourrait survenir à cause des émanations qui pourraient être reçues et lues par un tiers non autorisé. (Voir : émanation, TEMPEST.)
Usage : se réfère soit à empêcher ou limiter les émanations provenant d'un système, soit à empêcher ou limiter la capacité de tiers non autorisés à recevoir les émissions.

$ cryptographie incorporée *(embedded cryptography)*
(N) "Cryptographie introduite dans un équipement ou système dont la fonction de base n'est pas cryptographique." [C4009]

$ plan d'urgence *(emergency plan)*
(D) Synonyme de "plan de contingence".
Terme déconseillé : les IDOC NE DEVRAIENT PAS utiliser ce terme. À la place, pour la neutralité et la cohérence du langage, utiliser "plan de contingence".

$ réponse d'urgence *(emergency response)*
(O) Une réponse d'urgence à un feu, une inondation, un mouvement civil, un désastre naturel, une menace d'explosion, ou autre situation sérieuse, avec l'intention de protéger des vies, de limiter les dommages aux propriétés, et minimiser l'interruption du fonctionnement du système. [FP087] (Voir : disponibilité, CERT, plan d'urgence.)

$ EMV
(N) Abréviation de "Europay, MasterCard, Visa". Se réfère à une spécification de cartes à mémoire qui sont utilisées comme cartes de payement, et pour les terminaux et applications en rapport. [EMV1], [EMV2], [EMV3]

$ encapsulation de charge utile de sécurité (ESP, *Encapsulating Security Payload*)
(I) Protocole Internet [RFC2406], [RFC4303] conçu pour fournir un service de confidentialité des données et d'autres

services de sécurité pour les datagrammes IP. (Voir : IPsec. À comparer à : AH.)
Instructions : ESP peut être utilisé seul, ou combiné avec AH, ou incorporé avec le tunnelage. Les services de sécurité peuvent être fournis entre une paire d'hôtes communicants, entre une paire de passerelles de sécurité communicantes, ou entre un hôte et une passerelle. L'en-tête ESP est encapsulé par l'en-tête IP, et l'en-tête ESP encapsule soit l'en-tête de protocole de couche supérieure (mode transport) soit un en-tête IP (mode tunnel). ESP peut fournir des services de confidentialité des données, un service d'authentification d'origine des données, un service d'intégrité des données sans connexion, un service d'anti répétition, et la confidentialité limitée de flux de trafic. L'ensemble des services dépend du placement de la mise en œuvre et des options choisies lorsque l'association de sécurité est établie.

$ enclave
1. (I) Ensemble de ressources système qui fonctionnent dans le même domaine de sécurité et qui partagent la protection d'un seul périmètre de sécurité commun, continu. (À comparer à : domaine.)
2. (D) /Gouvernement des USA/ "Collection d'environnements de calcul connectés par un ou plusieurs réseaux internes sous le contrôle d'une seule autorité et politique de sécurité, incluant la sécurité personnelle et physique." [C4009]

Définition déconseillée : les IDOC NE DEVRAIENT PAS utiliser ce terme avec la définition 2 parce que cette définition s'applique à ce qui est habituellement appelé un "domaine de sécurité". C'est-à-dire, un domaine de sécurité est un ensemble d'une ou plusieurs enclaves de sécurité.

$ coder *(encode)*
1. (I) Utiliser un système de symboles pour représenter des informations, qui peuvent avoir originellement une autre représentation. Exemple : code Morse. (Voir : ASCII, BER.) (Voir : coder, décoder.)
2. (D) Synonyme de "chiffrer".

Définition déconseillée : les IDOC NE DEVRAIENT PAS utiliser ce terme comme synonyme de "chiffrer" ; coder n'est pas toujours destiné à dissimuler la signification.

$ chiffrer *(encrypt)*
(I) Transformer cryptographiquement des données pour produire un texte chiffré. (Voir : chiffrement. À comparer à : sceau.)

$ encryptage *(encryption)*
1. (I) Transformation cryptographique de données (appelées "texte source") sous une forme différente (appelée "texte chiffré") qui dissimule la signification originale des données et empêche la forme originale d'être utilisée. Le processus inverse correspondant est "décryptage", une transformation qui restaure les données chiffrées dans leur forme d'origine. (Voir : cryptographie.)
2. (O) "La transformation cryptographique de données pour produire le texte chiffré." [I7498-2]

Usage : pour ce concept, les IDOC DEVRAIENT utiliser le verbe "chiffrer" (et les variations en rapport : chiffrement, déchiffrement, et déchiffrage). Cependant, à cause des biais culturels impliquant la sépulture humaine, certains documents internationaux (en particulier les normes ISO et du CCITT) évitent "encrypter" et à la place utilisent le verbe "chiffrer" (et les variations en rapport : chiffrement, déchiffrement, déchiffrage).
Instructions : usuellement, l'entrée du texte source d'une opération de chiffrement est du texte en clair. Mais dans certains cas, le texte en clair peut être du texte chiffré qui est le résultat d'une autre opération de chiffrement. (Voir : super chiffrement.)
Encryptage et décryptage impliquent un algorithme mathématique pour la transformation des données. À côté des données à transformer, l'algorithme a une ou plusieurs entrées qui sont des paramètres de contrôle : (a) une clé qui change la transformation et, dans certains cas, (b) un IV qui établit l'état de début de l'algorithme.

$ certificat de chiffrement *(encryption certificate)*
(I) Certificat de clé publique qui contient une clé publique qui est destinée à être utilisée pour chiffrer les données, plutôt que pour vérifier les signatures numériques ou effectuer d'autres fonctions cryptographiques.
Instructions : un certificat de clé publique X.509 v3 peut avoir une extension "keyUsage" qui indique l'objet pour lequel est destinée la clé publique certifiée. (Voir : profil de certificat.)

$ unité cryptographique terminale (ECU, *end cryptographic unit*)
1. (N) Appareil de destination finale dans lequel une clé est chargée pour être utilisée dans le fonctionnement.
2. (N) Appareil qui (a) effectue des fonctions cryptographiques, (b) fait normalement partie d'un plus grand système pour lequel l'appareil fournit des services de sécurité, et (c) est le plus bas niveau de composant identifiable du point de vue de l'infrastructure de sécurité de prise en charge, comme un système de gestion de clé, avec lequel une transaction de gestion peut être effectuée.

$ entité d'extrémité *(end entity)*
1. (I) Entité système qui fait l'objet d'un certificat de clé publique et qui utilise, ou a la permission et est capable d'utiliser, la

clé privée correspondante pour des besoins autres que la signature d'un certificat numérique ; c'est-à-dire, une entité qui n'est pas une CA.

2. (O) "Sujet de certificat [qui] utilise sa clé publique pour des besoins autres que de signer des certificats." [X509]

Définition déconseillée : les IDOC NE DEVRAIENT PAS utiliser la définition 2, qui est trompeuse et incomplète. D'abord, cette définition aurait dû dire "clé privée" plutôt que "clé publique" parce que les certificats ne sont utilement signés qu'avec une clé publique. Ensuite, la définition de X.509 est ambiguë en ce qui concerne la possibilité qu'une entité d'extrémité utilise ou non la clé privée pour signer un certificat, c'est-à-dire, si le sujet peut être une CA. L'intention des auteurs de la Recommandation UIT-T X.509 était qu'un certificat d'entité d'extrémité ne soit pas valide pour être utilisé à la vérification d'une signature sur un certificat X.509 ou une CRL X.509. Donc, il aurait été préférable que la définition de X.509 dise "seulement pour un objet autre que de signer des certificats".

Usage : en dépit des problèmes de la définition de X.509, le terme lui-même est utile pour décrire des applications de cryptographie asymétrique. La façon dont le terme est utilisé dans X.509 implique qu'il était destiné à être défini, comme nous l'avons fait ici, par rapport aux rôles que joue une entité (qui est associée à un système d'extrémité OSI) ou qu'il lui est permis de jouer dans les applications de cryptographie asymétrique autres que PKI que prennent en charge les applications.

Instructions : qu'un sujet puisse jouer les deux rôles de CA et de non CA, avec les mêmes certificats ou des certificats différents, est une affaire de politique. (Voir : CPS.) Un certificat de clé publique X.509 v3 peut avoir une extension "basicConstraints" contenant une valeur de "cA" qui "indique spécifiquement si la clé publique peut ou non être utilisée pour vérifier les signatures de certificat". (Voir : profil de certificat.)

$ système d'extrémité *(end system)*

(N) /OSIRM/ Ordinateur qui met en œuvre toutes les sept couches de l'OSIRM et peut se rattacher à un sous réseau. Usage : Dans le contexte IPS, un système d'extrémité est appelé un "hôte".

$ chiffrement de bout en bout *(end-to-end encryption)*

(I) Protection continue des données qui s'écoulent entre deux points d'un réseau, effectué par le chiffrement des données lorsque elles quittent leur source, en les gardant chiffrées pendant qu'elles passent à travers tout ordinateur intermédiaire (comme des routeurs) et en ne les déchiffrant que lorsque elles arrivent à la destination finale prévue. (Voir : mise sur écoute. À comparer à : chiffrement de liaison.)

Exemples : on peut citer BLACKER, CANEWARE, IPLI, IPsec, PLI, SDNS, SILS, SSH, SSL, TLS.

Instructions : lorsque deux points sont séparés par plusieurs liaisons de communication qui sont connectées par un ou plusieurs relais intermédiaires, le chiffrement de bout en bout permet aux systèmes de source et de destination de protéger leurs communications sans dépendre des systèmes intermédiaires pour fournir la protection.

$ système d'utilisateur d'extrémité *(end user system)*

1. (I) /système d'information/ Entité système, usuellement un individu, qui utilise les ressources système, principalement pour des besoins d'application, par opposition à des besoins de gestion.
2. (D) /PKI/ Synonyme de "entité d'extrémité".

Définition déconseillée : les IDOC NE DEVRAIENT PAS utiliser "utilisateur d'extrémité" comme synonyme de "entité d'extrémité", parce que cela mélangerait les concepts d'une façon potentiellement trompeuse.

$ élément cryptographique approuvé pour données non classifiées (EUCI, *endorsed-for-unclassified cryptographic item*)

(O) /Gouvernement des USA/ "Équipement cryptographique non classifié qui incorpore une logique cryptographique classifiée par le gouvernement des USA et est approuvé par la NSA pour la protection des informations touchant à la sécurité nationale." [C4009] (À comparer à : CCI, produit de type 2.)

$ entité *(entity)* Voir : entité système.

$ chausse-trappe *(entrapment)*

(I) "Implantation délibérée de fautes apparentes dans un système afin de détecter des tentatives de pénétrations ou de perturber un intrus quant aux fautes à exploiter." [FP039] (Voir : pot de miel.)

$ entropie *(entropy)*

1. (I) Dans la théorie de l'information, mesure (normalement présentée comme un nombre de bits) de la quantité d'incertitude qu'un attaquant doit surmonter pour déterminer la valeur d'un secret. [SP63] (Voir : force.)

Exemple : Si un mot de passe est dit contenir au moins 20 bits d'entropie, cela signifie qu'il doit être aussi dur de trouver le mot de passe que de deviner un nombre aléatoire de 20 bits.

2. (I) Mesure de la théorie de l'information (normalement présentée comme un nombre de bits) de la quantité d'information dans un message; c'est-à-dire, le nombre minimum de bits nécessaire pour coder toutes les significations possibles de ce message. [Schn] (Voir : incertitude.)

$ éphémère *(ephemeral)*

(I) /adjectif/ Se réfère à une clé de chiffrement ou autre paramètre cryptographique ou objet de données de durée de vie limitée, temporaire, ou à utilisation unique. (Voir : clé de session. À comparer à : statique.)

$ écraser *(erase)*
1. (I) Supprimer des données mémorisées. (Voir : apurer, mettre à zéro.)
2. (O) /Gouvernement des USA/ Supprimer des données magnétiques mémorisées de telle sorte que les données ne puissent pas être récupérées par des moyens ordinaires, mais pourraient être recouvrables par des méthodes de laboratoire. [C4009] (À comparer à : /Gouvernement des USA/ purge.)

$ code de détection d'erreur *(error detection code)*
(I) Somme de contrôle conçue pour détecter, mais pas corriger, des changements accidentels (c'est-à-dire, non intentionnels) des données.

$ norme de récupération de chiffrement (EES, *Escrowed Encryption Standard*)
(N) Norme du gouvernement des USA [FP185] qui spécifie comment utiliser un algorithme de chiffrement symétrique (SKIPJACK) et créer un champ d'accès pour l'application de la loi (LEAF, *Law Enforcement Access Field*) pour mettre en œuvre une partie d'un système de tiers de confiance qui permet le déchiffrement de télécommunications lorsque l'interception est légale.
Instructions : SKIPJACK et le LEAF sont tous deux destinés à être utilisés dans les équipements de chiffrement et déchiffrement de données sensibles non classifiées de télécommunications.

$ Estelle
(N) Langage (ISO 9074-1989) pour la spécification formelle de protocoles de réseau informatique.

$ Institut européen des normes de télécommunications (ETSI, *European Telecommunication Standards Institute*)
(N) Organisation indépendante, à but non lucratif, installée en France, qui est reconnue officiellement par la Commission Européenne et est chargée de la normalisation des technologies de l'information et de la communication en Europe.
Instructions : ETSI établit les normes pour un certain nombre d'algorithmes de sécurité, incluant des algorithmes de chiffrement pour les systèmes de téléphonie mobile en Europe.

$ système évalué *(evaluated system)*
(I) Système qui a été évalué par rapport à des critères de sécurité (par exemple, le TCSEC, ou un profil fondé sur les critères communs).

$ évaluation *(evaluation)*
(I) Confrontation d'un système d'informations à des critères de sécurité définis (par exemple, le TCSEC ou un profil fondé sur les critères communs). (À comparer à : certification.)

$ niveau d'assurance d'évaluation (EAL, *evaluation assurance level*)
(N) Paquetage prédéfini de composants d'assurance qui représente un point sur l'échelle des critères communs pour étalonner la confiance dans la sécurité des produits et systèmes des technologies de l'information.
Instructions : les critères communs définissent une échelle de sept EAL hiérarchiquement ordonnés pour étalonner un TOE. Du plus élevé au plus faible, ce sont :
- EAL7. Conception formellement vérifiée et essayée.
- EAL6. Conception vérifiée et essayée de façon semi formelle.
- EAL5. Conçue et essayée de façon semi formelle.
- EAL4. Conçue, essayée et révisée de façon méthodique.
- EAL3. Essayée et vérifiée de façon méthodique.
- EAL2. Essayée structurellement.
- EAL1. Essayée fonctionnellement.

Un EAL est un ensemble cohérent d'exigences de base. L'augmentation de l'assurance d'un EAL à l'autre est réalisée en substituant des composants d'assurance plus élevés (c'est-à-dire, des critères de rigueur, portée ou profondeur croissants) à partir de sept classes d'assurance : (a) gestion de configuration, (b) livraison et fonctionnement, (c) développement, (d) documents explicatifs, (e) prise en charge du cycle de vie, (f) essais, et (g) établissement des faiblesses.
Les EAL ont été développés dans le but de préserver les concepts d'assurance qui ont été adoptés de critères antérieurs, de façon que les résultats des évaluations précédentes restent pertinents. Par exemple, les niveaux d'EAL 2 à 7 sont généralement équivalents aux portions d'assurance de l'échelle TCSEC C2-A1. Cependant, cette équivalence devrait être utilisée avec précaution. Les niveaux ne donnent pas l'assurance de la même manière, et une transposition exacte n'existe pas.

$ expire

(I) /accréditif/ Cesse d'être valide (c'est-à-dire, passe de l'état valide à l'état invalide) parce que la durée de vie qui lui a été allouée a été atteinte. (Voir : expiration de certificat.)

$ exposition *(exposure)*
(I) Type d'action de menace par laquelle des données sensibles sont directement livrées à une entité non autorisée. (Voir : divulgation non autorisée.)
Usage : Ce type d'action de menace inclut les sous-types suivants :
- "exposition délibérée" : livraison intentionnelle de données sensibles à une entité non autorisée.
- "fouillage de poubelle" : chercher dans des résidus de données dans un système pour obtenir une connaissance non autorisée de données sensibles.
- "erreur humaine" : /exposition/ Action ou inaction humaine qui résulte involontairement en ce qu'une entité obtienne une connaissance non autorisée de données sensibles. (À comparer à : corruption, incapacitation.)
- "erreur de matériel ou logiciel" : /exposition/ Échec d'un système qui résulte involontairement en ce qu'une entité obtienne la connaissance non autorisée de données sensibles. (À comparer à : corruption, incapacitation.)

$ option de sécurité étendue *(Extended Security Option)* (I) Voir : définition secondaire sous "IPSO".

$ protocole d'authentification extensible (EAP, *Extensible Authentication Protocol*)
(I) Cadre d'extension pour PPP qui prend en charge plusieurs mécanismes d'authentification facultatifs, incluant les mots de passe en clair, la mise au défi - réponse, et des séquences de dialogue arbitraires. [RFC3748] (À comparer à : GSS-API, SASL.)
Instructions : EAP fonctionne normalement directement sur des protocoles de liaison de données IPS ou des protocoles OSIRM de couche 2, c'est-à-dire, sans exiger IP. À l'origine, EAP a été développé pour être utilisé dans PPP, par un hôte ou un routeur qui se connecte à un serveur réseau via des circuits commutés ou des lignes à numérotation. Aujourd'hui, le domaine d'applicabilité des EAP inclut d'autres zones de contrôle d'accès réseau ; il est utilisé dans des LAN filaires et sans fils avec IEEE 802.1X, et dans IPsec avec IKEv2. EAP est conceptuellement en rapport avec d'autres cadres de mécanisme d'authentification, tels que SASL et GSS-API.

$ langage de balisage extensible (XML, *Extensible Markup Language*)
(N) Version de la norme de langage de balisage généralisé (ISO 8879) qui représente séparément le contenu d'un document et sa structure. XML a été conçu par le W3C pour être utilisé sur la Toile mondiale.

$ extension
(I) /protocole/ Élément de données ou mécanisme défini dans un protocole pour étendre les fonctions de base ou d'origine du protocole.
Instructions : de nombreux protocoles ont des mécanismes d'extension, et l'utilisation de ces extensions est habituellement facultative. IP et X.509 sont deux exemples de protocoles qui ont des extensions facultatives. Dans IP version 4, les extensions sont appelées des "options", et certaines des options ont un objet de sécurité (voir : IPSO).
Dans X.509, les formats de certificat et de CRL peuvent être étendus pour fournir des méthodes pour associer des attributs supplémentaires à des sujets et des clé publiques et pour gérer une hiérarchie de certification :
- Une "extension de certificat" : X.509 définit des extensions standard qui peuvent être incluses dans des certificats v3 pour fournir des informations supplémentaires de clés et de politique de sécurité, de sujet et d'attributs du producteur, et des contraintes du chemin de certification.
- Une "extension de CRL" : X.509 définit des extensions qui peuvent être incluses dans des CRL v2 pour fournir des informations supplémentaires sur le producteur de clé, son nom, les raisons et les contraintes de la révocation, et des informations sur les points de distribution et les CRL delta.
- Une "extension privée" : des extensions supplémentaires, chacune désignée par un OID, peuvent être définies localement comme nécessaire pour les applications ou des communautés. (Voir : extension d'accès aux informations d'autorité, extensions privées SET.)

$ contrôles externes *(external controls)*
(I) /COMPUSEC/ Se réfère à la sécurité administrative, à la sécurité personnelle, et à la sécurité physique. (À comparer à : contrôles internes.)

$ extranet
(I) Réseau informatique qu'utilise une organisation pour le trafic de données d'application entre l'organisation et ses partenaires commerciaux. (À comparer à : intranet.)
Instructions : un extranet peut être mis en œuvre de façon sécurisée, soit sur l'Internet, soit en utilisant la technologie Internet, en construisant l'extranet comme un VPN.

$ résistance à l'extraction *(extraction resistance)*

(O) Capacité d'un équipement cryptographique à résister aux efforts pour extraire le matériel de chiffrement directement de l'équipement (par opposition à l'acquisition de la connaissance du matériel de chiffrement par cryptanalyse). [C4009]

$ détection d'extrusion *(extrusion detection)*
(I) Surveillance des transferts non autorisés d'informations sensibles et autres communications qui ont leur origine à l'intérieur du périmètre de sécurité d'un système et sont dirigés vers l'extérieur ; c'est-à-dire, en gros l'opposé de la "détection d'intrusion".

$ à l'épreuve de l'échec *(fail-safe)*
1. (I) Synonyme de "sécurisé contre l'échec".
2. (I) Mode de terminaison des fonctions système qui empêche les dommages à des ressources système et des entités système spécifiées (c'est-à-dire, des données, des propriétés et une durée de vie spécifiées) lorsque survient ou qu'est détecté un échec dans le système (mais la défaillance peut quand même causer une compromission de la sécurité). (Voir : contrôle de défaillance.)

Instructions : Les définitions 1 et 2 opposent des conceptions différentes. Donc, les IDOC NE DEVRAIENT PAS utiliser ce terme sans en fournir une définition. Si la définition 1 est voulue, les IDOC peuvent éviter l'ambiguïté en utilisant "sécurisé contre l'échec" à la place.

$ sécurisé contre l'échec *(fail-secure)*
(I) Mode de terminaison des fonctions d'un système qui empêche la perte de l'état sûr lorsque survient ou qu'est détectée une défaillance dans le système (mais la défaillance peut quand même causer des dommages à certaines ressources système ou entités systèmes). (Voir : contrôle de défaillance. À comparer à : à l'épreuve de l'échec.)

$ échec en douceur *(fail-soft)*
(I) Terminaison sélective de fonctions système affectées, non essentielles, lorsque survient ou qu'est détectée une défaillance dans le système. (Voir : contrôle d'échec.)

$ contrôle d'échec *(failure control)*
(I) Méthodologie utilisée pour fournir une terminaison à l'épreuve de l'échec, sécurisée contre l'échec, ou d'échec en douceur et la récupération des fonctions d'un système. [FP039]

$ équité *(fairness)*
(I) Propriété d'un protocole d'accès pour une ressource système par laquelle la ressource est mise équitablement ou de façon impartiale à la disposition de tous les utilisateurs éligibles. (RFC3753)
Instructions : l'équité peut être utilisée pour se défendre contre certains types d'attaques de déni de service sur un système connecté à un réseau. Cependant, cette technique suppose que le système peut recevoir et traiter de façon appropriée les entrées venant du réseau. Donc, la technique peut atténuer une inondation mais est inefficace contre l'intrusion.

$ falsification
(I) Type d'action de menace par lequel de fausses données trompent une entité autorisée. (Voir : surveillance active, tromperie.)
Usage : ce type d'action de menace inclut les sous types suivants :
- "Substitution" : Altérer ou remplacer des données valides par de fausses données qui servent à tromper une entité autorisée.
- "Insertion" : Introduire de fausses données qui servent à tromper une entité autorisée.

$ arborescence des fautes *(fault tree)*
(I) Structure de données hiérarchisée à embranchements qui est utilisée pour représenter des événements et déterminer les diverses combinaisons de défaillances de composants et d'actions humaines qui pourraient résulter en un événement système indésirable spécifié. (Voir : arborescence d'attaques, méthodologie d'hypothèses de faute.)
Instructions : "l'analyse d'arborescence de fautes" est une technique dans laquelle un état non désiré d'un système est spécifié et le système est étudié dans le contexte de son environnement et de son fonctionnement pour découvrir toutes les façons crédibles dont l'événement pourrait se produire. L'événement fautif spécifié est représenté par la racine de l'arborescence. Le reste de l'arborescence représente les combinaisons ET ou OU des sous événements, et les combinaisons séquentielles des sous événements qui pourraient causer la survenance de l'événement racine. Le principal objet d'une analyse d'arborescence de fautes est de calculer la probabilité de l'événement racine, en utilisant des statistiques ou autres méthodes analytiques et en incorporant des données réelles ou prédites de fiabilité et maintenabilité quantitatives. Lorsque l'événement racine est une violation de la sécurité, et lorsque certains des sous événements sont des actes délibérés destinés à accomplir l'événement racine, l'arborescence des fautes est alors une arborescence d'attaques.

$ FEAL

(O) Famille de chiffrements de blocs symétrique qui a été développée au Japon ; elle utilise des blocs de 64 bits, des clés de 64 ou 128 bits, et un nombre variable de tours ; elle a été attaquée avec succès par la cryptanalyse. [Schn]

$ Normes fédérales de traitement de l'information (FIPS, *Federal Information Processing Standards*)
(N) La série des publications de normes fédérales de traitement de l'information (FIPS PUB) est produite par le NIST dans le cadre des dispositions de la Section 111(d) de l'Acte sur la propriété fédérale et les services administratifs de 1949 tel qu'amendé par l'acte sur la sécurité informatique de 1987 (Loi 100-235) comme lignes directrices techniques pour les dispositions sur les équipements et services de systèmes de traitement de l'information du gouvernement des USA. (Voir : éléments "[FPxxx]" dans la Section 7, Références pour information.)

$ infrastructure fédérale de clés publiques (FPKI, *Federal Public-key Infrastructure*)
(O) Une PKI qui est prévue pour établir les facilités, spécifications, et politiques nécessaires au gouvernement des USA pour utiliser les certificats de clé publique dans des systèmes qui impliquent des applications non classifiées mais sensibles et des interactions entre les agences fédérales ainsi qu'avec des entités des états et gouvernements locaux, la communauté des affaires, et le public. [FPKI]

$ norme fédérale 1027 *(Federal Standard 1027)*
(N) Document du gouvernement des USA qui définit les critères de l'émanation, de l'anti altération, de l'analyse de failles de sécurité, et de la gestion manuelle de clé pour les appareils de chiffrement en DES, principalement pour la couche 2 OSIRM. Elle a été renommée "FIPS PUB 140" lorsque la responsabilité de la protection des informations sensibles non classifiées a été transférée de la NSA au NIST, et a depuis été remplacée par de nouvelles versions de cette norme [FP140].

$ protocole de transfert de fichiers (FTP, *File Transfer Protocol*)
(I) Norme de protocole de l'Internet fondée sur TCP, de couche Application (RFC0959) pour déplacer des fichiers de données d'un ordinateur à un autre.

$ appareil de remplissage *(fill device)*
(N) /COMSEC/ Appareil utilisé pour transférer ou mémoriser du matériel de chiffrement en forme électronique ou pour insérer du matériel de chiffrement dans un équipement cryptographique.

$ filtre, filtrer *(filter)*
1. (I) /nom/ Synonyme de "garde". (À comparer à : filtre de contenu, routeur de filtrage.)
2. (I) /verbe/ Traiter un flux de données et bloquer ou permettre de façon sélective le passage des éléments de données individuels conformément à une politique de sécurité.

$ routeur de filtrage *(filtering router)*
(I) Routeur inter réseau qui empêche de façon sélective le passage des paquets de données conformément à une politique de sécurité. (Voir : garde.)
Instructions : un routeur a généralement deux connexions physiques, ou plus, aux réseaux ou autres systèmes, et quand le routeur reçoit un paquet sur une de ces connexions, il transmet le paquet sur une seconde connexion. Un routeur de filtrage fait la même chose, mais il décide d'abord, conformément à une politique de sécurité, si le paquet devrait être transmis. La politique est mise en œuvre par des règles (filtres de paquet) chargées dans le routeur. Les règles impliquent principalement des valeurs de champs de contrôle de paquets de données (en particulier les adresses IP de source et de destination et les numéros d'accès TCP) [RFC2179]. Un routeur de filtrage peut être utilisé seul comme un simple pare-feu ou être utilisé comme un composant d'un pare-feu plus complexe.

$ institution financière *(financial institution)*
(N) "Établissement chargé de faciliter les transactions initiées par un consommateur ou de la transmission de fonds pour l'extension d'un crédit ou la détention, le prêt, l'échange, ou la production de monnaie." [SET2]

$ empreinte digitale *(fingerprint)*
1. (I) Schéma de courbes formé par les crêtes papillaires d'une extrémité de doigt. (Voir : authentification biométrique. À comparer à : empreinte de pouce.)
2. (D) /PGP/ Résultat d'un hachage ("empreinte de clé") utilisé pour authentifier une clé publique ou d'autres données. [PGP]

Définition déconseillée : les IDOC NE DEVRAIENT PAS utiliser ce terme avec la définition 2, et NE DEVRAIENT PAS utiliser ce terme comme synonyme de "résultat de hachage" de *toute* sorte. L'une et l'autre utilisation mélangeraient les concepts d'une façon potentiellement trompeuse.

$ FIPS PUB 140
(N) Norme du gouvernement des USA [FP140] sur les exigences de sécurité auxquelles soit satisfaire un module

cryptographique lorsque il est utilisé pour protéger des informations non classifiées dans des systèmes informatiques et de communication. (Voir : Critères communs, FIPS, Norme fédérale 1027.)
Instructions : la norme spécifie quatre niveaux croissants (du "niveau 1" au "niveau 4") d'exigences pour couvrir une large gamme d'applications et environnements potentiels. Les exigences visent la conception de base et la documentation, les interfaces de modules, les rôles et services autorisés, la sécurité physique, la sécurité du logiciel, la sécurité du système d'exploitation, la gestion de clés, les algorithmes de chiffrement, les interférences électromagnétiques et la compatibilité électromagnétique (EMI/EMC), l'auto vérification. Le NIST et l'établissement canadien de la sécurité des communications certifient conjointement les modules.

$ FIREFLY
(O) /Gouvernement des USA/ "Protocole de gestion de clé fondé sur la cryptographie de clé publique." [C4009]

$ pare-feu *(firewall)*
1. (I) Passerelle inter réseaux qui restreint le trafic de communication des données de et vers un des réseaux connectés (celui dit être "à l'intérieur" du pare-feu) et qui protège donc les ressources systèmes de ce réseau contre les menaces provenant de l'autre réseau (celui qui est dit être "à l'extérieur" du pare-feu). (Voir : garde, passerelle de sécurité.)
2. (O) Appareil ou système qui contrôle le flux de trafic entre les réseaux en utilisant différentes postures de sécurité. [SP41]

Instructions : un pare-feu protège normalement un réseau plus petit, sécurisé (comme un LAN d'entreprise, ou même juste un hôte) d'un plus grand réseau (comme l'Internet). Le pare-feu est installé au point où le réseau se connecte, et le pare-feu applique des règles de politique pour contrôler le trafic qui s'écoule de et dans le réseau protégé. Un pare-feu n'est pas toujours un seul ordinateur. Par exemple, un pare-feu peut consister en une paire de routeurs de filtrage et d'un ou plusieurs serveurs mandataires fonctionnant sur un ou plusieurs hôtes forteresses, tous connectés à un petit LAN dédié (voir : zone tampon) entre les deux routeurs. Le routeur externe bloque les attaques qui utilisent IP pour déjouer la sécurité (usurpation d'adresse IP, acheminement de source, fragments de paquets) tandis que les serveurs mandataires bloquent les attaques qui exploiteraient la vulnérabilité dans un protocole ou service de couche supérieure. Le routeur interne bloque le trafic qui voudrait quitter le réseau protégé sauf à travers les serveurs mandataires. La partie difficile est de définir des critères selon lesquels le passage des paquets à travers le pare-feu est refusé, parce que le pare-feu non seulement empêche de pénétrer le trafic non autorisé (c'est-à-dire, les intrus) mais a aussi habituellement besoin de laisser passer le trafic autorisé dans les deux sens.

$ microcode *(firmware)*
(I) Programmes et données informatiques conservés dans le matériel – normalement dans une mémoire en lecture seule (ROM) ou une mémoire programmable en lecture seule (PROM) – de telle sorte que les programmes et les données ne puissent être écrits ou modifiés de façon dynamique durant l'exécution des programmes. (Voir : matériel, logiciel.)

$ faute *(flaw)*
1. (I) Erreur dans la conception, la mise en œuvre, ou le fonctionnement d'un système d'information. Une faute peut résulter en une vulnérabilité. (À comparer à : vulnérabilité.)
2. (D) "Erreur de commission, d'omission, ou de prévision dans un système qui permet que des mécanismes de protection soient outrepassés." [NCSSG] (À comparer à : vulnérabilité. Voir : cerveau endommagé.)

Définition déconseillée : les IDOC NE DEVRAIENT PAS utiliser ce terme avec la définition 2 ; toute faute n'est pas une vulnérabilité.

$ méthodologie d'hypothèse de faute *(flaw hypothesis methodology)*
(I) Technique d'évaluation ou d'attaque dans laquelle les spécifications et la documentation pour un système sont analysées pour faire des hypothèses sur les fautes dans le système. La liste des fautes supposées est assortie d'une priorité sur la base de la probabilité estimée qu'une faute existe et, en supposant qu'elle existe, sur la facilité de l'exploiter et sur la mesure du contrôle ou de la compromission qu'elle entraînerait. La liste avec ses priorités est utilisée pour conduire un essai de pénétration ou d'attaque contre le système. [NCS04] (Voir : arborescence des fautes, faute.)

$ inondation *(flooding)*
1. (I) Attaque qui tente de causer une défaillance dans un système en fournissant plus d'entrées que le système ne peut en traiter correctement. (Voir : déni de service, équité. À comparer à : embouteillage.)

Instructions : l'inondation utilise la "surcharge" comme un type "d'obstruction" destinée à causer une "interruption".
2. (I) Processus de livraison des données ou messages de contrôle à tous les nœuds d'un réseau. [RFC3753]

$ analyse de flux *(flow analysis)*
(I) Analyse effectuée sur une spécification système formelle non procédurale, qui localise les flux potentiels d'informations entre les variables système. En allouant des niveaux de sécurité aux variables, l'analyse peut trouver des types de canaux couverts. [Huff]

$ contrôle de flux *(flow control)*
1. (I) /sécurité des données/ Procédure ou technique pour s'assurer que des transferts d'informations au sein d'un système ne sont pas faits d'un niveau de sécurité à un autre niveau de sécurité, et en particulier d'un niveau supérieur à un niveau inférieur. [Denns] (Voir : canal couvert, propriété de confinement, politique de flux d'informations, propriété de sécurité simple.)
2. (O) /sécurité des données/ "Concept qui exige que les transferts d'informations au sein d'un système soient contrôlés de telle sorte que les informations dans certains types d'objets ne puissent pas, via un canal quelconque au sein du système, s'écouler vers certains autres types d'objets." [NCSSG]

$ seulement pour usage officiel (FOUO, *For Official Use Only*)
(O) /U.S. DoD/ Désignation du gouvernement des USA pour des informations qui n'ont pas reçu de classification de sécurité selon les critères d'une règlementation traitant de la sécurité nationale, mais qui peuvent être gardées non publiques parce que leur divulgation causerait un dommage prévisible à un intérêt protégé par une des exemptions déclarées dans l'Acte sur la liberté de l'information (Section 552 du Titre 5, Code des États Unis). (Voir : étiquette de sécurité, marquage de sécurité. À comparer à : classifié.)

$ formel *(formal)*
(I) Exprimé dans un langage de syntaxe restreinte avec une sémantique définie sur la base de concepts mathématiques bien définis. [CCIB] (À comparer à : informel, semi formel.)

$ approbation d'accès formelle *(formal access approval)*
(O) /Gouvernement des USA/ Approbation documentée par un propriétaire de données pour permettre l'accès à une catégorie particulière d'informations dans un système. (Voir : catégorie.)

$ méthodologie de développement formel *(Formal Development Methodology)* (O) Voir : Ina Jo.

$ modèle formel *(formal model)*
(I) Modèle de sécurité qui est formel. Exemple : modèle de Bell-LaPadula. [Land] (Voir : formel, modèle de sécurité.)

$ preuve formelle *(formal proof)*
(I) "Argument mathématique complet et convainquant, présentant la pleine justification logique de chaque étape de la preuve, pour la vérité d'un théorème ou d'un ensemble de théorèmes." [NCSSG]

$ spécification formelle *(formal specification)*
(I) Description précise du comportement (prévu) d'un système, usuellement écrite dans un langage mathématique, parfois pour les besoins du soutien d'une vérification formelle par une preuve rigoureuse. [Huff] (Voir : Affirmer, Gypsy, HDM, Ina Jo.) (Voir : formel.)
Instructions : une spécification formelle peut être écrite à tout niveau de détail mais est usuellement une spécification de niveau supérieur.

$ spécification formelle de niveau supérieur *(formal top-level specification)*
(I) "Spécification de niveau supérieur qui est écrite dans un langage mathématique formel pour permettre que des théorèmes montrant la correspondance de la spécification du système à ses exigences formelles fassent l'objet d'hypothèses et soient prouvés de façon formelle." [NCS04] (Voir : spécification formelle.)

$ formulaire *(formulary)*
(I) Technique pour permettre de prendre une décision d'accorder ou refuser l'accès de façon dynamique au moment de la tentative d'accès, plutôt que lorsque est créée une liste de contrôle d'accès ou un ticket.

$ FORTEZZA (marque déposée)
(O) Marque déposée de la NSA, utilisée pour une famille de produits de sécurité interopérables qui mettent en œuvre une suite d'algorithmes cryptographiques approuvés par le NIST/NSA pour la signature numérique, le hachage, le chiffrement, et l'échange de clés. Les produits incluent une carte de PC (qui contient un processeur CAPSTONE), et des modems d'accès série compatibles, de tableaux de serveurs, et des mises en œuvre de logiciels.

$ Forum des équipes de réponse aux incidents de sécurité (FIRST, *Forum of Incident Response and Security Teams*)
(N) Consortium international des CSIRT (par exemple, CIAC) qui fonctionnent ensemble pour traiter les incidents de sécurité informatiques et promouvoir les activités préventives. (Voir : CSIRT, incident de sécurité.)
Instructions : FIRST a été fondé en 1990 et, en juillet 2004, a plus de 100 membres sur l'ensemble du globe. Ses missions

incluent :
- de fournir aux membres des informations techniques, des outils, des méthodes, de l'assistance, et des directives,
- de coordonner des activités de liaison et de soutien analytique,
- d'encourager le développement de produits et services de qualité,
- d'améliorer la sécurité nationale et internationale des informations pour les gouvernements, l'industrie privée, l'université , et les individus,
- d'améliorer l'image et le statut de la communauté des CSIRT.

$ secret vers l'avant *(forward secrecy)*
(I) Voir : secret parfait vers l'avant.

$ fraggle attack (D) /argot/ synonyme de "attaque par surcharge".
Terme déconseillé : Il est vraisemblable que d'autres cultures utilisent des métaphores différentes pour ce concept. Donc, pour éviter l'incompréhension entre les nations, les IDOC NE DEVRAIENT PAS utiliser ce terme.
Dérivation : Les Fraggles sont une race fictive de petits humanoïdes (représentés comme des marionnettes dans une série télévisée enfantine, "Fraggle Rock") qui vivent sous terre.

$ saut de fréquence *(frequency hopping)*
(N) Commutation de fréquence répétée durant une émission radio conformément à un algorithme spécifié. [C4009] (Voir : spectre étalé.)
Instructions : Le saut de fréquence est une technique de TRANSEC pour minimiser le potentiel d'interception ou de brouillage non autorisé.

$ frais *(fresh)*
(I) Généré récemment ; non répété à partir d'une interaction antérieure du protocole.
Usage : décrit des données contenues dans une PDU qui est reçue et traitée pour la première fois. (Voir : vivacité, nom occasionnel, attaque en répétition.)

$ passerelle *(gateway)*
(I) Système intermédiaire (interface, relais) qui rattache deux (ou plus) réseaux informatiques qui ont des fonctions similaires mais des mises en œuvre dissemblables et qui permet des communications unidirectionnelles ou bidirectionnelles entre les réseaux. (Voir : pont, pare-feu, garde, inter réseau, serveur mandataire, routeur, et sous réseau.)
Instructions : les réseaux peuvent différer par un ou plusieurs aspects, incluant des mécanismes de protocoles et de sécurité. Lorsque deux réseaux informatiques diffèrent par le protocole par lequel ils offrent leurs services aux hôtes, une passerelle peut traduire un protocole dans l'autre ou autrement faciliter l'interopération des hôtes (voir : Protocole Internet). En théorie, les passerelles entre réseaux informatiques sont concevables à toutes les couches OSIRM. En pratique, ils fonctionnent usuellement à la couche 2 OSIRM (voir : pont), 3 (voir : routeur), ou 7 (voir : serveur mandataire).

$ GeldKarte
(O) Système de monnaie électronique fondé sur une carte à mémoire, qui est tenu par l'industrie bancaire allemande, incorpore un chiffrement, et peut être utilisé pour faire des payements via l'Internet. (Voir : IOTP.)

$ temps généralisé *(GeneralizedTime)*
(N) Le type de données ASN.1 "GeneralizedTime" (ISO 8601) contient une date calendaire (AAAAMMJJ) et une heure, qui est soit (a) l'heure locale, soit (b) le temps universel coordonné, soit (c) à la fois l'heure locale et un décalage qui permet de calculer le temps universel coordonné. (Voir : temps universel coordonné. À comparer à : heure UTC.)

$ interface de programme d'application de service de sécurité générique (GSS-API, *Generic Security Service Application Program Interface*)
(I) Protocole standard de l'Internet [RFC2743] qui spécifie les conventions d'appel par lesquelles une application (normalement un autre protocole de communication) peut obtenir les services d'authentification, d'intégrité, et de confidentialité indépendamment des mécanismes et technologies de sécurité sous-jacents, permettant ainsi au code source d'application d'être porté dans différents environnements. (À comparer à : EAP, SASL.)
Instructions : "un appelant GSS-API accepte des jetons qui lui sont fournis par sa mise en œuvre GSS-API locale et transfère les jetons à un homologue sur un système distant ; cet homologue passe les jetons reçus à sa mise en œuvre GSS-API locale pour traitement. Les services de sécurité disponibles de cette façon à travers une GSS-API peuvent être mis en œuvre (et l'ont été) sur une large gamme de mécanismes sous-jacents sur la base du chiffrement [symétrique] et [asymétrique]." [RFC2743]

$ autorité de certificat géopolitique (GCA, *geopolitical certificate authority*)
(O) /SET/ Dans une hiérarchie de certification SET, c'est un niveau facultatif qui est certifié par une BCA et qui peut

certifier des CA de détenteur de carte, des CA de commerçants, et des CA de passerelle de payement. Utiliser des GCA permet à une marque de répartir la responsabilité de la gestion des certificats à des régions géographiques ou politiques, afin que les politiques de la marque puissent varier comme nécessaire entre les régions.

$ grille d'informations mondiale (GIG, *Global Information Grid*)
(O) /U.S. DoD/ La GIG est "un ensemble de capacités d'informations mondialement interconnecté de bout en bout, de processus et de personnels associés pour collecter, traiter, mémoriser, disséminer, et gérer des informations à la demande pour les combattants, les hommes politiques et le personnel de soutien." [IATF] Usage : anciennement appelé le DII.

$ bonnes pratiques d'ingénierie *(good engineering practices)*
(N) Terme utilisé pour spécifier ou caractériser la conception, la mise en œuvre, l'installation, ou les pratiques de fonctionnement d'un système d'informations, lorsque une spécification plus explicite n'est pas possible. Compris généralement comme se référant à l'état de l'art de l'ingénierie pour des systèmes commerciaux qui ont des problèmes et des solutions équivalentes au système en question.

$ granularité *(granularity)*
1. (N) /contrôle d'accès/ Finesse relative à laquelle un mécanisme de contrôle d'accès peut être ajusté.
2. (N) /sécurité des données/ "Taille de la plus petite unité d'information protégeable" dans un système de confiance. [Huff]

$ Livre Vert *(Green Book)*
(D) /argot/ Synonyme de "Lignes directrices pour la gestion des mots de passe de la Défense *(Defense Password Management Guideline)*" [CSC2].
Terme déconseillé : sauf dans une notice explicative, les IDOC NE DEVRAIENT PAS utiliser ce terme, quelle que soit la définition associée. À la place, utiliser le nom approprié complet du document ou, dans les références suivantes, une abréviation conventionnelle. (Voir : Série Arc en ciel.)
Utilisation déconseillée : pour améliorer la compréhension internationale des normes de l'Internet et du processus de normalisation de l'Internet, les IDOC NE DEVRAIENT PAS utiliser de "jolis" synonymes. Quelle que soit la clarté ou la popularité d'un surnom dans une certaine communauté, il va vraisemblablement être cause de confusion ou de gène dans d'autres communautés. Par exemple, plusieurs autres normes du système d'information sont aussi appelées "Livre Vert" ; en voici quelques exemples :
- chaque volume des normes 1992 de l'UIT-T (appelé à l'époque le CCITT) ;
- "PostScript Language Program Design", Adobe Systems, Addison-Wesley, 1988.
- interface de système d'exploitation IEEE 1003.1 POSIX ;
- "Smalltalk-80: Bits of History, Words of Advice", Glenn Krasner, Addison-Wesley, 1983.
- "Guide de la compatibilité X/Open" ;
- un format particulier de CD-ROM développé par Phillips.

$ domaine d'interprétation de groupe (GDOI, *Group Domain of Interpretation*)
(I) Domaine d'interprétation ISAKMP/IKE pour la gestion de clés de groupe ; c'est-à-dire, un protocole de phase 2 dans ISAKMP. [RFC3547] (Voir : diffusion groupée sécurisée.)
Instructions : dans ce modèle de gestion de clé de groupe qui étend la norme ISAKMP, le protocole fonctionne entre un membre d'un groupe et un "contrôleur de groupe/serveur de clés", qui établit des associations de sécurité [RFC4301] entre les membres autorisés de groupe. Le protocole GDOI est lui-même protégé par une association ISAKMP de phase 1.
Par exemple, les applications de diffusion groupée peuvent utiliser ESP pour protéger leur trafic de données. GDOI porte les paramètres d'association de sécurité nécessaires pour ESP. De cette façon, GDOI prend en charge ESP en diffusion groupée avec l'authentification de groupe des paquets ESP en utilisant une clé de groupe partagée.

$ identité de groupe *(group identity)* (I) Voir : définition secondaire sous "identité".

$ association de sécurité de groupe *(group security association)*
(I) "Faisceau d'associations de sécurité (SA) qui ensemble définissent comment un groupe communique de façon sûre. La SA de groupe peut inclure une SA de protocole d'enregistrement, une SA de protocole de changement de clés, et une ou plusieurs SA de protocole de sécurité des données." [RFC3740]

$ garde *(guard)*
(I) Système informatique qui (a) agit comme passerelle entre deux systèmes d'information fonctionnant sous des politiques de sécurité différentes et (b) est de confiance pour les transferts de données d'informations entre les deux. (Voir : interface contrôlée, solution inter domaines, domaine, filtre. À comparer à : pare-feu.)
Usage : fréquemment compris comme signifiant qu'un système fonctionne à un niveau de sécurité supérieur à celui de l'autre, et que l'objet de la passerelle est d'empêcher la divulgation non autorisée des données provenant du système supérieur vers l'inférieur. Cependant, l'objet peut être aussi de protéger l'intégrité des données, la disponibilité, ou l'intégrité

générale d'un système contre les menaces résultant de la connexion avec l'autre système. La médiation peut être entièrement automatisée ou peut impliquer une "révision humaine fiable".

$ connexion d'invité *(guest login)* (I) Voir : connexion anonyme.

$ sécurité générique de couche supérieure (GULS, *Generic Upper Layer Security*)
(I) Élément de service de sécurité générique de couche supérieure (ISO 11586), norme en cinq parties pour les échanges d'informations de sécurité et de fonctions de transformation de sécurité qui protègent la confidentialité et l'intégrité de données d'application.

$ environnement de vérification Gypsy *(Gypsy verification environment)*
(O) Méthodologie, langage, et ensemble intégré d'outils logiciels développés à l'Université du Texas pour spécifier, coder, et vérifier le logiciel pour produire des programmes corrects et fiables. [Cheh]

$ champ H *(H field)* (D) Voir : Utilisation déconseillée sous "champ Restrictions de traitement".

$ bidouiller *(hack)*
1a. (I) /verbe/ Travailler sur quelque chose, en particulier pour programmer un ordinateur. (Voir : hacker.)
1b. (I) /verbe/ Commettre un méfait, en particulier jouer un mauvais tour à, ou pénétrer, un système. (Voir : hacker, craqueur.)
2. (I) /nom/ Élément d'un travail achevé, ou une solution à un problème, qui n'est pas généralisable, c'est-à-dire, est très spécifique du domaine d'application ou du problème à résoudre.
Instructions : souvent, le domaine d'application ou le problème implique de la programmation informatique ou un autre usage d'un ordinateur. Caractériser quelque chose comme un hack peut être un compliment, comme lorsque la solution est minimale et élégante ; ou cela peut être dérogatoire, comme lorsque la solution règle le problème mais laisse le système dans un état non maintenable.
Voir dans [Raym] plusieurs autres significations de ce terme et aussi des définitions de plusieurs termes dérivés.

$ pirate, fouineur, bidouilleur *(hacker)*
1. (I) Quelqu'un qui porte un fort intérêt à l'informatique, qui aime apprendre à son sujet, qui aime programmer les ordinateurs, et fait des expériences et travaille avec eux. (Voir : hack. À comparer à : adversaire, craqueur, intrus.)
Usage : la première définition est la signification originale du terme (autour de 1960) ; elle avait une connotation neutre ou positive de "quelqu'un qui représente bien les choses et fait arriver des choses sympathiques".
2. (O) "Un individu qui passe une quantité de temps extraordinaire à travailler sur un ordinateur pour des raisons autres que professionnelles." [NCSSG]
3. (D) Synonyme de "craqueur".
Utilisation déconseillée : aujourd'hui, le terme est fréquemment (mal) utilisé (en particulier par des journalistes) avec la définition 3.

$ traiter *(handle)*
1. (I) /verbe/ Effectuer des opérations de traitement sur des données, comme recevoir et transmettre, collecter et disséminer, créer et supprimer, mémoriser et restituer, lire et écrire, et comparer. (Voir : accéder.)
2. (I) /nom/ Bride : pseudonyme en ligne, particulièrement celui utilisé par un craqueur ; dérivé de la culture de la "citizens' band".

$ restriction de traitement *(handling restriction)*
(I) Type de contrôle d'accès autre que (a) les protections fondées sur des règles de contrôle d'accès obligatoire et (b) les protections fondées sur l'identité du contrôle d'accès discrétionnaire ; implique usuellement la sécurité administrative.

$ champ Restrictions de traitement *(Handling Restrictions field)*
(I) Champ de 16 bits qui spécifie un marquage de contrôle et de libération dans l'option de sécurité (type d'option 130) du format d'en-tête de datagramme IP. Les valeurs valides du champ sont des digraphes alphanumériques alloués par le gouvernement des USA, comme spécifié dans la RFC0791.
Abréviation déconseillées : les IDOC NE DEVRAIENT PAS utiliser l'abréviation "champ H" parce qu'elle est potentiellement ambiguë. À la place, utiliser "champ Restrictions de traitement".

$ prise de contact *(handshake)*
(I) Dialogue de protocole entre deux systèmes pour s'identifier et s'authentifier l'un à l'autre, ou pour synchroniser leurs opérations.

$ protocole de prise de contact *(Handshake Protocol)*
(I) /TLS/ Le protocole de prise de contact de TLS comporte trois parties (c'est-à-dire, sous protocoles) qui permettent aux entités homologues de se mettre d'accord sur les paramètres de sécurité pour la couche d'enregistrement, de s'authentifier les uns auprès des autres, d'instancier les paramètres de sécurité négociés, et de se faire les uns aux autres rapport des conditions d'erreur. [RFC4346]

$ durcir *(harden)*
(I) Protéger un système en le configurant pour fonctionner d'une façon qui élimine ou diminue les faiblesses connues. Exemple : [RSCG]. (Voir : compte par défaut.)

$ matériel *(hardware)*
(I) Les composants physiques matériels d'un système d'informations. (Voir : microcode, logiciel.)

$ erreur de matériel *(hardware error)*
(I) /action de menace/ Voir : définitions secondaires sous "corruption", "exposition", et "incapacitation".

$ jeton matériel *(hardware token)*. Voir : jeton.

$ code de hachage *(hash code)*
(D) Synonyme de "résultat de hachage" ou "fonction de hachage".
Terme déconseillé : les IDOC NE DEVRAIENT PAS utiliser ce terme ; il mélange les concepts d'une façon potentiellement trompeuse. Un résultat de hachage n'est pas un "code", et une fonction de hachage ne "code" en aucun sens défini par le présent glossaire. (Voir : valeur de hachage, résumé de message.)

$ fonction de hachage *(hash function)*
1. (I) Une fonction H qui transpose une chaîne binaire s arbitraire de longueur variable en une chaîne de longueur fixée h = H(s) (appelée le "résultat de hachage"). Pour la plupart des applications informatiques, il est souhaitable qu'étant données une chaîne s avec H(s) = h, tout changement de s qui crée une chaîne différente s' va résulter en un résultat de hachage imprévisible H(s') qui n'est, avec une forte probabilité, pas égal à H(s).
2. (O) "Une fonction (mathématique) qui transpose des valeurs d'un grand domaine (éventuellement très grand) en une plus petite gamme. Une "bonne" fonction de hachage est telle que le résultat de l'application de la fonction à un (grand) ensemble de valeurs dans le domaine va être équitablement réparti (et apparemment au hasard) sur la gamme." [X509]

Instructions : une fonction de hachage fonctionne sur des entrées de longueur variable (par exemple, un message ou un fichier) et donne un résultat de longueur fixe, qui est normalement plus court que la plupart des valeurs d'entrée. Si l'algorithme est "bon" comme décrit dans la définition "O", la fonction de hachage peut alors être candidate à l'utilisation dans un mécanisme de sécurité pour détecter les changements accidentels des données, mais pas nécessairement pour un mécanisme de détection des changements faits par une écoute active. (Voir : Instructions sous "somme de contrôle".)
Les mécanismes de sécurité exigent une "fonction de hachage cryptographique" (par exemple, MD2, MD4, MD5, SHA-1, Snefru) c'est-à-dire, une bonne fonction de hachage qui ait aussi la propriété d'être unidirectionnelle et une des deux propriétés d'évitement de collision suivantes :
- "propriété unidirectionnelle" : étant donné H et un résultat de hachage h = H(s), il est dur (c'est-à-dire, incalculable, "impossible") de trouver s. (Bien sûr, étant donnés H et une entrée s, il doit être relativement facile de calculer le résultat de hachage H(s).)
- "propriété de faible évitement de collision" : étant donnés H et une entrée s, il est dur (c'est-à-dire, incalculable, "impossible") de trouver une entrée différente, s', telle que H(s) = H(s').
- "propriété de fort évitement de collision" : étant donné H, il est difficile de trouver une paire d'entrées s et s' telle que H(s) = H(s').

Si H produit un résultat de hachage long de N bits, trouver alors un s' où H(s') = H(s) pour un s donné spécifique, la quantité de calcul requise est O(2**n) ; c'est-à-dire, il est nécessaire d'essayer de l'ordre de 2 à la puissance n valeurs de s' avant de trouver une collision. Cependant, pour simplement trouver une paire de valeurs s et s' qui coïncident, la quantité de calcul requise est seulement de O(2**(n/2)) ; c'est-à-dire qu'après avoir calculé H(s) pour 2 à la puissance n/2 valeurs choisies de façon aléatoire de s, la probabilité est supérieure à 1/2 que deux de ces valeurs aient le même résultat de hachage. (Voir : attaque de l'anniversaire.)

$ résultat de hachage *(hash result)*
1. (I) Le résultat d'une fonction de hachage. (Voir : code de hachage, valeur de hachage. À comparer à : valeur de hachage.)
2. (O) "Résultat produit par une fonction de hachage lors du traitement d'un message" (où "message" est défini de façon large comme "une représentation numérique de données"). [DSG]

Usage : les IDOC DEVRAIENT éviter l'utilisation inhabituelle de "message" qui est vue dans la définition "O".

$ valeur de hachage *(hash value)*

(D) Synonyme de "résultat de hachage".
Terme déconseillé : les IDOC NE DEVRAIENT PAS utiliser ce terme pour le résultat d'une fonction de hachage ; le terme pourrait facilement être confondu avec la "valeur hachée", qui signifie l'entrée d'une fonction de hachage. (Voir : code de hachage, résultat de hachage, résumé de message.)

$ méthodologie de développement hiérarchique (HDM, *Hierarchical Development Methodology*)
(O) Méthodologie, langage, et ensemble intégré d'outils logiciels développés par SRI International pour spécifier, coder, et vérifier un logiciel pour produire des programmes corrects et fiables. [Cheh]

$ PKI hiérarchique *(hierarchical PKI)*
(I) Architecture de PKI fondée sur une hiérarchie de certification. (À comparer à : PKI maillé, PKI de fichier de confiance.)

$ gestion de hiérarchie *(hierarchy management)*
(I) Processus de génération de données de configuration et de production de certificats de clé publique pour construire et faire fonctionner une hiérarchie de certification. (Voir : gestion de certificats.)

$ hiérarchie de confiance *(hierarchy of trust)*
(D) Synonyme de "hiérarchie de certification".
Terme déconseillé : les IDOC NE DEVRAIENT PAS utiliser ce terme ; il mélange les concepts d'une façon potentiellement trompeuse. (Voir : hiérarchie de certification, confiance, toile de confiance.)

$ garde de haute assurance *(high-assurance guard)*
(O) "Un oxymore" dit le Lt. Gen. William H. Campbell, ancien officier chef des informations de l'U.S. Army, parlant à une conférence de l'association des communications et de l'électronique des forces armées.
Usage : les IDOC qui utilisent ce terme DEVRAIENT en donner une définition parce que le terme mélange les concepts et pourrait facilement être mal compris.

$ capture *(hijack attack)*
(I) Forme d'écoute active dans laquelle l'attaquant prend le contrôle d'une association de communication préalablement établie. (Voir : attaque par interposition, capture de page, attaque de portage.)

$ acte de comptabilité et de portabilité des informations de santé (HIPAA, *Health Information Portability and Accountability Act*)
(N) Loi de 1996 des U.S.A (Loi 104-191) qui est destinée à protéger la confidentialité des dossiers médicaux des patients et des autres informations de santé sous toutes leurs formes, et rend obligatoire la sécurité de ces informations, incluant leur mémorisation et leur transmission électronique.

$ code d'authentification de message par hachage numérique (HMAC, *Keyed-Hashed Message Authentication Code*)
(I) Hachage numérique [RFC2104] qui peut se fonder sur tout hachage cryptographique itératif (par exemple, MD5 ou SHA-1) de sorte que la force cryptographique de HMAC dépend des propriétés du hachage cryptographique choisi. (Voir : [RFC2202], [RFC2403], [RFC2404].)
Dérivation : MAC fondé sur le hachage. (À comparer à : CMAC.)
Instructions : en supposant que H est un hachage cryptographique générique dans lequel une fonction est itérée sur des blocs de données d'une longueur de B octets, L est la longueur du résultat du hachage de H, K est une clé secrète de longueur $L \leq K \leq B$. Les valeurs IPAD et OPAD sont des chaînes fixes utilisées comme bourrage interne et externe et définies comme suit : IPAD = l'octet 0x36 répété B fois, et OPAD = l'octet 0x5C répété B fois. HMAC est calculé par H(K OUX OPAD, H(K OUX IPAD, données d'entrée)).
HMAC a les buts suivants :
- utiliser les fonctions de hachage cryptographique disponibles sans modification, en particulier les fonctions qui ont de bonnes performances dans le logiciel et pour lesquelles le logiciel est librement et largement disponible,
- préserver les performances originales du hachage choisi sans dégradation significative,
- utiliser et traiter les clés d'une façon simple,
- avoir une analyse cryptographique bien comprise de la force du mécanisme fondé sur des hypothèses raisonnables quant à la fonction de hachage sous-jacente,
- permettre un remplacement facile de la fonction de hachage au cas où un hachage plus rapide ou plus fort serait trouvé ou exigé.

$ pot de miel *(honey pot)*
(N) Système (par exemple, un serveur de la Toile) ou ressource système (par exemple, un fichier sur un serveur) qui est conçu pour être attirant pour des craqueurs ou intrus potentiels, comme le miel attire les ours. (Voir : chausse-trappe.)
Usage : il est vraisemblable que d'autres cultures utilisent des métaphores différentes pour ce concept. Donc, pour éviter

l'incompréhension entre les nations, un IDOC NE DEVRAIT PAS utiliser ce terme sans en fournir une définition. (Voir : Utilisation déconseillée sous "Livre Vert".)

$ hôte *(host)*
1. (I) /général/ Ordinateur rattaché à un sous réseau de communications ou un inter réseau et qui peut utiliser des services fournis par le réseau pour échanger des données avec d'autres systèmes rattachés. (Voir : système d'extrémité. À comparer à : serveur.)
2. (I) /IPS/ Ordinateur en réseau qui ne transmet pas de paquets IP non adressés à l'ordinateur lui-même. (À comparer à : routeur.)

Dérivation : vu par ses utilisateurs, un hôte les "entretient", leur fournissant des services de couche application ou des accès à d'autres ordinateurs rattachés au réseau. Cependant, même si des appareils de service périphériques traditionnels, comme des imprimantes, peuvent avoir des connexions indépendantes aux réseaux, ils ne sont généralement pas appelés hôtes.

$ https
(I) Lorsque utilisé dans la première partie d'un URL (la partie qui précède les deux points et spécifie un schéma ou protocole d'accès) ce terme spécifie l'utilisation de HTTP amélioré par un mécanisme de sécurité, qui est usuellement SSL. (À comparer à : S-HTTP.)

$ erreur humaine *(human error)*
(I) /action de menace/ Voir : définitions secondaires sous "corruption", "exposition", et "incapacitation".

$ chiffrement hybride *(hybrid encryption)*
(I) Application de cryptographie qui combine deux algorithmes de chiffrement ou plus, particulièrement une combinaison de chiffrement symétrique et asymétrique. Exemples : enveloppe numérique, MSP, PEM, PGP. (À comparer à : super chiffrement.)
Instructions : les algorithmes asymétriques exigent plus de calcul que ceux symétriques de force équivalente. Donc, le chiffrement asymétrique n'est normalement pas utilisé pour la confidentialité des données excepté pour distribuer une clé symétrique dans un schéma de chiffrement hybride, où la clé symétrique est usuellement très courte (en termes de bits) par rapport au fichier de données qu'elle protège. (Voir : clé en vrac).

$ hyperlien *(hyperlink)*
(I) En hypertexte ou hypermédia, un objet d'information (comme un mot, une phrase, ou une image, qui est usuellement soulignée par la couleur ou par un trait) qui pointe (c'est-à-dire, indique comment se connecter) sur les informations en rapport qui sont localisées ailleurs et peuvent être restituées en activant la liaison (par exemple, en choisissant l'objet avec une souris puis en cliquant).

$ hypermédia *(hypermedia)*
(I) Généralisation d'hypertexte ; tout support qui contient des hyperliens qui pointent sur du matériel dans le même ou un autre objet de données.

$ hypertexte*(hypertext)*
(I) Document informatique, ou partie d'un document, qui contient des hyperliens sur d'autres documents ; c'est-à-dire, du texte qui contient des pointeurs actifs sur d'autre texte. Usuellement écrit en HTML et accédé en utilisant un navigateur de la Toile. (Voir : hypermédia.)

$ langage de balisage hypertexte (HTML, *Hypertext Markup Language*)
(I) Système de syntaxe et de sémantique indépendant de la plate-forme (RFC1866) pour ajouter des caractères aux fichiers de données (particulièrement de fichier de texte) pour représenter la structure des données et pointer sur les données concernées, créant ainsi de l'hypertexte à utiliser dans la Toile mondiale et autres applications. (À comparer à : XML.)

$ protocole de transfert hypertexte (HTTP, *Hypertext Transfer Protocol*)
(I) Protocole Internet client-serveur fondé sur TCP, de couche application [RFC2616] qui est utilisé pour porter des demandes et réponses de données dans la Toile mondiale . (Voir : hypertexte.)

$ inondation ICMP *(ICMP flood)*
(I) Attaque de déni de service qui envoie à un hôte plus de paquets de demande d'écho ICMP ("ping") que la mise en œuvre de protocole ne peut en traiter. (Voir : inondation, surcharge.)

$ identification
(I) Acte ou processus qui présente un identifiant à un système afin que ce système puisse reconnaître une entité système et

la distinguer des autres entités. (Voir : authentification.)

$ informations d'identification *(identification information)*
(D) Synonyme de "identifier"; synonyme de "informations d'authentification". (Voir : authentification, informations identifiantes.)
Terme déconseillé : les IDOC NE DEVRAIENT PAS utiliser ce terme comme synonyme de l'un de ces termes ; ce terme (a) n'est pas aussi précis qu'eux et (b) mélange les concepts d'une façon potentiellement trompeuse. À la place, utiliser "identifier" ou "informations d'authentification", selon ce que l'on veut dire.

$ protocole d'identification *(Identification Protocol)*
(I) Protocole Internet client-serveur [RFC1413] pour apprendre l'identité d'un utilisateur d'une certaine connexion TCP.
Instructions : étant donnée une paire de numéros d'accès TCP, le serveur retourne une chaîne de caractères qui identifie le possesseur de cette connexion sur le système serveur. Le protocole ne fournit pas de service d'authentification et n'est pas destiné à l'autorisation ou au contrôle d'accès. Au mieux, il fournit des informations d'inspection supplémentaires par rapport à TCP.

$ identifiant *(identifier)*
(I) Objet de données – souvent une chaîne de caractères imprimables non blancs – qui représente de façon définitive l'identité spécifique d'une entité système, la distinguant de toutes les autres. (À comparer à : identité.)
Instructions : les identifiants des entités systèmes doivent être alloués avec beaucoup de soins, parce que les entités authentifiées sont à la base des autres services de sécurité, comme le service de contrôle d'accès.

$ accréditif d'identifiant *(identifier credential)*
1. (I) Voir : /authentification/ sous "accréditif".
2. (D) Synonyme de "certificat de signature".
Usage : les IDOC qui utilisent ce terme DEVRAIENT en donner une définition parce que le terme est utilisé dans de nombreux sens et pourrait facilement être mal compris.

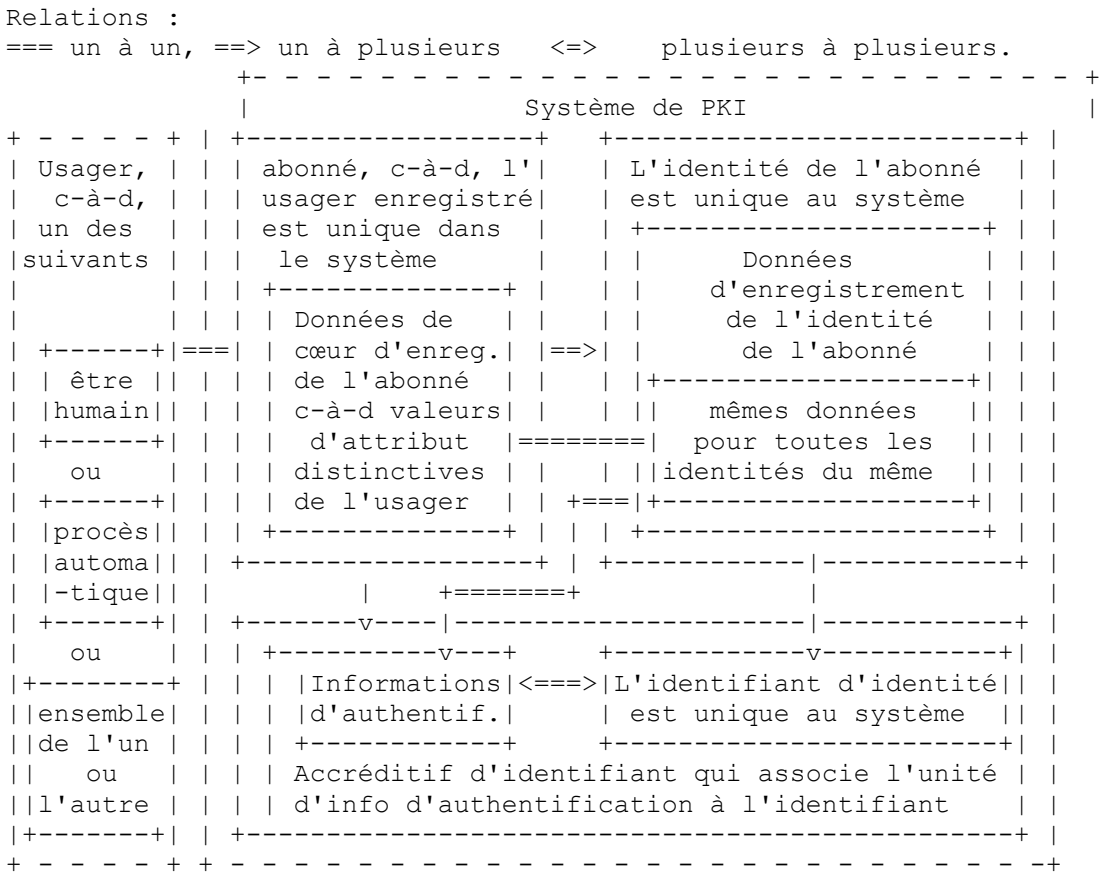
$ information identifiante *(identifying information)*
(D) Synonyme de "identifiant" ; synonyme de "informations d'authentification". (Voir : authentification, informations d'identification.)
Terme déconseillé : les IDOC NE DEVRAIENT PAS utiliser ce terme comme synonyme de l'un ou l'autre de ces termes ; ce terme (a) n'est pas aussi précis qu'eux et (b) mélange des concepts d'une façon potentiellement trompeuse. À la place, utiliser "identifiant" ou "informations d'authentification", selon ce que l'on veut dire.

$ identité *(identity)*
(I) Aspect collectif d'un ensemble de valeurs d'attribut (c'est-à-dire, un ensemble de caractéristiques) par lesquelles un utilisateur d'un système ou autre entité système est reconnaissable ou connu. (Voir : authentifier, enregistrement. À comparer à : identifier.)
Usage : un IDOC PEUT appliquer ce terme à une seule entité ou à un ensemble d'entités. Si un IDOC implique les deux significations, il DEVRAIT utiliser les termes et définitions suivants pour éviter les ambiguïtés :
- "identité singulière" : identité qui est enregistrée pour une entité qui est une seule personne ou processus ;
- "identité partagée" : identité qui est enregistrée pour une entité qui est un ensemble d'entités singulières (1) dans lequel chaque membre est autorisé à assumer l'identité individuellement et (2) pour lequel le système enregistrant tient la liste des entités singulières qui composent l'ensemble. Dans ce cas, on s'attend à ce que chaque entité membre soit enregistrée sous une identité singulière avant de devenir associée de l'identité partagée.
- "identité de groupe" : identité qui est enregistrée pour une entité (1) qui est un ensemble d'entités (2) pour lequel le système enregistreur ne tient pas de liste des entités singulières qui constituent l'ensemble.

Instructions : lorsque les services de sécurité se fondent sur les identités, deux propriétés sont souhaitables pour l'ensemble des attributs utilisés pour définir les identités :
- l'ensemble devrait être suffisant pour distinguer chaque entité de toutes les autres entités, c'est-à-dire, pour représenter chaque entité de façon univoque ;
- l'ensemble devrait être suffisant pour distinguer chaque identité de toute autre identité de la même entité.

La seconde propriété est nécessaire si un système permet à une entité d'enregistrer deux identités concurrentes ou plus. Avoir deux identités ou plus pour la même entité implique que l'entité a deux justifications distinctes pour s'enregistrer. Dans ce cas, l'ensemble des attributs utilisés pour les identités doit être suffisant pour représenter plusieurs identités pour une seule entité.
Avoir deux identités enregistrées ou plus pour la même entité est différent d'associer concurremment deux identifiants différents à la même identité, et est aussi différent d'une seule identité accédant concurremment au système dans deux rôles différents. (Voir : principal, contrôle d'accès fondé sur le rôle.)
Lorsque une identité d'un utilisateur est enregistrée dans un système, le système peut requérir la présentation de preuves de

l'authenticité de l'identité (c'est-à-dire que l'utilisateur a le droit de revendiquer ou d'utiliser l'identité) et son éligibilité (c'est-à-dire, que l'identité est qualifiée pour être enregistrée et a besoin d'être enregistrée).
Le diagramme qui suit illustre comment ce terme se rapporte à d'autres termes dans un système de PKI : informations d'authentification, identifiant, accréditif d'identifiant, enregistrement, usager enregistré, abonné, et usager.



$ politique de sécurité fondée sur l'identité *(identity-based security policy)*
(I) "Politique de sécurité fondée sur les identités et/ou attributs des usagers, d'un groupe d'usagers, ou des entités agissant au nom des usagers et des ressources/objets accédés." [I7498-2] (Voir : politique de sécurité fondée sur la règle.)

$ preuve d'identité *(identity proofing)*
(I) Processus qui valide et vérifie les informations qui sont utilisées pour établir l'identité d'une entité système. (Voir : enregistrement.)

$ IDOC
(I) Abréviation utilisée dans ce glossaire pour se référer à un document ou autre élément écrit qui est généré dans le processus de normalisation de l'Internet [RFC2026], c'est-à-dire, une RFC, un projet Internet, ou quelque autre élément de discours.
Utilisation déconseillée : cette abréviation NE DEVRAIT PAS être utilisée dans un IDOC à moins d'y être préalablement définie parce que l'abréviation a été inventée pour ce glossaire et n'est pas largement connue.

$ IEEE 802.10 (N) Comité de l'IEEE qui développe des normes de sécurité pour les LAN. (Voir : SILS.)

$ IEEE P1363
(N) Groupe de travail de l'IEEE, norme pour la cryptographie à clé publique, engagé dans le développement d'une norme de référence complète pour la cryptographie asymétrique. Couvre les logarithmes discrets (par exemple, DSA), les courbes elliptiques, et la factorisation d'entiers (par exemple, RSA) et couvre l'accord de clés, la signature numérique, et le chiffrement.

$ IMAP4 AUTHENTICATE
(I) Commande IMAP4 (mieux décrite comme un type de transaction, ou sous protocole) par lequel un client IMAP4 propose facultativement un mécanisme à un serveur IMAP4 pour authentifier le client auprès du serveur et fournir d'autres services de sécurité. (Voir : POP3.)

Instructions : si le serveur accepte la proposition, la commande est suivie d'un protocole d'authentification par mise au défi -réponse, et facultativement, par la négociation d'un mécanisme de protection pour les interactions POP3 ultérieures. Les mécanismes de sécurité qui sont utilisés par IMAP4 AUTHENTICATE – y compris Kerberos, GSS-API, et S/Key – sont décrits dans la [RFC1731].

$ impossible (O) Qui ne peut être réalisé dans un délai raisonnable. (Voir : casser, force brute, force, facteur de travail.)

$ en clair *(in the clear)* (I) Non chiffré. (Voir : texte en clair.)

$ Ina Jo
(O) Méthodologie, langage, et ensemble intégré d'outils logiciels développés par System Development Corporation pour spécifier, coder, et vérifier un logiciel pour produire des programmes corrects et fiables. Usage : autrement dit la méthodologie de développement formel. [Cheh]

$ incapacitation
(I) Type d'action de menace qui empêche ou interrompt le fonctionnement des systèmes en désactivant un composant d'un système. (Voir : interruption.)
Usage : Ce type d'action de menace inclut les sous types suivants :
- "logique malveillante" : dans un contexte d'incapacitation, tout matériel, logiciel, ou micro code (par exemple, bombe logique) intentionnellement introduit dans un système pour détruire des fonctions ou des ressources du système. (Voir : corruption, entrée principale pour "logique malveillante", mascarade, mauvais usage.)
- "destruction physique" : destruction délibérée d'un composant du système pour interrompre ou empêcher le fonctionnement du système.
- "erreur humaine" : /incapacitation/ Action ou inaction qui désactive de façon non intentionnelle un composant du système. (Voir : corruption, exposition.)
- "erreur de matériel ou de logiciel" : /incapacitation/ erreur qui cause de façon non intentionnelle la défaillance d'un composant du système et conduit à l'interruption du fonctionnement d'un système. (Voir : corruption, exposition.)
- "désastre naturel" : /incapacitation/ tout acte de force majeure (par exemple, feu, inondation, tremblement de terre, foudre, ou vent) qui désactive un composant d'un système. [FP031, Section 2]

$ incident. Voir : incident de sécurité.

$ INCITS (N) Voir : "Comité international de normalisation des technologies de l'information" sous "ANSI".

$ indicateur *(indicator)*
(N) Action – spécifique, généralisée, ou théorique – qu'un adversaire peut être supposé prendre pour la préparation d'une attaque. [C4009] (Voir : "détection d'attaque, avertissement, et réponse". À comparer à : indicateur de message.)

$ attaque indirecte *(indirect attack)*
(I) Voir : définition secondaire sous "attaque". À comparer à : attaque directe.

$ liste indirecte de révocation de certificat (ICRL, *indirect certificate revocation list*)
(N) Dans X.509, une CRL qui peut contenir des notifications de révocation de certificat pour des certificats produits par des CA autres que le producteur (c'est-à-dire, le signataire) de l'ICRL.

$ indistinguabilité *(indistinguishability)*
(I) Attribut d'un algorithme de chiffrement qui est une formalisation de la notion que le chiffrement d'une chaîne ne peut pas se distinguer du chiffrement d'une chaîne de longueur égale de non-sens. (À comparer à : sécurité sémantique.)

$ inférence *(inference)*
1. (I) Type d'action de menace qui raisonne à partir de caractéristiques ou sous-produits de communication et par là accède indirectement à des données sensibles, mais pas nécessairement les données contenues dans la communication. (Voir : analyse de trafic, analyse du signal.)
2. (I) Type d'action de menace qui obtient indirectement un accès non autorisé à des informations sensibles dans un système de gestion de base de données en corrélant les réponses aux interrogations aux informations déjà connues.

$ contrôle d'inférence *(inference control)*
(I) Protection de la confidentialité des données contre une attaque d'inférence. (Voir : confidentialité du flux de trafic.)
Instructions : un système de gestion de base de données qui contient N enregistrements sur des individus peut être obligé de fournir des statistiques résumées sur des sous ensembles de la population, tout en ne révélant pas d'informations sensibles

sur un seul individu. Un attaquant peut essayer d'obtenir des informations sensibles sur un individu en isolant un enregistrement désiré à l'intersection d'un ensemble d'interrogations qui se recoupent. Un système peut tenter d'empêcher cela en restreignant la taille et le recouvrement des ensembles d'interrogations, en faussant les réponses par des arrondis ou en perturbant autrement les valeurs de la base de données, et en limitant les questions à des échantillons aléatoires. Cependant, ces techniques peuvent être impraticables à la mise en œuvre ou à l'utilisation, et aucune technique n'est totalement efficace. Par exemple, restreindre la taille minimum d'un ensemble d'interrogations – c'est-à-dire, ne pas répondre aux questions pour lesquelles il y a moins de K ou plus de N-K enregistrements qui satisfont la demande – ne peut usuellement pas empêcher la divulgation non autorisée. Un attaquant peut bourrer de petits ensembles d'interrogations avec des enregistrements supplémentaires, et ensuite retirer l'effet des enregistrements supplémentaires. La formule pour identifier les enregistrements supplémentaires est appelée le "traceur". [Denns]

$ informel *(informal)*
(N) Exprimé en langage naturel. [CCIB] (À comparer à : formel, semi formel.)

$ information
1. (I) Faits et idées, qui peuvent être représentés (codés) sous diverses formes de données.
2. (I) Connaissance – par exemple, données, instructions – dans tout support ou forme qui peut être communiquée entre des entités système.

Instructions : la sécurité Internet pourrait être définie simplement comme la protection des informations dans l'Internet. Cependant, le besoin perçu d'utiliser différentes mesures protectrices pour différents types d'informations (par exemple, informations d'authentification, informations classifiées, informations collatérales, informations de sécurité nationale, informations personnelles, informations de contrôle de protocole, informations sensibles compartimentées, informations sensibles) a conduit à la diversité des terminologies énumérées dans le présent glossaire.

$ assurance d'informations *(information assurance)*
(N) /Gouvernement des USA/ "Mesures qui protègent et défendent les informations et les systèmes d'information en assurant leur disponibilité, leur intégrité, leur authentification, leur confidentialité, et leur non répudiation. Ces mesures incluent d'assurer la restauration des systèmes d'information en incorporant des capacités de protection, de détection, et de réaction." [C4009]

$ cadre technique d'assurance d'information (IATF, *Information Assurance Technical Framework*)
(O) Document disponible au public [IATF], développé par un effort collaboratif par des organisations du gouvernement des USA et de l'industrie, et produit par la NSA. Destiné aux gestionnaires de sécurité et aux ingénieurs de sécurité des systèmes comme un document guide et de référence sur les problèmes de sécurité dans les systèmes et réseaux d'information, pour améliorer le bien fondé des compromis entre les solutions technologiques disponibles et les caractéristiques désirées des approches de sécurité pour des problèmes particuliers. (Voir : ISO 17799, [SP14].)

$ domaine d'information *(information domain)*
(O) Voir : définition secondaire sous "domaine".

$ politique de flux d'informations *(information flow policy)*
(N) /modèle formel/ Triplet consistant en un ensemble de niveaux de sécurité (ou leurs étiquettes de sécurité équivalentes) un opérateur binaire qui transpose chaque paire de niveaux de sécurité en un niveau de sécurité, et une relation binaire sur l'ensemble qui sélectionne un ensemble de paires de niveaux tel qu'il soit permis aux informations de s'écouler d'un objet du premier niveau à un objet du second niveau. (Voir : contrôle de flux, modèle de treillis.)

$ conditions de fonctionnement de l'information (INFOCON, *information operations condition*)
(O) /U.S. DoD/ Position et réponse complètes de défense fondées sur l'état des systèmes d'information, des opérations militaires, et des hypothèses du renseignement sur les capacités et intentions de l'adversaire. (Voir : menace)
Dérivation : à partir de DEFCON, c'est-à-dire, conditions de la défense.
Instructions : le U.S. DoD définit cinq niveaux INFOCON : NORMAL (activité normale), ALPHA (risque d'attaque accru), BRAVO (risque d'attaque spécifique), CHARLIE (attaque limitée), et DELTA (attaque générale).

$ sécurité de l'information (INFOSEC, *information security*)
(N) Mesures qui mettent en œuvre et assurent des services de sécurité dans les systèmes d'information, y compris dans les systèmes informatiques (voir : COMPUSEC) et dans les systèmes de communication (voir : COMSEC).

$ système d'information *(information system)*
(I) Assemblée organisée de ressources et procédures de calcul et de communication – c'est-à-dire, les équipements et les services, avec leur infrastructure de soutien, les facilités, et le personnel – qui crée, collecte, enregistre, traite, mémorise, transporte, restitue, affiche, dissémine, contrôle, ou dispose l'information pour accomplir un ensemble spécifié de fonctions. (Voir : entité système, ressource système. À comparer à : plate-forme informatique.)

$ critères d'évaluation de la sécurité des technologie de l'information (ITSEC, *Information Technology Security Evaluation Criteria*)
(N) La norme [ITSEC] a été conjointement développée par la France, l'Allemagne, les Pays-Bas, et le Royaume Uni pour être utilisée dans l'Union Européenne ; elle traite une plus large gamme de combinaisons d'assurances et fonctionnalités de sécurité que le TCSEC. Supplantée par les critères communs.

$ filtrage d'entrée *(ingress filtering)*
(I) Méthode de la [RFC2827] pour contrer les attaques qui utilisent des paquets avec de fausses adresses IP de source, en bloquant ces paquets à la frontière entre les réseaux connectés.
Instructions : supposons que le réseau A d'un fournisseur d'accès Internet (FAI) comporte un routeur de filtrage qui est connecté au réseau consommateur B, et qu'un attaquant dans B à l'adresse IP de source "foo" tente d'envoyer des paquets avec la fausse adresse de source "bar" dans A. La fausse adresse peut être fixe ou changer de façon aléatoire, et elle peut être injoignable ou être une adresse forgée qui existe légitimement dans B ou un autre réseau C. Dans le filtrage d'entrée, le routeur du FAI bloque tous les paquets entrants qui arrivent de B avec une adresse de source qui n'est pas dans la gamme des adresses légitimement annoncées pour B. Cette méthode n'empêche pas toutes les attaques qui peuvent avoir B pour origine, mais la source réelle de telles attaques peut être plus facilement retracée parce que le réseau d'origine est connu.

$ valeur d'initialisation (IV, *initialization value*)
(I) /cryptographie/ Paramètre d'entrée qui établit l'état de départ d'un algorithme ou mode de chiffrement. (À comparer à : données d'activation.)
Instructions : un IV peut être utilisé pour synchroniser un processus cryptographique avec un autre ; par exemple, CBC, CFB, et OFB utilisent des IV. Un IV peut aussi être utilisé pour introduire la variance cryptographique (voir : sel) à côté de celle fournie par une clé.

$ vecteur d'initialisation *(initialization vector)*
(D) /cryptographie/ Synonyme de "valeur d'initialisation".
Terme déconseillé : pour éviter l'incompréhension entre les langues , les IDOC NE DEVRAIENT PAS utiliser ce terme dans le contexte de la cryptographie parce que la plupart des définitions des dictionnaires pour "vecteur" incluent un concept de direction ou de magnitude, qui ne sont pas pertinentes en cryptographie.

$ insertion
1. (I) /paquet/ Voir : définition secondaire sous "service d'intégrité de flux".
2. (I) /action de menace/ Voir : définition secondaire sous "falsification".

$ attaque de l'intérieur *(inside attack)*
(I) Voir : définition secondaire sous "attaque". À comparer à : interne.

$ interne *(insider)*
1. (I) Usager (usuellement une personne) qui accède à un système à partir d'une position qui est à l'intérieur du périmètre de sécurité du système. (À comparer à : usager autorisé, externe, usager non autorisé.)

Instructions : un interne a un rôle auquel sont alloués plus de privilèges pour accéder aux ressources système que n'en ont certains autres types d'usagers, ou peut accéder à ces ressources sans être contraint par des contrôles d'accès qui sont appliqués aux usagers extérieurs. Par exemple, un agent de ventes est un interne qui a accès au tiroir caisse, mais un consommateur du magasin est un externe.
Les actions effectuées par un interne dans l'accès au système peuvent être autorisées ou non autorisées ; c'est-à-dire, un interne peut agir soit comme usager autorisé, soit comme usager non autorisé.

2. (O) Personne qui a un accès physique autorisé au système. Exemple : dans ce sens, un surveillant de bureau est un interne, mais un cambrioleur ou un visiteur occasionnel ne l'est pas. [NRC98]
3. (O) Personne qui a un statut dans l'organisation qui fait que le système ou les membres de l'organisation voient ses demandes d'accès comme étant autorisées. Exemple : dans ce sens, un agent d'achat est un interne mais un vendeur ne l'est pas. [NRC98]

$ espace inspectable *(inspectable space)*
(O) /EMSEC/ "Espace tridimensionnel entourant un équipement qui traite des informations classifiées et/ou sensibles au sein desquelles l'exploitation de TEMPEST n'est pas considérée comme pratique ou où l'autorité légale pour identifier et/ou

retirer une exploitation potentielle TEMPEST existe." [C4009] (À comparer à : zone de contrôle, zone TEMPEST.)

$ Institut des ingénieurs en électricité et électronique (IEEE, *Institute of Electrical and Electronics Engineers, Inc.*)
(N) L'IEEE est une association à but non lucratif d'approximativement 300 000 membres individuels dans 150 pays. L'IEEE produit près d'un tiers de la littérature publiée dans le monde sur l'ingénierie électrique, l'informatique, et la technologie de contrôle ; elle tient des centaines de conférences annuelles majeures, et entretient plus de 800 normes actives, et bien plus encore en préparation . (Voir : SILS.)

$ intégrité *(integrity)* Voir : intégrité des données, service d'intégrité de datagramme, intégrité correcte, intégrité de source, service d'intégrité de flux, intégrité du système.

$ vérification d'intégrité *(integrity check)*
(D) Calcul qui fait partie d'un mécanisme qui assure un service d'intégrité des données ou un service d'authentification d'origine des données. (À comparer à : somme de contrôle.)
Terme déconseillé : les IDOC NE DEVRAIENT PAS utiliser ce terme comme synonyme de "hachage cryptographique" ou "somme de contrôle protégée". Ce terme duplique sans nécessité la signification d'autres termes bien établis ; ce terme mentionne seulement l'intégrité, bien que le service visé puisse être l'authentification d'origine des données ; et toutes les sommes de contrôle ne sont pas cryptographiquement protégées.

$ étiquette d'intégrité *(integrity label)*
(I) Étiquette de sécurité qui indique le degré de confiance qui peut être accordé aux données, et peut aussi dire l'application de quelles contre-mesures est exigée pour protéger les données de l'altération et de la destruction. (Voir : intégrité. À comparer à : étiquette de classification.)

$ menace intelligente *(intelligent threat)*
(I) Circonstance dans laquelle un adversaire a la capacité technique et opérationnelle de détecter et exploiter une vulnérabilité et a aussi l'intention démontrée, présumée, ou inférée de le faire. (Voir : menace.)

$ interception
(I) Type d'action de menace par laquelle une entité non autorisée accède directement à des données sensibles alors que les données voyagent entre des sources et destinations autorisées. (Voir : divulgation non autorisée.)
Usage : ce type d'action de menace inclut les sous types suivants :
- "vol" : obtenir l'accès à des données sensibles en volant la cargaison d'un support physique, comme une bande ou disque magnétique, qui contient les données.
- "écoute (passive)" : surveillance et enregistrement de données qui s'écoulent entre deux points dans un système de communications. (Voir : écoute.)
- "analyse des émanations" : obtenir la connaissance directe des données communiquées en surveillant et résolvant un signal qui est émis par un système et qui contient les données mais n'était pas destiné à communiquer les données. (Voir : émanation.)

$ interférence *(interference)* (I) /action de menace/ Voir : définition secondaire sous "obstruction".

$ CA intermédiaire *(intermediate CA)*
(D) CA qui produit un certificat croisé à une autre CA. [X509] (Voir : certification croisée.)
Terme déconseillé : les IDOC NE DEVRAIENT PAS utiliser ce terme parce qu'il n'est pas largement connu et mélange les concepts d'une façon potentiellement trompeuse. Par exemple, supposons que l'entité finale 1 ("EE1) soit dans une PKI ("PKI1"), que l'entité finale 2 ("EE2) soit dans une autre PKI ("PKI2"), et que la racine dans PKI1 ("CA1") fasse la certification croisée de la CA racine dans PKI2 ("CA2"). Alors, si EE1 construit le chemin de certification CA1-à-CA2-à-EE2 pour valider un certificat de EE2, l'usage français conventionnel va décrire CA2 comme étant dans une position "intermédiaire" dans ce chemin, et non CA1.

$ contrôles internes *(internal controls)*
(I) /COMPUSEC/ Fonctions, dispositifs, et caractéristiques techniques de matériel et logiciels informatique, en particulier de systèmes d'exploitation. Inclut des mécanismes pour réguler le fonctionnement d'un système informatique par rapport au contrôle d'accès, au contrôle de flux, et au contrôle d'inférence. (À comparer à : contrôles externes.)

$ algorithmes international de chiffrement de données (IDEA, *International Data Encryption Algorithm*)
(N) Chiffrement de bloc symétrique breveté qui utilise une clé de 128 bits et fonctionne sur des blocs de 64 bits. [Schn] (Voir : chiffrement symétrique.)

$ norme internationale *(International Standard)* (N) Voir : définition secondaire sous "ISO".

$ règles du trafic international des armes (ITAR, *International Traffic in Arms Regulations*)
(O) Règles produites par le Département d'État des U.S.A, par délégation de la Loi sur le contrôle de l'exportation des armes (22 U.S.C. 2778) pour contrôler l'exportation et l'importation des articles et des services de défense, incluant les systèmes de sécurité de l'information, comme les systèmes cryptographiques, et la technologie de suppression TEMPEST. (Voir : produit de type 1, Arrangement Wassenaar.)

$ internet, Internet
1. (I) /en minuscules/ Abréviation de "inter réseau".
2. (I) /en majuscules/ L'Internet est le seul système mondial interconnecté de réseaux informatiques commerciaux, gouvernementaux, d'éducation, et autres qui partage (a) la suite de protocoles spécifiée par l'IAB [RFC2026] et (b) les espaces de noms et d'adresses gérés par l'ICANN. (Voir : couche Internet, suite de protocoles Internet.)
Usage : à utiliser avec l'article défini ("le") quand il s'agit d'un nom. Par exemple, on dit "mon LAN est petit, mais l'Internet est grand." On ne dit pas "mon LAN est petit, mais Internet est grand."

$ Bureau de l'architecture de l'Internet (IAB, *Internet Architecture Board*)
(I) Groupe consultatif technique de l'ISOC, mandaté par les membres de l'ISOC pour fournir la vue d'ensemble de l'architecture et des protocoles de l'Internet, et dans le contexte des normes de l'Internet, un organe auquel il peut être fait appel des décisions de l'IESG. Responsable de l'approbation des nominations à l'IESG entre les désignés soumis par le comité des nominations de l'IETF. [RFC2026]

$ Autorité d'allocation des numéros de l'Internet (IANA, *Internet Assigned Numbers Authority*)
(I) Depuis les premiers jours de l'Internet, l'IANA a été mandatée par l'ISOC et le conseil des réseaux fédéraux du gouvernement des USA pour être l'organe central de coordination, d'allocation, et d'enregistrement des paramètres des protocoles de l'Internet. Supervisée par l'ICANN.

$ protocole des messages de contrôle de l'Internet (ICMP, *Internet Control Message Protocol*)
(I) Norme de protocole Internet [RFC0792] qui est utilisée pour rapporter les conditions d'erreur durant le traitement des datagrammes IP et pour échanger d'autres informations concernant l'état du réseau IP.

$ Corporation Internet pour l'allocation des noms et des numéros (ICANN, *Internet Corporation for Assigned Names and Numbers*)
(I) Corporation privée à but non lucratif qui a assumé la responsabilité de l'allocation de l'espace d'adresses IP, de l'allocation des paramètres des protocoles, la gestion du DNS, et les fonctions de gestion du système de serveur racine anciennement assurées par contrat du gouvernement des USA par l'IANA et d'autres entités.
Instructions : la suite des protocoles de l'Internet (IPS), telle que définie par l'IETF et l'IESG, contient de nombreux paramètres, tels que les adresses Internet, les noms de domaines, les numéros de systèmes autonomes, les numéros de protocoles, les numéros d'accès, les OID de base d'information de gestion, incluant les numéros d'entreprise privées, et de nombreux autres. La communauté de l'Internet exige que les valeurs utilisées dans ces champs de paramètres soient allouées de façon univoque. ICANN fait ces allocations comme demandé et tient un registre des valeurs actuelles.
L'ICANN a été formée en octobre 1998, par une coalition des communautés des affaires, des techniciens et des universitaires de l'Internet. Le gouvernement des USA a désigné l'ICANN pour servir d'entité mondiale de consensus avec la responsabilité de la coordination de quatre fonctions clés de l'Internet : l'allocation de l'espace d'adresses IP, l'allocation des paramètres des protocoles, la gestion du DNS, et la gestion du système de serveur racine du DNS.

$ projet-Internet *(Internet-Draft)*
(I) Document de travail de l'IETF, de ses domaines, et de ses groupes de travail. [RFC2026] (À comparer à : RFC.)
Usage : le terme est généralement muni d'un trait d'union lorsque utilisé comme nom ou comme adjectif, bien que dans ce dernier cas ce ne soit pas strictement conforme aux règles de la grammaire française.
Instructions : un projet-Internet n'est pas un document archivé comme l'est une RFC. À la place, un projet-Internet est un document préliminaire ou de travail qui est valide pour une durée maximum de six mois et peut être mis à jour, remplacé, ou rendu obsolète par d'autres documents à tout moment. Il est inapproprié d'utiliser un projet-Internet comme matériel de référence ou de le citer autrement que comme "travail en cours". Bien que la plupart des projets-Internet soient produits par l'IETF, toute organisation intéressée peut demander que ses documents de travail soient publiés comme projets-Internet.

$ groupe de pilotage de l'ingénierie de l'Internet (IESG, *Internet Engineering Steering Group*)
(I) Partie de l'ISOC responsable de la gestion technique des activités de l'IETF et de l'administration du processus de normalisation de l'Internet conformément aux procédures approuvées par les membres de l'ISOC. Directement responsable des actions le long de la "voie de la normalisation", incluant l'approbation finale des spécifications comme normes de l'Internet. Composé des directeurs de zone de l'IETF et du président de l'IETF, qui préside aussi l'IESG. [RFC2026]

$ équipe d'ingénierie de l'Internet (IETF, *Internet Engineering Task Force*)
(I) Groupe auto organisé de personnes qui font des contributions au développement de la technologie de l'Internet. Principal corps engagé dans le développement des normes de l'Internet, bien que ne faisant pas lui-même partie de l'ISOC. Composé de groupes de travail, qui sont disposés en zones (comme la zone Sécurité), chacune coordonnée par un ou plusieurs directeurs de zone *(Area Directors)*. Les nominations à l'IAB et à l'IESG sont faites par un comité choisi au hasard parmi les participants réguliers aux réunions de l'IETF qui se sont portés volontaires. [RFC2026], [RFC3935], [RFC2323]

$ échange de clés Internet (IKE, *Internet Key Exchange*)
(I) Protocole d'établissement de clés IPsec de l'Internet [RFC4306] pour mettre en place du matériel de clés authentifié (a) à utiliser avec ISAKMP et (b) pour d'autres associations de sécurité, comme dans AH et ESP.
Instructions : IKE se fonde sur trois concepts de protocole antérieurs : ISAKMP, OAKLEY, et SKEME.

$ couche Internet *(Internet Layer)* (I) Voir : Suite des protocoles de l'Internet.

$ protocole d'accès au message Internent version (IMAP4, *Internet Message Access Protocol, version 4*)
(I) Protocole Internet [RFC2060] par lequel une station de travail cliente peut accéder de façon dynamique à une boîte aux lettres sur un hôte serveur pour manipuler et restituer des messages électroniques que le serveur a reçus et qu'il détient pour le client. (Voir : POP3.)
Instructions : IMAP4 a des mécanismes facultatifs pour authentifier un client auprès d'un serveur et fournir d'autres services de sécurité. (Voir : IMAP4 AUTHENTICATE.)

$ protocole de commerce ouvert sur l'Internet (IOTP, *Internet Open Trading Protocol*)
(I) Protocole Internet [RFC2801] proposé comme cadre général du commerce sur l'Internet, capable d'encapsuler des transactions de divers systèmes de payement propriétaires (par exemple, GeldKarte, Mondex, SET, Visa Cash). Fournit des services de sécurité facultatifs en incorporant divers mécanismes (par exemple, MD5) et protocoles (par exemple, TLS) de sécurité Internet.

$ autorité d'enregistrement de politique Internet (IPRA, *Internet Policy Registration Authority*)
(I) CA conforme à X.509 qui est la CA supérieure de la hiérarchie de certification Internet qui fonctionne sous les auspices de l'ISOC [RFC1422]. (Voir : /PEM/ sous "hiérarchie de certification".)

$ interface de ligne privée Internet (IPLI, *Internet Private Line Interface*)
(O) Successeur de la PLI, mise à jour pour utiliser TCP/IP et de plus récents équipements militaires de COMSEC (TSEC/KG-84). La PLI était un système modulaire portable qui a été développé pour être utilisé dans des réseaux radio par paquet tactiques. (Voir : chiffrement de bout en bout.)

$ protocole Internet (IP, *Internet Protocol*)
(I) Norme Internet, protocole de couche Internet qui déplace les datagrammes (des ensembles discrets de bits) d'un ordinateur à un autre à travers un inter réseau mais n'assure par la livraison fiable, le contrôle de flux, le séquençage, ni les autres services de bout en bout que fournit TCP. IP version 4 (IPv4) est spécifié dans la RFC 791, et IP version 6 (IPv6) est spécifié dans la RFC 2460. (Voir : adresse IP, TCP/IP.)
Instructions : si IP était utilisé dans une pile OSIRM, IP serait placé au sommet de la couche 3, au dessus des autres protocoles de couche 3 de la pile.
Dans toute pile IPS, IP est toujours présent dans la couche Internet et est toujours placé au sommet de cette couche, par dessus tous les autres protocoles utilisés dans cette couche. Dans un certain sens, IP est le seul protocole spécifié pour la couche Internet IPS ; les autres protocoles qui sont utilisés là, comme AH et ESP, sont juste des variantes de IP.

$ sécurité du protocole Internet *(Internet Protocol security)* Voir : protocole de sécurité IP.

$ option de sécurité du protocole Internet (IPSO, *Internet Protocol Security Option*)
(I) Se réfère à un des trois types d'options de sécurité IP, qui sont des champs qui peuvent être ajoutés à un datagramme IP pour porter des informations de sécurité sur le datagramme. (À comparer à : IPsec.)
Utilisation déconseillée : les IDOC NE DEVRAIENT PAS utiliser ce terme sans un modificateur pour indiquer duquel de ces trois types il s'agit :
- "Option de sécurité de base du DoD" (type d'option IP 130) : définie pour être utilisée sur les réseaux de données d'utilisation courante de l'U.S. DoD. Identifie le niveau de classification du DoD auquel le datagramme doit être protégé et les autorités de protection dont les règles s'appliquent au datagramme. (Une "autorité de protection" est un programme d'accès national (par exemple, GENSER, SIOP-ESI, SCI, NSA, Ministère de l'Énergie) ou un programme d'accès spécial qui spécifie les règles de protection pour la transmission et le traitement des informations contenues dans le datagramme.) [RFC1108]

- "Option de sécurité étendue du DoD" (type d'option IP 133) : permet que des informations d'étiquetage de sécurité supplémentaires, au delà de celles présentes dans l'option de sécurité de base, soient fournies dans le datagramme pour satisfaire aux besoins des autorités enregistrées. [RFC1108]
- "Option de sécurité IP commune" (CIPSO) (type d'option IP 134) : conçue par TSIG pour porter des étiquettes de sécurité hiérarchiques et non hiérarchiques. (Anciennement appelée "Option de sécurité IP commerciale" ; un projet de version 2.3 a été publié le 9 mars 1993 comme projet-Internet mais n'a pas atteint le statut de RFC.) [CIPSO]

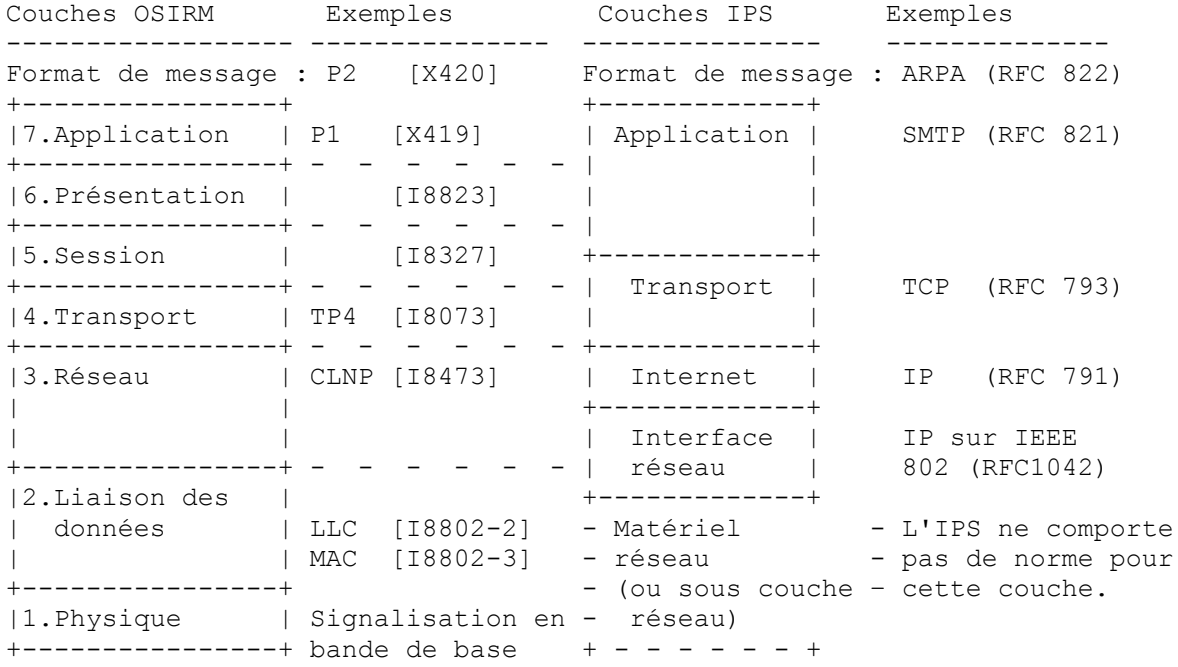
$ suite des protocoles Internet (IPS, *Internet Protocol Suite*)

(I) Ensemble des protocoles de communication réseau qui ont été spécifiés par l'IETF, et approuvés comme normes de l'Internet par l'IESG, sous la direction de l'IAB. (Voir : Architecture de sécurité OSIRM. À comparer à : OSIRM.)

Usage : Cet ensemble de protocoles est populaire sous le nom de "TCP/IP" parce que TCP et IP sont ses composants de base les plus importants. Dans un souci de clarté, le présent glossaire se réfère aux couches de protocoles IPS par leur nom en majuscules, et se réfère aux couches de protocole OSIRM par leur numéro.

Instructions : l'IPS n'a pas de principes architecturaux [RFC1958], mais il n'y a pas de norme de l'Internet qui définisse un modèle de référence d'IPS en couches comme l'OSIRM. Malgré cela, la littérature de la communauté Internet s'est référée (de façon inconséquente) aux couches IPS depuis les premiers développements de l'Internet [Padl].

Le présent glossaire traite l'IPS comme ayant cinq couches de protocole -- Application, Transport, Internet, Interface réseau, et Matériel réseau (ou sous couche réseau) – qui sont illustrées dans le diagramme suivant :



Le diagramme donne une vue approximative de la façon dont les cinq couches IPS s'alignent avec les sept couches OSIRM, et propose des exemples de piles de protocoles qui fournissent des services de messagerie électronique en gros équivalents sur un LAN privé qui utilise la signalisation en bande de base.

- couche d'application IPS : l'usager fait fonctionner un programme d'application. Le programme choisit le service de transport de données dont il a besoin – une séquence de messages de données ou un flux continu de données – et traite les données d'application à la couche Transport pour la livraison.
- couche de transport IPS : cette couche divise les données d'application en paquets, ajoute une adresse de destination à chacun, et les communique de bout en bout – d'un programme d'application à un autre – régulant facultativement le flux et assurant une livraison fiable (sans erreur et en séquence).
- couche Internet IPS : cette couche porte les paquets de transport dans les datagrammes IPS. Elle déplace indépendamment chaque datagramme, de son ordinateur source à l'ordinateur de son adresse de destination, acheminant le datagramme à travers une suite de réseaux et relais et choisissant en route les interfaces réseau appropriées.
- couche d'interface réseau IPS : cette couche accepte des datagrammes à transmettre sur un réseau spécifique. Cette couche spécifie des conventions d'interface pour porter IP sur des protocoles OSIRM de couche 3 et sur des protocoles de sous couche de contrôle d'accès du support de la couche 2 OSIRM. Un exemple est IP sur IEEE 802 (RFC1042).
- couche IPS de matériel réseau : cette couche consiste en des supports de communication physiques spécifiques. Cependant, l'IPS ne spécifie pas ses propres protocoles d'homologue à homologue dans cette couche. À la place, les conventions de mise en couche spécifiées par la couche Interface réseau utilisent des protocoles de couche 2 et 3 qui sont spécifiés par des organismes autres que l'IETF. C'est-à-dire, les fonctions IPS d'adresses *inter*-réseau et pas les fonctions d'adresse *intra*-réseau.

Les deux modèles sont très dissemblables dans les couches supérieures, où le modèle IPS ne comporte pas les couches Session et Présentation. Cependant, cette omission cause moins de différences fonctionnelles entre les modèles qu'on pourrait l'imaginer, et les différences ont relativement peu d'implications pour la sécurité :

- la séparation formelle des couches OSIRM 5, 6, et 7 n'est pas nécessaire dans les mises en œuvre ; les fonctions de ces couches sont parfois mélangées dans une seule unité de logiciel, même dans les protocoles de la suite OSI.
- certains services de couche 5 OSIRM – par exemple, la terminaison de connexion – sont construits dans TCP, et le reste des fonctions de couche 5 et 6 est construit lorsque nécessaire dans les protocoles IPS de couche Application.
- l'OSIRM ne place aucun service de sécurité dans la couche 5 (voir : Architecture de sécurité OSIRM).
- l'absence d'une couche Présentation explicite dans IPS rend parfois plus simple de mettre en œuvre la sécurité dans les applications IPS. Par exemple, une fonction principale de la couche 6 est de convertir les données entre les formes internes et externes, en utilisant une syntaxe de transfert pour coder sans ambiguïté les données à transmettre. Si une application OSIRM chiffre des données pour les protéger contre la divulgation durant la transmission, le codage de transfert doit être fait avant le chiffrement. Si une application fait le chiffrement, comme c'est fait dans le traitement de message OSI et dans les protocoles de service de répertoire, les fonctions de couche 6 doivent alors être dupliquées dans la couche 7. [X400, X500].

Les deux modèles sont presque identiques au sommet de la couche 3 OSIRM, où le protocole de couche réseau sans connexion (CLNP, *Connectionless Network Layer Protocol*) OSI et l'IP d'IPS sont presque similaires. Les services de sécurité en mode connexion offerts dans la couche 3 OSIRM sont inapplicables dans l'IPS, parce que la couche IPS Internet n'a pas le service explicite en mode connexion offert dans l'OSIRM.

$ protocole d'association de sécurité et de gestion de clé Internet (ISAKMP, *Internet Security Association and Key Management Protocol*)

(I) Protocole IPsec Internet [RFC2408] pour négocier, établir, modifier, et supprimer les associations de sécurité, et pour échanger les données de génération de clé et d'authentification, indépendamment des détails de la technique spécifique de génération de clé, du protocole d'établissement de clés, de l'algorithme de chiffrement, ou du mécanisme d'authentification.

Instructions : ISAKMP prend en charge la négociation des associations de sécurité pour des protocoles à toutes les couches IPS. En centralisant la gestion des associations de sécurité, ISAKMP réduit la duplication de fonctionnalités au sein de chaque protocole. ISAKMP peut aussi réduire le temps d'établissement de connexion en négociant en une seule fois toute une pile de services. Une authentification forte est exigée dans les échanges ISAKMP, et un algorithme de signature numérique fondé sur la cryptographie asymétrique est utilisé dans le composant d'authentification ISAKMP.

Les négociations ISAKMP sont conduites en deux "phases" :

- "négociation de phase 1". Elle établit une association de sécurité à utiliser par ISAKMP pour protéger ses propres opérations de protocole.
- "négociation de phase 2". Une négociation de phase 2 (qui est protégée par une association de sécurité établie par une négociation de phase 1) établit une association de sécurité à utiliser pour protéger les opérations d'un protocole autre que ISAKMP, comme ESP.

$ Société Internet (ISOC, *Internet Society*)

(I) Société professionnelle concernée par le développement de l'Internet (y compris celui des normes techniques de l'Internet) par la façon dont l'Internet est et peut être utilisé, et par les aspects sociaux, politiques, et techniques qui en résultent. Le conseil d'administration *(Board of Trustees)* de l'ISOC approuve les nominations à l'IAB parmi les candidats retenus par le comité des nominations de l'IETF. [RFC2026]

$ norme Internet *(Internet Standard)*

(I) Spécification, approuvée par l'IESG et publiée comme RFC, qui est stable et bien comprise, est techniquement compétente, a plusieurs mises en œuvre indépendantes et interopérables avec une expérience de fonctionnement substantielle, jouit d'un soutien public significatif, et est reconnue comme utile dans certaines, ou toutes, les parties de l'Internet. (RFC2026) (À comparer à : RFC.)

Instructions : le "processus de normalisation de l'Internet" est une activité de l'ISOC qui est organisée et gérée par l'IAB et l'IESG. Le processus concerne tous les protocoles, procédures, et conventions utilisés dans ou par l'Internet, qu'ils fassent ou non partie de l'IPS. La "voie de normalisation Internet" a trois niveaux de maturité croissants : proposition de norme, projet de norme et norme. (À comparer à : ISO, W3C.)

$ inter réseau *(internetwork)*

(I) Système de réseaux interconnectés ; un réseau de réseaux. Usuellement abrégé en "internet". (Voir : internet, Internet.)

Instructions : un internet peut être construit en utilisant des passerelles de couche 3 OSIRM pour mettre en œuvre les connexions entre un ensemble de sous réseaux similaires. Avec des sous réseaux dissemblables, c'est-à-dire, des sous réseaux qui diffèrent par le service de protocole de couche 3 qu'ils offrent, un internet peut être construit en mettant en œuvre un protocole d'inter réseautage uniforme (par exemple, IP) qui fonctionne par dessus la couche 3 et cache

l'hétérogénéité des sous réseaux sous-jacents aux hôtes qui utilisent les services de communication fournis par l'internet. (Voir : routeur.)

$ intranet
(I) Réseau informatique, en particulier celui fondé sur la technologie Internet, qu'utilise une organisation pour ses besoins internes (et généralement privés) et qui est fermé aux externes. (Voir : extranet, VPN.)

$ intrus *(intruder)*
(I) Entité qui obtient ou tente d'obtenir l'accès à un système ou à des ressources système sans avoir l'autorisation de le faire, (Voir : intrusion. À comparer à : adversaire, craqueur, hacker.)

$ intrusion
1. (I) Événement de sécurité ou combinaison de plusieurs événements de sécurité, qui constitue un incident de sécurité dans lequel un intrus obtient, ou tente d'obtenir, l'accès à un système ou à une ressource système sans avoir l'autorisation de le faire, (Voir : IDS.)
2. (I) Type d'action de menace par laquelle une entité non autorisée obtient l'accès à des données sensibles en circonvenant les protections d'un système. (Voir : divulgation non autorisée.)

Usage : ce type d'action de menace inclut les sous types suivants :
- "franchissement" : obtenir l'accès physique à des données sensibles en circonvenant les protections d'un système ;
- "pénétration" : obtenir l'accès logique aux données sensibles en circonvenant les protections d'un système ;
- "ingénierie inverse" : acquérir des données sensibles en désassemblant et en analysant la conception d'un composant d'un système.
- "cryptanalyse" : transformer des données chiffrées en texte source sans avoir antérieurement la connaissance des paramètres ou processus de chiffrement. (Voir : principale entrée sous "cryptanalyse".)

$ détection d'intrusion *(intrusion detection)*
(I) Percevoir et analyser les événements d'un système dans le but de remarquer (c'est-à-dire, se mettre au courant des) tentatives d'accès sans autorisation aux ressources d'un système. (Voir : détection d'anomalie, IDS, détection de mauvais usage. À comparer à : détection d'extrusion.) [IDSAN], [IDSSC], [IDSSE], [IDSSY]

Usage : cela inclut les sous-types suivants :
- "détection active" : analyse en temps réel ou presque réel des données d'événement d'un système pour détecter les intrusions en cours, qui résulte en une réponse de protection immédiate ;
- "détection passive" : analyse hors ligne des données d'audit pour détecter les intrusions passées, qui sont rapportées à l'officier de sécurité du système pour une action corrective. (À comparer à : audit de sécurité.)

$ système de détection d'intrusion (IDS, *intrusion detection system*)
1. (N) Processus ou sous système, mis en œuvre dans le logiciel ou le matériel, qui (a) automatise les tâches de surveillance des événements qui surviennent dans un réseau informatique et (b) les analyse à la recherche de signes de problèmes de sécurité. [SP31] (Voir : détection d'intrusion.)
2. (N) Système d'alarme de sécurité pour détecter une entrée non autorisée. [DC6/9].

Instructions : les processus de détection d'intrusion active peuvent être fondés sur l'hôte ou sur le réseau :
- "fondé sur l'hôte" : les composants de détection d'intrusion -- capteurs et analyseurs de trafic -- fonctionnent directement sur les hôtes qu'ils sont destinés à protéger ;
- "fondé sur le réseau" : des capteurs sont placés sur des composants de sous réseau, et les composants d'analyse fonctionnent soit sur des composants de sous réseau, soit sur les hôtes.

$ date d'invalidité *(invalidity date)*
(N) Extension d'entrée de CRL X.509 qui "indique la date à laquelle il est connu ou suspecté que la [clé privée du certificat révoqué] a été compromise ou à laquelle le certificat devrait autrement être considéré comme invalide." [X509].

Instructions : cette date peut être plus tôt que la date de révocation dans l'entrée de la CRL, et peut même être plus tôt que la date de production des CRL antérieures. Cependant, la date d'invalidité n'est pas, par elle-même, suffisante pour les besoins du service de non répudiation. Par exemple, pour répudier frauduleusement une signature générée de façon valide, un détenteur de clé privée peut prétendre faussement que la clé a été compromise à un instant passé.

$ adresse IP *(IP address)*
(I) Adresse inter réseau d'un ordinateur qui est allouée pour être utilisée par IP et d'autres protocoles.

Instructions : une adresse IP version 4 (RFC 791) a quatre parties de 8 bits et est écrite comme une série de quatre nombres décimaux séparés par des points. Exemple : l'adresse de l'hôte nommé "rosslyn.bbn.com" est 192.1.7.10.

Une adresse IP version 6 (RFC2373) a huit parties de 16 bits et est écrite avec huit nombres hexadécimaux séparés par deux points. Exemples : 1080:0:0:0:8:800:200C:417A et FEDC:BA98:7654:3210:FEDC:BA98:7654:3210.

$ option de sécurité IP *(IP Security Option)* (I) Voir : option de sécurité du protocole Internet.

$ protocole de sécurité IP (IPsec, *IP Security Protocol*)

1a. (I) Nom du groupe de travail de l'IETF qui spécifie une architecture [RFC2401], [RFC4301] et un ensemble de protocoles pour fournir des services de sécurité pour le trafic IP. (Voir : AH, ESP, IKE, SAD, SPD. À comparer à : IPSO.)

1b. (I) Nom collectif pour l'architecture de sécurité IP [RFC4301] et l'ensemble associé de protocoles (principalement AH, ESP, et IKE).

Usage : dans les IDOC qui utilisent l'abréviation "IPsec", les lettres "IP" DEVRAIENT être en majuscules, et les lettres "sec" NE le DEVRAIENT PAS.

Instructions : les services de sécurité fournis par IPsec incluent le service de contrôle d'accès, le service d'intégrité des données sans connexion, le service d'authentification d'origine des données, la protection contre les répétitions (détection de l'arrivée de datagrammes dupliqués, au sein d'une fenêtre restreinte) le service de confidentialité des données, et la confidentialité limitée des flux de trafic. IPsec spécifie (a) des protocoles de sécurité (AH et ESP), (b) des associations de sécurité (ce qu'elles sont, comment elles fonctionnent, comment elles sont gérées, et le traitement associé) (c) la gestion des clés (IKE), et (d) des algorithmes d'authentification et de chiffrement. La mise en œuvre de IPsec est facultative pour IP version 4, mais obligatoire pour IP version 6. (Voir : mode transport, mode tunnel.)

$ ISO

(I) Organisation internationale de normalisation, organisation volontaire, non gouvernementale, non soumise à un traité, établie en 1947, dont les membres votants sont les organisations de normalisation des nations participantes et les organisations non votantes sont des observateurs. (À comparer à : ANSI, IETF, UIT-T, W3C.)

Instructions : légalement, l'ISO est une organisation privée suisse à but non lucratif. L'ISO et la CEI (le comité électrotechnique international) forment le système spécialisé de la normalisation mondiale. Les organismes nationaux qui sont membres de l'ISO ou de la CEI participant au développement des normes internationales à travers les comités techniques de l'ISO et de la CEI qui traitent des champs d'activité particuliers. D'autres organisations internationales gouvernementales et non gouvernementales, en liaison avec l'ISO et la CEI, y prennent aussi part. (AFNOR est le membre votant français de l'ISO. L'ISO est un membre de classe D de l'UIT-T.)

Le processus de développement des normes de l'ISO a quatre niveaux croissants de maturité : document de travail (WD, *Working Draft*), projet de comité (CD, *Committee Draft*), projet de norme internationale (DIS, *Draft International Standard*), et norme internationale (IS, *International Standard*). (À comparer à : "voie de la normalisation de l'Internet" sous "Norme Internet".) Dans les technologies de l'information, l'ISO et la CEI ont un comité technique conjoint, le JTC 1 ISO/CEI. Les DIS adoptés par le JTC 1 circulent entre les organismes nationaux pour les votes, et la publication comme IS exige l'approbation d'au moins 75 % des organismes nationaux qui formulent un vote.

$ ISO 17799

(N) Norme internationale qui est un code de conduite, dérivé de la partie 1 de la norme anglaise BSI 7799, pour la gestion de la sécurité des systèmes d'information dans une organisation. Cette norme ne donne aucun matériel définitif ou spécifique sur un des sujets de la sécurité. Il donne des lignes directrices générales sur des sujets très divers, mais ne rentre normalement pas dans les détails. (Voir : IATF, [SP14].)

$ produire *(issue)*

(I) /PKI/ Générer et signer un certificat numérique (ou une CRL) et, généralement, le distribuer et le rendre disponible aux utilisateurs potentiels de certificat (ou utilisateurs de CRL). (Voir : création de certificat.)

Usage : le terme "produire" est généralement compris comme ne se référant pas seulement à la création d'un certificat numérique (ou d'une CRL) mais aussi à le rendre disponible aux utilisateurs potentiels, comme en le mémorisant dans un répertoire ou autre ou en le publiant par d'autres moyens. Cependant, ABA [DSG] limite explicitement ce terme au processus de création et exclut tout son processus de publication ou distribution.

$ producteur *(issuer)*

1. (I) /certificat, CRL/ CA qui signe un certificat ou une CRL.

Instructions : un certificat X.509 comporte toujours le nom du producteur. Le nom peut inclure une valeur de nom commun.

2. (O) /carte de payement, SET/ "L'institution financière ou son agent qui produit le numéro de compte univoque principal du détenteur de la carte pour la marque de carte de payement." [SET2]

Instructions : l'institution qui établit le compte pour un détenteur de carte et produit la carte de payement garantit aussi le payement pour les transactions autorisées qui utilisent la carte en accord avec les règles de la marque de carte et la législation locale. [SET1]

$ UIT-T (ITU-T, *International Telecommunications Union, Telecommunication Standardization Sector*)

(N) Union internationales des télécommunications, secteur de la normalisation des télécommunications (anciennement le "CCITT, Comité consultatif international des téléphones et télégraphes") une organisation du traité des Nations Unies qui

est composée principalement des autorités postales, téléphoniques, et télégraphiques des états membres et qui publie des normes appelées "Recommandations". (Voir : X.400, X.500.)
Instructions : le Département d'État représente les USA. L'UIT-T travaille sur de nombreuses sortes de systèmes de communication. L'UIT-T coopère avec l'ISO sur les normes de protocole de communication, et de nombreuses Recommandations dans ce domaine sont aussi publiées comme norme ISO avec un nom et un numéro ISO.

$ brouillage *(jamming)*
(N) Attaque qui tente d'interférer avec la réception de communications diffusées. (Voir : anti brouillage, déni de service. À comparer à : inondation.)
Instructions : le brouillage utilise "l'interférence" comme type "d'obstruction" destinée à causer "l'interruption". Le brouillage d'un signal diffusé est normalement fait en diffusant un second signal que les receveurs ne peuvent pas séparer du premier. Le brouillage est principalement considéré dans les communications sans fil, mais peut aussi être fait dans certaines technologies filaires, comme les LAN qui utilisent des techniques de contention pour partager un support de diffusion.

$ Kerberos
(I) Système développé au Massachusetts Institute of Technology qui dépend de mots de passe et de chiffrement symétrique (DES) pour mettre en œuvre un service d'authentification d'entité homologue fondé sur un ticket et un service de contrôle d'accès réparti dans un environnement de réseau client-serveur. [RFC4120], [Stei] (Voir : domaine.)
Instructions : Kerberos a été à l'origine développé par le Projet Athena est tire son nom du chien mythique à trois têtes qui garde l'Hadès. L'architecture du système comporte des serveurs d'authentification et des serveurs qui accordent des tickets qui fonctionnent comme un ACC et un KDC.
La RFC4556 décrit les extensions à la spécification Kerberos qui modifient l'échange initial d'authentification entre un client et le KDC. Les extensions emploient la cryptographie à clé publique pour permettre au client et au KDC de s'authentifier mutuellement et établir des clés partagées symétriques qui sont utilisées pour achever l'échange. (Voir : PKINIT.)

$ noyau *(kernel)*
(I) Petite partie de confiance d'un système qui fournit des services dont dépendent d'autres parties du système. (Voir : noyau de sécurité.)

$ système d'exploitation à noyau sécurisé (KSOS, *Kernelized Secure Operating System*)
(O) Système d'exploitation d'ordinateur MLS, conçu pour être un remplacement d'une sécurité démontrée pour UNIX Version 6, et consistant en un noyau de sécurité, des programmes hors noyau d'utilitaires en rapport avec la sécurité, et des environnements de développement et de soutien facultatifs d'application UNIX. [Perr]
Instructions : KSOS-6 était la mise en œuvre sur un SCOMP. KSOS-11 était la mise en œuvre de Ford Aerospace and Communications Corporation sur les ordinateurs DEC PDP-11/45 et PDP-11/70.

$ clé *(key)*
1a. (I) /cryptographie/ Paramètre d'entrée utilisé pour faire varier une fonction de transformation effectuée par un algorithme de chiffrement. (Voir : clé privée, clé publique, clé de mémorisation, clé symétrique, clé de trafic. À comparer à : valeur d'initialisation.)
1b. (O) /cryptographie/ Utilisée en forme singulière comme nom collectif se référant au matériel de clés ou de chiffrement. Exemple : un appareil de remplissage peut être utilisé pour transférer une clé entre deux appareils cryptographiques.
2. (I) /anti brouillage/ Paramètre d'entrée utilisé pour faire varier un processus qui détermine des schémas pour une mesure anti brouillage. (Voir : saut de fréquence, spectre étalé.)
Instructions : une clé est normalement spécifiée comme une séquence de bits ou d'autres symboles. Si une valeur de clé doit être gardée secrète, la séquence de symboles qui la comprend devrait être aléatoire, ou au moins pseudo aléatoire, parce que cela rend la clé plus difficile à deviner pour un adversaire. (Voir : attaque en force brute, cryptanalyse, force.)

$ accord de clé *(key agreement)* (algorithme ou protocole)
1. (I) Méthode d'établissement de clé (en particulier qui implique un chiffrement asymétrique) par laquelle deux entités ou plus, sans accord préalable sauf un échange public de données (comme des clés publiques) peuvent chacune générer la même valeur de clé. C'est-à-dire que la méthode n'envoie pas un secret d'une entité à l'autre ; à la place, les deux entités, sans arrangement préalable sauf un échange public de données, peuvent calculer la même valeur secrète, mais cette valeur ne peut pas être calculée par d'autres entités non autorisées. (Voir : Diffie-Hellman-Merkle, établissement de clé, KEA, MQV. À comparer à : transport de clé.)
2. (O) "Méthode pour négocier une valeur de clé en ligne sans transférer la clé, même sous une forme chiffrée, par exemple, la technique Diffie-Hellman." [X509] (Voir : Diffie-Hellman-Merkle.)
3. (O) "Procédure par laquelle deux parties différentes génèrent des clés symétriques partagées telle que toute clé symétrique partagée est une fonction des informations apportées par tous les participants légitimes, afin qu'aucune

partie [seule] ne puisse prédéterminer la valeur de la clé." [A9042]
Exemple : un générateur de message et le receveur prévu peuvent chacun utiliser leur propre clé privée et la clé publique de l'autre avec l'algorithme Diffie-Hellman-Merkle pour calculer d'abord une valeur de secret partagé et, à partir de cette valeur, déduire une clé de session pour chiffrer le message.

$ authentification de clé *(key authentication)*
(N) "Assurance des participants légitimes à un accord de clé [c'est-à-dire, dans un protocole d'accord de clé] qu'aucune partie non légitime ne possède la clé symétrique partagée." [A9042]

$ clé auto clé (KAK, *key-auto-key*)
(D) "Logique cryptographique [c'est-à-dire, mode de fonctionnement] qui utilise la clé précédente pour produire la clé." [C4009], [A1523] (Voir : CTAK, /fonctionnement cryptographique/ sous "mode".)
Terme déconseillé : les IDOC NE DEVRAIENT PAS utiliser ce terme ; il n'est ni bien connu ni précisément défini. À la place, utiliser les termes associés aux modes qui sont définis dans les normes, tels que CBC, CFB, et OFB.

$ centre de clés *(key center)*
(I) Processus centralisé de distribution de clés (utilisé dans la cryptographie symétrique) usuellement un système informatique séparé, qui utilise des clés maîtresses (c'est-à-dire, des KEK) pour chiffrer et distribuer les clés de session nécessaires à une communauté d'utilisateurs.
Instructions : une norme ANSI [A9017] définit deux types de centres de clés : "centre de distribution de clés" et "centre de traduction de clés".

$ confirmation de clé *(key confirmation)*
(N) "Assurance [fournie aux] participants légitimes à un protocole d'établissement de clé que les [parties qui sont destinées à partager] la clé symétrique possèdent réellement la clé symétrique partagée." [A9042]

$ distribution de clé *(key distribution)*
(I) Processus qui livre une clé de chiffrement provenant de la localisation où elle a été générée à la localisations où elle est utilisée dans un algorithme de chiffrement. (Voir : établissement de clé, gestion de clé.)

$ centre de distribution de clés (KDC, *key distribution center*)
1. (I) Type de centre de clés (utilisé dans la cryptographie symétrique) qui met en œuvre un protocole de distribution de clés pour fournir des clés (usuellement, des clés de session) à deux entités (ou plus) qui souhaitent communiquer en toute sécurité. (À comparer à : centre de traduction de clés.)
2. (N) "Facilité de COMSEC pour générer et distribuer des clé de façon électrique." [C4009]

Instructions : un KDC distribue les clés à Alice et Bob, qui (a) souhaitent communiquer ensemble mais ne partagent pas actuellement de clés, (b) chacun partage une KEK avec le KDC, et (c) peut n'être pas capable de générer ou acquérir de clés par lui-même. Alice demande les clés au KDC. Le KDC génère ou acquiert les clés et fait deux ensembles identiques. Le KDC chiffre un ensemble dans la KEK qu'il partage avec Alice, et envoie l'ensemble chiffré à Alice. Le KDC chiffre le second ensemble dans la KEK qu'il partage avec Bob, et (a) envoie l'ensemble chiffré à Alice pour qu'elle le transmette à Bob ou (b) l'envoie directement à Bob (bien que cette dernière option ne soit pas acceptée dans la norme ANSI [A9017]).

$ encapsulation de clé *(key encapsulation)*
(N) Technique de récupération de clé pour mémoriser la connaissance d'une clé de chiffrement en la chiffrant avec une autre clé et en s'assurant que seuls certains tiers appelés "agents de récupération" peuvent effectuer l'opération de déchiffrement pour restaurer la clé mémorisée. L'encapsulation de clé permet normalement la restitution directe d'une clé secrète utilisée pour assurer la confidentialité des données. (À comparer à : tiers de confiance.)

$ clé de chiffrement de clé (KEK, *key-encrypting key*)
(I) Clé cryptographique qui (a) est utilisée pour chiffrer d'autres clés (soit des DEK, soit d'autres TEK) pour transmettre ou mémoriser mais (b) (usuellement) n'est pas utilisée pour chiffrer des données d'application. Usage : parfois appelée "clé chiffrante de clé".

$ tiers de confiance *(key escrow)*
(N) Technique de récupération de clé pour mémoriser la connaissance d'une clé cryptographique ou de parties d'elle par la garde d'un ou plusieurs tiers appelés "agents de confiance", afin que la clé puisse être récupérée et utilisée dans des circonstances spécifiées. (À comparer à : encapsulation de clé.)
Instructions : le tiers de confiance est normalement mis en œuvre avec des techniques de connaissance partagée. Par exemple, la norme de chiffrement par tiers de confiance *(Escrowed Encryption Standard)* [FP185] confie deux composants d'une clé partagée d'un appareil unique à deux tiers de confiance séparés. Les agents ne fournissent le composant qu'à quelqu'un qui est légalement autorisé à conduire la surveillance électronique de télécommunications chiffrées par cet

appareil spécifique. Les composants sont utilisés pour reconstruire la clé d'appareil unique, et elle est utilisée pour obtenir la clé de session nécessaire pour déchiffrer les communications.

$ établissement de clé *(key establishment)* (algorithme ou protocole)
1. (I) Procédure qui combine les étapes de génération et de distribution de clés nécessaires pour établir ou installer une association de communication sûre.
2. (I) Procédure qui résulte en le partage du matériel de chiffrement entre deux entités système ou plus. [A9042], [SP56]
Instructions : les deux techniques de base pour l'établissement de clé sont "l'accord de clé" et "le transport de clé".

$ algorithme d'échange de clés (KEA, *Key Exchange Algorithm*)
(N) Méthode d'accord de clés [SKIP], [RFC2773] qui se fonde sur l'algorithme Diffie-Hellman-Merkle et utilise des clés asymétriques de 1024 bits. (Voir : CAPSTONE, CLIPPER, FORTEZZA, SKIPJACK.)
Instructions : KEA a été développé par la NSA et était anciennement classifié au niveau "Secret" de l'US DoD. Le 23 juin 1998, la NSA a annoncé que KEA avait été déclassifié.

$ génération de clé *(key generation)*
(I) Processus qui crée la séquence de symboles qui constitue une clé de chiffrement. (Voir : gestion de clé.)

$ générateur de clé *(key generator)*
1. (I) Algorithme qui utilise des règles mathématiques pour produire de façon déterministe une séquence pseudo aléatoire de valeurs de clés de chiffrement.
2. (I) Appareil de chiffrement qui incorpore un mécanisme de génération de clés et applique la clé au texte source pour produire le texte chiffré (par exemple, en traitant avec l'opérateur OU exclusif (a) une représentation en chaîne binaire de la clé avec (b) une représentation en chaîne binaire du texte source).

$ longueur de clé *(key length)*
(I) Nombre de symboles (usuellement déclaré comme un nombre de bits) nécessaire pour être capable de représenter toute valeur possible d'une clé de chiffrement. (Voir : espace de clés.)

$ durée de vie de clé *(key lifetime)*
1. (D) Synonyme de "période de cryptage".
Définition déconseillée : les IDOC NE DEVRAIENT PAS utiliser ce terme avec la définition 1 parce que la période de cryptage d'une clé peut être seulement une partie de la durée de vie d'une clé. Une clé pourrait être générée à un moment antérieur au début de sa cryptopériode et pourrait ne pas pouvoir être détruite (c'est-à-dire, mise à zéro) tant qu'un certain délai n'est pas écoulé après la fin de sa période de cryptage.
2. (O) /MISSI/ Attribut d'une paire de clés MISSI qui spécifie un espace de temps qui borde la période de validité de tout certificat MISSI de clé publique X.509 qui contient le composant public de la paire. (Voir : période de cryptage.)

$ chargeur de clés *(key loader)* (N) Synonyme de "appareil de remplissage".

$ facilité de chargement et d'initialisation de clé (KLIF, *key loading and initialization facility*)
(N) Endroit où le matériel ECU est activé après avoir été fabriqué. (À comparer à : CLEF.)
Instructions : avant d'aller à son KLIF, un ECU n'est pas prêt à être mis en fonction, généralement parce que il n'est pas encore capable de recevoir des DEK. Le KLIF emploie des processus de confiance pour achever l'ECU en installant les données nécessaires comme les KEK, les valeurs de germe, et, dans certains cas, un logiciel de chiffrement. Après le traitement de KLIF, l'ECU est prêt à être déployé.

$ gestion de clé *(key management)*
1a. (I) Processus de traitement du matériel de chiffrement durant son cycle de vie dans un système cryptographique, et la supervision et le contrôle de ce processus. (Voir : distribution de clé, tiers de confiance, matériel de chiffrement, infrastructure de clé publique.)
Usage : généralement compris comme incluant la commande, la génération, la mémorisation, l'archivage, l'engagement, la distribution, le chargement, la destruction, l'analyse, et la comptabilité du matériel.
1b. (O) /NIST/ "Les activités qui impliquent le traitement des clés de chiffrement et des autres paramètres de sécurité qui s'y rapportent (par exemple, les IV, les compteurs) durant la totalité du cycle de vie des clés, incluant leur génération, leur mémorisation, leur distribution, leur entrée et leur utilisation, leur suppression ou destruction, et leur archivage." [FP140], [SP57]
2. (O) /OSIRM/ "Génération, mémorisation, distribution, suppression, archivage et application de clés en accord avec une politique de sécurité." [I7498-2]

$ protocole de gestion de clés (KMP, *Key Management Protocol*)

(N) Protocole pour établir une clé symétrique partagée entre une paire (ou un groupe) d'utilisateurs. (Une version de KMP a été développée par SDNS, et une autre par SILS.) Rendu obsolète par ISAKMP et IKE.

$ matériel de clé *(key material)*
(D) Synonyme de "matériel de chiffrement".
Utilisation déconseillée : les IDOC NE DEVRAIENT PAS utiliser ce terme comme synonyme de "matériel de chiffrement".

$ paire de clés *(key pair)*
(I) Ensemble de clés mathématiquement liées – une clé publique et une clé privée – qui sont utilisées pour un chiffrement asymétrique et sont générées d'une façon qui rend infaisable le calcul pour déduire la clé privée de la connaissance de la clé publique. (Voir : Diffie-Hellman-Merkle, RSA.)
Instructions : le possesseur d'une paire de clé divulgue la clé publique aux autres entités système afin qu'elles puissent utiliser la clé pour (a) chiffrer les données, (b) vérifier une signature numérique, ou (c) générer une clé avec un algorithme d'accord de clé. La clé privée correspondante est gardée secrète par le possesseur, qui l'utilise pour (a') déchiffrer les données, (b') générer une signature numérique, ou (c') générer une clé avec un algorithme d'accord de clé.

$ récupération de clé *(key recovery)*
1. (I) /cryptanalyse/ Processus pour apprendre la valeur d'une clé cryptographique qui était précédemment utilisée pour effectuer une opération cryptographique. (Voir : cryptanalyse, récupération.)
2. (I) /sauvegarde/ Techniques qui fournissent des moyens de remplacement intentionnels pour accéder à la clé utilisée pour le service de confidentialité des données dans une association chiffrée. [DoD4] (À comparer à : récupération.)

Instructions : on suppose que le système cryptographique comporte un moyen principal pour obtenir la clé à travers un algorithme ou protocole d'établissement de clé. Pour le moyen secondaire, il y a deux classes de techniques de récupération de clé : l'encapsulation de clé et le tiers de confiance,

$ espace de clés *(key space)*
(I) Gamme des valeurs possibles d'une clé de chiffrement ; ou nombre des transformations distinctes supportées par un algorithme cryptographique particulier. (Voir : longueur de clé.)

$ centre de traduction de clés *(key translation center)*
(I) Type de centre de clés qui met en œuvre un protocole de distribution de clés (fondé sur la cryptographie symétrique) pour convoyer des clés entre deux parties (ou plus) qui souhaitent communiquer de façon sûre. (À comparer à : centre de distribution de clés.)
Instructions : un centre de traduction de clés transfère les clés pour une future communication entre Bob et Alice, qui (a) souhaitent communiquer ensemble mais ne partagent actuellement pas de clés, (b) chacun partage une KEK avec le centre, et (c) a la capacité de générer ou acquérir des clés par lui-même. Alice génère ou acquiert un ensemble de clés pour la communication avec Bob. Alice chiffre l'ensemble dans la KEK qu'elle partage avec le centre et envoie l'ensemble chiffré au centre. Le centre déchiffre l'ensemble, chiffre à nouveau l'ensemble avec la KEK qu'il partage avec Bob, et (a) envoie cet ensemble rechiffré à Alice pour qu'elle le transmette à Bob ou (b) l'envoie directement à Bob (bien que la distribution directe ne soit pas acceptée par la norme ANSI [A9017]).

$ transport de clé *(key transport)* (algorithme ou protocole)
1. (I) Méthode d'établissement de clé par laquelle une clé secrète est générée par une entité système dans une association de communication et envoyée en toute sécurité à une autre entité dans l'association. (À comparer à : accord de clé.)
   Instructions : soit (a) une entité génère une clé secrète et l'envoie en toute sécurité à l'autre entité, soit (b) chaque entité génère une valeur secrète et l'envoie en toute sécurité à l'autre entité, où les deux valeurs sont combinées pour former une clé secrète. Par exemple, un générateur de message peut générer une clé de session aléatoire et ensuite utiliser l'algorithme RSA pour chiffrer cette clé avec la clé publique du receveur prévu.
2. (O) "La procédure pour envoyer une clé symétrique d'une partie aux autres parties. Par suite, tous les participants légitimes partagent une clé symétrique commune d'une façon telle que la clé symétrique soit entièrement déterminée par une seule partie." [A9042]

$ mise à jour de clé *(key update)*
1. (I) Déduire une nouvelle clé d'une clé existante. (À comparer à : changement de clé.)
2. (O) Processus de chiffrement irréversible qui modifie une clé pour produire une nouvelle clé. [C4009]

$ validation de clé *(key validation)*
1. (I) "Procédure qui permet au receveur d'une clé publique de vérifier que la clé est conforme aux exigences arithmétiques d'une telle clé afin de déjouer certains types d'attaques." [A9042] (Voir : clé faible)
2. (D) Synonyme de "validation de certificat".

Utilisation déconseillée : Les IDOC NE DEVRAIENT PAS utiliser ce terme comme synonyme de "validation de certificat" ; cela dupliquerait sans nécessité la signification du dernier terme et mélangerait les concepts d'une façon potentiellement trompeuse. En validant un certificat de clé publique X.509, la clé publique contenue dans le certificat est normalement traitée comme un objet de données opaque.

$ hachage chiffré *(keyed hash)*
(I) Hachage cryptographique (par exemple, selon la [RFC1828]) dans lequel la transposition en un résultat de hachage est modifiée par un second paramètre d'entrée qui est une clé de chiffrement. (Voir : somme de contrôle.)
Instructions : si l'objet de données d'entrée est changé, un nouveau résultat de hachage correspondant ne peut pas être correctement calculé sans connaître la clé secrète. Donc, la clé secrète protège le résultat du hachage afin qu'il puisse être utilisé comme somme de contrôle même lorsque il y a une menace d'attaque active contre les données. Il y a deux types de base de hachage chiffré :
- une fonction fondée sur un algorithme de chiffrement à clé. Exemple : code d'authentification de données.
- une fonction fondée sur un hachage sans clé qui est amélioré en combinant (par exemple, par enchaînement) le paramètre d'objet des données d'entrée avec un paramètre de clé avant de transposer en résultat de hachage. Exemple : HMAC.

$ matériel de chiffrement *(keying material)*
1. (I) Données qui sont nécessaires pour établir et maintenir une association de sécurité cryptographique, comme des clés, des paires de clé, et des IV.
2. (O) "Informations de clé, de code, ou d'authentification sous une forme physique ou magnétique." [C4009] (À comparer à : matériel COMSEC.)

$ identifiant de matériel de chiffrement (KMID, *keying material identifier*)
1. (I) Identifiant alloué à un élément de matériel de chiffrement.
2. (O) /MISSI/ Identifiant de 64 bits qui est alloué à une paire de clés lorsque la clé publique est liée dans un certificat MISSI de clé publique X.509.

$ Khafre
(N) Chiffrement de bloc symétrique breveté conçu par Ralph C. Merkle comme remplacement incorporé de DES. [Schn]
Instructions : Khafre a été conçu pour un chiffrement efficace de petites quantités de données. Cependant, parce que Khafre ne précalcule pas les tableaux utilisés pour le chiffrement, il est plus lent que Khufu pour les grandes quantités de données.

$ Khufu
(N) Chiffrement de bloc symétrique breveté conçu par Ralph C. Merkle comme remplacement incorporé de DES. [Schn]
Instructions : Khufu a été conçu pour le chiffrement rapide de grandes quantités de données. Cependant, parce que Khufu précalcule les tableaux utilisés dans le chiffrement, il est moins efficace que Khafre pour les petites quantités de données.

$ attaque de texte source connu *(known-plaintext attack)*
(I) Technique de cryptanalyse dans laquelle l'analyste essaye de déterminer la clé à partir de la connaissance de paires de texte source - texte chiffré connues (bien que l'analyste puisse aussi avoir d'autres indices, comme de connaître l'algorithme de chiffrement).

$ kracker (O) Ancienne orthographe de "cracker".

$ KSOS, KSOS-6, KSOS-11 (O) Voir : système d'exploitation à noyau sécurisé *(Kernelized Secure Operating System.)*

$ étiquette *(label)* Voir : horodatage, étiquette de sécurité.

$ attaque de laboratoire *(laboratory attack)*
(O) "Utilisation d'équipement de récupération de signal sophistiqué dans un environnement de laboratoire pour récupérer des informations à partir d'un support de mémorisation de données." [C4009]

$ LAN (I) Abréviation pour "local area network", réseau de zone locale [RFC1983]. (Voir : [FP191].)

$ attaque terrestre *(land attack)*
(I) Attaque de déni de service qui envoie un paquet IP qui (a) a la même adresse dans les deux champs d'adresse de source et d'adresse de destination et (b) contient un paquet TCP SYN qui a le même numéro d'accès dans les deux champs d'accès de source et d'accès de destination.
Dérivation : cette attaque d'un seul paquet a été nommée d'après "land", le programme publié à l'origine par le craqueur qui

a inventé cet exploit. Peut-être que le nom a été choisi parce que l'inventeur pensait que les attaques multi-paquets (c'est-à-dire, d'inondation) arrivaient par la mer.

$ spécification du langage d'ordre temporel (LOTOS, *Language of Temporal Ordering Specification*)
(N) Langage (ISO 8807-1990) pour la spécification formelle de protocoles de réseau informatique ; décrit l'ordre dans lequel se produisent les événements.

$ treillis *(lattice)*
(I) Ensemble fini avec un ordre partiel de ses éléments tel que pour chaque paire d'éléments il y ait au moins une limite supérieure et une plus grande limite inférieure.
Exemple : un treillis est formé par un ensemble fini S de niveaux de sécurité – c'est-à-dire, un ensemble S de toutes les paires ordonnées (x,c), où x est un des niveaux de l'ensemble fini X des niveaux de classification hiérarchiquement ordonnés X(1), des catégories non hiérarchiques C(1), ..., C(M) – avec la relation "dominant". Le niveau de sécurité (x,c) est dit "dominer" (x',c') si et seulement si (a) x est supérieur (plus élevé que) ou égal à x' et si (b) c inclut au moins tous les éléments de c'. (Voir : dominer, modèle en treillis.)
Instructions : les treillis sont utilisés dans certaines branches de la cryptographie, à la fois comme base de problèmes de calcul difficiles sur lesquels des algorithmes cryptographiques peuvent être définis, et aussi comme base d'attaques des algorithmes cryptographiques.

$ modèle en treillis *(lattice model)*
1. (I) Description de la structure sémantique formée par un ensemble fini de niveaux de sécurité, tels que ceux utilisés dans les organisations militaires. (Voir : dominer, treillis, modèle de sécurité.)
2. (I) /modèle formel/ Modèle de contrôle de flux dans un système, fondé sur le treillis qui est formé par les niveaux de sécurité finis dans un système et leur ordonnancement partiel. [Denn]

$ champ d'accès d'application de la loi (LEAF, *Law Enforcement Access Field*)
(N) Élément de données qui est automatiquement incorporé dans les données chiffrées par les appareils (par exemple, le microprocesseur CLIPPER) qui mettent en œuvre la norme de chiffrement par tiers de confiance.

$ couche 1, 2, 3, 4, 5, 6, 7 (N) Voir : OSIRM.

$ protocole de transmission de couche 2 (L2F, *Layer 2 Forwarding Protocol*)
(N) Protocole Internet (développé à l'origine par Cisco Corporation) qui utilise le tunnelage de PPP sur IP pour créer une extension virtuelle d'une liaison à numérotation à travers un réseau, initiée par le serveur de numérotation et transparente pour l'utilisateur qui numérote. (Voir : L2TP.)

$ protocole de tunnelage de couche 2 (L2TP, *Layer 2 Tunneling Protocol*)
(N) Protocole client-serveur Internet qui combine des aspects de PPTP et de L2F et prend en charge le tunnelage de PPP sur un réseau IP ou sur relais de trame ou autre réseau commuté . (Voir : VPN.)
Instructions : PPP peut à son tour encapsuler tout protocole de couche 3 OSIRM. Donc, L2TP ne spécifie pas de services de sécurité ; il dépend des protocoles mis en couche par dessus ou par dessous lui pour fournir la sécurité nécessaire.

$ mécanisme le moins courant *(least common mechanism)*
(I) Principe qu'une architecture de sécurité devrait minimiser l'appui sur des mécanismes qui sont partagés par de nombreux utilisateurs.
Instructions : les mécanismes partagés peuvent inclure des chemins de diaphonie qui permettent de faire une brèche dans la sécurité des données, et il est difficile de faire fonctionner un seul mécanisme d'une façon correcte et de confiance à la satisfaction d'une large gamme d' utilisateurs.

$ moindre privilège *(least privilege)*
(I) Principe qu'une architecture de sécurité devrait être conçue de façon telle que chaque entité système se voit accorder le minimum de ressources système et d'autorisations dont l'entité a besoin pour faire son travail. (À comparer à : économie de mécanisme, moindre confiance.)
Instructions : ce principe tend à limiter les dommages qui peuvent être causés par accident, erreur, ou acte non autorisé. Ce principe tend aussi à réduire la complexité et à promouvoir la modularité, ce qui peut rendre la certification plus facile et plus efficace. Ce principe est similaire au principe de la mise en couche de protocoles, par lequel chaque couche fournit des services de communication spécifiques limités, et les fonctions dans une couche sont indépendantes de celles des autres couches.

$ moindre confiance *(least trust)*
(I) Principe qu'une architecture de sécurité devrait être conçue de façon à minimiser (a) le nombre de composants qui

exigent la confiance et (b) la confiance accordée à chaque composant. (À comparer à : moindre privilège, niveau de confiance.)

$ système hérité *(legacy system)*
(I) Système qui fonctionne mais ne sera pas amélioré ou étendu tandis que un nouveau système est en cours de développement pour le remplacer.

$ non répudiation légale *(legal non-repudiation)* (I) Voir : définition secondaire sous "non-répudiation".

$ saut de confiance *(leap of faith)*
1. (I) /sécurité générale/ Faire fonctionner un système comme si il commençait dans un état sûr, bien qu'il ne puisse être prouvé qu'un tel état ait été établi (c'est-à-dire, bien qu'une compromission de la sécurité ait pu se produire avant ou au moment de la mise en route).
2. (I) /COMSEC/ La partie initiale, c'est-à-dire, la ou les premières étapes de communication d'un protocole qui est vulnérable à l'attaque (en particulier une attaque par interposition) durant cette partie, mais si cette partie est achevée sans être attaquée, n'est ensuite pas vulnérable dans les étapes ultérieures (c'est-à-dire, résulte en une association de communication sûre pour laquelle aucune attaque par interposition n'est possible).

Usage : ce terme figure dans les dictionnaires, mais sa définition est large et peut être interprétée de nombreuses façons dans les contextes de l'Internet. De même, la définition donnée ici peut être interprétée de plusieurs façons. Donc, les IDOC qui utilisent ce terme (en particulier les IDOC qui sont des spécifications de protocole) DEVRAIENT en donner une définition plus spécifique.
Instructions : dans un protocole, un saut de confiance consiste normalement à accepter la revendication d'identité, d'origine de données, ou d'intégrité des données d'un homologue sans authentifier cette revendication. Lorsque un protocole comporte une telle étape, le protocole peut aussi être conçu de telle sorte que si une attaque par interposition réussit pendant la première partie vulnérable, l'attaquant doit alors rester interposé pour tous les échanges suivants sinon une des parties légitimes sera capable de détecter l'attaque.

$ niveau d'implication *(level of concern)*
(N) /U.S. DoD/ Classement alloué à un système d'informations qui indique dans quelle mesure les mesures, techniques et procédures de protection doivent être appliquées. (Voir : critique, sensible, niveau de robustesse.)

$ niveau de robustesse *(level of robustness)*
(N) /U.S. DoD/ Caractérisation de (a) la force d'une fonction, mécanisme, service, ou solution de sécurité et (b) l'assurance (ou confiance) qu'il est mis en œuvre et fonctionne. [Cons], [IATF] (Voir : niveau d'implication.)

$ Liberty Alliance
(O) Consortium international de plus de 150 organisations commerciales, gouvernementales, et non gouvernementales créé en 2001 pour traiter des problèmes techniques, commerciaux, et politiques des services d'identité et fondés sur l'identité sur la Toile et développer une norme pour l'identité de réseaux fédérés qui prennent en charge les appareils réseau actuels et émergeants.

$ protocole léger d'accès à un répertoire (LDAP, *Lightweight Directory Access Protocol*)
(I) Protocole client-serveur Internet (RFC3377) qui prend en charge l'utilisation de base de l'annuaire X.500 (ou d'autres serveurs de répertoires) sans subir les exigences de ressources du protocole d'accès à un répertoire (DAP, *Directory Access Protocol*) complet.
Instructions : conçu pour des applications simples de gestion et de navigation qui fournissent un simple service de répertoire interactif en lecture écriture. Prend en charge à la fois la simple authentification et l'authentification forte du client auprès du serveur de répertoire.

$ liaison *(link)*
1a. (I) Facilité de communication ou support physique qui peut supporter des communications de données entre plusieurs nœuds réseau, dans la couche de protocole immédiatement en dessous de IP. (RFC3753)
1b. (I) /sous réseau/ Canal de communication qui connecte des relais de sous réseau (en particulier entre deux commutateurs de paquets) qui est mis en œuvre à la couche 2 OSIRM. (Voir : chiffrement de liaison.)

Instructions : les ordinateurs relais supposent que les liaisons sont logiquement passives. Si un ordinateur à une extrémité d'une liaison envoie une séquence de bits, la séquence arrive simplement à l'autre extrémité après un délai fini, bien que certains bits puissent avoir été changés soit accidentellement (erreurs) soit par une action d'écoute active.
2. (I) /Toile mondiale/ Voir : hyperliaison.

$ chiffrement de liaison *(link encryption)*
(I) Protection étape par étape (liaison par liaison) des données qui s'écoulent entre deux points dans un réseau, fournie par

le chiffrement séparé des données dans chaque réseau, c'est-à-dire, en chiffrant les données lorsque elles quittent un hôte ou un relais de sous réseau et en les déchiffrant lorsque elles arrivent au prochain hôte ou relais. Chaque liaison peut utiliser une clé différente ou même un algorithme différent. [RFC1455] (À comparer à : chiffrement de bout en bout.)

$ vivant *(liveness)*
(I) Propriété d'une association de communication ou d'une caractéristique d'un protocole de communication qui donne une assurance au receveur des données que celles-ci ont été récemment transmises par leur générateur, c'est-à-dire, que les données n'ont pas été répétées, ni par l'origine ni par un tiers, à partir d'une transmission antérieure. (Voir : frais, nom occasionnel, attaque en répétition.)

$ bombe logique *(logic bomb)*
(I) Logique malveillante qui s'active lorsque les conditions spécifiées sont satisfaites. Généralement destinée à causer un déni de service ou autrement à endommager des ressources système. (Voir : cheval de Trois, virus, ver.)

$ connexion *(login)*
1a. (I) Acte par lequel une entité système établit une session dans laquelle l'entité peut utiliser des ressources systèmes. (Voir : principal, session.)
1b. (I) Acte par lequel un utilisateur d'un système a son identité qui est authentifiée par le système. (Voir : principal, session.)
Usage : compris généralement comme étant accomplie par la fourniture d'un identifiant et les informations d'authentification correspondantes (par exemple, un mot de passe) à un mécanisme de sécurité qui authentifie l'identité de l'utilisateur ; mais parfois se réfère à l'établissement d'une connexion avec un serveur lorsque aucune authentification ou autorisation spécifique n'est impliquée.
Dérivation : se réfère au fichier "log", un chemin d'audit de sécurité qui enregistre (a) les événements concernant la sécurité, comme de début d'une session, et (b) les noms des entités système qui initient les événements.

$ titre long *(long title)*
(O) /Gouvernement des USA/ "Titre descriptif d'un élément de matériel COMSEC." [C4009] (À comparer à : titre court.)

$ faible probabilité de détection *(low probability of detection)*
(I) Résultat des mesures TRANSEC utilisées pour cacher ou déguiser une communication.

$ faible probabilité d'interception *(low probability of intercept)*
(I) Résultat des mesures TRANSEC utilisées pour empêcher l'interception d'une communication.

$ MAC
(N) Voir : contrôle d'accès obligatoire, code d'authentification de message.
Utilisation déconseillée : les IDOC qui utilisent ce terme DEVRAIENT en donner une définition parce que cette abréviation est ambiguë.

$ rémanence magnétique *(magnetic remanence)*
(N) Représentation magnétique des informations résiduelles restant sur un support magnétique après la suppression du support. [NCS25] (Voir : suppression, dégausser, purge.)

$ mode principal *(main mode)* (I) Voir : /IKE/ sous "mode".

$ crochet de maintenance *(maintenance hook)*
(N) "Instructions spéciales (portes dérobées) dans le logiciel qui permettent une maintenance facile et le développement de caractéristiques supplémentaires. Comme les crochets de maintenance permettent souvent d'entrer dans le code sans les vérifications usuelles, il y a un risque sérieux de sécurité si ils ne sont pas retirés avant la mise en œuvre réelle." [C4009] (Voir : porte de derrière.)

$ logique malveillante *(malicious logic)*
(I) Matériel, progiciel ou logiciel qui est inclus ou inséré intentionnellement dans un système dans un but malveillant. (Voir bombe logique, cheval de Troie, logiciel espion, virus, ver. À comparer à : définitions secondaires sous "corruption", "incapacitation", "mascarade", et "mauvais usage".)

$ malgiciel *(malware)*
(D) Contraction de "logiciel malveillant". (Voir : logique malveillante.)
Terme déconseillé : les IDOC NE DEVRAIENT PAS utiliser ce terme ; il ne figure pas dans la plupart des dictionnaires et

pourrait dérouter les lecteurs étrangers.

$ MAN (I) réseau de zone métropolitaine *(metropolitan area network.)*

$ attaque par interposition *(man-in-the-middle attack)*
(I) Forme active d'attaque de mise sur écoute dans laquelle l'attaquant intercepte et modifie de façon sélective les données communiquées pour se faire passer pour une ou plusieurs des entités impliquées dans une association de communication. (Voir : attaque par capture, attaque par portage.)
Instructions : par exemple, supposons qu'Alice et Bob essayent d'établir une clé de session en utilisant l'algorithme Diffie-Hellman-Merkle sans service d'authentification d'origine des données, Un "interposé" pourrait (a) bloquer la communication directe entre Alice et Bob et ensuite (b) se faire passer pour Alice qui envoie des données à Bob, (c) se faire passer pour Bob qui envoie des données à Alice, (d) établir des clés de session séparées avec chacun d'eux, et (e) fonctionner comme un serveur mandataire clandestin entre eux pour capturer ou modifier des informations sensibles qu'Alice et Bob pensent n'envoyer qu'entre eux.

$ gestionnaire *(manager)*
(I) Personne qui contrôle la configuration de service d'un système ou les privilèges fonctionnels d'opérateurs et des autres utilisateurs. (Voir : sécurité administrative. À comparer à : opérateur, SSO, utilisateur.)

$ contrôle d'accès obligatoire *(mandatory access control)*
1. (I) Service de contrôle d'accès qui met en application une politique de sécurité fondée sur la comparaison (a) des étiquettes de sécurité, qui indiquent le niveau de sensibilité ou de criticité de ressources système, avec (b) des accréditifs de sécurité, qui indiquent que les entités système sont éligibles à l'accès à certaines ressources. (Voir : contrôle d'accès discrétionnaire, MAC, politique de sécurité fondée sur la règle.)

Dérivation : cette sorte de contrôle d'accès est appelée "obligatoire" parce que une entité qui est accréditée pour accéder à une ressource n'est pas habilitée, par sa seule volonté, à permettre à une autre entité d'accéder à cette ressource.

2. (O) "Moyen de restreindre l' accès aux objets sur la base de la sensibilité (représentée par une étiquette) des informations contenues dans les objets et de l'autorisation formelle (c'est-à-dire, les accréditations) des sujets à accéder aux informations d'une telle sensibilité." [DoD1]

$ code de manipulation de détection *(manipulation detection code)*
(D) Synonyme de "somme de contrôle".
Terme déconseillé : les IDOC NE DEVRAIENT PAS utiliser ce terme comme synonyme de "somme de contrôle" ; le mot "manipulation" implique une protection contre les attaques actives, qu'une somme de contrôle ordinaire pourrait ne pas fournir. À la place, si une telle protection est voulue, utiliser "somme de contrôle protégée" ou d'un autre type particulier, selon ce qu'on veut dire. Si une telle protection n'est pas voulue, utiliser "code de détection d'erreur" ou autre type spécifique de somme de contrôle qui n'est pas protégée.

$ marquage *(marking)* Voir : horodatage, marquage de sécurité.

$ MARS
(O) Chiffrement de bloc symétrique de 128 bits avec longueur de clé variable (de 128 à 448 bits) développé par IBM comme candidat pour l'AES.

$ martien *(martian)*
(D) /argot/ Paquet qui arrive de façon inattendue à la mauvaise adresse ou sur le mauvais réseau à cause d'un acheminement incorrect ou parce il a une adresse IP non enregistrée ou mal formée. [RFC1208]
Terme déconseillé : il est vraisemblable que d'autres cultures utilisent des métaphores différentes pour ce concept. Donc, pour éviter l'incompréhension entre les nations, les IDOC NE DEVRAIENT PAS utiliser ce terme. (Voir : utilisation déconseillée sous "Livre Vert".)

$ mascarade *(masquerade)*
(I) Type d'action de menace par laquelle une entité non autorisée obtient l'accès à un système ou effectue un acte malveillant en se faisant illégitimement passer pour une entité autorisée. (Voir : tromperie.)
Usage : ce type d'action de menace inclut les sous types suivants :
- "usurpation" : tentative par une entité non autorisée d'obtenir l'accès à un système en se faisant passer pour un utilisateur autorisé.
- "logique malveillante" : dans le contexte d'une mascarade, tout matériel, progiciel ou logiciel (par exemple, un cheval de Troie) qui paraît effectuer une fonction utile ou désirable, mais en fait obtient un accès non autorisé à des ressources système ou trompe un usager en exécutant une autre logique malveillante. (Voir : corruption, incapacitation, principale entrée pour "logique malveillante", mauvais usage.)

$ MD2
(N) Hachage cryptographique [RFC1319] qui produit un résultat de hachage de 128 bits, qui a été conçu par Ron Rivest, et est similaire à MD4 et MD5 mais plus lent.
Dérivation : Apparemment, abréviation de "message digest" (résumé de message), mais ce terme est déconseillé dans le présent glossaire.

$ MD4
(N) Hachage cryptographique [RFC1320] qui produit un résultat de hachage de 128 bits et a été conçu par Ron Rivest. (Voir : Dérivation sous "MD2", SHA-1.)

$ MD5
(N) Hachage cryptographique [RFC1321] qui produit un résultat de hachage de 128 bits et a été conçu par Ron Rivest pour être une version améliorée de MD4. (Voir : Dérivation sous "MD2".)

$ marchand *(merchant)*
(O) /SET/ "Celui qui vend des biens, services, et/ou autres informations et qui accepte le payement électronique de ces éléments." [SET2] Un marchand peut aussi fournir des services de vente électronique et/ou de livraison électronique des éléments à vendre. Avec SET, le marchand peut offrir à ses détenteurs de carte des interactions électroniques sécurisées, mais un marchand qui accepte des cartes de payement est obligé d'avoir une relation avec un acquéreur. [SET1], [SET2]

$ certificat de marchand *(merchant certificate)*
(O) /SET/ Certificat de clé publique produit à un marchand. Parfois utilisé pour se référer à une paire de tels certificats où l'un est pour l'utilisation d'une signature numérique et l'autre est pour le chiffrement.

$ autorité de certification de marchand (MCA, *merchant certification authority*)
(O) /SET/ Une CA qui produit des certificats numériques aux marchands et fonctionne au nom d'une marque de cartes de payement, d'un acquéreur, ou d'une autre partie selon les règles de la marque. Les acquéreurs vérifient et approuvent les demandes de certificat de marchand avant la production par la MCA. Une MCA ne produit pas de CRL, mais distribue les CRL produites par les CA racines, les CA de marque, les CA géopolitiques, et les CA de passerelle de payement. [SET2]

$ PKI maillée *(mesh PKI)*
(I) Architecture de PKI non hiérarchique dans laquelle il y a plusieurs CA de confiance plutôt qu'une seule racine. Chaque utilisateur de certificat fonde les validations de chemin sur la clé publique d'une des CA de confiance, usuellement celle qui a produit le propre certificat de clé publique de l'utilisateur. Plutôt que d'avoir une relation de supérieur à subordonné entre les CA, la relation est d'homologue à homologue, et les CA produisent des certificats croisés l'une à l'autre. (À comparer à : PKI hiérarchique, PKI de fichier de confiance.)

$ code d'authentification de message (MAC, *Message Authentication Code*)
1. (N) /en majuscules/ Norme ANSI spécifique pour une somme de contrôle qui est calculée avec un hachage à clés qui se fonde sur DES. [A9009] Usage : autrement dit un code d'authentification des données, qui est une norme du gouvernement des USA. [FP113] (Voir : MAC.)
2. (D) /en minuscules/ Synonyme de "code de détection d'erreur".

Terme déconseillé : les IDOC NE DEVRAIENT PAS utiliser la forme en minuscules de "code d'authentification de message". À la place, utiliser "somme de contrôle", "code de détection d'erreur", "hachage", "hachage à clé", "code d'authentification de message", ou "somme de contrôle protégée", selon ce que l'on veut dire. (Voir : code d'authentification.)
La forme en minuscules mélange les concepts d'une façon potentiellement trompeuse. Le mot "message" est trompeur parce que il implique que le mécanisme convient particulièrement pour, ou est limité à, la messagerie électronique (voir : système de traitement de message). Le mot "authentification" est trompeur parce que le mécanisme sert principalement une fonction d'intégrité des données plutôt qu'une fonction d'authentification. Le mot "code" est trompeur parce qu'il suggère que du codage ou du chiffrement est impliqué ou que le terme se réfère à du logiciel informatique,

$ résumé de message *(message digest)*
(D) Synonyme de "résultat de hachage". (Voir : hachage cryptographique.)
Terme déconseillé : les IDOC NE DEVRAIENT PAS utiliser ce terme comme synonyme de "résultat de hachage" ; ce terme duplique sans nécessité la signification de l'autre terme plus général et mélange des concepts d'une façon potentiellement trompeuse. Le mot "message" est trompeur parce qu'il implique que le mécanisme convient particulièrement pour, ou se limite, à la messagerie électronique (voir : système de traitement de message).

$ système de traitement de message *(message handling system)*

(D) Synonyme de système de messagerie électronique Internet.
Terme déconseillé : les IDOC NE DEVRAIENT PAS utiliser ce terme parce que il pourrait être confondu avec le Système de traitement de message. À la place, utiliser "messagerie électronique Internet" ou quelque autre terme plus spécifique.

$ Système de traitement de message *(Message Handling System)*
(O) Concept de système de l'UIT-T qui englobe la notion de messagerie électronique mais définit des systèmes et services OSI plus complets qui permettent aux utilisateurs d'échanger des messages sur la base de la livraison différée *(store-and-forward)*. (L'équivalent ISO est "système d'échange de texte en mode message".) (Voir : X.400.)

$ indicateur de message *(message indicator)*
1. (D) /fonction cryptographique/ Synonyme de "valeur d'initialisation". (À comparer à : indicateur.)
2. (D) "Séquence de bits transmise sur un système de communications pour synchroniser les équipements cryptographiques." [C4009]

Terme déconseillé : les IDOC NE DEVRAIENT PAS utiliser ce terme comme synonyme de "valeur d'initialisation" ; le terme mélange des concepts d'une façon potentiellement trompeuse. Le mot "message" est trompeur parce qu'il suggère que le mécanisme serait spécifique de la messagerie électronique. (Voir : système de traitement de message.)

$ vérification d'intégrité de message *(message integrity check)*
$ code d'intégrité de message (MIC, *message integrity code*)
(D) Synonymes de certaines formes de "somme de contrôle".
Terme déconseillé : les IDOC NE DEVRAIENT PAS utiliser ce terme pour une forme de somme de contrôle. À la place, utiliser "somme de contrôle", "code de détection d'erreur", "hachage", "hachage à clé", "code d'authentification de message", ou "somme de contrôle protégée", selon ce que l'on veut dire.
Ces deux termes mélangent les concepts d'une façon potentiellement trompeuse. Le mot "message" est trompeur parce qu'il suggère que le mécanisme convient particulièrement, ou se limite, à la messagerie électronique. Le mot "intégrité" est trompeur parce que la somme de contrôle peut être utilisée pour effectuer une fonction d'authentification de l'origine des données plutôt qu'une fonction d'intégrité. Le mot "code" est trompeur parce que il suggère que du codage ou du chiffrement est impliqué ou que le terme se réfère à du logiciel informatique.

$ protocole de sécurité de message (MSP, *Message Security Protocol*)
(N) Protocole sûr de traitement de message [SDNS7] à utiliser avec les protocoles X.400 et de messagerie Internet. Développé par le programme SDNS de la NSA et utilisé dans le système de message de défense de l'U.S. DoD.

$ méta-données *(meta-data)*
(I) Informations descriptives sur un objet de données ; c'est-à-dire, des données sur des données, ou des étiquettes de données qui décrivent d'autres données. (Voir : étiquette de sécurité. À comparer à : métadonnées)
Instructions : les méta-données peuvent servir plusieurs objectifs de gestion :
- gestion de système : nom, type, taille, date de création d'un fichier.
- gestion d'application : titre, version, auteur d'un document.
- gestion d'usage : catégories de données, mots clés, classifications.

Les méta-données peuvent être associées à des objets de données de deux façons principales :
- Explicitement : en faisant partie de l'objet de données (par exemple, un champ d'en-tête d'un fichier ou paquet de données) ou en étant lié à l'objet.
- Implicitement : en étant associé à l'objet de données à cause d'un autre attribut explicite de l'objet.

$ métadonnées *(metadata)*, Metadata(marque déposée), METADATA(marque déposée)
(D) Variantes brevetées de "méta-données". (Voir : SPAM(marque déposée).)
Utilisation déconseillée : les IDOC NE DEVRAIENT PAS utiliser ces formes sans trait d'union ; les IDOC DEVRAIENT utiliser seulement la forme "méta-données" en minuscules avec trait d'union. Les termes "Metadata" et "METADATA" sont revendiqués comme marques commerciales déposées (numéros 1 409 260 et 2 185 504) propriété de The Metadata Company, appelée à l'origine Metadata Information Partners, une société fondée par Jack Myers. Le statut de "metadata" n'est pas clair.

$ services de sécurité d'objet MIME (MOSS, *MIME Object Security Services*)
(I) Protocole Internet [RFC1848] qui s'applique au chiffrement et à la signature numérique de contenu de message MIME de bout en bout, en utilisant le chiffrement symétrique pour le chiffrement et le chiffrement asymétrique pour la distribution de clé et la signature. MOSS se fonde sur les caractéristiques et les spécifications de PEM. (Voir : S/MIME.)

$ spécification d'interopérabilité minimum pour composants PKI (MISPC, *Minimum Interoperability Specification for PKI Components*)
(N) Description technique pour donner une base d'interopération entre les composants PKI de fabricants différents,

consistant principalement en un profil de certificat et des extensions de CRL et un ensemble de transactions pour le fonctionnement de PKI. [SP15]

$ appropriation illégitime *(misappropriation)*
(I) Type d'action de menace par laquelle une entité s'empare du contrôle logique ou physique non autorisé d'une ressource système. (Voir : usurpation.)
Usage : ce type de d'action de menace inclut les sous types suivants :
- vol de données : acquisition et utilisation non autorisée des données contenues dans un système ;
- vol de service : utilisation non autorisée d'un service du système ;
- vol de fonctionnalité : acquisition non autorisée du matériel, progiciel ou logiciel d'un composant du système.

$ initiative de sécurité des systèmes d'information (MISSI, *Multilevel Information System Security Initiative*)
(O) Programme de la NSA pour encourager le développement de produits interopérables et modulaires pour construire des systèmes d'information réseau sûrs pour le soutien d'une large diversité de missions du gouvernement des USA. (Voir : MSP, SP3, SP4.)

$ utilisateur MISSI *(MISSI user)*
(O) /MISSI/ Entité système qui est le sujet d'un ou plusieurs certificats de clé publique MISSI X.509 produits sous une hiérarchie de certification MISSI. (Voir : personnalité.)
Instructions : les utilisateurs MISSI incluent à la fois des utilisateurs finaux et les autorités qui produisent les certificats. Un utilisateur MISSI est usuellement une personne mais peut être une machine ou un autre processus automatisé. Les machines qui doivent fonctionner en continu peuvent recevoir leurs propres certificats pour éviter les délais nécessaires pour échanger les cartes FORTEZZA des opérateurs de machine aux changements de programme.

$ mission
(I) Déclaration d'un objectif (à relativement long terme) ou d'une tâche (à relativement court terme) qui est alloué à une organisation ou système, qui indique l'objet et les buts de la tâche, et peut indiquer les actions à entreprendre pour la réaliser.

$ mission critique *(mission critical)*
(I) Condition d'un service système ou d'autres ressources systèmes comme un déni d'accès, ou un manque de disponibilité de la ressource qui annihilerait la capacité de l'utilisateur d'un système à effectuer une fonction de mission principale ou résulterait en d'autres conséquences sérieuses. (Voir : critique. À comparer à : essentiel à la mission.)

$ essentiel à la mission *(mission essential)*
(O) /U.S. DoD/ Se réfère à du matériel qui est autorisé et disponible pour le combat, le soutien au combat, le soutien au service du combat, et aux forces d'entraînement au combat pour accomplir les missions allouées. [JP1] (À comparer à : mission critique.)

$ mauvais usage *(misuse)*
1. (I) Utilisation intentionnelle (par des usagers autorisés) de ressources système pour des objets autres que ceux autorisés. Exemple : un administrateur système autorisé crée un compte non autorisé pour un ami. (Voir : détection de mauvais usage.)
2. (I) Type d'action de menace qui cause l'exécution d'une fonction ou d'un service par un composant d'un système qui se fait au détriment de la sécurité du système. (Voir : usurpation.)

Usage : ce type d'action de menace inclut les sous types suivants :
- "altération" : /mauvais usage/ Altération délibérée de la logique, des données ou des informations de contrôle pour causer l'exécution par le système de fonctions ou services non autorisés. (Voir : corruption, principale entrée sous "altération".)
- "logique malveillante" : /mauvais usage/ Tout matériel, progiciel ou logiciel introduit intentionnellement dans un système pour effectuer ou commander l'exécution d'une fonction ou service non autorisé. (Voir : corruption, incapacitation, principale entrée sous "logique malveillante", mascarade.)
- "violation d'autorisations" : action, par une entité, qui excède les privilèges système de l'entité, lorsque elle exécute une fonction non autorisée. (Voir : autorisation.)

$ détection de mauvais usage *(misuse detection)*
(I) Méthode de détection d'intrusion qui se fonde sur des règles qui spécifient les événements du système, les séquences d'événements, ou les propriétés observables d'un système dont on pense qu'ils sont symptomatiques des incidents de sécurité. (Voir : IDS, mauvais usage. À comparer à : détection d'anomalie.)

$ code mobile *(mobile code)*

1a. (I) Logiciel généré par un serveur distant, est transmis à travers un réseau, et est chargé et exécuté sur un système client local sans initialisation explicite par l'utilisateur du client, et dans certains cas, à l'insu de cet utilisateur. (À comparer à : contenu actif.)

Instructions : une forme de code mobile est le contenu actif dans un fichier qui est transféré à travers un réseau.

1b. (O) /U.S. DoD/ "Modules logiciels obtenus de systèmes distants, transférés à travers un réseau, et ensuite téléchargés et exécutés sur des systèmes locaux sans installation ou exécution explicite par le receveur." [JP1]

2a. (O) /U.S. DoD/ Technologie qui permet la création d'informations exécutables qui peuvent être livrées à un système d'information et exécutées directement sur toute architecture de matériel/logiciel qui a un environnement d'hôte d'exécution approprié.

2b. (O) "Programmes (par exemple, script, macro, ou autre instruction portable) qui peuvent être transportés inchangés à une collection hétérogène de plates-formes et exécutés avec une sémantique identique." [SP28]. (Voir : contenu actif.)

Instructions : le code mobile peut être malveillant. Utiliser des techniques telles que la "signature de code" et une "boîte à sable" peut réduire les risques de réception et d'exécution de code mobile.

$ mode

$ mode de fonctionnement *(mode of operation)*

1. (I) /fonctionnement cryptographique/ Technique pour améliorer l'effet d'un algorithme de chiffrement ou pour adapter l'algorithme pour une application, telle que d'appliquer un chiffrement de bloc à une séquence de blocs de données ou à un flux de données. (Voir : CBC, CCM, CMAC, CFB, CTR, ECB, OFB.)
2. (I) /fonctionnement d'un système/ Type de politique de sécurité qui déclare la gamme des niveaux de classification des informations qu'il est permis de traiter à un système, et la gamme d'accréditifs et d'autorisations d'utilisateurs à laquelle il est permis d'accéder au système. (Voir : mode de sécurité compartimentée, mode de sécurité contrôlée, mode de sécurité dédiée, mode de sécurité multi niveaux, mode de sécurité partitionnée, mode de sécurité au niveau du système. À comparer à : niveau de protection.)
3. (I) /IKE/ IKE se réfère à ses divers types d'échanges de messages décrits en ISAKMP comme à des "modes". Parmi ceux-ci, il y a les suivants :
   - "mode principal" : un des deux modes de phase 1 de IKE. (Voir : ISAKMP.)
   - "mode rapide" : le seul mode de phase 2 de IKE. (Voir : ISAKMP.)

$ modèle *(model)* Voir : modèle formel, modèle de sécurité.

$ modulo *(modulus)*

(I) Constante définissante dans l'arithmétique modulaire, qui est généralement une partie de la clé publique dans le chiffrement asymétrique qui se fonde sur l'arithmétique modulaire. (Voir : Diffie-Hellman-Merkle, RSA.)

$ Mondex

(O) Système de monnaie électronique fondé sur une carte à mémoire qui incorpore de la cryptographie et peut être utilisé pour faire des payements via l'Internet. (Voir : IOTP.)

$ ver de Morris *(Morris Worm)*

(I) Programme de ver qui a inondé l'ARPANET en novembre 1988, causant des problèmes à des milliers d'hôtes. [RFC1135] (Voir : risque communautaire, ver)

$ MQV

(N) Protocole d'accord de clé [Mene] qui a été proposé par A.J. Menezes, M. Qu, et S.A. Vanstone en 1995 et se fonde sur l'algorithme Diffie-Hellman-Merkle.

$ sécurité de diffusion groupée *(multicast security)*. Voir : diffusion groupée sûre.

$ Multics, MULTiplexed Information and Computing Service

(N) Service de calcul et d'informations multiplexées, un système d'ordinateur MLS en temps partagé conçu et mis en œuvre durant les années 1965-69 par un consortium incluant le Massachusetts Institute of Technology, General Electric, et Bell Laboratories, et proposé ensuite par Honeywell sur le plan commercial.

Instructions : Multics était un des premiers grands systèmes d'exploitation d'usage général à inclure la sécurité comme objectif principal depuis le début de la conception et du développement et a été classé en B2 dans TCSEC. Ses nombreux mécanismes de sécurité innovants dans le matériel et le logiciel (par exemple, anneau de protection) ont été adoptés par les systèmes ultérieurs.

$ multi niveau sécurisé (MLS, *multilevel secure*)

(I) Décrit un système d'informations qui est de confiance et contient, et entretient, la séparation entre des ressources (en particulier des données mémorisées) de niveaux de sécurité différents. (Exemples : BLACKER, CANEWARE, KSOS,

Multics, SCOMP.)
Usage : compris généralement comme signifiant que le système permet des accès concurrents par des utilisateurs qui diffèrent par leurs autorisations d'accès, tout en refusant aux usagers l'accès aux ressources pour lesquelles ils n'ont pas d'autorisation.

$ mode de sécurité multi niveaux *(multilevel security mode)*
1. (N) Mode de fonctionnement d'un système dans lequel (a) le traitement concurrent de deux niveaux de sécurité des informations ou plus est permis au sein du même système lorsque des utilisateurs qui ont accès au système n'ont ni un niveau d'habilitation ni le besoin de savoir pour certaines des données traitées par le système et (b) la séparation des usagers et du matériel classifié sur la base, respectivement, du niveau d'accréditation et de classification, dépend du contrôle du système d'exploitation. (Voir : /fonctionnement du système/ sous "mode", besoin de savoir, niveau de protection, niveau d'habilitation. À comparer à : mode contrôlé.)

Usage : généralement abrégé en "mode multi niveau". Ce terme a été défini dans la politique du gouvernement des USA concernant l'accréditation de système, mais le terme est aussi utilisé en dehors des sphères gouvernementales.

2. (O) Mode de fonctionnement de système dans lequel sont vraies les trois déclarations suivantes : (a) des usagers autorisés n'ont pas un niveau d'habilitation pour toutes les informations traitées dans le système ; (b) tous les usagers autorisés ont le niveau d'habilitation approprié et une approbation d'accès spécifique appropriée pour les informations auxquelles ils ont accès ; (c) tous les usagers autorisés n'ont besoin de savoir que pour les informations auxquelles ils ont accès. [C4009] (Voir : approbation formelle d'accès, niveau de protection.)

$ extensions multi-usage de messagerie Internet (MIME, *Multipurpose Internet Mail Extensions*)
(I) Protocole Internet (RFC2045) qui améliore le format de base des messages de la messagerie électronique de l'Internet (RFC0822) (a) pour permettre d'utiliser des jeux de caractères autres que l'U.S.-ASCII pour les en-têtes textuels et le contenu et (b) pour porter un contenu non textuel et multi parties. (Voir : S/MIME.)

$ suspicion mutuelle *(mutual suspicion)*
(I) État qui existe entre deux entités système interagissantes dans lequel aucune des entités ne peut faire confiance à l'autre pour fonctionner correctement à l'égard de certaines exigences de sécurité.

$ nom (I) Synonyme de "identifiant".

$ autorité de désignation *(naming authority)*
(O) /U.S. DoD/ Entité organisationnelle responsable d'allouer des noms de domaine et d'assurer que chaque DN est significatif et unique au sein de son domaine. [DoD9]

$ centre national de sécurité informatique (NCSC, *National Computer Security Center*)
(O) Organisation du ministère de la Défense U.S., hébergé par la NSA, qui a la responsabilité d'encourager la plus large disponibilité des systèmes de confiance dans le gouvernement fédéral des U.S.A. Il a établi des critères et effectué des évaluations de systèmes informatiques et de réseau qui ont un TCB. (Voir : série Arc en ciel, TCSEC.)

$ partenariat national d'assurance de l'information (NIAP, *National Information Assurance Partnership*)
(N) Initiative conjointe du NIST et de la NSA pour améliorer la qualité des produits commerciaux de la sécurité de l'information et augmenter la confiance du consommateur dans ces produits par des évaluations et des méthodes d'essai objectives.
Instructions : NIAP est enregistré, à travers le U.S. DoD, comme laboratoire national d'invention et de révision des performances. Les fonctions du NIAP incluent ce qui suit :
- de développer des essais, des méthodes d'essai, et d'autres outils que peuvent utiliser les développeurs et les laboratoires d'essai pour améliorer et évaluer les produits de sécurité.
- de collaborer avec l'industrie et d'autres à des programmes de recherche et d'essais.
- d'utiliser les critères communs pour développer les profils de protection et les jeux d'essais associés pour les produits et systèmes de sécurité.
- de coopérer avec le programme national d'accréditation de laboratoires volontaires du NIST pour développer un programme d'accréditation de laboratoires du secteur privé pour les essais des produits de sécurité de l'information qui utilisent les critères communs.
- travailler à établir un schéma formel de reconnaissance internationale mutuelle pour une évaluation fondée sur les critères communs.

$ Institut national des normes et de la technologie (NIST, *National Institute of Standards and Technology*)
(N) Organisation du Ministère américain du Commerce qui s'attache à la promotion économique des U.S.A en travaillant avec l'industrie pour développer et appliquer la technologie, les mesures, et les normes. Il a la principale responsabilité du gouvernement des USA pour les normes INFOSEC sur les informations sensibles non classifiées. (Voir : ANSI, DES, DSA,

DSS, FIPS, NIAP, NSA.)

$ Conseil national de la fiabilité et de l'interopérabilité (NRIC, *National Reliability and Interoperability Council*)
(N) Comité consultatif mandaté par la Commission fédérale des communications (FCC, *Federal Communications Commission*) des USA, avec la participation des opérateurs de service réseau et des fabricants, pour fournir des recommandations à la FCC pour assurer la fiabilité, l'interopérabilité, la robustesse, et la sécurité des réseaux de communication publics sans fil, filaires, par satellite, par câble, et de données.

$ sécurité nationale *(national security)*
(O) /Gouvernement des USA/ La défense nationale ou les relations étrangères des États Unis d'Amérique.

$ Agence nationale de sécurité (NSA, *National Security Agency*)
(N) Organisation du ministère américain de la Défense *(U.S. DoD)* qui a la principale responsabilité au sein du gouvernement des USA des normes INFOSEC pour les informations classifiées et pour les informations sensibles non classifiées traitées par les systèmes de sécurité nationaux. (Voir : FORTEZZA, KEA, MISSI, système de sécurité national, NIAP, NIST, SKIPJACK.)

$ informations de la sécurité nationale *(national security information)*
(O) /Gouvernement des USA/ Informations dont il a été déterminé, conformément à l'Ordre exécutif 12958 ou tout ordre antérieur, qu'elles requièrent une protection contre la divulgation non autorisée. [C4009]

$ système de sécurité nationale *(national security system)*
(O) /Gouvernement des USA/ Tout système d'information gouvernemental pour lequel la fonction, le fonctionnement ou l'utilisation (a) implique des activités, de renseignement, (b) implique des activités cryptologiques en rapport avec la sécurité nationale, (c) implique la commande et le contrôle de forces militaires, (d) implique des équipements qui font partie intégrante d'armes ou de systèmes d'armes, ou (e) est critique pour la réalisation directe de missions militaires ou de renseignement et n'inclut pas de système qui soit utilisé pour des applications administrative et commerciales de routine (incluant les applications de paye, financières, logistiques, et de gestion du personnel). [Titre 40 U.S.C. Section 1552, de l'Acte de réforme de la gestion des technologies de l'information de 1996.] (Voir : produit de type 2.)

$ catastrophe naturelle *(natural disaster)*
(I) /action de menace/ Voir : définitions secondaires sous "corruption" et "incapacitation".

$ besoin de savoir *(need to know, need-to-know)*
(I) Nécessité d'accéder à, de connaître, ou de posséder les informations spécifiques requises pour accomplir des missions officielles.
Usage : la locution "besoin de savoir " est couramment utilisée comme adjectif ou comme nom.
Instructions : le critère besoin de savoir est utilisé dans les procédures de sécurité qui exigent un gardien des informations sensibles, avant de divulguer les informations à quelqu'un d'autre, pour établir que le receveur prévu a l'autorisation appropriée d'accéder aux informations.

$ réseau *(network)*
(I) Système d'informations qui comporte une collection de nœuds interconnectés. (Voir : réseau informatique.)

$ couche de matériel réseau *(Network Hardware Layer)* (I) Voir : suite des protocoles Internet.

$ couche d'interface réseau *(Network Interface Layer)* (I) Voir : suite des protocoles Internet.

$ protocole de sécurité de couche réseau (NLSP, *Network Layer Security Protocol*).
(N) Protocole OSI (IS0 11577) pour des services de chiffrement de bout en bout par dessus la couche 3 OSIRM. NLSP est dérivé de SP3 mais est plus complexe. (À comparer à : IPsec.)

$ couche de sous réseau *(Network Substrate Layer)* (I) Synonyme de "Network Hardware Layer".

$ entrelaçage de réseau *(network weaving)*
(I) Technique de pénétration dans laquelle un intrus évite la détection et le suivi en utilisant plusieurs réseaux de communication reliés entre eux pour accéder et attaquer un système. [C4009]

$ quartet *(nibble)*
(D) Demi octet (c'est-à-dire, habituellement, 4 bits).

Terme déconseillé : pour éviter l'incompréhension entre nations, les IDOC NE DEVRAIENT PAS utiliser ce terme ; déclarer plutôt explicitement la taille du bloc (par exemple, "bloc de 4 bits"). (Voir : Utilisation déconseillée sous "Livre Vert".)

$ NIPRNET
(O) Réseau d'acheminement au protocole Internet non classifié d'usage courant du Ministère de la Défense américain ; c'est la partie de l'Internet qui est entièrement contrôlée par le U.S. DoD et est utilisée pour les affaires officielles du DoD.

$ zone d'accompagnement obligatoire *(no-lone zone)*
(I) Pièce ou autre espace ou zone à laquelle personne ne peut avoir accès sans être accompagné et où, lorsque occupé, il est exigé qu'il y ait deux, ou plus, personnes dûment autorisées. [C4009] (Voir : contrôle dual.)

$ ORA sans PIN (NORA, *no-PIN ORA*)
(O) /MISSI/ RA organisationnel qui fonctionne dans un mode dans lequel l'ORA n'effectue aucune fonction de gestion de carte, et donc n'exige pas la connaissance du PIN SSO ou du PIN de l'usager pour une carte PC FORTEZZA d'utilisateur final.

$ nœud *(node)*
(I) Collection de sous systèmes en rapports localisés sur une ou plusieurs plateformes informatiques sur un seul site. (Voir : site.)

$ nom occasionnel *(nonce)*
(I) Valeur aléatoire ou non répétitive qui est incluse dans des données échangées par un protocole, généralement afin de garantir la vivacité et donc de détecter et protéger contre les attaques en répétition. (Voir : frais.)

$ non critique *(non-critical)* Voir : critique.

$ service de non répudiation *(non-repudiation service)*
1. (I) Service de sécurité qui assure la protection contre un faux déni d'implication dans une association (en particulier une association de communication qui transfère des données). (Voir : répudiation, horodatage.)

Instructions : deux types séparés de déni sont possibles – une entité peut nier qu'elle ait envoyé un objet de données, ou elle peut nier qu'elle ait reçu un objet de données – et donc, deux types séparés de service de non répudiation sont possibles. (Voir : non répudiation avec preuve d'origine, non répudiation avec preuve de réception.)

2. (D) "Assurance [que] l'envoyeur de données reçoit la preuve de la livraison et que le receveur reçoit la preuve de l'identité de l'envoyeur, afin que ni l'un ni l'autre puisse nier ultérieurement avoir traité les données." [C4009]

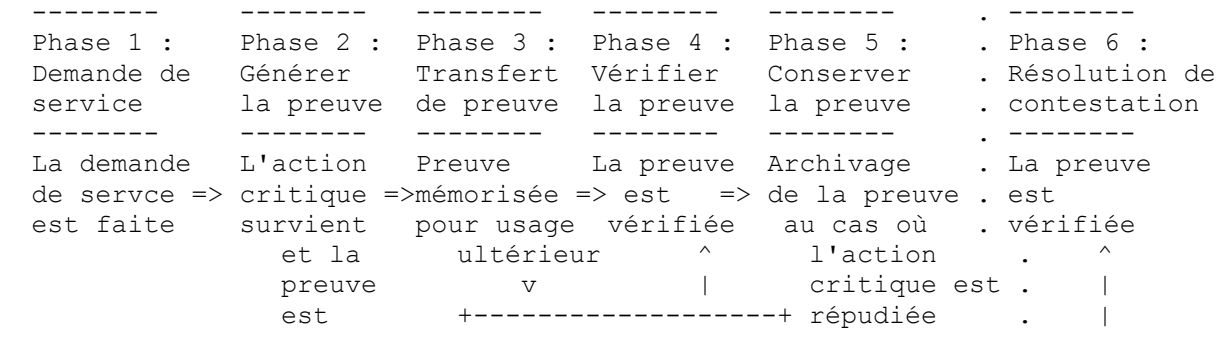
Définition déconseillée : les IDOC NE DEVRAIENT PAS utiliser la définition 2 parce qu'elle met ensemble deux services de sécurité – la non répudiation avec preuve d'origine, et la non répudiation avec preuve de réception – qui peuvent être fournis indépendamment l'un de l'autre.

Usage : les IDOC DEVRAIENT distinguer les aspects techniques et les aspects juridiques d'un service de non répudiation :

- "non répudiation technique " : se réfère à l'assurance qu'a le consommateur d'assertion que si une clé publique est utilisée pour valider une signature numérique, cette signature doit avoir été faite par la clé de signature privée correspondante. [SP32]
- "non répudiation juridique" : se réfère à la façon de bien établir la possession ou le contrôle de la clé de signature privée. [SP32]

Instructions : le service de non répudiation n'empêche pas une entité de répudier une communication. À la place, le service fournit la preuve qui peut être mémorisée et présentée ultérieurement à un tiers pour résoudre les contestations qui surviennent si et quand une communication est répudiée par une des entités impliquées.

Ford décrit les six phases d'un service complet de non répudiation et utilise une "action critique" pour se référer à l'acte de communication qui fait l'objet du service [For94], [For97]:



```
générée     | Preuve vérifiable |------>   ... . ----+
              +-------------------+
```

Phase / Explication

1. Demande de service : avant l'action critique, le demandeur du service demande, implicitement ou explicitement, d'avoir la preuve que l'action a été générée.
2. Générer la preuve : lorsque l'action critique survient, la preuve est générée par un processus qui implique le répudiation potentiel et éventuellement aussi un tiers de confiance.
3. Transfert de preuve : la preuve est transférée au demandeur ou mémorisée par un tiers pour utilisation ultérieure (si nécessaire).
4. Vérifier la preuve : l'entité qui détient la preuve la vérifie pour être sûr qu'elle va suffire si une contestation a lieu.
5. Conserver la preuve : la preuve est conservée pour une éventuelle restitution et utilisation futures.
6. Résoudre une contestation : dans cette phase, qui ne survient que si l'action critique est répudiée, la preuve est restituée de sa mémorisation, présentée, et vérifiée pour résoudre la contestation.

$ non répudiation avec preuve d'origine *(non-repudiation with proof of origin)*
(I) Service de sécurité qui fournit au receveur des données la preuve qui démontre l'origine des données, et donc protège le receveur contre la tentative, par le générateur, de nier faussement avoir envoyé les données. (Voir : service de non répudiation.)
Instructions : ce service est une version forte du service d'authentification d'origine des données. Ce service peut non seulement vérifier l'identité d'une entité système qui est la source originale des données reçues, mais il peut aussi fournir la preuve de cette identité à un tiers.

$ non répudiation avec preuve de réception *(non-repudiation with proof of receipt)*
(I) Service de sécurité qui fournit au générateur des données la preuve qui démontre que les données ont été reçues comme adressées, et protège donc le générateur contre une tentative du receveur de nier faussement avoir reçu les données. (Voir : service de non répudiation.)

$ support non volatile *(non-volatile media)*
(I) Support de mémorisation qui une fois écrit, fournit une mémorisation stable des informations sans la fourniture d'énergie externe. (À comparer à : mémorisation permanente, support volatile.)

$ notarisation *(notarization)*
(I) Enregistrement de données sous l'autorité ou au bons soins d'un tiers de confiance, rendant ainsi possible de fournir l'assurance ultérieure de la précision des caractéristiques revendiquées pour les données, comme leur contenu, origine, durée d'existence, et heure de livraison. [I7498-2] (Voir : notaire numérique.)

$ nul *(null)*
(N) /chiffrement/ "Lettre factice, symbole de lettre, ou groupe de code inséré dans un message chiffré pour retarder ou empêcher son déchiffrement ou pour compléter des groupes chiffrés pour les besoins de la transmission ou de la sécurité de transmission." [C4009]

$ algorithme de chiffrement NUL *(NULL encryption algorithm)*
(I) Algorithme [RFC2410] qui est spécifié comme ne faisant rien pour transformer les données du texte source ; c'est-à-dire, un non fonctionnement. Il a été généré parce que ESP spécifie toujours l'utilisation d'un algorithme de chiffrement pour la confidentialité. L'algorithme de chiffrement NUL est un moyen pratique pour représenter l'option de ne pas appliquer de chiffrement dans ESP (ou dans tout autre contexte où un non fonctionnement est nécessaire). (À comparer à : nul.)

$ OAKLEY
(I) Protocole d'établissement de clé (proposé pour IPsec mais supplanté par IKE) fondé sur l'algorithme Diffie-Hellman-Merkle et conçu pour être un composant compatible de ISAKMP. [RFC2412]
Instructions : OAKLEY établit une clé partagée avec un identifiant alloué et des identités authentifiées associées pour les parties ; c'est-à-dire que OAKLEY fournit un service d'authentification pour assurer les entités de l'identité de l'autre entité, même si l'échange Diffie-Hellman-Merkle est menacé par une écoute active. Il fournit aussi un secret de transmission de clé publique pour la clé partagée et prend en charge les mises à jour de clés, l'incorporation de clés distribuées par des mécanismes hors bande, et des structures de groupe abstrait définies par l'usager à utiliser avec Diffie-Hellman-Merkle.

$ objet *(object)*
(I) /modèle formel/ Usage en modélisation de système de confiance : un composant de système qui contient ou reçoit de l'information. (Voir : modèle Bell-LaPadula, réutilisation d'objet, système de confiance.)

$ identifiant d'objet (OID, *object identifier*)
1. (N) Nom officiel, unique au monde pour une chose, écrit comme une séquence d'entiers (qui sont formés et alloués comme défini dans la norme ASN.1) et utilisé pour faire référence à la chose dans des spécifications abstraites et durant la négociation des services de sécurité dans un protocole.
2. (O) "Valeur (distinguable de toute autre valeur de ce genre) [qui] est associée à un objet." [X680]

Instructions : les objets nommés par des OID sont les feuilles de l'arborescence des identifiants d'objet (qui est similaire, mais différente de l'arborescence d'information de répertoire X.500). Chaque arc (c'est-à-dire, chaque branche de l'arborescence) est étiquetée avec un entier non négatif. Un OID est la séquence des entiers sur le chemin qui conduit de la racine de l'arborescence à un objet désigné.

L'arborescence des OID a trois arcs immédiatement en dessous de la racine : {0} pour l'usage de l'UIT-T, {1} pour l'usage de l'ISO, et {2} pour l'usage conjoint des deux. En dessous de l'UIT-T se trouvent quatre arcs, où {0 0} est pour les Recommandations UIT-T. En dessous de {0 0} sont 26 arcs, un pour chaque série de Recommandations commençant par les lettres A à Z, et en dessous sont des arcs pour chaque Recommandation. Donc, l'OID pour la Recommandation UIT-T X.509 est {0 0 24 509}. En dessous de l'ISO sont quatre arcs, où {1 0 }est pour les normes ISO, et en dessous sont des arcs pour chaque norme ISO. Donc, l' OID pour la norme ISO/CEI 9594-8 (le numéro ISO pour X.509) est {1 0 9594 8}.

L'ANSI enregistre les noms d'organisation sous la branche {joint-iso-ccitt(2) country(16) US(840) organization(1) gov(101) csor(3)}. Le NIST CSOR enregistre les objets PKI sous la branche {joint-iso-itu-t(2) country(16) us(840) organization (1) gov(101) csor(3)}. Le U.S. DoD enregistre les objets INFOSEC sous la branche {joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) dod(2) infosec(1)}.

Le groupe de travail Public-Key Infrastructure (pkix) de l'IETF enregistre les objets PKI sous la branche {iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7)}. [RFC3280]

$ réutilisation d'objet *(object reuse)*

(N) /COMPUSEC/ Réallocation et réutilisation d'une zone d'un support de mémorisation (par exemple, une mémoire à accès aléatoire, une disquette, une bande magnétique) qui a déjà contenu des objets de données sensibles. Avant qu'elle soit réallouée pour être utilisée par un nouvel objet, la zone doit être écrasée, ou dans certains cas, purgée. [NCS04] (Voir : objet.)

$ obstruction

(I) Type d'action de menace qui interrompt la livraison de services système en gênant le fonctionnement du système. (Voir : interruption.)

Instructions : ce type d'action de menace inclut les sous types suivants :
- "Interférence" : interruption des opérations d'un système en bloquant la communication des données d'utilisateur ou les informations de contrôle. (Voir : embouteillage.)
- "Surcharge" : gêne apportée au fonctionnement d'un système par le placement d'une charge excessive sur les capacités de performance d'un composant du système. (Voir : inondation.)

$ octet

(I) Unité de données de huit bits. (À comparer à : byte.)

Usage : ce terme est utilisé en réseautage (en particulier dans les normes OSI) de préférence à "byte", parce que certains systèmes utilisent "byte" pour des unités de mémorisation de données d'une taille autre que huit bits.

$ attaque hors ligne *(off-line attack)* (I) Voir : définition secondaire sous "attaque".

$ ohnosecond

(D) Cette minuscule fraction de temps dans laquelle vous réalisez que votre clé privée a été compromise.

Utilisation déconseillée : les IDOC NE DEVRAIENT PAS utiliser ce terme ; c'est une plaisanterie pour locuteurs anglais. (Voir : Utilisation déconseillée sous "Livre Vert".)

$ protocole d'état de certificat en ligne (OSCP, *Online Certificate Status Protocol*)

(I) Protocole Internet [RFC2560] utilisé par un client pour obtenir d'un serveur l'état de validité et d'autres informations sur un certificat numérique. (Mentionné mais non spécifié dans [X509].)

Instructions : dans certaines applications, comme celles impliquant des transactions commerciales de grande valeur, il peut être nécessaire (a) d'obtenir des états de révocation de certificat qui sont plus frais qu'il n'est possible avec les CRL ou (b) d'obtenir d'autres sortes d'informations d'état. OCSP peut être utilisé pour déterminer l'état actuel de révocation d'un certificat numérique, au lieu de ou en plus de la vérification périodique d'une CRL. Un client OCSP produit une demande d'état à un serveur OCSP et suspend l'acceptation du certificat en question jusqu'à ce que le serveur fournisse une réponse.

$ bourrage à utilisation unique *(one-time pad)*
1. (N) Système de chiffrement manuel sous la forme d'un bourrage papier pour utilisation unique.
2. (I) Algorithme de chiffrement dans lequel la clé est une séquence aléatoire de symboles et chaque symbole est utilisé une

seule fois pour le chiffrement – c'est-à-dire, utilisé pour chiffrer seulement un symbole de texte source et fournit donc un seul symbole de texte chiffré – et une copie de la clé est utilisée de façon similaire pour le déchiffrement.

Instructions : pour assurer l'utilisation unique, la copie de la clé utilisée pour le chiffrement est détruite après usage, comme l'est la copie utilisée pour le déchiffrement. C'est le seul algorithme de chiffrement qui soit vraiment incassable, même avec des ressources illimitées pour la cryptanalyse [Schn], mais la gestion de clés a un coût et les problèmes de synchronisation le rendent impraticable sauf dans des situations particulières.

$ mot de passe à utilisation unique (OTP, *one-time password, One-Time Password*)

1. (I) /en minuscules/ Un "mot de passe à utilisation unique " est une simple technique d'authentification dans laquelle chaque mot de passe est utilisé une seule fois comme information d'authentification qui vérifie une identité. Cette technique contre les menaces d'attaque en répétition qui utilisent des mots de passe capturés par écoute.
2. (I) /en majuscules/ "One-Time Password" est un protocole Internet [RFC2289] qui se fonde sur S/KEY et utilise une fonction de hachage cryptographique pour générer des mots de passe à utilisation unique à utiliser comme informations d'authentification dans la connexion au système et dans d'autres processus qui ont besoin de protection contre les attaques en répétition.

$ chiffrement unidirectionnel *(one-way encryption)*

(I) Transformation irréversible de texte source en texte chiffré, de telle sorte que le texte source ne peut pas être récupéré à partir du texte chiffré autrement que par des procédures exhaustives même si la clé de chiffrement est connue . (Voir : force brute, chiffrement.)

$ fonction unidirectionnelle *(one-way function)*

(I) "Fonction (mathématique) f, [qui] est facile à calculer, mais pour une valeur générale y dans la gamme, il est difficile de calculer une valeur x dans le domaine telle que f(x) = y. Il peut y avoir quelques valeurs de y pour lesquelles trouver x n'est pas d'un calcul difficile." [X509]

Utilisation déconseillée : les IDOC NE DEVRAIENT PAS utiliser ce terme comme synonyme de "hachage cryptographique".

$ acheminement en oignon *(onion routing)*

(I) Système qui peut être utilisé pour fournir à la fois (a) la confidentialité des données et (b) la confidentialité des flux de trafic pour les paquets du réseau, et fournir aussi (c) l'anonymat de la source des paquets.

Instructions : la source, au lieu d'envoyer un paquet directement à la destination prévue, l'envoie à un "mandataire d'acheminement en oignon" qui construit une connexion anonyme à travers plusieurs autres "routeurs en oignon" vers la destination. Le mandataire définit un chemin à travers le "réseau d'acheminement en oignon" en encapsulant la charge utile d'origine dans un paquet de données en couches appelé un "oignon", dans lequel chaque couche définit le prochain bond dans le chemin et chaque couche est aussi chiffrée. Le long du chemin, chaque routeur oignon qui reçoit l'oignon pèle une couche, déchiffre cette couche, et y lit l'adresse du prochain routeur oignon sur le chemin ; il bourre l'oignon restant à une certaine taille constante, et envoie l'oignon bourré à ce prochain routeur.

$ environnement de sécurité ouvert *(open security environment)*

(O) /U.S. DoD/ Environnement de système qui satisfait au moins une des deux conditions suivantes : (a) les développeurs d'application (y compris de maintenance) n'ont pas les accréditifs ou autorisations suffisants pour fournir une présomption acceptable qu'ils n'ont pas introduit de logique malveillante ; (b) le contrôle de configuration ne fournit pas une assurance suffisante que les applications et l'équipement sont protégés contre l'introduction d'une logique malveillante avant et durant le fonctionnement des applications du système. [NCS04] (Voir : "première loi" sous "Lois de Courtney". À comparer à : environnement de sécurité clos.)

$ mémorisation ouverte *'open storage)*

(N) /Gouvernement des USA/ "Mémorisation d'informations classifiées au sein d'une facilité accréditée, mais pas dans des conteneurs sûrs approuvés par l'administration générale des services, alors que la facilité n'est pas occupée par des personnels autorisés." [C4009]

$ modèle de référence de connexion des systèmes ouverts (OSIRM, *Open Systems Interconnection Reference Model*)

(N) Norme conjointe ISO/UIT-T [I.7498-1] pour un cadre d'architecture de communication en sept couches pour l'interconnexion des ordinateurs dans les réseaux. (Voir : Architecture de sécurité OSIRM. À comparer à : Suite des protocoles Internet.)

Instructions : les normes fondées sur OSIRM incluent des protocoles de communication qui sont pour la plupart incompatibles avec l'IPS, mais incluent aussi des modèles de sécurité, tels que X.509, qui sont utilisés dans l'Internet.

Les couches OSIRM, de la plus élevée à la plus basse sont : (7) Application, (6) Présentation, (5) Session, (4) Transport, (3) Réseau, (2) Liaison des données, et (1) Physique.

Usage : le présent glossaire se réfère aux couches OSIRM par des numéros pour éviter de les confondre avec les couches

IPS, qui sont appelées par un nom.
Une personne inconnue a décrit comment les couches OSIRM correspondent aux sept péchés capitaux :
7. Colère : l'application est toujours en colère au cause du désordre qu'elle voit en dessous d'elle. (Hé ! qui est montré du doigt ?)
6. Paresse : la présentation est trop paresseuse pour faire par elle-même quelque chose de productif.
5. Luxure : la session implore toujours et réclame ce qui en réalité appartient aux fonctionnalités de l'application.
4. Avarice : le transport veut toutes les fonctions de bout en bout. (Bien sûr, il le mérite, mais la vie n'est pas juste.)
3. Gourmandise : le réseau (en mode connexion) est surchargé et en surpoids après avoir essayé trop souvent de manger le déjeuner du Transport.
2. Envie : la pauvre liaison des données est toujours affamée d'attentions. (Avec le mode de transfert asynchrone, peut-être se sent elle moins négligée.)
1. Orgueil : la couche physique s'est arrangée pour éviter la controverse, et presque tous les embarras subis par les autres.
John G. Fletcher a décrit comment les couches OSIRM correspondent aux nains de Blanche Neige :
7. Doc : l'application agit comme si elle était le patron, mais elle se prend parfois les pieds dans la syntaxe.
6. Dormeur : la présentation est indolente, étant coupable du péché de paresse.
5. Stupide : la session est confuse parce que son mandat n'est pas très clair.
4. Grognon : le transport est irrité parce que le réseau s'est accroché aux basques du transport.
3. Joyeux : le réseau sourit pour la raison même qui irrite le transport.
2. Atchoum : la liaison des données fait du raffut dans l'espoir d'attirer l'attention.
1. Timide : la couche physique fait tranquillement son travail, à l'insu des autres.

$ intégrité de fonctionnement *(operational integrity)*
(I) Synonyme de "intégrité système" ; ce synonyme souligne les performance réelles des fonctions du système plutôt que juste la capacité de les effectuer.

$ sécurité de fonctionnement *(operational security)*
1. (I) Capacités d'un système, ou performances des fonctions d'un système, qui sont nécessaires soit (a) pour gérer en toute sécurité un système, soit (b) pour gérer les caractéristiques de sécurité d'un système. (À comparer à : sécurité des opérations (OPSEC).)
Usage : les IDOC qui utilisent ce terme DEVRAIENT en donner une définition parce que (a) la définition donnée ici est générale et vague et (b) le terme pourrait facilement être confondu avec celui de "sécurité des opérations", qui est un concept différent.
Instructions : par exemple, dans le contexte d'un fournisseur d'accès Internet, le terme pourrait se référer aux capacités de gérer les appareils du réseau en cas d'attaque, de simplifier la localisation des pannes, de garder trace des événements qui affectent l'intégrité du système, d'aider à analyser les sources des attaques, et de fournir aux administrateurs le contrôle des adresses et protocoles réseau pour aider à atténuer les attaques les plus courantes. [RFC3871]
2. (D) Synonyme de "sécurité administrative".
Définition déconseillée : les IDOC NE DEVRAIENT PAS utiliser ce terme comme synonyme de "sécurité administrative". Tout type de sécurité peut affecter les opérations du système ; donc, le terme peut être trompeur. À la place, utiliser "sécurité administrative", "sécurité de communication", "sécurité informatique", "sécurité des émanations", "sécurité personnelle", "sécurité physique", ou le type voulu. (Voir : architecture de sécurité. À comparer à : intégrité de fonctionnement, OPSEC.)

$ sécurité des opérations (OPSEC, *operations security*)
(I) Processus pour identifier, contrôler, et protéger la preuve de la planification et de l'exécution d'activités et opérations sensibles, et empêcher par là que des adversaires potentiels obtiennent la connaissance de vos capacités et intentions. (Voir : communications couvertes. À comparer à : sécurité de fonctionnement.)

$ opérateur *(operator)*
(I) Personne qui a été autorisée à diriger des fonctions choisies d'un système. (À comparer à : gérant, usager.)
Usage : les IDOC qui utilisent ce terme DEVRAIENT en donner une définition parce qu'un opérateur de système peut être ou non traité comme un "usager".

$ OPSEC
1. (I) Abréviation de "sécurité des opérations".
2. (D) Abréviation de "sécurité de fonctionnement".
Utilisation déconseillée : les IDOC NE DEVRAIENT PAS utiliser cette abréviation pour "sécurité de fonctionnement" (comme défini dans le présent glossaire) parce que son utilisation pour "sécurité des opérations" a été bien établie depuis de nombreuses années, en particulier dans les milieux militaires.

$ Livre Orange *(Orange Book)*

(D) /argot/ Synonyme de "critères d'évaluation de système informatique de confiance *(Trusted Computer System Evaluation Criteria)*" [CSC1], [DoD1].
Utilisation déconseillée : les IDOC NE DEVRAIENT PAS utiliser ce terme comme synonyme de "critères d'évaluation de système informatique de confiance" [CSC1], [DoD1]. À la place, utiliser le nom approprié complet du document ou, dans les références suivantes, l'abréviation "TCSEC". (Voir : utilisation déconseillée sous "Livre Vert".)

$ certificat d'organisation *(organizational certificate)*
1. (I) Certificat de clé publique X.509 dans lequel le champ "subject" contient le nom d'une institution ou d'un ensemble (par exemple, une société, un gouvernement, une école, un syndicat, club, groupe ethnique, nationalité, système, ou groupe d'individus jouant le même rôle) plutôt que le nom d'une personne ou appareil individuel. (À comparer à : certificat personnel, certificat de rôle.)

Instructions : un tel certificat peut être produit dans un des buts suivants :
- permettre à un individu de prouver qu'il est membre de l'organisation,
- permettre à un individu de représenter l'organisation, c'est-à-dire, agir en son nom et avec ses pouvoirs ou permissions.

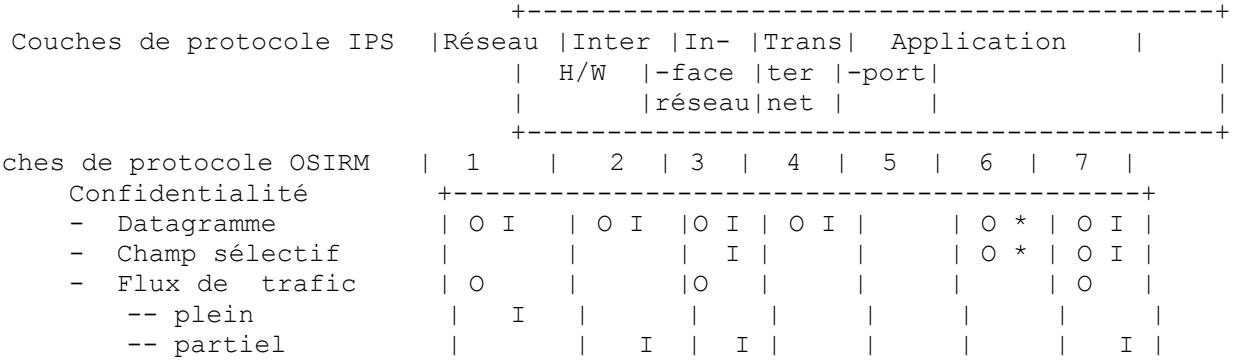
2. (O) /MISSI/ Type de certificat de clé publique X.509 MISSI qui est produit pour prendre en charge le traitement des messages organisationnels du système de messages de Défense de l'U.S. DoD.

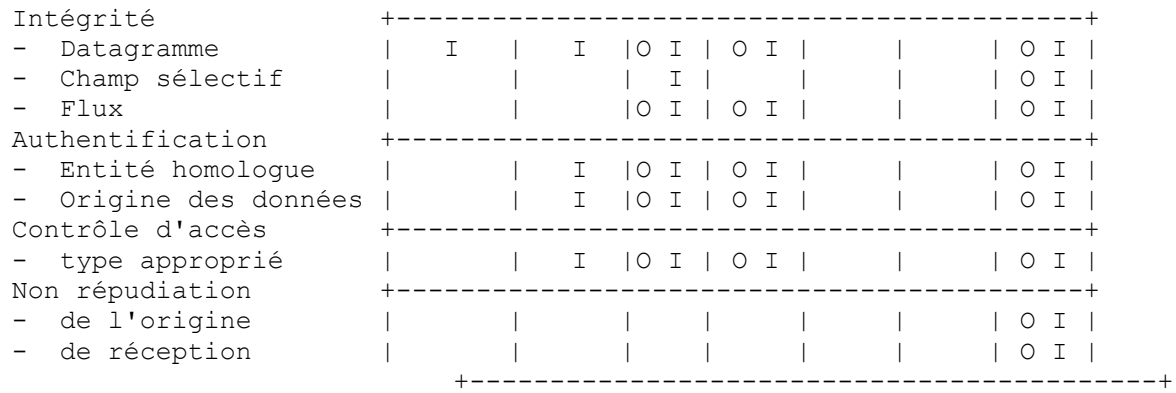
$ autorité d'enregistrement d'organisations (ORA, *organizational registration authority*)
1. (I) /PKI/ RA pour une organisation.
2. (O) /MISSI/ Entité d'extrémité qui (a) assiste une PCA, CA, ou SCA à enregistrer d'autres entités d'extrémité en rassemblant, vérifiant, et en entrant les données et en les faisant suivre à l'autorité de signature, et (b) peut aussi aider aux fonctions de gestion de cartes. Un ORA est une autorité administrative locale, et le terme se réfère à la fois au rôle et à la personne qui joue ce rôle. Un ORA ne signe pas de certificat, de CRL, ou de CKL. (Voir : ORA sans PIN, ORA SSO-PIN, ORA à PIN d'utilisateur.)

$ authentification d'origine *(origin authentication)*
(D) Synonyme de "authentification d'origine des données". (Voir : authentification, authentification d'origine des données.)
Terme déconseillé : les IDOC NE DEVRAIENT PAS utiliser ce terme ; il suggère une utilisation négligente du terme normalisé internationalement "authentification d'origine des données" et pourrait aussi être confondu avec "authentification d'entité homologue."

$ authenticité d'origine *(origin authenticity)*
(D) Synonyme de "authentification d'origine des données". (Voir : authenticité, authentification d'origine des données.)
Terme déconseillé : les IDOC NE DEVRAIENT PAS utiliser ce terme ; il suggère une utilisation négligente du terme normalisé internationalement "authentification d'origine des données" et mélange des concepts d'une façon potentiellement trompeuse.

$ architecture de sécurité OSIRM *(OSIRM Security Architecture)*
(N) Partie de l'OSIRM [I7498-2] qui spécifie les services de sécurité et les mécanismes de sécurité qui peuvent être appliqués pour protéger les communications entre deux systèmes. (Voir : architecture de sécurité.)
Instructions : cette partie de l'OSIRM inclut une allocation de services de sécurité aux couches de protocole. Le tableau qui suit montre quels services de sécurité (voir leurs définitions dans ce glossaire) sont permis par l'OSIRM dans chacune de ses couches. (Aussi, un processus d'application qui fonctionne par dessus la couche Application peut lui-même fournir des services de sécurité.) De façon similaire, le tableau suggère quels services conviennent pour chaque couche de l'IPS. Cependant, expliquer et justifier ces allocations sort du domaine de ce glossaire.
Légende des entrées du Tableau :
O = oui, [I7498-2] permet le service dans cette couche OSIRM.
I = oui, le service peut être incorporé dans cette couche IPS.
* = cette couche est englobée dans la couche Application dans l'IPS.





$ hors bande *(out-of-band)*
(I) /adjectif, adverbe/ Transfert d'informations en utilisant un canal ou une méthode qui est en dehors (c'est-à-dire, séparé ou différente) du canal principal ou de la méthode normale.
Instructions : les mécanismes hors bande sont souvent utilisés pour distribuer les secrets partagés (par exemple, une clé symétrique) ou d'autres éléments d'informations sensibles (par exemple, une clé racine) qui sont nécessaires pour initialiser ou permettre par ailleurs le fonctionnement d'un chiffrement ou d'autres mécanismes de sécurité. Exemple : utiliser le courrier postal pour distribuer des supports imprimés ou magnétiques contenant des clés de chiffrement symétriques à utiliser dans des appareils de chiffrement Internet. (Voir : distribution de clé.)

$ retour de résultat (OFB, *output feedback*)
(N) Mode de chiffrement de bloc qui modifie le mode ECB pour fonctionner sur des segments de texte source de longueur variable inférieure ou égale à la longueur de bloc. [FP081] (Voir : chiffrement de bloc, [SP38A].)
Instructions : ce mode fonctionne en utilisant directement le bloc de résultat généré précédemment par l'algorithme comme prochain bloc d'entrée de l'algorithme (c'est-à-dire, en "réalimentant" le bloc de résultat) et en combinant (par OU exclusif) le bloc de résultat avec le prochain segment de texte source (de la longueur du bloc ou moins) pour former le prochain segment de texte chiffré.

$ attaque de l'extérieur *(outside attack)*
(I) Voir : définition secondaire sous "attaque". À comparer à : externe.)

$ externe *(outsider)*
(I) Usager (généralement une personne) qui accède à un système d'une position qui est en dehors du périmètre de sécurité du système. (À comparer à : usager autorisé, interne, usager non autorisé.)
Instructions : les actions effectuées par un externe en accédant au système peuvent être autorisées ou non autorisées ; c'est-à-dire, un externe peut agir soit comme un usager autorisé, soit comme un usager non autorisé.

$ changement de clé au vol (OTAR, *over-the-air rekeying*)
(N) Changer une clé dans un appareil cryptographique distant en envoyant une nouvelle clé directement à l'appareil via un canal que protège l'appareil. [C4009]

$ surcharge *(overload)* (I) /action de menace/ Voir : définition secondaire sous "obstruction".

$ P1363 (N) Voir : IEEE P1363.

$ paquetage *(package)*
(N) /Critères communs/ Ensemble réutilisable de composants fonctionnels ou d'assurance, combinés en une seule unité pour satisfaire un ensemble d'objectifs de sécurité identifiés. (À comparer à : profil de protection.)
Exemple : les sept EAL définis à la partie 3 des critères communs sont des paquetages prédéfinis d'assurance.
Instructions : un paquetage est une combinaison de composants d'exigence de sécurité et est destiné à être réutilisable dans la construction de paquetages plus complexes ou de profils de protection et de cibles de sécurité. Un paquetage exprime un ensemble d'exigences fonctionnelles ou d'assurance qui satisfont un besoin particulier exprimé par un ensemble d'objectifs de sécurité.

$ paquet *(packet)*
(I) Bloc de données qui est porté d'une source à une destination à travers un canal de communication, ou plus généralement, à travers un réseau. (À comparer à : datagramme, PDU.)

$ filtre de paquet *(packet filter)* (I) Voir : définition secondaire sous "routeur de filtrage".

$ packet monkey
(D) /argot/ Quelqu'un qui inonde un système de paquets, créant une condition de déni de service pour les utilisateurs du système. (Voir : craqueur.)
Terme déconseillé : il est vraisemblable que les autres cultures utilisent des métaphores différentes pour ce concept. Donc, pour éviter l'incompréhension entre les nations, les IDOC NE DEVRAIENT PAS utiliser ce terme. (Voir : Utilisation déconseillée sous "Livre Vert".)

$ pagejacking
(D) /argot/ Contraction de "capture de page de la Toile". Une attaque de mascarade dans laquelle l'attaquant copie (vole) une page d'accueil ou d'autre matériel du serveur cible, recharge la page sur un serveur qu'il contrôle, et provoque l'indexation de la page réhébergée par les moteurs de recherche majeurs de la Toile, détournant ainsi les navigateurs du serveur cible vers le serveur de l'attaquant.
Terme déconseillé : les IDOC NE DEVRAIENT PAS utiliser cette contraction. Le terme ne figure pas dans la plupart des dictionnaires et pourrait induire en erreur les lecteurs internationaux. (Voir : Utilisation déconseillée sous "Livre Vert".)

$ bit de parité *(parity bit)*
(I) Somme de contrôle qui est calculée sur un bloc de bits en calculant la somme binaire des bits individuels dans le bloc et ensuite en éliminant tous les bits qui ne sont pas de poids fort dans la somme. (Voir : somme de contrôle.)

$ mode de sécurité partitionné *(partitioned security mode)*
(N) Mode de système d'exploitation dans lequel tous les usagers qui ont accès au système ont les accréditifs de sécurité nécessaires pour toutes les données traitées par le système, mais certains usagers peuvent ne pas avoir l'approbation d'accès formelle, soit le besoin de savoir pour toutes les données. (Voir : /système d'exploitation/ sous "mode", approbation d'accès formelle, besoin de savoir, niveau de protection, niveau d'habilitation.)
Usage : généralement abrégé en "mode partitionné". Ce terme a été défini dans la politique du gouvernement des USA sur les accréditations de systèmes.

$ attaque passive *(passive attack)* (I) Voir : définition secondaire sous "attaque".

$ utilisateur passif *(passive user)* (I) Voir : définition secondaire sous "utilisateur système".

$ écoute passive *(passive wiretapping)*
(I) Attaque d'écoute qui tente seulement d'observer un flux de communication et d'obtenir la connaissance des données qu'il contient, mais n'altère pas ce flux ni ne l'affecte par ailleurs . Voir : écoute. À comparer à : attaque passive, écoute active.)

$ mot de passe *(password)*
1a. (I) Valeur de données secrète, usuellement une chaîne de caractères, qui est présentée à un système par un utilisateur pour authentifier l'identité de l'utilisateur. (Voir : informations d'authentification, défi-réponse, PIN, authentification simple.)
1b. (O) "Chaîne de caractères utilisée pour authentifier une identité." [CSC2]
1c. (O) "Chaîne de caractères (lettres, nombres, et autres symboles) utilisée pour authentifier une identité ou pour vérifier une autorisation d'accès." [FP140]
1d. (O) "Secret qu'un prétendant mémorise et utilise pour authentifier son identité. Les mots de passe sont normalement des chaînes de caractères." [SP63]
Instructions : un mot de passe est généralement apparié à un identifiant d'utilisateur qui est explicite dans le processus d'authentification, bien que dans certains cas, l'identifiant puisse être implicite. Un mot de passe est généralement vérifié en le confrontant à une valeur mémorisée détenue par le système de contrôle d'accès pour cet identifiant.
Utiliser un mot de passe comme informations d'authentification se fonde sur la supposition que le mot de passe n'est connu que par l'entité système pour laquelle l'identité est authentifiée. Donc, dans un environnement de réseau où l'écoute est possible, la simple authentification qui s'appuie sur la transmission de mots de passe statiques (c'est-à-dire, utilisés de façon répétitive) en clair est inadéquate. (Voir : mot de passe à utilisation unique, authentification forte.)

$ protocole d'authentification par mot de passe (PAP, *Password Authentication Protocol*)
(I) Mécanisme simple d'authentification dans PPP. Dans PAP, un identifiant d'utilisateur et un mot de passe sont transmis en clair. [RFC1334] (Voir : CHAP.)

$ reniflage de mot de passe *(password sniffing)*
(D) /argot/ Écoute passive pour acquérir la connaissance des mots de passe. (Voir : Utilisation déconseillée sous "reniflage".)

$ découverte de chemin *(path discovery)*
(I) Pour un certificat numérique, processus pour trouver un ensemble de certificats de clé publique qui comporte un chemin de certification d'une clé de confiance à ce certificat spécifique.

$ validation de chemin *(path validation)*
(I) Processus de validation de (a) tous les certificats numériques dans un chemin de certification et (b) des relations nécessaires entre ces certificats, validant donc les contenus du dernier certificat sur le chemin. (Voir : validation de certificat.)
Instructions : pour promouvoir des applications PKI interopérables dans l'Internet, la RFC3280 spécifie un algorithme détaillé pour la validation d'un chemin de certification.

$ carte de payement *(payment card)*
(N) /SET/ Se réfère collectivement aux "cartes de crédit, cartes de débit, et cartes bancaires délivrées par une institution financière et qui reflètent une relation entre le détenteur de carte et l'institution financière." [SET2]

$ passerelle de payement *(payment gateway)*
(O) /SET/ Système géré par un acheteur, ou par un tiers désigné par un acheteur, pour fournir des services de commerce électronique aux commerçants pour la prise en charge de l'acheteur, et qui sert d'interface à l'acheteur pour la prise en charge de l'autorisation, la capture, et le traitement des messages de payement commerciaux, y compris les instructions de payement des détenteurs de cartes. [SET1], [SET2]

$ autorité de certification de passerelle de payement (SET PCA, *payment gateway certification authority*)
(O) /SET/ CA qui produit des certificats numériques aux passerelles de payement et est gérée au nom d'une marque de cartes de payement, un acheteur, ou une autre partie conformément aux règles de la marque. Une SET PCA produit une CRL pour les certificats de passerelle de payement compromis. [SET2] (Voir : PCA.)

$ carte PC *(PC card)*
(N) Type d'appareil périphérique enfichable de la taille d'une carte de crédit qui a été à l'origine développée pour fournir une extension de mémoire aux ordinateurs portables, mais est aussi utilisé pour d'autres sortes d'extensions fonctionnelles. (Voir : FORTEZZA, PCMCIA.)
Instructions : la norme internationale de carte PC définit un facteur de forme non brevetée de trois tailles -- Types I, II, et III -- dont chacune a une interface à 68 broches entre la carte et la prise dans laquelle elle s'enfiche. Les trois types ont la même longueur et largeur, en gros la taille d'une carte de crédit, mais elles diffèrent en épaisseur de 3,3 à 10,5 mm. Les exemples incluent des modules de mémorisation, des modems, des adaptateurs d'interface d'appareil, et des modules cryptographiques.

$ PCA
(D) Abréviation de diverses sortes "d'autorité de certification". (Voir : autorité de certification de politique Internet, (MISSI) autorité de création de politique, (SET) autorité de certification de passerelle de payement.)
Utilisation déconseillée : un IDOC qui utilise cette abréviation DEVRAIT la définir à sa première utilisation.

$ PCI (N) Voir : "informations de contrôle de protocole" sous "unité de données de protocole".

$ PCMCIA
(N) L'Association internationale des cartes à mémoire d'ordinateur personnel *(Personal Computer Memory Card International Association)* est un groupe de fabricants, développeurs, et commerçants, fondé en 1989 pour normaliser les cartes à mémoire enfichables pour les ordinateurs personnels et qui s'étend maintenant à toutes les technologies qui fonctionnent sous la forme d'une carte PC . (Voir : carte PC.)

$ authentification d'entité homologue *(peer entity authentication)*
(I) "Corroboration qu'une entité homologue dans une association est celle qu'elle prétend être." [I7498-2] (Voir : authentification.)

$ service d'authentification d'entité homologue *(peer entity authentication service)*
(I) Service de sécurité qui vérifie une identité revendiquée par ou pour une entité système dans une association. (Voir : authentification, service d'authentification.)
Instructions : ce service est utilisé au moment de l'établissement d'une association ou pendant son existence pour confirmer l'identité d'une entité auprès d'une autre, protégeant ainsi contre une mascarade de la première entité. Cependant, à la différence du service d'authentification de l'origine des données, ce service exige qu'il existe une association entre les deux

entités, et la corroboration fournie par le service n'est valide qu'au moment où le service est fourni. (Voir : "relations entre service d'intégrité des données et services d'authentification" sous "service d'intégrité des données").

$ pénétrer *(penetrate)*
1a. (I) Circonvenir les protections de sécurité d'un système. (Voir : attaque, casser, violation.)
1b. (I) Réussir à obtenir de façon répétée l'accès non autorisé à une ressource système protégée. [Huff]

$ pénétration *(penetration)* (I) /action de menace/ Voir : définition secondaire sous "intrusion".

$ essai de pénétration *(penetration test)*
(I) Essai système, souvent au titre de la certification d'un système, dans lequel les évaluateurs tentent de circonvenir les dispositifs de sécurité d'un système. [NCS04], [SP42] (Voir : tiger team.)
Instructions : l'essai de pénétration évalue la vulnérabilité relative d'un système aux attaques et identifie les méthodes pour obtenir l'accès à un système en utilisant des outils et techniques qui sont disponibles à des adversaires. L'essai peut être effectué sous diverses contraintes et conditions, incluant un niveau de connaissances spécifié de la conception et de la mise en œuvre du système. Pour une évaluation TCSEC, les essayeurs sont supposés avoir toute la documentation de conception et de mise en œuvre du système, incluant le code source, les manuels, et les diagrammes des circuits, et fonctionner sous des contraintes supérieures à celles appliquées aux utilisateurs ordinaires.

$ secret parfait vers l'avant *(perfect forward secrecy)*
(I) Pour un protocole d'accord de clé, c'est la propriété que le matériel de chiffrement compromis à long terme ne compromette pas les clés de session qui ont été précédemment déduites du matériel à long terme. (À comparer à : secret de transmission de clé publique.)
Usage : certaines RFC existantes utilisent ce terme mais ne le définissent pas, ou pas avec précision. En préparant ce glossaire, on a trouvé le terrain glissant. Les experts ne sont pas d'accord. Pour tous les aspects pratiques, la littérature définit le "secret parfait vers l'avant" en citant l'algorithme Diffie-Hellman-Merkle. Le terme de "secret de transmission de clé publique" (suggéré par Hilarie Orman et la définition qui en est donnée dans ce glossaire a été forgé pour être compatible avec les documents Internet actuels) est étroit et laisse la possibilité d'améliorer la terminologie.
Défi à la communauté de la sécurité Internet : on a besoin d'une taxonomie de termes et définitions qui couvre les propriétés de base discutées ici pour toute la gamme des algorithmes et protocoles de chiffrement utilisés dans les normes de l'Internet :
Implication des clés de session ou de clés à long terme : les experts sont en désaccord sur les idées de base impliquées :
- un concept de "secret vers l'avant" est que, étant donnée l'observation du fonctionnement d'un protocole d'établissement de clé jusqu'à l'instant t, et que certaines des clés de session déduites de ce protocole fonctionnent, on ne peut pas déduire des clés de session passées inconnues ou de futures clés de session.
- une propriété en rapport est que, étant donnée l'observation du protocole et la connaissance des clés de session dérivées, on ne peut pas déduire une ou plusieurs des clés privées à long terme.
- la définition "I" présentée ci-dessus implique un troisième concept de "secret vers l'avant" qui se réfère à l'effet de la compromission des clés à long terme.
- les trois concepts impliquent tous l'idée que la compromission de "cette" clé de chiffrement n'est pas supposée compromettre la "prochaine". Il y a aussi l'idée que la compromission d'une seule clé va compromettre seulement les données protégées par cette seule clé. Dans la littérature Internet, l'accent a été mis sur la protection contre le déchiffrement du trafic de retour dans l'éventualité de la compromission d'un matériel de clé secrète détenu par une ou plusieurs parties d'une communication.

Vers l'avant ou vers l'arrière : les experts sont mal à l'aise avec le terme "vers l'avant", parce que la compromission de "cette" clé de chiffrement n'est aussi pas supposée compromettre la "précédente", qui est "vers l'arrière" plutôt que vers l'avant. Dans S/KEY, si la clé utilisée au temps t est compromise, alors toutes les clés utilisées avant elle sont compromises. Si la clé à "long terme" (c'est-à-dire, la base du schéma de hachage) est compromise, alors toutes les clés passées et futures sont compromises ; donc, on peut dire que S/KEY n'a de secret ni vers l'avant ni vers l'arrière,
Chiffrement asymétrique ou symétrique : les experts ne sont pas d'accord sur le secret vers l'avant dans le contexte de systèmes cryptographiques symétriques. En l'absence de chiffrement asymétrique, la compromission de toute clé à long terme semble compromettre toute clé de session déduite de la clé à long terme. Par exemple, Kerberos n'est pas à secret vers l'avant, parce que compromettre le mot de passe d'un client (compromettant donc la clé partagée par le client et le serveur d'authentification) compromet les futures clés de session partagées par le client et le serveur qui accorde les tickets.
Secret vers l'avant ordinaire ou secret vers l'avant "parfait" : les experts ne sont pas d'accord sur la différence entre les deux. Certains disent qu'il n'y a pas de différence, et d'autres disent que la désignation initiale était malheureuse et suggèrent de laisser tomber le mot "parfait". Certains suggèrent d'utiliser "secret de transmission" pour le cas où une clé privée à long terme est compromise, et d'ajouter "parfait" lorsque les deux clés privées (ou, lorsque le protocole est multi partie, toutes les clés privées) sont compromises.
Remerciements : Bill Burr, Burt Kaliski, Steve Kent, Paul Van Oorschot, Jonathan Trostle, Michael Wiener, et particulièrement Hilarie Orman ont contribué aux idées de cette discussion.

$ périmètre *(perimeter)* Voir : périmètre de sécurité.

$ traitement par périodes *(periods processing)*
(I) Mode de fonctionnement de système dans lequel les informations de sensibilités différentes sont traitées à des moments distinctement différents par le même système, le système étant proprement purgé ou désinfecté entre les périodes. (Voir : changement de couleur.)
Instructions : le mode de sécurité du fonctionnement et la classification maximum des données traitées par le système sont établis pour un intervalle de temps et spnt ensuite changés pour l'intervalle de temps suivant. Une période s'étend de l'initialisation sûre du système à l'achèvement de toute purge de données sensibles traitées par le système dans la période.

$ mémorisation permanente *(permanent storage)*
(I) Support non volatile qui, une fois écrit, ne peut jamais être complètement écrasé.

$ permission
1a. (I) Synonyme de "autorisation". (À comparer à : privilège.)
1b. (N) Autorisation ou ensemble d'autorisations d'effectuer des fonctions en rapport avec la sécurité dans le contexte d'un contrôle d'accès fondé sur le rôle. [ANSI]
Instructions : une permission est une autorisation déclarée de façon positive pour l'accès qui (a) peut être associé à un ou plusieurs rôles et (b) permet à un usager dans un rôle d'accéder à un ensemble spécifié de ressources système en causant l'exécution d'un ensemble spécifique d'actions systèmes sur les ressources.

$ certificat à un nom d'emprunt *(persona certificate)*
(I) Certificat X.509 produit à une entité système qui souhaite utiliser un pseudonyme pour dissimuler sa véritable identité lors de l'utilisation de PEM ou autres services Internet qui dépendent de la prise en charge de PKI. (Voir : anonymat.) [RFC1422]
Instructions : les concepteurs de PEM entendaient que (a) une CA produisant des certificats sous un nom d'emprunt ne garantirait explicitement pas l'identité de l'entité système à qui le certificat est produit, (b) de tels certificats ne seraient produits que par des CA subordonnées à une CA politique ayant une politique établissant cet objet (c'est-à-dire, qui préviendrait les consommateurs que le champ "subject" du DN représente seulement un pseudonyme et non une identité d'utilisateur véritable dûment contrôlée) et (c) la CA n'aurait pas besoin de garder les traces de la véritable identité du sujet du certificat.
Cependant, les concepteurs de PEM avaient aussi l'intention qu'une CA qui produit des certificats sous nom d'emprunt établirait des procédures (d) pour permettre au "détenteur d'un certificat sous un nom d'emprunt de demander que ce certificat soit révoqué" et (e) pour s'assurer qu'elle n'a pas produit le même sujet DN à plusieurs usagers. Cette dernière condition implique qu'un certificat sous un nom d'emprunt n'est pas un certificat d'organisation sauf si l'organisation a juste un membre ou représentant.

$ numéro d'identification personnel (PIN, *personal identification number*)
1a. (I) Chaîne de caractères utilisée comme mot de passe pour obtenir l'accès à une ressource système. (Voir : informations d'authentification.)
Exemple : un jeton cryptographique exige normalement que son utilisateur entre un PIN afin d'accéder aux informations mémorisées dans le jeton et d'invoquer les fonctions cryptographiques du jeton.
1b. (O) Code alphanumérique ou mot de passe utilisé pour authentifier une identité.
Instructions : en dépit des mots "identification" et "numéro", un PIN sert rarement d'identifiant d'utilisateur, et les caractères d'un PIN ne sont pas nécessairement tous numériques. Les applications bancaires de commerce de détail utilisent des PIN d'utilisateur à quatre chiffres, mais la carte PC FORTEZZA utilise des PIB SSO de 12 caractères alphanumériques. (Voir : PIN SSO, PIN d'utilisateur.)
Un meilleur nom pour ce concept aurait été ce lui de "chaîne de système d'authentification personnelle" (PASS), et dans ce cas, une chaîne de caractères alphanumériques servant à cela aurait évidement été appelée un "PASSword".

$ informations personnelles *(personal information)*
(I) Information sur une personne particulière, et spécialement des informations de nature intime ou critique, qui pourraient causer un dommage ou une souffrance à cette personne si elles étaient divulguées à des tiers non autorisés. Exemples : dossier médical, casier judiciaire, liste des crédits, inscriptions académiques, rapport d'apprentissage, demande d'embauche, numéro de carte de crédit, numéro de carte de sécurité sociale. (Voir : confidentialité.)

$ personnalité *(personality)*
1. (I) Synonyme de "principal".
2. (O) /MISSI/ Ensemble de certificats de clé publique MISSI X.509 qui ont le même DN sujet, avec leurs clés privées associées et leurs spécifications d'usage, qui est mémorisé sur une carte PC FORTEZZA pour prendre en charge un rôle joué par l'utilisateur de la carte.

Instructions : lorsque un utilisateur de carte choisit une personnalité à utiliser dans une application à capacité FORTEZZA, les données déterminent les traits de comportement (la personnalité) de l'application. Un utilisateur de carte peut avoir plusieurs personnalités sur la carte. Chacune a une "étiquette de personnalité", une chaîne de caractères familière à l'utilisateur que les applications peuvent afficher à l' usager pour choisir la personnalité à utiliser ou en changer. Par exemple, la carte d'un utilisateur militaire pourrait contenir trois personnalités : GENERAL HALFTRACK, COMMANDANT DE FORT SWAMPY, et PRESIDENT DE LA SOIREE DE NOUVEL AN. Chaque personnalité comporte un ou plusieurs certificats de différents types (comme DSA ou RSA) pour des objets différents (comme une signature numérique ou un chiffrement) ou avec différentes autorisations.

$ chaîne de système d'authentification personnelle (PASS, *personnel authentication system string*)
(N) Voir : Instructions sous "numéro d'identification personnel.

$ sécurité personnelle *(personnel security)*
(I) Procédures pour s'assurer que des personnes qui accèdent à un système ont les accréditifs appropriés, l'autorisation, et le besoin de savoir requis par la politique de sécurité du système. (Voir : architecture de sécurité.)

$ PGP(marque déposée) (O) Voir : Pretty Good Privacy(marque déposée).

$ négociation de phase 1 (*phase 1 negotiation, phase 2 negotiation*)
(I) /ISAKMP/ Voir : définition secondaire sous "Association de sécurité Internet et protocole de gestion de clé".

$ hameçonnage *(phishing)*
(D) /argot/ Technique pour tenter d'acquérir des données sensibles, comme des numéros de comptes bancaires, par des sollicitations frauduleuses par des messages électroniques ou un site de la Toile, dans laquelle l'auteur se fait passer pour un commerçant légitime ou une personne respectable. (Voir : ingénierie sociale.)
Dérivation : pourrait venir de "pêche factice *(phony fishing)*" ; la sollicitation implique généralement une sorte de leurre ou d'appât pour accrocher les récepteurs sans méfiance. (À comparer à : viol de commutateur privé.)
Terme déconseillé : les IDOC NE DEVRAIENT PAS utiliser ce terme ; il ne figure pas dans la plupart des dictionnaires et pourrait n'être pas compris des lecteurs internationaux. (Voir : Utilisation déconseillée sous "Livre Vert".)

$ Photuris
(I) Protocole d'établissement de clés fondé sur UDP pour les clés de session, conçu pour être utilisé avec les protocoles IPsec AH et ESP. Remplacé par IKE.

$ viol de commutateur privé *(phreaking)*
(D) Contraction de "cassage de téléphone *(telephone breaking)*". Attaque contre, ou pénétration, d'un système de téléphonie, ou par extension, de tout autre système de communication ou d'information. [Raym]
Terme déconseillé : les IDOC NE DEVRAIENT PAS utiliser cette contraction ; elle n'est pas dans la plupart des dictionnaires et pourrait tromper les lecteurs internationaux. (Voir : Utilisation déconseillée sous "Livre Vert".)

$ destruction physique *(physical destruction)*
(I) /action de menace/ Voir : définition secondaire sous "incapacitation".

$ sécurité physique *(physical security)*
(I) Moyens tangibles d'empêcher l'accès physique non autorisé à un système. Exemples : barrières, murs, et autres obstacles, verrous, coffres et chambres fortes, chiens et gardes armés, détecteurs et sonnettes d'alarme. [FP031], [RFC1455] (Voir : architecture de sécurité.)

$ attaque de substitution d'identité *(piggyback attack)*
(I) Forme d'écoute active dans laquelle l'attaquant obtient l'accès à un système via des intervalles d'inactivité dans la connexion de communications légitimes d'un autre utilisateur. Parfois appelée attaque "entre les lignes". (Voir : attaque de capture, attaque par interposition.)
Utilisation déconseillée : les IDOC qui utilisent ce terme DEVRAIENT en donner une définition parce que le terme pourrait tromper les lecteurs internationaux.

$ ping de mort *(ping of death)*
(D) Attaque de déni de service qui envoie un paquet de demande d'écho ICMP (un "ping") d'une longueur inappropriée dans l'intention de causer la défaillance du système de destination. (Voir : balayage de ping, attaque des larmes.)
Terme déconseillé : les IDOC NE DEVRAIENT PAS utiliser ce terme ; à la place, utiliser "attaque de surcharge de paquets de ping" ou un autre terme spécifique du mécanisme d'attaque.

Instructions : cette attaque cherche à exploiter une faiblesse de la mise en œuvre. La spécification IP exige des hôtes qu'ils soient prêts à accepter des datagrammes de jusqu'à 576 octets, mais permet aussi que les datagrammes IP fassent jusqu'à 65 535 octets. Si une mise en œuvre IP ne traite pas correctement les très longs paquets IP, le paquet ping peut faire déborder la mémoire tampon d'entrée et causer une erreur système fatale.

$ balayage de ping *(balayage de ping)*
(I) Attaque qui envoie des demandes d'écho ICMP ("ping") à une gamme d'adresses IP, dans le but de trouver des hôtes qui peuvent être sujets à des vulnérabilités. (Voir : ping de mort. À comparer à : analyse d'accès.)

$ PKCS n° 5 *(PKCS #5)*
(N) Norme [PKC05] (voir : RFC2898) de la série PKCS ; définit une méthode de chiffrement d'une chaîne d'octets avec une clé secrète déduite d'un mot de passe.
Instructions : bien que la méthode puisse être utilisée pour des chaînes d'octets arbitraires, elle est destinée principalement aux application de chiffrement à clé publique pour le chiffrement de clés privées lors de leur transfert d'un système informatique à un autre, comme décrit dans PKCS n° 8.

$ PKCS n° 7 *(PKCS #7)*
(N) Norme [PKC07] (voir : RFC2315) de la série PKCS ; définit une syntaxe pour les données qui peuvent avoir un chiffrement qui leur est appliqué, comme pour les signatures et enveloppes numériques. (Voir : CMS.)

$ PKCS n° 10 *(PKCS #10)*
(N) Norme [PKC10] (voir : RFC2986) de la série PKCS ; définit une syntaxe pour les demandes de certification. (Voir : demande de certification.)
Instructions : une demande PKCS n° 10 contient un DN et une clé publique, et peut contenir d'autres attributs, et est signée par l'entité qui fait la demande. La demande est envoyée à une CA, qui la convertit en un certificat de clé publique X.509 (ou d'une autre forme) et la retourne, éventuellement en format PKCS n° 7.

$ PKCS n° 11 *(PKCS #11)*
(N) Norme [PKC11] de la série PKCS ; définit une CAPI appelée "Cryptoki" pour les appareils qui détiennent des informations de chiffrement et effectuent des fonctions cryptographiques.

$ PKINIT
(I) Abréviation de "chiffrement à clé publique pour l'authentification initiale dans Kerberos *(Public Key Cryptography for Initial Authentication in Kerberos)*" (RFC4556). (Voir : Instructions sous "Kerberos".)

$ PKIX
1a. (I) Contraction de "infrastructure de clé publique X,509 *(Public-Key Infrastructure (X.509)*", nom du groupe de travail de l'IETF qui spécifie une architecture [RFC3280] et établit des protocoles [RFC4210] pour fournir des services de PKI fondés sur X.509 pour l'Internet.
1b. (I) Nom collectif pour cette architecture de PKI Internet et l'ensemble de protocoles associés.
Instructions : le but de PKIX est de faciliter l'utilisation des certificats de clé publique X.509 dans plusieurs applications Internet et de promouvoir l'interopérabilité entre des mises en œuvre différentes qui utilisent ces certificats. La PKI résultante est destinée à fournir un cadre qui prenne en charge une gamme de confiance et des environnements hiérarchisés et une gamme d'environnements d'utilisation. PKIX spécifie (a) des profils de la version 3 de la norme de certificat de clé publique X.509 et de la version 2 des normes de CRL X.509 pour l'Internet, (b) des protocoles opérationnels utilisés par les consommateurs d'assertions pour obtenir des informations telles que des certificats ou des états de certificat, (c) des protocoles de gestion utilisés par des entités système pour échanger les informations nécessaires pour une gestion appropriée de la PKI, et (d) des informations sur les politiques de certificat et les CPS, couvrant les domaines de la sécurité de PKI non directement traités dans le reste de PKIX.

$ texte source *(plain text)*
1. (I) /nom/ Données qui sont entrées dans un processus de chiffrement. (Voir : plaintext. À comparer à : texte chiffré, texte en clair.)
2. (D) /nom/ Synonyme de "texte en clair".
Définition déconseillée : les IDOC NE DEVRAIENT PAS utiliser ce terme comme synonyme de "texte en clair". Le texte source qui est entré dans une opération de chiffrement est parfois du texte en clair, mais d'autres fois le texte source est du texte chiffré qui est le résultat d'une précédente opération de chiffrement. (Voir : super chiffrement.)

$ plaintext
1. (O) /nom/ Synonyme de "texte source *(plain text)*".
2. (I) /adjectif/ Se réfère au texte source. Usage : couramment utilisé à la place de "texte source". (À comparer à : texte

chiffré, texte en clair.)
3. (D) /nom/ Synonyme de "texte en clair".
Définition déconseillée : les IDOC NE DEVRAIENT PAS utiliser ce terme comme synonyme de "texte en clair". Les données du texte en clair sont, par définition, non chiffrées, mais les données du texte source qui sont entrées dans une opération de chiffrement peuvent être des données en clair ou des données chiffrées qui sont le résultat d'une opération de chiffrement précédente. (Voir : super chiffrement.)

$ protocole point à point (PPP, *Point-to-Point Protocol*)
(I) Protocole normalisé de l'Internet (RFC1661) pour l'encapsulation et le transport bidirectionnel de paquets de données de protocole dans la couche 3 OSIRM sur une liaison de couche 2 OSIRM entre deux homologues, et pour multiplexer différents protocoles de couche 3 sur la même liaison. Il inclut une négociation facultative pour choisir et utiliser un protocole d'authentification d'entité homologue pour que les homologues s'authentifient mutuellement avant d'échanger des données de couche 3. (Voir : CHAP, EAP, PAP.)

$ protocole de tunnelage point à point (PPTP, *Point-to-Point Tunneling Protocol*)
(I) Protocole client-serveur Internet (RFC2637) (développé à l'origine par Ascend et Microsoft) qui permet à un usager du service téléphonique de créer une extension virtuelle de la liaison à numérotation à travers un réseau en tunnelant PPP sur IP. (Voir : L2TP.)
Instructions : PPP peut encapsuler tout protocole de couche d'interface réseau de l'IPS ou protocole de la couche 3 OSIRM. Donc, PPTP ne spécifie pas de service de sécurité ; il dépend des protocoles au dessus et en dessous de lui pour fournir la sécurité nécessaire. PPTP rend possible le divorce entre la localisation du serveur de numérotation initial (c'est-à-dire, le concentrateur d'accès PPTP, le client, qui fonctionne sur un hôte dédié) de la localisation à laquelle se termine la connexion à numérotation du protocole (PPP) et où est fourni l'accès au réseau (c'est-à-dire, au serveur de réseau PPTP, qui fonctionne sur un hôte d'usage général).

$ politique *(policy)*
1a. (I) Plan d'action qui est déclaré pour un système ou une organisation et est destiné à affecter et orienter les décisions et faits des composants ou membres de cette entité. (Voir : politique de sécurité.)
1b. (O) Objectif, cours, ou méthode, défini d'action pour guider et déterminer les décisions présentes et futures, qui est mis en œuvre ou exécuté dans un contexte particulier, tel que dans une unité commerciale. [RFC3198]
Abréviation déconseillée : les IDOC NE DEVRAIENT PAS utiliser "politique" comme abréviation de "politique de sécurité" ou de "politique de certificat". À la place, pour éviter l'incompréhension, utiliser un terme pleinement qualifié, au moins à la première utilisation.
Instructions : l'introduction de nouvelles technologies pour remplacer les systèmes traditionnels peut résulter en ce que de nouveaux systèmes sont déployés sans une définition adéquate de politique et avant que les implications de la nouvelle technologie soient pleinement comprises. Dans certains cas, il peut être difficile d'établir des politiques pour une nouvelle technologie avant que le fonctionnement de celle-ci soit essayé et évalué. Donc, les changements de politique tendent à courir derrière les changements technologiques, de sorte que soit les vieilles politiques empêchent l'innovation technique, soit que la nouvelle technologie est déployée sans des politiques adéquates pour gouverner son utilisation.
Lorsque la nouvelle technologie change la façon dont les choses sont faites, de nouvelles "procédures" doivent être définies pour établir des lignes directrices de fonctionnement pour utiliser la technologie et réaliser des résultats satisfaisants, et de nouvelles "pratiques" doivent être établies pour gérer les nouveaux systèmes et surveiller les résultats. Les pratiques et procédures sont plus directement couplées aux systèmes et opérations commerciales réelles que ne le sont les politiques, qui tendent à être plus abstraites.
- Les "pratiques" définissent comment un système doit être géré et quels contrôles sont en place pour surveiller le système et détecter un comportement anormal ou des problèmes de qualité. Les pratiques sont établies pour assurer qu'un système est géré conformément aux politiques déclarées. Les audits de système sont principalement concernés par le fait que les pratiques sont ou non respectées. Les auditeurs évaluent les contrôles pour s'assurer qu'ils se conforment aux normes acceptées de l'industrie, et confirment ensuite que les contrôles sont en place et que les mesures de contrôle sont collectées. Les chemins d'audit sont des exemples de mesures de contrôle qui sont enregistrées au titre des opérations du système.
- Les "procédures" définissent comment un système fonctionne, et se rapportent étroitement à la question de la technologie utilisée, qui sont les opérateurs, et comment le système est déployé physiquement. Les procédures définissent les circonstances de fonctionnement normales aussi bien qu'anormales.
- Pour chaque contrôle défini par une déclaration de pratique, il devrait y avoir des procédures correspondantes pour mettre en œuvre le contrôle et fournir la mesure courante des paramètres de contrôle. À l'inverse, les procédures exigent des pratiques de gestion pour assurer un comportement de fonctionnement cohérent et correct.

$ autorité d'approbation de politique *(policy approval authority)*
(D) /PKI/ Synonyme de "autorité de gestion de politique". [PAG]
Terme déconseillé : les IDOC NE DEVRAIENT PAS utiliser ce terme comme synonyme de "autorité de gestion de politique". Le terme suggère un rôle passif limité qui n'est pas caractéristique des PMA.

$ autorité approuvant la politique (PAA, *policy approving authority*)
(O) /MISSI/ Autorité signataire de niveau supérieur d'une hiérarchie de certification MISSI. Le terme se réfère à la fois au bureau ou rôle d'autorisation et à la personne qui joue de rôle. (Voir : autorité de gestion de politique, registre racine.)
Instructions : une PAA MISSI (a) enregistre les PCA MISSI et signe leurs certificats X.509 de clé publique, (b) produit des CRL mais ne produit pas de CKL, et (c) peut produire des certificats croisés avec les autres PAA.

$ autorité de politique *(policy authority)*
(D) /PKI/ Synonyme de "autorité de gestion de politique". [PAG]
Terme déconseillé : les IDOC NE DEVRAIENT PAS utiliser ce terme comme synonyme de "autorité de gestion de politique". Le terme est inutilement vague et peut donc être confondu avec d'autres entités de PKI, comme les CA et les RA, qui mettent en application divers aspects de politique de PKI.

$ autorité de certification de politique (Internet PCA, *policy certification authority*)
(I) CA conforme à X.509 au second niveau de la hiérarchie de certification Internet, sous le IPRA. Chaque PCA fonctionne selon sa politique de sécurité publiée (voir : politique de certificat, CPS) et dans les contraintes établies par le IPRA pour toutes les PCA. [RFC1422]. (Voir : autorité de création de politique.)

$ autorité de création de politique (MISSI PCA, *policy creation authority*)
(O) /MISSI/ Second niveau d'une hiérarchie de certification MISSI ; la racine administrative d'un domaine de politique de sécurité des utilisateurs de MISSI, et autres autorités subsidiaires. Le terme se réfère à la fois au bureau ou rôle d'autorisation et à la personne qui tient cet office. (Voir : autorité de certification de politique.)
Instructions : le certificat d'une PCA MISSI est produit par une PAA. La PCA enregistre les CA dans son domaine, définit leurs configurations, et produit leurs certificats de clé publique X.509. (La PCA peut aussi produire des certificats pour les SCA, ORA, et autres entités d'extrémité, mais une PCA ne le fait généralement pas.) La PCA produit périodiquement des CRL et des CKL pour son domaine.

$ autorité de gestion de politique (PMA, *policy management authority*)
(I) /PKI/ Personne, rôle, ou organisation au sein d'une PKI qui est responsable de (a) créer ou approuver le contenu des politiques de certificat et des CPS qui sont utilisées dans la PKI, (b) assurer l'administration de ces politiques, et (c) approuver tous les accords de certification croisée ou d'interopérabilité avec les CA externes à la PKI et toutes les transpositions de politique en rapport. La PMA peut aussi être l'accréditeur pour la PKI comme un tout, ou pour certaines de ses composantes ou applications. [DoD9], [PAG] (Voir : autorité d'approbation de politique.)
Exemple : au ministère US de la Défense, une organisation appelée Autorité de gestion de politique est responsable de la PKI du DoD [DoD9].

$ transposition de politique *(policy mapping)*
(I) "Reconnaître que, lorsque une CA dans un domaine certifie une CA dans un autre domaine, une certaine politique de certificat dans le second domaine peut être considérée par l'autorité du premier domaine comme étant équivalente (mais pas nécessairement identique dans tous ses aspects) à une certaine politique de certificat dans le premier domaine." [X509]

$ règle de politique *(policy rule)*
(I) Élément de construction d'une politique de sécurité ; elle (a) définit un ensemble de conditions du système et (b) spécifie un ensemble d'actions du système qui sont à effectuer si ces conditions surviennent. [RFC3198]

$ POP3 APOP
(I) Commande POP3 (mieux décrite comme un type de transaction, ou un sous protocole) par laquelle un client POP3 utilise facultativement un hachage chiffré (fondé sur MD5) pour s'authentifier auprès d'un serveur POP3 et, selon la mise en œuvre de serveur, pour se protéger contre les attaques en répétition. (Voir : CRAM, POP3 AUTH, IMAP4 authentifier.)
Instructions : le serveur comporte un horodatage unique dans son message d'accueil au client. La commande APOP suivante envoyée par le client au serveur contient le nom du client et le résultat de hachage de l'application de MD5 à une chaîne formée à partir de l'horodatage et d'une valeur de secret partagé qui n'est connue que du client et du serveur. APOP a été conçu pour fournir une solution de remplacement à l'utilisation de la paire de commandes POP3 USER et PASS (c'est-à-dire, le mot de passe) dans laquelle le client envoie un mot de passe en clair au serveur.

$ POP3 AUTH
(I) Commande POP3 [RFC1734] (mieux décrite comme un type de transaction, ou un sous protocole) par laquelle un client POP3 utilise facultativement un mécanisme à un serveur POP3 pour authentifier le client auprès du serveur et fournir d'autres services de sécurité. (Voir : POP3 APOP, IMAP4 AUTHENTICATE.)
Instructions : si le serveur accepte la proposition, la commande est suivie de l'exécution d'un protocole d'authentification par mise au défi-réponse et, facultativement, de la négociation d'un mécanisme de protection pour les interactions POP3

suivantes. Les mécanismes de sécurité utilisés par POP3 AUTH sont ceux utilisés par IMAP4.

$ examen de l'accès *(port scan)*
(I) Technique qui envoie les demandes du client à une gamme d'adresses d'accès de service sur un hôte. (Voir : sonde. À comparer à : balayage de ping.)
Instructions : un examen de l'accès peut être utilisé pour une surveillance avant une attaque, dans le but de trouver un accès actif et d'exploiter ensuite une vulnérabilité connue du service de cet accès. Un examen de l'accès peut aussi être utilisé comme attaque d'inondation.

$ autorisation positive *(positive authorization)*
(I) Principe qu'une architecture de sécurité devrait être conçue de telle sorte que l'accès aux ressources du système ne soit permis que lorsque il est explicitement accordé ; c'est-à-dire qu'en l'absence d'une autorisation explicite qui accorde l'accès, l'action par défaut devra être de refuser l'accès. (Voir : autorisation, accès.)

$ interface de système d'exploitation portable pour environnements informatiques (POSIX, *Portable Operating System Interface for Computer Environments*)
(N) Norme [FP151], [I9945] (à l'origine, la norme IEEE P1003.1) qui définit une interface et un environnement de système d'exploitation pour prendre en charge la portabilité d'applications au niveau du code source. Elle est destinée à être utilisée à la fois par les développeurs d'application et par les mises en œuvre de systèmes.
Instructions : P1003.1 prend en charge des fonctions de sécurité comme celles de la plupart des systèmes UNIX, incluant un contrôle d'accès discrétionnaire et des privilèges. Le projet de norme IEEE P1003.6 spécifie des fonctions supplémentaires qui ne sont pas dans la norme de base, incluant (a) le contrôle d'accès discrétionnaire, (b) des mécanismes de chemin d'audit, (c) des mécanismes de privilège, (d) le contrôle d'accès obligatoire, et (e) des mécanismes d'étiquettes d'information.

$ protocole Post Office (POP3, *Post Office Protocol*, version 3)
(I) Norme de protocole Internet (RFC1939) par laquelle une station de travail cliente peut accéder de façon dynamique à une boîte aux lettres sur un hôte serveur pour récupérer les messages électroniques que le serveur a reçus et détient pour le client. (Voir : IMAP4.)
Instructions : POP3 a des mécanismes pour authentifier facultativement un client auprès d'un serveur et pour fournir d'autres services de sécurité. (Voir : POP3 APOP, POP3 AUTH.)

$ pré autorisation *(preauthorization)*
(N) /PKI/ Dispositif de CAW qui permet aux demandes de certification d'être automatiquement validées contre les données fournies à l'avance à la CA par une entité d'autorisation.

$ préséance *(precedence)*
1. (I) /système d'information/ Classement alloué aux événements ou objets de données et qui détermine l'ordre relatif dans lequel ils sont traités.
2. (N) /système de communication/ Désignation allouée à une communication (c'est-à-dire, paquet, message, flux de données, connexion, etc.) par le générateur pour déclarer l'importance ou l'urgence de cette communication par rapport à d'autres communications, et qui indique donc au système de transmission l'ordre relatif de traitement, et indique au receveur l'ordre dans lequel la communication doit être notée. [F1037] (Voir : disponibilité, critique, préemption.)

Exemple : le sous champ "Precedence" du champ "Type de service" de l'en-tête IPv4 prend en charge les désignations suivantes (en ordre d'importance décroissant) : 111 contrôle réseau, 110 contrôle inter réseaux, 101 CRITIC/ECP (Critical Intelligence Communication/Emergency Command Precedence), 100 Flash Override, 011 Flash, 010 Immédiat, 001 Priorité, et 000 Routine. Ces désignations ont été adoptées des systèmes U.S. DoD qui existaient avant l'ARPANET.

$ préemption
(N) Saisie, généralement automatique, de ressources système qui sont utilisées pour desservir une communication de préséance inférieure, afin de servir immédiatement une communication de préséance supérieure. [F1037]

$ Pretty Good Privacy(marque déposée) (PGP(marque déposée))
(O) marque déposée de Network Associates, Inc., se référant à un programme informatique (et aux protocoles qui s'y rapportent) qui utilise la cryptographie pour assurer la sécurité des données pour la messagerie électronique et autres applications sur l'Internet. (À comparer à : DKIM, MOSS, MSP, PEM, S/MIME.)
Instructions : PGP chiffre les messages avec un algorithme symétrique (à l'origine IDEA en mode CFB) distribue les clés symétriques en les chiffrant avec un algorithme asymétrique (à l'origine, RSA) et crée des signatures numériques sur les messages avec un hachage cryptographique et un algorithme de chiffrement asymétrique (à l'origine, MD5 et RSA). Pour établir la possession des clés publiques, PGP dépend d'une "toile de confiance".

$ prévention (I) Voir : définition secondaire sous "sécurité".

$ numéro de compte principal (PAN, *primary account number*)
(O) /SET/ "Numéro alloué qui identifie le producteur de la carte et le détenteur de la carte. Ce numéro de compte est composé d'un numéro d'identification de producteur, d'un identification de numéro de compte individuel, et est accompagné d'une numéro de vérification comme défini par ISO 7812-1985." [SET2], [I7812] (Voir : numéro d'identification bancaire.)
Instructions : le PAN est gravé, codé, ou les deux, sur une carte de crédit à bande magnétique. Le PAN identifie le producteur auquel une transaction sera acheminée et le compte auquel elle s'appliquera sauf si des instructions spécifiques en disposent autrement. L'autorité qui alloue la partie BIN du PAN est *(aux USA)* la American Bankers Association.

$ principal
(I) Identité spécifique revendiquée par un usager lors de l'accès à un système.
Usage : compris généralement comme une identité qui est enregistrée dans le système et est authentifiée par lui ; équivalent à la notion d'identifiant de compte de connexion. Chaque principal est normalement alloué à un seul utilisateur, mais un seul utilisateur peut recevoir (ou tenter d'utiliser) plus d'un principal. Chaque principal peut engendrer un ou plusieurs sujets, mais chaque sujet est associé à seulement un principal. (À comparer à : rôle, sujet, utilisateur.)
(I) /Kerberos/ Instance de client ou serveur identifié de façon univoque (c'est-à-dire, désigné de façon univoque) qui participe à une communication sur le réseau.

$ priorité *(priority)*
(I) /système d'informations/ Préséance de traitement d'un événement ou objet de données, déterminée par l'importance de la sécurité ou d'autres facteurs. (Voir : préséance.)

$ intimité *(privacy)*
1. (I) Droit d'une entité (normalement une personne) agissant en son nom propre, de déterminer le degré auquel elle va interagir avec son environnement, incluant le degré auquel l'entité veut partager ses informations personnelles avec les autres. (Voir : HIPAA, informations personnelles, Privacy Act de 1974. À comparer à : anonymat, confidentialité des données.) [FP041]
2. (O) "Droit des individus de contrôler ou influencer quelles informations relatives à eux-mêmes peuvent être collectées et mémorisées et par qui et à qui ces informations peuvent être divulguées." [I7498-2]
3. (D) Synonyme de "confidentialité des données".

Définition déconseillée : les IDOC NE DEVRAIENT PAS utiliser ce terme comme synonyme de "confidentialité des données" ou de "service de confidentialité des données", qui sont des concepts différents. L'intimité est une raison pour la sécurité plutôt qu'une sorte de sécurité. Par exemple, un système qui mémorise des données personnelles a besoin de protéger les données pour prévenir les dommages, embarras, inconvénients, ou injustices à toute personne sur laquelle des données sont conservées, et de protéger l'intimité de la personne. Pour cette raison, le système peut devoir fournir un service de confidentialité des données.
Instructions : le terme "intimité" est utilisé pour divers concepts séparés mais en rapport, incluant l'intimité corporelle, l'intimité territoriale, la confidentialité des informations personnelles, et la confidentialité des communications. Les IDOC sont supposés s'adresser seulement à la confidentialité des communications, qui dans le présent glossaire est définie principalement par la "confidentialité des données" et secondairement par "l'intégrité des données".
Les IDOC ne sont pas supposés traiter de la confidentialité des informations mais le présent glossaire donne la définition 1 pour ce concept parce que la confidentialité des informations personnelles est souvent confondue avec la confidentialité de communication. Les IDOC ne sont pas supposés traiter de l'intimité corporelle ou de l'intimité territoriale, et ce glossaire ne définit pas ces concepts parce qu'on ne les confondra pas facilement avec la confidentialité de communication.

$ Privacy Act de 1974
(O) Loi fédérale des USA (Section 552a du Titre 5 du Code des États Unis) qui cherche à équilibrer le besoin du gouvernement des USA de conserver des données sur les individus avec le droits des individus à être protégés contre des invasions sans garanties de leur intimité découlant de la collecte, conservation, utilisation et divulgation par les agences fédérales de données personnelles. (Voir : intimité.)
Instructions : en 1974, le Congrès des U.S.A était inquiet des abus potentiels pouvant résulter de l'utilisation croissante par le gouvernement d'ordinateurs pour mémoriser et restituer des données personnelles. Donc, l'acte a quatre objectifs de politique de base :
- Restreindre la divulgation des enregistrements identifiables personnels conservés par les agences fédérales.
- Accorder aux individus des droits d'accès accrus aux enregistrements des agences fédérales conservés sur eux-mêmes.
- Accorder aux individus le droit de faire amender les enregistrements des agences les concernant lorsque ils montrent que l'enregistrement n'est pas précis, pertinent, actuel ou complet.
- Établir un code de "bonnes pratiques d'informations" qui exige des agences qu'elles se conforment aux normes statutaires pour la collecte, la conservation, et la dissémination des enregistrements.

$ messagerie à confidentialité améliorée (PEM, *Privacy Enhanced Mail*)
(I) Protocole Internet pour fournir la confidentialité des données, l'intégrité des données, et l'authentification d'origine des données pour la messagerie électronique. [RFC1421], [RFC1422]. (À comparer à : DKIM, MOSS, MSP, PGP, S/MIME.)
Instructions : PEM chiffre les messages avec un algorithme symétrique (à l'origine, DES en mode CBC), fournit une distribution des clés symétriques en les chiffrant avec un algorithme asymétrique (à l'origine RSA) et signe les messages avec un algorithme de chiffrement asymétrique sur un hachage cryptographique (à l'origine, RSA sur MD2 ou MD5). Pour établir la possession des clés publiques, PEM utilise une hiérarchie de certification, avec des certificats de clé publique X.509 et des CRL X.509 qui sont signés avec un algorithme de chiffrement asymétrique sur un hachage cryptographique (à l'origine, RSA sur MD2).
PEM est conçu comme compatible avec une large gamme de méthodes de gestion de clés, mais est se limite à spécifier des services de sécurité pour les messages de texte et, comme MOSS, n'a pas été largement mis en œuvre dans l'Internet.

$ composant privé *(private component)*
(I) Synonyme de "clé privée".
Utilisation déconseillée : dans la plupart des cas, les IDOC NE DEVRAIENT PAS utiliser ce terme ; à la place, pour éviter la confusion des lecteurs, utiliser "clé privée". Cependant, le terme PEUT être utilisé lorsque on parle d'une paire de clés, par exemple, "une paire de clés a un composant public et un composant privé."

$ extension privée *(private extension)* (I) Voir : définition secondaire sous "extension".

$ clé privée *(private key)*
1. (I) Composante secrète d'une paire de clés de chiffrement utilisées pour la cryptographie asymétrique. (Voir : paire de clés, clé publique, clé secrète.)
2. (O) Dans un système de chiffrement à clé publique, "c'est la clé de la paire de clés d'un utilisateur qui n'est connue que de lui." [X509]

$ interface de ligne privée (PLI, *Private Line Interface*)
(I) Premier système de chiffrement de paquet de bout en bout pour un réseau informatique, développé par BBN qui a commencé en 1975 pour le U.S. DoD, incorporant des équipements COMSEC de caractère militaire fournis par le gouvernement des USA (TSEC/KG-34). [B1822] (À comparer à : IPLI.)

$ privilège *(privilege)*
1a. (I) /contrôle d'accès/ Synonyme de "autorisation". (Voir autorisation. À comparer à : permission.)
1b. (I) /plateforme informatique/ Autorisation d'effectuer une fonction relevant de la sécurité dans le contexte du système d'exploitation d'un ordinateur.

$ infrastructure de gestion des privilèges *(privilege management infrastructure)*
(O) "Infrastructure capable de prendre en charge la gestion des privilèges à l'appui d'un service complet d'autorisations et en relations avec une" PKI ; c'est-à-dire, les processus concernés par les certificats d'attributs. [X509]
Utilisation déconseillée : les IDOC NE DEVRAIENT PAS utiliser ce terme avec cette définition. Elle est vague, et il n'y a pas de consensus sur une définition plus spécifique.

$ processus privilégié *(privileged process)*
(I) Processus informatique qui est autorisé (et donc, de confiance) pour effectuer des fonctions en rapport avec la sécurité que les processus ordinaires ne sont pas autorisés à faire. (Voir : privilège, processus de confiance.)

$ utilisateur privilégié *(privileged user)*
(I) Utilisateur qui a accès au contrôle, à la surveillance ou aux fonctions d'administration d'un système. (Voir : privilège, /UNIX/ sous "racine", super utilisateur, utilisateur.)
Instructions : les utilisateurs privilégiés incluent les types suivants :
- Usagers avec un contrôle complet ou presque complet d'un système, qui sont autorisés à établir et administrer les comptes d'utilisateurs, les identifiants, et les informations d'authentification, ou sont autorisés à allouer ou changer l'accès d'autres usagers aux ressources systèmes.
- Usagers qui sont autorisés à changer les paramètres de contrôle (par exemple, les adresses réseau, les tableaux d'acheminement, les priorités de traitement) sur les routeurs, multiplexeurs, et autres équipements importants.
- Usagers qui sont autorisés à surveiller ou effectuer des recherches de pannes des fonctions de sécurité d'un système, normalement en utilisant des outils et dispositifs spéciaux qui ne sont pas accessibles aux usagers ordinaires.

$ sonder *(probe)*
(I) /verbe/ Technique qui tente d'accéder à un système pour en apprendre quelque chose. (Voir : examen de l'accès.)
Instructions : l'objet d'une sonde peut être offensif, par exemple, tenter de rassembler des informations pour circonvenir les

protections d'un système ; ou défensif, par exemple, vérifier que le système fonctionne correctement.

$ sécurité procédurale *(procedural security)*
(D) Synonyme de "sécurité administrative".
Terme déconseillé : les IDOC NE DEVRAIENT PAS utiliser ce terme comme synonyme de "sécurité administrative". Le terme peut être trompeur parce que tout type de sécurité peut impliquer des procédures, et les procédures peuvent être externes au système ou internes. À la place, utiliser "sécurité administrative", "sécurité de communication", "sécurité informatique", "sécurité des émanations", "sécurité personnelle", "sécurité physique", ou le type spécifique qu'on vise. (Voir : architecture de sécurité.)

$ profil *(profile)* Voir : profil de certificat, profil de protection.

$ protocole de preuve de possession *(proof-of-possession protocol)*
(I) Protocole par lequel une entité système prouve à une autre qu'il possède et contrôle une clé de chiffrement ou une autre information secrète. (Voir : preuve à connaissance zéro.)

$ propriétaire *(proprietary)*
(I) Se réfère aux informations (ou autres propriétés) qui sont possédées par un individu ou organisation et pour lesquelles l'utilisation est restreinte par cette entité.

$ somme de contrôle protégée *(protected checksum)*
(I) Somme de contrôle calculée pour un objet de données par des moyens qui protègent contre les attaques actives qui tenteraient de changer la somme de contrôle pour la faire coïncider aux changements apportés à l'objet de données. (Voir : signature numérique, hachage chiffré, Instructions sous "somme de contrôle".)

$ paquetage protecteur *(protective packaging)*
(N) "Techniques de paquetage pour le matériel COMSEC qui décourage la pénétration, révèle une pénétration qui s'est produite ou a été tentée, ou inhibe le visionnage ou la copie du matériel de chiffrement avant le moment où il est exposé pour utilisation." [C4009] (Voir : altération évidente, résistant à l'altération. À comparer à : QUADRANT.)

$ autorité de protection *(protection authority)*
(I) Voir : définition secondaire sous "option de sécurité du protocole Internet".

$ niveau de protection *(protection level)*
(N) /Gouvernement des USA/ Indication de la confiance qui est nécessaire dans la capacité technique d'un système de mettre en application une politique de sécurité pour la confidentialité. (À comparer à : /opérations d'un système/ sous "mode de fonctionnement".)
Instructions : la politique de sécurité d'une organisation pourrait définir des niveaux de protection fondés sur la comparaison (a) de la sensibilité des informations traitées par un système, (b) des autorisations des usagers qui reçoivent les informations du système sans intervention manuelle ni révision humaine fiable. Pour chaque niveau, la politique pourrait spécifier les caractéristiques et assurances de sécurité qui doivent être incluses dans tout système destiné à fonctionner à ce niveau.
Exemple : soit un ensemble d'objets de données qui sont classifiés à un ou plusieurs niveaux hiérarchiques et dans une ou plusieurs catégories non hiérarchiques, le tableau suivant définit cinq niveaux de protection pour les systèmes qui vont traiter des données. En commençant par PL1 et en évoluant jusqu'à PL5, chaque niveau successif va exiger des caractéristiques et assurances plus fortes pour traiter l'ensemble de données. (Voir : accréditif, approbation formelle d'accès, et besoin de savoir.)

	Plus faibles accréditifs de tous.	Approbation d'accès formelle des usagers	Besoin de savoir des usagers
PL5 Haut	Certains usagers n'ont pas d'accréditif	[pas d'importance]	[pas d'importance]
PL4	Tous sont supprimés pour certaines données	[pas d'importance]	[pas d'importance]
PL3	Tous sont supprimés pour toutes les données	Certains non approuvés pour toutes les données	[pas d'importance]
PL2	Tous sont supprimés	Tous sont approuvés	Certains n'ont pas

```
       | pour toutes les données|pour toutes les données|besoin de connaître|
       |                        |                      | toutes les données|
       +------------------------+----------------------+-------------------+
PL1    | Tous sont supprimés    |  Tous sont approuvés  | Tous ont besoin de|
Bas    | pour toutes les données|pour toutes les données|  connaître tout.  |
       +------------------------+----------------------+-------------------+
```

Chacun de ces niveaux de protection peut être vu comme équivalent à un ou plusieurs modes de fonctionnement de système définis dans ce glossaire :
- PL5 est équivalent au mode de sécurité multi niveau.
- PL4 est équivalent au mode de sécurité multi niveau ou compartimenté, selon les détails des accréditifs de l'usager.
- PL3 est équivalent au mode de sécurité partitionné.
- PL2 est équivalent au mode de sécurité à la hauteur du système.
- PL1 est équivalent au mode de sécurité dédié.

$ profil de protection *(protection profile)*
(N) /Critères communs/ Ensemble indépendant de la mise en œuvre des exigences de sécurité pour une catégorie de cibles d'évaluation qui satisfont des besoins spécifiques du consommateur. [CCIB] Exemple : [IDSAN]. (Voir : cible d'évaluation. À comparer à : profil de certificat, paquetage.)
Instructions : un profil de protection (PP) est une sorte de document utilisé par les consommateurs pour spécifier les exigences fonctionnelles qu'ils attendent d'un produit, et une cible de sécurité (ST) est le document utilisé par les fabricants pour faire des revendications fonctionnelles sur un produit.
Un PP est destiné à être une déclaration réutilisable des besoins de sécurité d'un produit, dont il est connu qu'ils sont utiles et efficaces pour un ensemble de produits de sécurité des technologies de l'information qui pourraient être construits. Un PP contient un ensemble d'exigences de sécurité, de préférence tirées des catalogues des parties 2 et 3 des critères communs, et devrait inclure une EAL. Un PP pourrait être développé par des communautés d'utilisateurs, de développeurs de produits, ou toute autre partie intéressée par la définition d'un ensemble commun d'exigences.

$ anneau de protection *(protection ring)*
(I) Élément d'une hiérarchie de modes de fonctionnement privilégiés d'un système qui donne certains droits d'accès à des processus autorisés à fonctionner dans ce mode. (Voir : Multics.)

$ système de distribution protecteur (PDS, *protective distribution system*)
(N) Système de communication filaire ou de fibre optique utilisé pour transmettre des informations classifiées en clair à travers une zone de moindre classification ou contrôle. [N7003]

$ protocole *(protocol)*
1a. (I) Ensemble de règles (c'est-à-dire, de formats et de procédures) pour mettre en œuvre et contrôler certains types d'association (par exemple, communication) entre des systèmes. Exemple : Protocole Internet.
1b. (I) Série d'étapes ordonnées de calcul et de communication qui sont effectuées par deux entités systèmes ou plus pour réaliser un objectif commun. [A9042]

$ informations de contrôle de protocole (PCI, *protocol control information*)
(N) Voir : définition secondaire sous "unité de données de protocole".

$ unité de données de protocole (PDU, *protocol data unit*)
(N) Paquet de données qui est défini pour des transferts d'homologue à homologue dans une couche de protocole.
Instructions : une PDU consiste en deux sous ensembles disjoints de données : la SDU et la PCI. (Bien que ces termes -- PDU, SDU, et PCI -- trouvent leur origine dans l'OSIRM, ils sont aussi utiles et permis dans le contexte d'IPS.)
- une "unité de données de service" (SDU, *service data unit*) dans un paquet est des données que le protocole transfère entre des entités de protocole homologues au nom des utilisateurs des services de cette couche. Pour les couches 1 à 6, les utilisateurs de la couche sont des entités de protocole homologues à une couche supérieure ; pour la couche 7, les utilisateurs sont des entités d'application en dehors du domaine d'application d'OSIRM.
- les "information de contrôle de protocole" (PCI) dans un paquet sont des données qu'échangent les entités homologues de protocole entre elles-mêmes pour contrôler leur fonctionnement commun dans la couche.

$ suite de protocoles *(protocol suite)*
(I) Collection complémentaire de protocoles de communication utilisés dans un réseau informatique. (Voir : IPS, OSI.)

$ mandataire *(proxy)*
1. (I) Processus informatique qui agit au nom d'un usager ou client.

2. (I) Processus informatique -- souvent utilisé comme, ou au titre d'un, pare-feu -- qui relaie les transactions ou les protocoles d'application entre des systèmes informatiques client et serveur, en apparaissant au client comme serveur et au serveur comme client. (Voir : SOCKS.)

Instructions : dans un pare-feu, un serveur mandataire fonctionne généralement comme un hôte forteresse, qui peut prendre en charge des mandataires pour plusieurs applications et protocoles (par exemple, FTP, HTTP, et TELNET). À la place d'un client dans l'enclave protégée qui connecte directement à un serveur externe, le client interne se connecte au serveur mandataire, qui à son tour se connecte au serveur externe. Le serveur mandataire attend une demande de l'intérieur du pare-feu, transmet la demande au serveur à l'extérieur du pare-feu, obtient la réponse, puis renvoie la réponse au client. Le mandataire peut être transparent au clients, ou il peut avoir besoin de se connecter d'abord au serveur mandataire, et utiliser ensuite cette association pour initier aussi une connexion avec le serveur réel.

Les mandataires sont généralement préférés à SOCKS pour leur capacité à effectuer la mise en mémoire tampon, des connexions de haut niveau, et le contrôle d'accès. Un mandataire peut fournir des services de sécurité au delà de ce qui fait normalement partie du protocole relayé, comme le contrôle d'accès fondé sur l'authentification de l'entité homologue des clients, ou l'authentification d'entité homologue des serveurs lorsque les clients n'ont pas cette capacité. Un mandataire à la couche 7 OSIRM peut aussi fournir un service de sécurité de granularité plus fine qu'un routeur filtrant à la couche 3. Par exemple, un mandataire FTP pourrait permettre des transferts sortants, mais pas entrants dans un réseau protégé.

$ certificat de mandataire *(proxy certificate)*

(I) Certificat de clé publique X.509 déduit d'un certificat d'entité d'extrémité, ou d'un autre certificat de mandataire, afin d'établir des mandataires et de déléguer des autorisations dans le contexte d'un système d'authentification fondé sur PKI. [RRC3820]

Instructions : un certificat de mandataire a les propriétés suivantes :

- Il contient une extension critique qui (a) l'identifie comme certificat de mandataire et (b) peut contenir une contrainte sur la longueur du chemin de certification et des contraintes de politique.
- Il contient le composant public d'une paire de clés qui est distinct de celui associé à tout autre certificat.
- Il est signé par le composant privé d'une paire de clés qui est associée à un certificat d'entité d'extrémité ou à un autre certificat de mandataire.
- Sa clé privée associée ne peut être utilisée que pour signer d'autres certificats de mandataire (et pas des certificats d'entité d'extrémité).
- Son DN "sujet" est déduit de son DN "producteur" et est univoque.
- Son DN "producteur" est le DN "sujet" d'un certificat d'entité d'extrémité ou d'un autre certificat de mandataire.

$ pseudo aléatoire *(pseudorandom)*

(I) Séquence de valeurs qui paraissent être aléatoires (c'est-à-dire, imprévisibles) mais est en fait générée par un algorithme déterministe. (Voir : compression, aléa, générateur de nombres aléatoires.)

$ générateur de nombres pseudo aléatoires (PRNG, *pseudorandom number generator*)

(I) Voir : définition secondaire sous "générateur de nombres aléatoires ".

$ composant public *(public component)*

(I) Synonyme de "clé publique".

Utilisation déconseillée : dans la plupart des cas, les IDOC NE DEVRAIENT PAS utiliser ce terme ; pour éviter la confusion des lecteurs, utiliser "clé privée" à la place. Cependant, le terme PEUT être utilisé quand on parle d'une paire de clés ; par exemple, "une paire de clé a un composant public et un composant privé."

$ clé publique *(clé publique)*

1. (I) Composant qui peut être divulgué publiquement d'une paire de clés de chiffrement utilisée pour le chiffrement asymétrique. (Voir : paire de clé. À comparer à : clé privée.)
2. (O) Dans un système de chiffrement à clé publique, "la clé de la paire de clé d'un utilisateur qui est connue du public." [X509]

$ certificat de clé publique *(clé publique certificate)*

1. (I) Certificat numérique qui lie l'identifiant d'une entité système à une valeur de clé publique, et éventuellement à des éléments de données secondaires supplémentaires ; c'est-à-dire, une structure de données signée numériquement qui atteste de la possession d'une clé publique. (Voir : certificat de clé publique X.509.)
2. (O) "Clé publique d'un utilisateur, avec d'autres informations, rendue infalsifiable par le chiffrement avec la clé privée de l'autorité de certification qui l'a produite." [X509]

Instructions : la signature numérique sur un certificat de clé publique est infalsifiable. Donc, le certificat peut être publié, comme en le postant dans un répertoire, sans que celui-ci ait à protéger l'intégrité des données du certificat.

$ chiffrement à clé publique *(public-key cryptography)* (I) Synonyme de "chiffrement asymétrique".

$ normes de chiffrement à clé publique (PKCS, *Public-Key Cryptography Standards*)
(N) Série de spécifications publiées par RSA Laboratories pour des structures et algorithmes de données utilisés dans les applications de base du chiffrement asymétrique. [PKCS] (Voir : PKCS n° 5 à PKCS n° 11.)
Instructions : les PKCS ont commencé en 1991 en coopération avec l'industrie et l'Université, incluant à l'origine Apple, Digital, Lotus, Microsoft, Northern Telecom, Sun, et le MIT. Aujourd'hui, les spécifications sont largement utilisées, mais elles ne sont pas sanctionnées par une organisation de normalisation officielle, comme l'ANSI, l'UIT-T, ou l'IETF. RSA Laboratories conserve seul l'autorité de décision sur les PKCS.

$ secret de clé publique vers l'avant (PFS, *public-key forward secrecy*)
(I) Pour un protocole d'accord de clé fondé sur le chiffrement asymétrique, c'est la propriété qu'une clé de session déduite d'un ensemble de clés publiques et privées de long terme ne soit pas compromise si une des clés privées est compromise à l'avenir. (Voir : Note d'usage et le reste de la discussion sous "secret parfait vers l'avant".)

$ Kerberos à clé publique *(public-key Kerberos)* (I) Voir : Instructions sous "Kerberos", PKINIT.

$ infrastructure de clé publique (PKI, *public-key infrastructure*)
1. (I) Système de CA (et facultativement, de RA et autres serveurs et agents de soutien) qui effectue un ensemble de fonctions de gestion de certificat, de gestion d'archive, de gestion de clé , et de gestion de jetons pour une communauté d'utilisateurs dans une application de chiffrement asymétrique. (Voir : PKI hiérarchique, maillage de PKI, infrastructure de gestion de sécurité, PKI à fichier de confiance.)
2. (I) /PKIX/ Ensemble des matériels, logiciels, personnes, politiques, et procédures nécessaires pour créer, gérer, mémoriser, distribuer, et révoquer des certificats numériques fondés sur le chiffrement asymétrique.

Instructions : les fonctions centrales de PKI sont (a) d'enregistrer les utilisateurs et produire leurs certificats de clé publique, (b) de révoquer les certificats lorsque nécessaire, et (c) archiver les données nécessaires pour valider les certificats ultérieurement. Les paires de clés pour la confidentialité des données peuvent être générées (et peut-être garanties) par les CA ou les RA, mais exiger d'un client PKI qu'il génère sa propre paire de clés de signature numérique aide à maintenir l'intégrité système du système cryptographique, parce qu'alors c'est toujours le client seul qui possède la clé privée qu'il utilise. Aussi, une autorité peut être établie pour approuver ou coordonner les CPS, qui sont les politiques de sécurité sous lesquelles fonctionnent les composants d'une PKI.
Un certain nombre d'autres serveurs et agents peuvent prendre en charge la PKI centrale, et les clients de PKI peuvent obtenir d'eux des services, comme de validation de certificats. La gamme complète de ces services n'est pas encore parfaitement bien comprise et évolue, mais les rôles de support peuvent inclure celui d'agent d'archive, d'agent de livraison certifié, d'agent de confirmation, de notaire numérique, de répertoire, d'agent de notaire de clé, d'agent de génération de clé, d'agent de désignation qui s'assure que producteurs et sujets ont des identifiants uniques au sein du répertoire PKI, d'agent d'allocation de ticket, d'agent d'horodatage, et d'agent de validation.

$ purger *(purge)*
1. (I) Synonyme de "écraser".
2. (O) /Gouvernement des USA/ Utiliser le dégaussage ou d'autres méthodes pour rendre inutilisables des données mémorisées par un moyen magnétique et irrécupérables par quelque moyen que ce soit, y compris des méthodes de laboratoire. [C4009] (À comparer à : /Gouvernement des USA/ écraser.)

$ QUADRANT
(O) /Gouvernement des USA/ Nom abrégé d'une technologie et de méthodes qui protègent les équipements cryptographiques en les rendant résistants aux altérations. [C4009] (À comparer à : paquetage protecteur, TEMPEST.)
Instructions : les équipements ne peuvent pas être rendus complètement à l'épreuve de l'altération, mais ils peuvent être rendus résistants à l'altération ou l'altération peut être rendue évidente.

$ certificat qualifié *(qualified certificate)*
(I) Certificat de clé publique qui a pour principal objet d'identifier une personne avec un haut degré d'assurance, où le certificat satisfait certaines exigences de qualification définies par le cadre légal applicable, comme la Directive européenne sur les signatures électroniques . [RFC3739]

$ mode rapide *(quick mode)* (I) Voir : /IKE/ sous "mode".

$ domaines d'autorité d'enregistrement *(RA domains)*
(I) Caractéristique d'une CAW qui permet à une CA de diviser la responsabilité des demandes de certificat entre plusieurs RA.
Instructions : cette capacité peut être utilisée pour restreindre l'accès aux données d'autorisation privées qui sont fournies avec une demande de certificat, et de partager la responsabilité de réviser et approuver les demandes de certificat dans des

environnements à gros volumes. Les domaines de RA peuvent séparer les demandes de certificat selon un attribut du sujet du certificat, comme une unité organisationnelle.

$ séries arc en ciel *(Rainbow Series)*
(O) /COMPUSEC/ Ensemble de plus de 30 documents techniques et politiques avec des couvertures de couleur, produit par le NCSC, qui expose en détails la TCSEC et fournit des lignes directrices pour satisfaire et appliquer les critères. (Voir : Livre Vert, Livre Orange, Livre Rouge, Livre Jaune.)

$ aléatoire *(random)*
(I) Par essence, "aléatoire" signifie "imprévisible". [SP22], [Knut], [RFC4086] (Voir : clé de chiffrement, pseudo aléatoire.)
- "Séquence aléatoire" : séquence dans laquelle chaque valeur successive est obtenue simplement au hasard et ne dépend pas de la valeur précédente de la séquence. Dans une séquence aléatoire de bits, chaque bit est imprévisible; c'est-à-dire, (a) la probabilité que chaque bit soit "0" ou "1" est 1/2, et (b) la valeur de chaque bit est indépendante de celle de tout autre bit de la séquence.
- "valeur aléatoire" : valeur individuelle qui est imprévisible ; c'est-à-dire, chaque valeur de la population totale des possibilités a une probabilité égale d'être choisie.

$ générateur de nombres aléatoires *(random number generator)*
(I) Processus qui est invoqué pour générer une séquence aléatoire de valeurs (généralement une séquence de bits) ou une valeur aléatoire individuelle.
Instructions : il y a deux types de base de générateurs. [SP22]
- "(Vrai) générateur de nombres aléatoires" : il utilise une ou plusieurs sources de bits non déterministes (par exemple, le bruit d'un circuit électrique, le rythme de processus humains tels que la frappe de touches du clavier ou les mouvements de la souris, les effets quantiques d'un semi-conducteur, et d'autres phénomènes physiques) et une fonction de traitement qui formate les bits, et il sort une séquence de valeurs qui sont imprévisibles et uniformément réparties.
- "générateur de nombres pseudo aléatoires (PRNG, *Pseudorandom number generator*)" : il utilise un processus de calcul déterministe (généralement mis en œuvre par un logiciel) qui a une ou plusieurs entrées appelées "germes", et il sort une séquence de valeurs qui paraissent aléatoires selon des essais statistiques spécifiés.

$ RBAC (N) Voir : contrôle d'accès fondé sur le rôle *(role-based access control)* contrôle d'accès fondé sur la règle *(rule-based access control)*.
Utilisation déconseillée : les IDOC qui utilisent ce terme DEVRAIENT en donner une définition parce que l'abréviation est ambiguë.

$ RC2, RC4, RC6 (N) Voir : chiffrement Rivest n° 2, n° 4, n° 6.

$ lecture *(read)*
(I) /modèle de sécurité/ Fonctionnement de système qui cause un flux d'informations d'un objet à un sujet. (Voir : mode d'accès. À comparer à : écriture.)

$ royaume *(realm)*
(I) /Kerberos/ Domaine consistant en un ensemble de clients kerbérisés, de serveurs d'application kerbérisés, et d'un ou plusieurs serveurs d'authentification Kerberos et de serveurs d'allocation de tickets qui prennent en charge les clients et applications, tous fonctionnant sous la même politique de sécurité. (Voir : domaine.)

$ récupération *(recovery)*
1. (I) /cryptographie/ Processus d'acquisition ou d'obtention de données cryptographiques ou de texte en clair par l'analyse cryptographique. (Voir : récupération de clé, récupération de données,)

2a. (I) /intégrité de système/ Processus de restauration d'un état sûr dans un système après une défaillance accidentelle ou une attaque réussie. (Voir : définition secondaire sous "sécurité", intégrité de système.)

2b. (I) /intégrité de système / Processus de restauration des bases et du fonctionnement d'un système d'information suite à des dommages ou à la destruction. (Voir : plan de contingence.)

$ ROUGE *(RED)*
1. (N) Désignation de données qui consistent seulement en texte en clair, et d'éléments et facilités d'équipement de système d'information qui traitent le texte en clair. Exemple : "clé RED". (Voir : BCR, changement de couleur, séparation ROUGE/NOIR. À comparer à : NOIR.)

Dérivation : tiré de la pratique de marquage des équipements avec des couleurs pour prévenir les erreurs opérationnelles.

2. (O) /Gouvernement des USA/ Désignation appliquée aux systèmes d'information, et aux zones, circuits, composants, et équipements associés, "dans lesquels des informations de sécurité nationale non chiffrées sont traitées ." [C4009]

$ séparation NOIR/ROUGE *(RED/BLACK separation)*
(N) Concept architectural pour les systèmes cryptographiques qui séparent strictement les parties d'un système qui traite le texte en clair (c'est-à-dire, les informations ROUGES) des parties qui traitent le texte chiffré (c'est-à-dire, les informations NOIRES). (Voir : NOIR, ROUGE.)

$ Livre Rouge *(Red Book)*
(D) /argot/ Synonyme de "interprétation du réseau de confiance des critères d'évaluation d'un système informatique de confiance" *(Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria)* [NCS05].
Terme déconseillé : les IDOC NE DEVRAIENT PAS utiliser ce terme. À la place, utiliser le nom approprié complet du document ou, dans les références suivantes, une abréviation plus conventionnelle, par exemple, TNI-TCSEC. (Voir : TCSEC, Série Arc-en-ciel, Utilisation déconseillée sous "Livre Vert".)

$ clé ROUGE *(RED key)*
(N) Clé de texte en clair, qui est utilisable dans sa forme présente (c'est-à-dire, il n'est pas besoin de la déchiffrer avant de l'utiliser). (Voir : ROUGE. À comparer à : clé NOIRE.)

$ surveillant de référence *(reference monitor)*
(I) "Concept de contrôle d'accès qui se réfère à une machine abstraite qui s'interpose sur tous les accès aux objets par les sujets." [NCS04] (Voir : noyau de sécurité.)
Instructions : ce concept a été décrit dans le rapport Anderson. Un surveillant de référence devrait être (a) complet (c'est-à-dire qu'il s'interpose sur tous les accès), (b) isolé (c'est-à-dire qu'il ne peut pas être modifié par d'autres entités système) et (c) vérifiable (c'est-à-dire, assez petit pour être soumis à des analyses et des essais pour s'assurer qu'il est correct).

$ attaque en reflet *(reflection attack)*
(I) Attaque dans laquelle une transmission de données valide est rejouée à son générateur par un attaquant qui intercepte la transmission d'origine. (À comparer à : attaque indirecte, attaque en répétition.)

$ attaque du réflecteur *(reflector attack)*
(D) Synonyme de "attaque indirecte".
Terme déconseillé : les IDOC NE DEVRAIENT PAS utiliser ce terme ; cela pourrait être confondu avec "attaque en reflet", qui est un concept différent.

$ utilisateur enregistré *(registered user)*
(I) Entité système qui est autorisée à recevoir les produits et services d'un système ou autrement à accéder aux ressources système. (Voir : enregistrement, usager.)

$ enregistrement *(registration)*
1. (I) /système d'information/ Processus système qui (a) initialise une identité (d'une entité système) dans le système, (b) établit un identifiant pour cette identité, (c) peut associer des informations d'authentification à cet identifiant, et (d) peut produire un accréditif d'identifiant (selon le type de mécanisme d'authentification utilisé). (Voir : informations d'authentification, accréditif, identifiant, identité, preuve d'identité.)
2. (I) /PKI/ Acte ou processus administratif par lequel le nom et les autres attributs d'une entité sont établis pour la première fois chez une CA, avant que la CA ne produise un certificat numérique qui a le nom de l'entité comme sujet. (Voir : autorité d'enregistrement.)

Instructions : l'enregistrement peut être accompli soit directement par la CA, soit indirectement, par une RA séparée. Une entité est présentée à la CA ou RA, et l'autorité enregistre le ou les noms revendiqués pour l'entité ou alloue le ou les noms à l'entité. L'autorité détermine et enregistre aussi d'autres attributs de l'entité qui sont à lier à un certificat (comme une clé publique ou des autorisations) ou conservés dans la base de données de l'autorité (comme une adresse postale et un numéro de téléphone). L'autorité est responsable, éventuellement assistée par une RA, de la vérification de l'identité de l'entité et de vérifier les autres attributs, conformément à la CPS de la CA.
Parmi les questions d'enregistrement que peut traiter une CPS figurent [RFC3647] :
- comment sont vérifiés une identité revendiquée et les autres attributs,
- comment sont vérifiées l'affiliation ou la représentation à une organisation,
- quelles formes de noms sont permises, comme DN X.500, nom de domaine, ou adresse IP,
- si les noms doivent être significatifs ou uniques, et dans quel domaine,
- comment sont résolus les conflits de noms, y compris le rôle des marques commerciales,
- comment sont produits les certificats aux entités qui ne sont pas des personnes,
- si une personne doit paraître devant la CA ou RA, ou si à la place elle peut être représentée par un agent,
- si et comment une entité prouve la possession de la clé privée qui correspond à la clé publique.

$ autorité d'enregistrement (RA, *registration authority*)

1. (I) Entité PKI facultative (séparée des CA) qui ne signe ni certificats numériques ni CRL mais est chargée d'enregistrer et de vérifier certaines des informations (en particulier, les identités des sujets) nécessaires à une CA pour produire les certificats et les CRL et d'effectuer d'autres fonctions de gestion de certificat. (Voir : ORA, enregistrement.)
2. (I) /PKIX/ Composant PKI facultatif, distinct des CA. Les fonctions effectuées par la RA vont varier selon le cas, mais peuvent inclure l'authentification de l'identité et l'allocation de nom, la génération de clé et l'archivage des paires de clés, la distribution des jetons, et le rapport des révocations. [RFC4210]

Instructions : parfois, une CA peut effectuer des fonctions de gestion de certificat pour tous les utilisateurs finaux dont la CA signe les certificats. D'autres fois, comme dans une communauté vaste ou dispersée géographiquement, il peut être nécessaire ou souhaitable de décharger une CA de fonctions secondaires et de les déléguer à un assistant, tandis que la CA conserve les fonctions principales (de signature des certificats et des CRL). Les tâches qui sont déléguées à une RA par une CA peuvent inclure l'authentification personnelle, l'allocation de noms, la distribution des jetons, les rapports de révocation, la génération des clés , et l'archivage.

Une RA est une entité PKI facultative, séparée de la CA, à qui sont allouées des fonctions secondaires. Les tâches allouées aux RA varient selon les cas mais peuvent inclure de :

- vérifier l'identité d'un sujet, c'est-à-dire, d'effectuer des fonctions d'authentification personnelle,
- allouer un nom à un sujet, (voir : nom distinctif)
- vérifier qu'un sujet est habilité à avoir les attributs demandés pour un certificat,
- vérifier qu'un sujet possède la clé privée qui correspond à la clé publique demandée pour un certificat,
- effectuer des fonctions au delà du simple enregistrement, comme de générer des paires de clés, de distribuer des jetons, de traiter les rapports de révocation, et d'archiver les données. (De telles fonctions peuvent être allouées à un composant PKI qui est séparé aussi bien de la CA que de la RA.)

3. (O) /SET/ "Organisation tierce indépendante qui traite les applications de carte de payement pour plusieurs marques de cartes de payement et transmet les applications aux institutions financières appropriées." [SET2]

$ rétrograder *(regrade)*

(I) Changer délibérément le niveau de sécurité (en particulier le niveau de classification hiérarchique) des informations d'une façon autorisée. (Voir : dégrader, mettre à niveau.)

$ changer de clé *(rekey)*

(I) Changer la valeur d'une clé de chiffrement qui est utilisée dans une application d'un système cryptographique. (Voir : changement de clé de certificat.)

Instructions : le changement de clés est requis à la fin d'une cryptopériode ou de la durée de vie d'une clé.

$ fiabilité *(reliability)*

(I) Capacité d'un système à effectuer une fonction requise dans des conditions établies pendant une durée spécifiée. (À comparer à : disponibilité, capacité de survie.)

$ révision fiable par l'homme *(reliable human review)*

(I) Tout processus ou procédure manuel, automatique, ou hybride qui assure qu'un humain qui examine un objet numérique, comme un texte ou une image, pour déterminer si il peut être permis à l'objet, conformément à une politique de sécurité, d'être transféré à travers une interface contrôlée. (Voir : garde.)

$ consommateur d'assertion *(relying party)*

(I) Synonyme de "utilisateur de certificat".

Usage : utilisé dans un contexte juridique pour signifier un receveur de certificat qui agit en confiance sur ce certificat. (Voir : lignes directrices ABA.)

$ rémanence *(remanence)*

(I) Informations résiduelles qui peuvent être récupérées d'un support de mémorisation après son effacement. (Voir : éliminer, rémanence magnétique, purge.)

$ service d'accès commuté entrant d'utilisateur distant (RADIUS, *Remote Authentication Dial-In User Service*)

(I) Protocole Internet [RFC2865] pour porter des informations d'authentification d'utilisateur appelant et des informations de configuration entre un serveur d'authentification centralisé (le serveur RADIUS) et un serveur d'accès réseau (le client RADIUS) qui ont besoin d'authentifier les utilisateurs de leurs points d'accès réseau. (Voir : TACACS.)

L'utilisateur présente ses informations d'authentification et éventuellement d'autres informations au client RADIUS (par exemple, des informations de santé concernant l'appareil utilisateur).

Instructions : un usager présente des informations d'authentification et éventuellement d'autres informations au client RADIUS, et le client passe ces informations au serveur RADIUS. Le serveur authentifie le client à l'aide d'une valeur de secret partagé et vérifie les informations présentées, et retourne ensuite au client toutes les informations d'autorisation et de

configuration nécessaires au client pour servir l'usager.

$ renouvellement *(renew)* Voir : renouvellement de certificat.

$ réarrangement *(reordering)* (I) /paquet/ Voir : définition secondaire sous "service d'intégrité de flux".

$ attaque en répétition *(replay attack)*
(I) Attaque dans laquelle une transmission de données valide est répétée par malveillance ou fraude, soit par l'origine; soit par un tiers qui intercepte les données et les retransmet, éventuellement au titre d'une attaque de mascarade. (Voir : écoute active, frais, vivant, nom occasionnel. À comparer à : attaque indirecte, attaque en reflet.)

$ dépôt *(repository)*
1. (I) Système pour mémoriser et distribuer des certificats numériques et les informations qui s'y rapportent (y compris des CRL, des CPS, et des politiques de certificat) aux utilisateurs de certificat. (À comparer à : archive, répertoire.)
2. (O) "Système de confiance pour mémoriser et restituer des certificats ou autres informations relevant des certificats." [DSG]

Instructions : un certificat est publié pour ceux qui pourraient en avoir besoin en le mettant dans un dépôt. Le dépôt est normalement accessible au public sur un serveur en ligne. Dans la FPKI, par exemple, le dépôt attendu est un répertoire qui utilise LDAP, mais peut aussi être un annuaire X.500 qui utilise DAP, ou un serveur HTTP, ou un serveur FTP qui permet une connexion anonyme.

$ répudiation *(repudiation)*
1. (I) Refus par une entité système qui a été impliquée dans une association (en particulier une association de communication qui transfère des données) d'avoir participé à la relation. (Voir : traçabilité, service de non répudiation.)
2. (I) Type d'action de menace par laquelle une entité en trompe une autre en niant faussement la responsabilité d'un acte. (Voir : tromperie.)

Usage : ce type d'action de menace inclut les sous types suivants :
- faux déni d'origine : action par laquelle l'origine nie la responsabilité de l'envoi des données,
- faux déni de réception : action par laquelle un receveur nie avoir reçu et traité les données.

3. (O) /OSIRM/ "Déni par une des entités impliquées dans une communication d'avoir participé à tout ou partie de la communication." [I7498-2]

$ appel à commentaires (RFC, *Request for Comment*)
1. (I) Un des documents de la série archivée qui est le canal officiel des IDOC et autres publications de l'équipe de direction de l'ingénierie de l'Internet (IESG) du Bureau d'architecture de l'Internet, et de la communauté de l'Internet en général. (RFC 2026, 2223) (Voir : norme Internet.)
2. (D) Synonyme utilisé (à tort) de façon courante pour un document sur la voie de la normalisation Internet, c'est-à-dire, une norme de l'Internet, un projet de norme, ou une proposition de norme. (Voir : norme Internet.)

Définition déconseillée : les IDOC NE DEVRAIENT PAS utiliser ce terme avec la définition 2 parce que de nombreux autres types de documents sont aussi publiés comme RFC.

$ risque résiduel *(residual risk)*
(I) Portion d'un risque ou ensemble de risques originels qui reste après que des contre-mesures ont été appliquées. (À comparer à : risque acceptable, analyse de risque.)

$ restaurer *(restore)* Voir : restauration de carte.

$ ingénierie inverse *(reverse engineering)*
(I) /action de menace/ Voir : définition secondaire sous "intrusion".

$ révocation *(revocation)* Voir : révocation de certificat.

$ date de révocation *(revocation date)*
(N) /X.509/ Dans une entrée de CRL, c'est un champ date heure qui déclare quand est survenue la révocation du certificat, c'est-à-dire, quand la CA a déclaré que le certificat numérique est invalide. (Voir : date d'invalidité.)
Instructions : la date de révocation ne peut pas résoudre certaines disputes parce que, dans le pire des cas, toutes les signatures faites durant la période de validité du certificat peuvent avoir été considérées comme invalides. Cependant, il peut être souhaitable de traiter une signature numérique comme valide même si la clé privée utilisée pour signer était compromise après la signature. Si on en sait plus sur le moment où la compromission est réellement intervenue, une seconde date et heure, une "date d'invalidité", peut être incluse dans une extension de l'entrée de la CRL.

$ liste de révocation *(revocation list)* Voir : liste de révocation de certificats.

$ révoquer *(revoke)* (I) Voir : révocation de certificat.

$ Rijndael
(N) Chiffrement symétrique de bloc qui a été conçu par Joan Daemen et Vincent Rijmen comme candidat pour l'AES, et qui a gagné cette compétition. [Daem] (Voir : Norme de chiffrement avancé.)

$ risque *(risk)*
1. (I) Espérance de perte exprimée comme la probabilité qu'une certaine menace va exploiter une certaine vulnérabilité avec un certain résultat dommageable. (Voir : risque résiduel.)
2. (O) /SET/ "Possibilité de perte à cause d'une ou plusieurs menaces pour des informations (à ne pas confondre avec le risque financier ou commercial)." [SET2]

Instructions : il y a quatre façons de base de traiter un risque [SP30] :
- "évitement de risque" : éliminer le risque soit en contrant la menace soit en supprimant la faiblesse. (À comparer à : "évitement" sous "sécurité".)
- "transfert de risque" : faire glisser le risque sur un autre système ou entité, par exemple, en s'assurant pour compenser la perte potentielle.
- "limitation de risque" : limiter le risque en mettant en œuvre des contrôles qui minimisent les pertes résultantes.
- "hypothèse de risque" : accepter un potentiel de pertes et continuer de faire fonctionner le système.

$ analyse de risque *(risk analysis)*
(I) Processus d'évaluation qui (a) identifie systématiquement les ressources systèmes valables et les menaces qui pèsent sur ces ressources, (b) quantifie les expositions aux pertes (c'est-à-dire, le potentiel de pertes) sur la base des fréquences estimées et des coûts de survenance, et (c) (facultativement) recommande comment allouer les ressources disponibles aux contre-mesures afin de minimiser l'exposition totale. (Voir : gestion de risque, analyse de cas d'affaires. À comparer à : analyse de menace.)
Instructions : usuellement, il est financièrement et techniquement infaisable d'éviter ou de transférer tous les risques (voir : "premier corollaire" de la deuxième loi sous "Lois de Courtney") et des risques résiduels vont rester, même après que toutes les contre-mesures disponibles ont été déployées (voir : "second corollaire" de la deuxième loi sous "Lois de Courtney"). Donc, une analyse de risque fait normalement la liste des risques dans l'ordre des coûts et de criticité, déterminant ainsi où les contre-mesures devraient d'abord être appliquées. [FP031], [RFC2196]
Dans certains contextes, il est infaisable ou inenvisageable de tenter une analyse de risques complète ou quantitative parce que les données, le temps et l'expertise nécessaires ne sont pas disponibles. À la place, les réponses de base aux questions sur les menaces et les risques peuvent être déjà précisées dans les politiques de sécurité institutionnelles. Par exemple, les politiques de l'U.S. DoD pour la confidentialité des données "ne classent pas explicitement la gamme des menaces attendues" mais à la place "reflètent une approche opérationnelle ...en déclarant les contrôles de gestion particuliers qui doivent être utilisés pour assurer la [confidentialité] ... Donc, elles évitent de faire la liste des menaces, ce qui représenterait un risque sévère en soi, et évitent le risque d'une mauvaise conception de la sécurité implicite en prenant une approche fraîche de chaque nouveau problème". [NRC91]

$ hypothèse de risque *(risk assumption)* (I) Voir : définition secondaire sous "risque".

$ évitement de risque *(risk avoidance)* (I) Voir : définition secondaire sous "risque".

$ limitation de risque *(risk limitation)* (I) Voir : définition secondaire sous "risque".

$ gestion de risque *(risk management)*
1. (I) Processus d'identification, de mesure, et de contrôle (c'est-à-dire, d'atténuation) des risques dans les systèmes d'information afin de réduire les risques d'un niveau comparable à la valeur des biens protégés. (Voir : analyse de risque.)
2. (I) Processus de contrôle des événements incertains qui peuvent affecter les ressources du système d'information.
3. (O) "Processus total d'identification, de contrôle, et d'atténuation des risques relatifs au système d'informations. Il inclut l'évaluation des risques, l'analyse coûts avantages, et le choix, la mise en œuvre, l'essai, et l'évaluation de la sécurité des sauvegardes. Cette révision complète de la sécurité du système prend en compte aussi bien l'efficacité que l'efficience, incluant l'impact sur la mission et les contraintes dues à la politique, aux règlements, et aux lois." [SP30]

$ transfert de risque *(risk transference)* (I) Voir : définition secondaire sous "risque".

$ chiffrement Rivest n° 2 (RC2, *Rivest Cipher #2*)
(N) Chiffrement de bloc propriétaire, à longueur de clé variable, inventé par Ron Rivest pour RSA Data Security, Inc.

$ chiffrement Rivest n° 4 (RC4, *Rivest Cipher #4*)
(N) Chiffrement de flux propriétaire, à longueur de clef variable, inventé par Ron Rivest pour RSA Data Security, Inc.

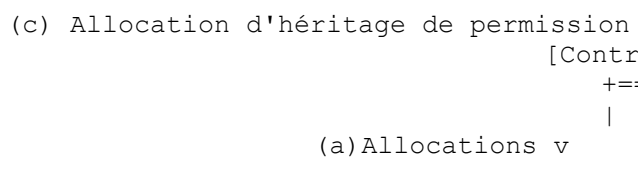
$ chiffrement Rivest n° 6 (RC6, *Rivest Cipher #6*)
(N) Chiffrement de bloc symétrique avec une clé de 128 bits ou plus, développé par Ron Rivest pour RSA Data Security, Inc. comme candidat pour l'AES.

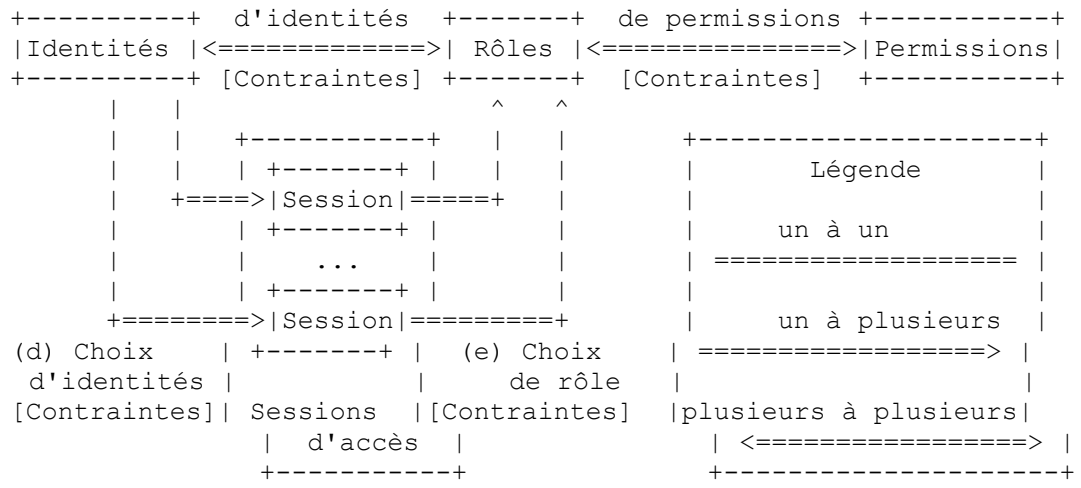
$ Rivest-Shamir-Adleman (RSA)
(N) Algorithme de chiffrement asymétrique, inventé en 1977 par Ron Rivest, Adi Shamir, et Leonard Adleman [RSA78].
Instructions : RSA utilise l'exponentiation modulo le produit de deux grands nombre premiers. La difficulté de casser RSA est estimée être équivalente à la difficulté de factoriser des entiers qui sont le produit de deux grands nombres premiers de taille approximativement égale.
Pour créer une paire de clés RSA, on choisit au hasard deux grands nombres premiers, p et q, et on calcule le module, n = pq. On choisit au hasard le nombre e, l'exposant public, qui est inférieur à n et premier par rapport à (p-1)(q-1). On choisit un autre nombre d, l'exposant privé, tel que ed-1 soit un diviseur entier de (p-1)(q-1). La clé publique est l'ensemble des nombres (n,e), et la clé privée est l'ensemble (n,d).
On suppose qu'il est difficile de calculer la clé privée (n,d) à partir de la clé publique (n,e). Cependant, si n peut être mis en facteurs par p et q, la clé privée d peut alors être facilement calculée. Donc, la sécurité RSA dépend de l'hypothèse qu'il est difficile de factoriser un nombre qui est le produit de deux grands nombres premiers. (Bien sûr, p et q sont traités au titre de la clé privée, ou autrement, ils sont détruits après le calcul de n.)
Pour le chiffrement d'un message, m, à envoyer à Bob, Alice utilise la clé publique (n,e) de Bob pour calculer m**e (mod n) = c. Elle envoie c à Bob. Bob calcule c**d (mod n) = m. Seul Bob connait d, de sorte que seul Bob peut calculer c**d (mod n) pour retrouver m.
Pour assurer l'authentification d'origine des données d'un message, m, à envoyer à Bob, Alice calcule m**d (mod n) = s, où (d,n) est la clé privée d'Alice. Elle envoie m et s à Bob. Pour retrouver le message que seule Alice pourrait avoir envoyé, Bob calcule s**e (mod n) = m, où (e,n) est la clé publique d'Alice.
Pour assurer l'intégrité des données en plus de l'authentification d'origine des données, il faut des étapes de calcul supplémentaires dans lesquelles Alice et Bob utilisent une fonction de hachage cryptographique h (voir : signature numérique). Alice calcule la valeur du hachage h(m) = v, puis chiffre v avec sa clé privée pour obtenir s. Elle envoie m et s. Bob reçoit m' et s', dont l'un et l'autre peuvent avoir été changés à partir des m et s de l'envoi d'Alice. Pour vérifier cela, il déchiffre s' avec la clé publique d'Alice pour obtenir v'. Il calcule alors h(m') = v''. Si v' égal v'', Bob est assuré que m' est le même m qu'envoyé par Alice.

$ robustesse *(robustness)* (N) Voir : niveau de robustesse.

$ rôle *(role)*
1. (I) Fonction de travail ou position d'emploi à laquelle des gens ou autres entités système peuvent être affectés dans un système. (Voir : contrôle d'accès fondé sur le rôle. À comparer à : service, billet, principal, usager.)
2. (O) /Critères communs/ Ensemble prédéfini de règles établissant les interactions permises entre un usager et le TOE.

$ contrôle d'accès fondé sur le rôle *(role-based access control)*
(I) Forme de contrôle d'accès fondé sur l'identité par laquelle les entités système qui sont identifiées et contrôlées sont dans une position fonctionnelle dans une organisation ou procès. [Sand] (Voir : autorisation, contrainte, identité, principal, rôle.)
Instructions : les administrateurs accordent comme nécessaire des permissions aux rôles pour effectuer leurs fonctions dans le système. Les administrateurs allouent séparément les identités d'utilisateur aux rôles. Lorsque un utilisateur accède au système sous une identité (pour laquelle l'usager a été enregistré) et initie une session en utilisant un rôle (auquel l'usager a été affecté) les permissions qui ont été accordées au rôle sont disponibles pour être exercées par l'usager.
Le diagramme suivant montre que le contrôle d'accès fondé sur le rôle implique cinq relations différentes : (a) les administrateurs allouent des identités aux rôles, (b) les administrateurs allouent des permissions aux rôles, (c) les administrateurs allouent des rôles aux rôles, (d) les usagers choisissent des identités dans les sessions, et (e) les usagers choisissent des rôles dans les sessions. Les politiques de sécurité peuvent définir des contraintes sur ces allocations et sélections.





$ certificat de rôle *(role certificate)*
(I) Certificat d'organisation qui est produit à une entité système qui est membre de l'ensemble d'utilisateurs dont les identités ont été allouées au même rôle. (Voir : contrôle d'accès fondé sur le rôle.)

$ racine, CA racine *(root, root CA)*
1. (I) /PKI/ CA qui est directement de confiance pour une entité d'extrémité. (Voir : ancre de confiance, CA de confiance.)
2. (I) /PKI hiérarchique/ CA qui est celle de plus haut niveau (la plus de confiance) dans une hiérarchie de certification, c'est-à-dire, l'autorité sur la clé publique de laquelle tous les utilisateurs de certificat fondent leur validation de certificats, de CRL, de chemins de certification, et des autres constructions. (Voir : CA supérieure.)

Instructions : la CA racine dans une hiérarchie de certification produit des certificats de clé publique à une ou plusieurs CA supplémentaires qui forment le second plus haut niveau. Chacune de ces CA peut produire des certificats à plus de CA au troisième niveau le plus élevé, et ainsi de suite. Pour initialiser le fonctionnement d'une PKI hiérarchique, la clé publique initiale de la racine est distribuée de façon sûre à tous les utilisateurs de certificat d'une façon qui ne dépend pas des relations de certification de la PKI, c'est-à-dire, par une procédure hors bande. La clé publique de la racine peut être distribuée simplement comme une valeur numérique, mais normalement, elle est distribuée dans un certificat auto signé dans lequel la racine est le sujet. Le certificat de la racine est signé par la racine elle-même parce qu'il n'y a pas de plus haute autorité dans une hiérarchie de certification. Le certificat de la racine est alors le premier certificat dans tout chemin de certification.

3. (I) /DNS/ Base de la structure d'arborescence qui définit l'espace de noms pour le DNS Internet. (Voir : nom de domaine.)
4. (O) /MISSI/ Nom précédemment utilisé pour une autorité de création de politique MISSI, qui n'est pas une racine comme défini ci-dessus pour l'usage général, mais est une CA au second niveau de la hiérarchie MISSI, immédiatement subordonnée à une autorité d'approbation de politique MISSI.
5. (O) /UNIX/ Compte d'utilisateur (autrement dit "super utilisateur") qui a tous les privilèges (y compris tous les privilèges en rapport avec la sécurité) et peut donc gérer le système et ses autres comptes d'utilisateurs.

$ certificat racine *(root certificate)*
1. (I) /PKI/ Certificat pour lequel le sujet est une racine. (Voir : certificat d'ancre de confiance, certificat de confiance.)
2. (I) /PKI hiérarchique/ Certificat auto signé de clé publique au sommet d'une hiérarchie de certification.

$ clé racine *(root key)*
(I) /PKI/ Clé publique pour laquelle la clé privée correspondante est détenue par une racine. (Voir : clé d'ancre de confiance, clé de confiance.)

$ registre racine *(root registry)* (O) /MISSI/ Nom précédemment utilisé pour une PAA MISSI.

$ ROT13 (I) Voir : définition secondaire sous "chiffrement César".

$ routeur *(router)*
1a. (I) /IP/ Ordinateur sur un réseau, qui transmet les paquets IP qui ne lui sont pas adressés. (À comparer à : hôte.)
1b. (I) /IPS/ Passerelle qui fonctionne dans la couche IPS Internet pour connecter deux ou plusieurs sous réseaux.
1c. (N) /OSIRM/ Ordinateur qui est une passerelle entre deux réseaux à la couche 3 OSIRM et qui relaie et dirige les paquets de données à travers l'inter réseau. (À comparer à : pont, mandataire.)

$ règle *(rule)* Voir : règle de politique.

$ politique de sécurité fondée sur la règle *(rule-based security policy)*
(I) "Politique de sécurité fondée sur des règles globales [c'est-à-dire, des règles de politique] imposée à tous les utilisateurs. Ces règles s'appuient généralement sur la comparaison de la sensibilité de la ressource accédée et la possession des attributs correspondants des utilisateurs, d'un groupe d'utilisateurs, ou d'entités agissant au nom des utilisateurs." [I7498-2] (À comparer à : politique de sécurité fondée sur l'identité, règle de politique, RBAC.)

$ règles de comportement *(rules of behavior)*
(I) Corps de politique de sécurité qui a été établi et mis en œuvre et qui concerne les responsabilités et le comportement étendu des entités qui ont accès à un système. (À comparer à : [RFC1281].)
Instructions : pour les personnes employées par une corporation ou un gouvernement, les règles peuvent couvrir des questions comme le travail à domicile, l'accès à distance, l'utilisation de l'Internet, l'utilisation de travaux couverts par des droits de reproduction, l'utilisation des ressources système pour des besoins non officiels, l'allocation et la limitation des privilèges système, et la traçabilité individuelle.

$ champ S *(S field)* (D) Voir : champ niveau de sécurité.

$ S/Key
(I) Mécanisme de sécurité qui utilise une fonction de hachage cryptographique pour générer une séquence de 64 bits, des mots de passe à utilisation unique, pour la connexion d'utilisateurs distants. [RFC1760]
Instructions : le client génère un mot de passe à utilisation unique en appliquant plusieurs fois la fonction de hachage cryptographique MD4 à la clé secrète de l'utilisateur. Pour chaque authentification successive de l'utilisateur, le nombre d'applications du hachage est réduit de un. (Donc, un intrus qui utilise l'écoute ne peut pas calculer un mot de passe valide à partir de la connaissance de celui utilisé précédemment.) Le serveur vérifie un mot de passe en hachant le mot de passe présenté actuellement (ou la valeur d'initialisation) une fois et en comparant le résultat du hachage avec le mot de passe présenté antérieurement.

$ sûreté *(safety)*
(I) Propriété d'un système qui est libéré du risque de causer des dommages (en particulier des dommages physiques) à ses entités système. (À comparer à : sécurité.)

$ rondelle de saucisson *(salami swindle)*
(D) /argot/ "Découpage d'une petite quantité de chaque transaction. Cette sorte de vol devient rentable grâce à l'automatisation. Dans un grand flux de transactions, même l'arrondi au plus proche centième et le détournement du 'reste' dans un compte ad hoc peut être très profitable." [NCSSG]
Terme déconseillé : il est vraisemblable que les autres cultures utilisent des métaphores différentes pour ce concept. Donc, pour éviter l'incompréhension entre les nations, les IDOC NE DEVRAIENT PAS utiliser ce terme. (Voir : Utilisation déconseillée sous "Livre Vert".)

$ sel *(salt)*
(I) Valeur utilisée pour faire varier les résultats d'un calcul dans un mécanisme de sécurité, de sorte que l'exposition d'un résultat de calcul par une instance d'application du mécanisme ne puisse pas être réutilisée par un attaquant dans une autre instance. (À comparer à : valeur d'initialisation.)
Exemple : un mécanisme de contrôle d'accès fondé sur le mot de passe peut protéger contre la capture ou la divulgation accidentelle de son fichier de mot de passe en appliquant un algorithme de chiffrement unidirectionnel aux mots de passe avant de les mémoriser dans le fichier. Pour augmenter la difficulté d'attaques de dictionnaires hors ligne qui confrontent les valeurs chiffrées des éventuels mots de passe à une copie du fichier des mots de passe, ce mécanisme peut enchaîner chaque mot de passe à sa propre valeur aléatoire de sel avant d'appliquer la fonction unidirectionnelle.

$ bac à sable *(sandbox)*
(I) Environnement d'exécution restreint et contrôlé qui empêche l'accès de logiciels potentiellement malveillants, comme du code mobile, aux ressources système sauf à celles pour lesquelles le logiciel est autorisé.

$ épurer *(sanitize)*
1. (I) Supprimer les données sensibles d'un fichier, appareil ou système. (Voir : écraser, zéroiser.)
2. (I) Modifier des données de façon à être capable de (a) les déclassifier complètement, ou (b) les dégrader à un niveau de sécurité inférieur.

$ fouillage de poubelle *(scavenging)*
(I) /action de menace/ Voir : définition secondaire sous "exposition".

$ processeur de communications sûres (SCOMP, *Secure COMmunications Processor*)
(N) Version MLS améliorée de l'ordinateur Honeywell Level 6. Il a été le premier système classé dans la classe A1 de TCSEC. (Voir : KSOS.)

$ chambre à écran *(screen room)*
(D) /argot/ Synonyme de "clôture blindée" dans le contexte des émanations électromagnétiques. (Voir : EMSEC, TEMPEST.)
Terme déconseillé : pour éviter l'incompréhension dans d'autres langues, les IDOC NE DEVRAIT PAS utiliser ce terme.

$ routeur à écran *(screening router)* (I) Synonyme de "routeur de filtrage".

$ script kiddy
(D) /argot/ Craqueur qui est capable d'utiliser les techniques d'attaque existantes (c'est-à-dire, de lire les scripts) et d'exécuter les logiciels d'attaque existants, mais n'est pas capable d'inventer de nouveaux exploits ou de fabriquer les outils pour les accomplir ; péjoratif, pour un craquer pas mûr ou novice.
Terme déconseillé : il est vraisemblable que les autres cultures utilisent des métaphores différentes pour ce concept. Donc, pour éviter l'incompréhension entre les nations, les IDOC NE DEVRAIENT PAS utiliser ce terme. (Voir : Utilisation déconseillée sous "Livre Vert".)

$ SDU (N) Voir : "unité de données de service" sous "unité de données de protocole".

$ sceller *(seal)*
1. (I) Utiliser la cryptographie asymétrique pour chiffrer le texte source avec une clé publique d'une façon telle que seul le détenteur de la clé privée correspondante puisse découvrir quel était le texte source [Chau]. (À comparer à : linceul, enveloppe.)

Utilisation déconseillée : un IDOC NE DEVRAIT PAS utiliser ce terme avec la définition 1 sauf si l'IDOC inclut la définition, parce que celle-ci n'est pas très connue et le concept peut être exprimé par l'utilisation d'autres termes standard. À la place, utiliser "saler et chiffrer" ou une autre terminologie spécifique par rapport au mécanisme utilisé.
Instructions : la définition ne dit pas "seul le détenteur de la clé privée correspondante peut déchiffrer le texte chiffré pour savoir ce qu'était le texte en clair" ; sceller est plus fort que cela. Si Alice chiffre simplement un texte en clair P avec une clé publique K pour produire le texte chiffré C = K(P), alors, si Bob conjecture que P = X, Bob pourrait vérifier la conjecture en vérifiant si K(P) = K(X). Pour "sceller" P et bloquer l'attaque en conjecture de Bob, Alice pourrait lier une longue chaîne R de bits aléatoires à P avant de chiffrer pour produire C = K(P,R) ; si Bob conjecture que P = X, Bob peut seulement vérifier la conjecture en devinant aussi R. (Voir : sel.)
2. (D) Utiliser la cryptographie pour assurer le service d'intégrité pour un objet de données. (Voir : signer.)
Définition déconseillée : les IDOC NE DEVRAIENT PAS utiliser ce terme avec la définition 2. Utiliser à la place un terme plus spécifique par rapport au mécanisme utilisé pour fournir le service d'intégrité des données ; par exemple, utiliser "signer" lorsque le mécanisme est la signature numérique.

$ secret
1a. (I) /adjectif/ Condition des informations protégées contre la connaissance par toute entité système sauf celles dont il est prévu qu'elles les connaissent. (Voir : confidentialité des données.)
1b. (I) /nom/ Élément d'information qui est protégé ainsi.
Usage : ce terme s'applique aux clés symétriques, aux clés privées, et aux mots de passe.

$ clé secrète *(secret key)*
(D) Clé qui est gardée secrète ou doit être gardée secrète.
Terme déconseillé : les IDOC NE DEVRAIENT PAS utiliser ce terme ; il mélange des concepts d'une façon potentiellement trompeuse. Dans le contexte de la cryptographie asymétrique, les IDOC DEVRAIENT utiliser "clé privée". Dans le contexte de la cryptographie symétrique, l'adjectif "secret" n'est pas nécessaire parce que toutes les clés doivent être gardées secrètes.

$ chiffrement à clé secrète *(secret-key cryptography)*
(D) Synonyme de "chiffrement symétrique".
Terme déconseillé : les IDOC NE DEVRAIENT PAS utiliser ce terme ; cela pourrait être confondu avec "chiffrement asymétrique", dans lequel la clé secrète privée est gardée secrète.
Dérivation : le chiffrement symétrique est parfois appelé "chiffrement à clé secrète" parce que les entités qui partagent la clé, comme le générateur et le receveur d'un message, ont besoin de garder la clé secrète à l'égard des autres entités.

$ BGP sûr (S-BGP, *Secure BGP*)

(I) Projet de BBN Technologies, parrainé par l'Agence pour les projets de recherche de défense avancées de l'U.S. DoD, pour concevoir et démontrer une architecture pour sécuriser le protocole de passerelle frontière (BGP, *Border Gateway Protocol*) (RFC 1771) et promouvoir le déploiement de cette architecture dans l'Internet.
Instructions : S-BGP incorpore trois mécanismes de sécurité :
- Une PKI prend en charge l'authentification de la possession des blocs d'adresse IP, des numéros de système autonome (AS), d'une identité d'AS, et d'une identité de routeur BGP et de son autorisation de représenter une AS. Cette PKI suit le système existant d'allocation des adresses IP et des numéros d'AS de l'Internet et en tire parti.
- Un nouvel attribut facultatif de chemin BGP transitif porte les signatures numériques (dans des "attestations") couvrant les informations d'acheminement dans un BGP UPDATE. Ces signatures avec les certificats provenant de la PKI S-BGP permettent au receveur d'une UPDATE d'acheminement BGP de valider l'attribut et d'obtenir la confiance dans les préfixes d'adresse et les informations de chemin qu'il contient.
- IPsec fournit l'intégrité des données et de la séquence partielle, et permet aux routeurs BGP de s'authentifier les uns les autres pour les échanges de trafic de contrôle BGP.

$ échange de données sécurisé (SDE, *Secure Data Exchange*)
(N) Protocole de sécurité de LAN défini par la norme IEEE 802.10.

$ système de réseau à données sécurisées (SDNS, *Secure Data Network System*)
(O) Programme de la NSA qui développe des protocoles de sécurité pour la messagerie électronique (voir : MSP), la couche 3 d'OSIRM (voir : SP3), la couche 4 d'OSIRM (voir : SP4), et l'établissement de clés (voir : KMP).

$ distribution sûre *(secure distribution)* (I) Voir : distribution de confiance.

$ algorithme de hachage sécurisé (SDH, *Secure Hash Algorithm*)
(N) Fonction de hachage cryptographique (spécifiée dans SHS) qui produit un résultat (voir : "résultat de hachage") -- de longueur choisie de 160, 224, 256, 384, ou 512 bits -- pour des données d'entrée de toute longueur < 2**64 bits.

$ norme de hachage sécurisé (SHS, *Secure Hash Standard*)
(N) Norme du gouvernement des USA [FP180] qui spécifie SHA.

$ protocole de transfert sécurisé (S-HTTP, *Secure Hypertext Transfer Protocol*)
(I) Protocole Internet [RFC2660] pour fournir des services de sécurité client-serveur pour les communications HTTP. (À comparer à : https.)
Instructions : S-HTTP était à l'origine spécifié par CommerceNet, une coalition d'entreprises intéressées par le développement d'utilisations commerciales de l'Internet. Plusieurs formats de message peuvent être incorporés dans les clients et serveurs S-HTTP, en particulier CMS et MOSS. S-HTTP prend en charge le choix des politiques de sécurité, des mécanismes de gestion de clés, et des algorithmes de chiffrement par une négociation d'options entre les parties pour chaque transaction. S-HTTP prend en charge des modes de fonctionnement pour les chiffrements asymétriques aussi bien que symétriques. S-HTTP tente d'éviter de présumer un modèle de confiance particulier, mais il tente de faciliter une confiance hiérarchisée, multi racines, et prévoit que les principaux peuvent avoir de nombreux certificats de clé publique.

$ MIME sécurisé (S/MIME, *Secure/MIME*)
(I) Extensions de messagerie Internet multi objets sécurisées, un protocole Internet [RFC3851] qui assure le chiffrement et des signatures numériques pour les messages de la messagerie Internet.

$ diffusion groupée sécurisée *(secure multicast)*
(I) Se réfère généralement à la fourniture de services de sécurité pour des groupes de diffusion groupée de divers types (par exemple, d'un à plusieurs et de plusieurs à plusieurs) et à des classes de protocoles utilisés pour protéger les paquets de diffusion groupée.
Instructions : les applications de diffusion groupée incluent la diffusion de vidéo et le transfert de fichiers en diffusion groupée, et beaucoup de ces applications exigent des services de sécurité du réseau. Le cadre de référence de la sécurité de la diffusion groupée [RFC3740] couvre trois domaines fonctionnels :
- traitement des données de diffusion groupée : le traitement en matière de sécurité des données de diffusion groupée par l'envoyeur et le receveur.
- gestion des clés de groupe : la distribution sécurisée et le rafraîchissement du matériel de chiffrement. (Voir : Domaine d'interprétation de groupe.)
- politique de sécurité de diffusion groupée : la traduction et l'interprétation de la politique à travers plusieurs domaines administratifs qui sont normalement couverts par une application de diffusion groupée.

$ coquille sécurisée (SSH(marque déposée), *Secure Shell(*marque déposée))
(N) Se réfère à un protocole de connexion sûre à distance et d'autres services réseau sûrs.

Usage : sur le côté de la Toile de SSH Communication Security Corporation, à http://www.ssh.com/legal_notice.html, il est dit, "SSH [et] le logo SSH ... sont soit des marques commerciales, soit des marques déposées de SSH." Le présent glossaire attire l'attention des lecteurs sur cette revendication de marque déposée mais ne prend pas position sur sa validité.
Instructions : SSH a trois parties principales :

- protocole de couche Transport : assure l'authentification, la confidentialité, et l'intégrité du serveur; et peut facultativement fournir la compression. Cette couche fonctionne normalement sur une connexion TCP, mais peut aussi fonctionner par dessus tout autre flux de données fiable.
- protocole d'authentification d'usager : authentifie l'usager côté client auprès du serveur. Il fonctionne sur le protocole de couche Transport.
- protocole de connexion : il multiplexe le tunnel chiffré en plusieurs canaux logiques. Il fonctionne sur le protocole d'authentification de l'usager.

$ couche de connexion sécurisée (SSL, *Secure Sockets Layer*)
(N) Protocole Internet (développé à l'origine par Netscape Communications, Inc.) qui utilise le chiffrement de bout en bout en mode connexion pour fournir un service de confidentialité des données et un service d'intégrité des données pour le trafic entre un client (souvent un navigateur de la Toile) et un serveur, et cela peut facultativement fournir l'authentification de l'entité homologue entre le client et le serveur. (Voir : sécurité de la couche Transport.)
Instructions : SSL a deux couches ; la couche inférieure de SSL, le protocole d'enregistrement SSL, est mise en couche par dessus un protocole de couche transport de l'IPS et encapsule les protocoles qui fonctionnent dans la couche supérieure. Les protocoles de couche supérieure sont les trois protocoles de gestion SSL -- protocole de prise de contact SSL, protocole SSL de spécification de changement de chiffrement, ou protocole d'alerte SSL -- et un protocole de couche Application (par exemple, HTTP).
Les protocoles de gestion SSL fournissent un chiffrement asymétrique pour l'authentification du serveur (vérifiant l'identité du serveur pour le client) et une authentification facultative du client (vérifiant l'identité du client pour le serveur) et aussi leur permet, avant que le protocole d'application transmette ou reçoive les données, de négocier un algorithme de chiffrement symétrique et une clé de session secrète (à utiliser pour le service de confidentialité des données) et un hachage chiffré (à utiliser pour le service d'intégrité des données).
SSL est indépendant de l'application qu'il encapsule, et toute application peut se mettre en couche en toute transparence au dessus de SSL. Cependant, de nombreuses applications Internet seraient mieux servies par IPsec.

$ état sûr *(secure state)*
1a. (I) Condition d'un système dans laquelle celui-ci est en conformité avec la politique de sécurité applicable. (À comparer à : système propre, transaction.)
1b. (I) /modèle formel/ Condition d'un système dans laquelle aucun sujet ne peut accéder à un objet d'une façon non autorisée. (Voir : définition secondaire sous "modèle de Bell-LaPadula".)

$ sécurité *(security)*
1a. (I) Condition d'un système qui résulte de l'établissement et de la maintenance de mesures de protection du système.
1b. (I) Condition d'un système dans laquelle les ressources du système sont exemptes d'accès non autorisé et de changement non autorisé ou accidentel, de destruction, ou de perte. (À comparer à : sûreté.)
2. (I) Mesures prises pour protéger un système.
Instructions : Parker [Park] suggère que fournir une condition de sécurité d'un système peut impliquer les six fonctions de base suivantes, qui se chevauchent dans une certaine mesure :

- "Dissuasion" : réduire une menace intelligente en décourageant l'action, comme par la crainte ou le doute. (Voir : attaque, action de menace.)
- "Évitement" : réduire un risque en réduisant la valeur de la perte potentielle ou en réduisant la probabilité que survienne la perte. (Voir : analyse de risque. À comparer à : "évitement de risque" sous "risque".)
- "Prévention" : empêcher ou déjouer une potentielle violation de sécurité en déployant une contre mesure.
- "Détection" : déterminer qu'une violation de la sécurité est imminente, est en cours, ou s'est récemment produite, et rend donc possible de réduire la perte potentielle. (Voir : détection d'intrusion.)
- "Récupération" : opération de restauration de l'état normal d'un système pour compenser une violation de la sécurité, éventuellement en éliminant ou en réparant ses effets. (Voir : plan de contingence, entrée sous "récupération".)
- "Correction" : changer une architecture de sécurité pour éliminer ou réduire le risque de réapparition d'une violation de la sécurité ou de conséquence d'une menace, comme par l'élimination d'une faiblesse.

$ architecture de sécurité *(security architecture)*
(I) Plan et ensemble de principes qui décrivent (a) les services de sécurité qu'il est exigé que fournisse un système pour assurer la satisfaction des besoins de ses utilisateurs, (b) les composants du système exigés pour mettre en œuvre les services, et (c) les niveaux de performance requis dans les composants pour faire face à l'environnement de menaces (par exemple, [RFC2179]). (Voir : défense en profondeur, IATF, architecture de sécurité OSIRM, contrôles de sécurité, instructions sous "politique de sécurité".)
Instructions : une architecture de sécurité est le résultat de l'application du processus d'ingénierie du système. Une

architecture de sécurité de système complète inclut la sécurité administrative, la sécurité de communication, la sécurité informatique, la sécurité des émanations, la sécurité du personnel, et la sécurité physique. Une architecture de sécurité complète doit considérer les menaces intelligentes intentionnelles et les menaces accidentelles.

$ langage de balisage d'assertion de sécurité (SAML, *Security Assertion Markup Language*)
(N) Protocole consistant en formats de messages de demandes et réponses fondés sur XML pour échanger des informations de sécurité, exprimées sous la forme d'assertions sur les sujets, entre les partenaires d'affaires en ligne. [SAML]

$ association de sécurité *(security association)*
1. (I) Relation établie entre deux entités ou plus pour leur permettre de protéger les données qu'elles échangent. (Voir : association, ISAKMP, SAD. À comparer à : session.)

Instructions : la relation est représentée par un ensemble de données qui sont partagées d'un commun accord entre les entités et est considérée comme contractuelle entre elles. Les données décrivent comment les entités associées utilisent conjointement les services de sécurité. La relation est utilisé pour négocier les caractéristiques des mécanismes de sécurité, mais la relation est généralement comprise comme excluant les mécanismes eux-mêmes.

2. (I) /IPsec/ Connexion logique unidirectionnelle créée pour des besoins de sécurité et mise en œuvre soit avec AH, soit avec ESP (mais pas les deux). Les services de sécurité offerts par une association de sécurité dépendent du protocole (AH ou ESP) du mode IPsec (transport ou tunnel) des points d'extrémité, et du choix de services facultatifs au sein du protocole. Une association de sécurité est identifiée par un triplet consistant en (a) une adresse IP de destination, (b) un identifiant de protocole (AH ou ESP) et (c) un indice de paramètre de sécurité.
3. (O) "Ensemble de politique et de clés de chiffrement qui assure des services de sécurité au trafic réseau qui correspond à cette politique". [RFC3740] (Voir : association cryptographique, association de sécurité de groupe.)
4. (O) "Totalité des mécanismes et fonctions de communications et de sécurité (par exemple, protocoles de communication, protocoles de sécurité, mécanismes et fonctions de sécurité) qui lient ensemble en toute sécurité deux contextes de sécurité dans des systèmes d'extrémité ou systèmes relais différents et qui prennent en charge le même domaine d'informations." [DoD6]

$ base de données d'association de sécurité (SAD, *Security Association Database*)
(I) /IPsec/ Dans une mise en œuvre IPsec qui fonctionne dans un nœud du réseau, c'est une base de données qui contient des paramètres pour décrire l'état et le fonctionnement de chacune des associations de sécurité actives que le nœud a établi avec les autres nœuds. Des SAD d'entrée et de sortie séparées sont nécessaires à cause de la directionnalité des associations de sécurité IPsec. [RFC4301] (À comparer à : SPD.)

$ identifiant d'association de sécurité (SAID, *security association identifier*)
(I) Champ de données dans un protocole de sécurité (comme NLSP ou SDE) utilisé pour identifier l'association de sécurité à laquelle est liée une PDU. La valeur de SAID est généralement utilisée pour choisir une clé de déchiffrement ou d'authentification à la destination. (Voir : indice de paramètre de sécurité.)

$ assurance de sécurité *(security assurance)*
1. (I) Attribut d'un système d'information qui sert de base pour établir la confiance dans le fonctionnement du système de façon à mettre en application la politique de sécurité du système. (À comparer à : confiance.)
2. (I) Procédure qui assure qu'un système est développé et fonctionne comme prévu par la politique de sécurité du système.
3. (D) "Degré de confiance qu'on a que les contrôles de sécurité fonctionnent correctement et protègent le système comme prévu." [SP12]

Définition déconseillée : les IDOC NE DEVRAIENT PAS utiliser la définition 3 ; c'est une définition de "niveau d'assurance" plutôt que "d'assurance".

4. (D) /Gouvernement des USA, authentification d'identité/ Le (a) "degré de confiance dans le processus de vérification utilisé pour établir l'identité de l'individu à qui l'accréditif [d'identité] a été fourni" et le (b) "degré de confiance que les individus qui utilisent l'accréditif sont les individus à qui les accréditifs ont été fournis". [M0404]

Définition déconseillée :les IDOC NE DEVRAIENT PAS utiliser la définition 4 ; elle mélange des concepts d'une façon potentiellement trompeuse. La partie "a" est une définition pour "niveau d'assurance" (plutôt que pour "assurance de sécurité") d'un processus d'enregistrement d'identité, et la partie "b" est une définition pour "niveau d'assurance" (plutôt que pour "assurance de sécurité") d'un processus d'authentification d'identité. Aussi, le processus d'enregistrement d'une authentification devrait être défini et conçu séparément pour assurer la clarté de la certification.

$ examen de sécurité *(security audit)*
(I) Révision et examen indépendant des enregistrements et activités d'un système pour déterminer l'adéquation des contrôles d'un système, assurer la conformité avec la politique et les procédures de sécurité établies, détecter les failles des services de sécurité, et recommander tout changement qui est indiqué pour les contre mesures. [I7498-2], [NCS01] (À comparer à : traçabilité, détection d'intrusion.)
Instructions : l'objectif de l'audit de base est d'établir la traçabilité des entités système qui initient ou participent aux

événements et actions en rapport avec la sécurité. Donc, des moyens sont nécessaires pour générer et enregistrer un chemin d'audit de sécurité et pour réviser et analyser le chemin d'audit pour découvrir et étudier les violations de la sécurité.

$ journal d'audit de sécurité *(security audit trail)*
(I) Enregistrement chronologique des activités d'un système qui sont suffisantes pour permettre la reconstruction et l'examen de la séquence des environnements et des activités qui entourant ou conduisent à une opération, procédure, ou événement dans une transaction en rapport avec la sécurité depuis la conception jusqu'au résultat final. [NCS04] (Voir : audit de sécurité.)

$ sécurité par l'obscurité *(security by obscurity)*
(O) Tentative de maintenir ou augmenter la sécurité d'un système en gardant secrète la conception ou la construction d'un mécanisme de sécurité.
Instructions : cette approche a été longtemps discréditée en cryptographie, où la phrase se réfère à essayer de garder un algorithme secret, plutôt que de juste dissimuler les clés [Schn]. On doit supposer que des appareils cryptographiques produits en masse ou largement diffusés seront finalement perdus ou volés et que donc, les algorithmes feront l'objet d'une ingénierie inverse et seront connus des adversaires. Donc, on ne devrait s'appuyer que sur les algorithmes et protocoles qui sont assez forts pour avoir été largement publiés, et ont été revus par des pairs assez longtemps pour que leurs fautes aient été trouvées et retirées. Par exemple, le NIST a utilisé un long processus public pour sélectionner AES pour remplacer DES. Dans la sécurité des ordinateurs et des réseaux, le principe de "pas de sécurité par l'obscurité" s'applique aussi aux mécanismes de sécurité autres que cryptographiques. Par exemple, si la conception et la mise en œuvre d'un protocole de contrôle d'accès sont fortes, la lecture du code source du protocole ne devrait pas permettre de trouver un moyen de contourner la protection et de pénétrer le système.

$ classe de sécurité *(security class)* (D) Synonyme de "niveau de sécurité".
Terme déconseillé : les IDOC NE DEVRAIENT PAS utiliser ce terme. À la place, utiliser "niveau de sécurité", qui est plus largement établi et compris.

$ niveau d'habilitation *(security clearance)*
(I) Détermination qu'une personne est éligible, selon les standard d'une politique de sécurité spécifique, à être autorisée à accéder à des informations sensibles ou autres ressources système. (Voir : niveau d'accréditation.)

$ compromission de la sécurité *(security compromise)*
(I) Violation de la sécurité dans laquelle une ressource système est exposée, ou est potentiellement exposée, à un accès non autorisé. (À comparer à : compromission de données, exposition, violation.)

$ contrôles de sécurité *(security controls)*
(N) Contrôles de la gestion, du fonctionnement et des techniques (sauvegardes ou contre mesures) prescrites pour un système d'information qui satisfait aux exigences globales de sécurité spécifiées et protège de façon adéquate la confidentialité, l'intégrité, et la disponibilité du système et de ses informations. [FP199] (Voir : architecture de sécurité.)

$ doctrine de sécurité *(security doctrine)*
(I) Ensemble spécifié de procédures ou pratiques qui dirigent ou donnent des lignes directrices sur la façon de se conformer à une politique de sécurité. (À comparer à : mécanisme de sécurité, politique de sécurité.)
Instructions : politique de sécurité et doctrine de sécurité sont en relations étroites. Cependant, la politique traite principalement de stratégie, et la doctrine de la tactique. Doctrine de sécurité est souvent compris comme se référant principalement à la sécurité administrative, à la sécurité personnelle, et à la sécurité physique. Par exemple, les mécanismes et appareils de sécurité qui les mettent en œuvre sont normalement conçus pour fonctionner dans une gamme limitée de conditions environnementales et administratives, et ces conditions doivent être satisfaites pour compléter et assurer la protection technique due au matériel, progiciels et logiciels des appareils. La doctrine de sécurité spécifie comment réaliser ces conditions. (Voir : "première loi" sous "Lois de Courtney".)

$ domaine de sécurité *(security domain)* (I) Voir : domaine.

$ environnement de sécurité *(security environment)*
(I) Ensemble des entités externes, procédures, et conditions qui affectent le développement, le fonctionnement, et la maintenance sûrs d'un système. (Voir : "première loi" sous "Lois de Courtney".)

$ événement de sécurité *(security event)*
(I) Occurrence dans un système qui relève de la sécurité du système. (Voir : incident de sécurité.)
Instructions : le terme couvre à la fois les événements qui sont des incidents de sécurité et ceux qui ne le sont pas. Dans une station de travail d'une CA, par exemple, une liste des événements de sécurité pourrait inclure ce qui suit :

- connecter un opérateur avec le système ou le déconnecter ;
- effectuer une opération de chiffrement, par exemple, signer un certificat numérique ou une CRL ;
- effectuer une opération, création, insertion, retrait, ou sauvegarde de carte cryptographique ;
- effectuer une opération sur la durée de vie d'un certificat numérique : changement de clé, renouvellement, révocation, ou mise à jour ;
- envoi d'un certificat numérique à un répertoire X.500 ;
- recevoir une notification de compromission de clé ;
- recevoir une demande de certification impropre ;
- détection d'une condition d'alarme rapportée par un module cryptographique ;
- échouer à un auto essai de matériel incorporé ou à une vérification d'intégrité système d'un logiciel.

$ analyse des fautes de sécurité *(security fault analysis)*
(I) Analyse de sécurité, généralement effectuée sur un matériel au niveau de la logique d'un accès, accès par accès, pour déterminer les propriétés de sécurité d'un appareil lorsque se rencontre une faute du matériel.

$ fonction de sécurité *(security function)*
(I) Fonction dans un système qui relève de la sécurité du système; c'est-à-dire, une fonction système qui doit opérer correctement pour assurer l'adhésion à la politique de sécurité du système.

$ passerelle de sécurité *(security gateway)*
1. (I) Passerelle inter réseaux qui sépare les hôtes de confiance (ou relativement plus de confiance) d'un côté et les hôtes qui ne sont pas de confiance (ou moins de confiance) de l'autre côté. (Voir : pare-feu et garde.)
2. (O) /IPsec/ "Système intermédiaire qui met en œuvre les protocoles IPsec." [RFC4301]

Instructions : AH ou ESP d'IPsec peuvent être mis en œuvre sur une passerelle entre un réseau protégé et un réseau non protégé, pour fournir des services de sécurité aux hôtes du réseau protégé lorsque ils communiquent à travers le réseau non protégé avec d'autres hôtes et passerelles.

$ incident de sécurité *(security incident)*
1. (I) Événement de sécurité qui implique une violation de la sécurité. (Voir : CERT, événement de sécurité, intrusion de sécurité, violation de sécurité.)

Instructions : en d'autres termes, un événement de sécurité dans lequel la politique de sécurité du système n'est pas obéie ou est enfreinte d'une certaine façon.

2. (D) "Tout événement contraire [qui] compromet un aspect de la sécurité des ordinateurs ou du réseau." [RFC2350]
   Définition déconseillée : les IDOC NE DEVRAIENT PAS utiliser la définition 2 parce que (a) un incident de sécurité peut survenir sans être réellement dommageable (c'est-à-dire, contraire) et parce que (b) le présent glossaire définit "compromission" d'une façon en relation plus étroite avec l'accès non autorisé.
3. (D) "Une violation ou une menace imminente de violation des politiques de sécurité informatique, des politiques d'usage acceptable, ou des pratiques standard de sécurité informatique." [SP61]
   Définition déconseillée : les IDOC NE DEVRAIENT PAS utiliser la définition 3 parce qu'elle mélange des concepts d'une façon qui n'est pas en accord avec l'usage commun ; un incident de sécurité est généralement compris comme impliquant une réalisation d'une menace (voir : action de menace) et non juste une menace.

$ intrusion dans la sécurité *(security intrusion)*
(I) Événement de sécurité, ou combinaison de plusieurs événements de sécurité, qui constitue un incident de sécurité dans lequel un intrus obtient, ou tente d'obtenir, l'accès à un système ou ressource système sans avoir l'autorisation de le faire.

$ noyau de sécurité *(security kernel)*
(I) "Éléments de matériel, progiciel ou logiciel d'une base informatique de confiance qui mettent en œuvre le concept de surveillance de référence. Il doit s'interposer sur tous les accès, être protégé contre la modification, et être vérifiable." [NCS04] (Voir : noyau, TCB.)
Instructions : un noyau de sécurité est la mise en œuvre d'une surveillance de référence pour une certaine base de matériel. [Huff]

$ étiquette de sécurité *(security label)*
(I) Élément de métadonnées qui désigne la valeur d'un ou plusieurs attributs qui relèvent de la sécurité (par exemple, niveau de sécurité) d'une ressource système. (Voir : [RFC1457]. À comparer à : marquage de sécurité.)
Utilisation déconseillée : pour éviter la confusion, les IDOC NE DEVRAIENT PAS utiliser "étiquette de sécurité" pour "marquage de sécurité", ou vice versa, même si cela se fait couramment (y compris dans certaines normes nationales et internationales qui devraient bien le savoir).
Instructions : les mécanismes de sécurité humains et automatiques utilisent une étiquette de sécurité d'une ressource système pour déterminer, conformément à la politique de sécurité applicable, comment contrôler l'accès à la ressource (et

ils fixent des marquages de sécurité appropriés correspondants aux instances physiques de la ressource). Les étiquettes de sécurité sont le plus souvent utilisées pour prendre en charge une politique de confidentialité des données, et parfois pour une politique d'intégrité des données.
Comme expliqué dans la [RFC1457], la forme prise par des étiquettes de sécurité des paquets d'un protocole varie selon la couche OSIRM dans laquelle fonctionne le protocole. Comme le sont généralement les métadonnées, une étiquette de sécurité d'un paquet de données peut être explicite (par exemple, IPSO) ou implicite (par exemple, Alice traite tous les messages reçus de Bob comme étiquetés "Ne pas publier"). Dans un protocole sans connexion, chaque paquet peut avoir une étiquette explicite ; mais dans un protocole en mode connexion, tous les paquets peuvent avoir la même étiquette implicite qui est déterminée au moment de l'établissement de la connexion. Les ressources systèmes classifiées et non classifiées peuvent requérir une étiquette de sécurité. (Voir : FOUO.)

$ niveau de sécurité *(security level)*
(I) Combinaison d'un niveau de classification hiérarchique et d'un ensemble de désignations de catégories non hiérarchiques qui représente la sensibilité qu'un type ou élément d'informations spécifiés. (Voir : domaine, modèle en treillis. À comparer à : niveau de classification.)
Usage : les IDOC qui utilisent ce terme DEVRAIENT en déclarer une définition. Le terme est généralement compris comme impliquant une sensibilité à la divulgation, mais il est aussi utilisé de nombreuses autres façons et pourrait facilement être mal compris.

$ champ Niveau de sécurité *(Security Level field)*
(I) Champ de 16 bits qui spécifie une valeur de niveau de sécurité dans l'option Sécurité (option type 130) d'un format d'en-tête de datagramme IP version 4.
Abréviation déconseillée : les IDOC NE DEVRAIENT PAS utiliser l' abréviation "Champ S", qui peut être ambiguë.

$ infrastructure de gestion de la sécurité (SMI, *security management infrastructure*)
(I) Composants et activités système qui prennent en charge la politique de sécurité en surveillant et contrôlant les services et mécanismes de sécurité, en distribuant les informations de sécurité, et en rapportant les événements de sécurité.
Instructions : les fonctions associées sont les suivantes [I7498-4] :
- Contrôler (accorder ou refuser) l'accès aux ressources système : cela inclut de vérifier les autorisations et les identités, de contrôler l'accès aux données de sécurité sensibles, et de modifier les priorités et procédures d'accès dans l'éventualité d'attaques.
- Restituer (rassembler) et archiver (mémoriser) les informations de sécurité : cela inclut de tenir le journal des événements de sécurité et d'analyser les journaux, de surveiller et de faire des profils d'usage, et de rapporter les violations de la sécurité.
- Gérer et contrôler le processus de chiffrement : cela inclut d'effectuer les fonctions de gestion de clés et de faire rapport des problèmes de gestion de clés. (Voir : PKI.)

$ marquage de sécurité *(security marking)*
(I) Marquage physique qui est lié à une instance de ressource système et qui représente une étiquette de sécurité de la ressource, c'est-à-dire, qui nomme ou désigne la valeur d'un ou plusieurs attributs pertinents pour la sécurité de la ressource. (À comparer à : étiquette de sécurité.)
Instructions : une étiquette de sécurité peut être représentée par divers marquages équivalents selon la forme physique prise par la ressource étiquetée. Par exemple, un document pourrait avoir un marquage composé d'un schéma binaire [FP188] lorsque le document est mémorisé électroniquement comme fichier dans un ordinateur, et aussi un marquage de caractères alphabétiques imprimés lorsque le document est sous forme papier.

$ mécanisme de sécurité *(security mechanism)*
(I) Méthode ou processus (ou un appareils qui l'incorpore) qui peut être utilisé dans un système pour mettre en œuvre un service de sécurité qui est fourni par ou dans le système. (Voir : Instructions sous "politique de sécurité". À comparer à : doctrine de sécurité.)
Usage : généralement compris comme se référant principalement aux composants de la sécurité de la communication, à la sécurité informatique et à la sécurité des émanations.
Exemples : échange d'authentification, somme de contrôle, signature numérique, chiffrement, et bourrage de trafic.

$ modèle de sécurité *(security model)*
(I) Description schématique d'un ensemble d'entités et de relations par lesquelles un ensemble spécifié de services de sécurité est fourni par ou au sein d'un système. Exemple : modèle de Bell-LaPadula, OSIRM. (Voir : Instructions sous "politique de sécurité".)

$ indice des paramètres de sécurité (SPI, *security parameters index*)
1. (I) /IPsec/ Identifiant de 32 bits utilisé pour distinguer les associations de sécurité qui se terminent à la même destination

(adresse IP) et utilisent le même protocole de sécurité (AH ou ESP). Porté dans AH et ESP pour permettre au système receveur de déterminer sous quelle association de sécurité traiter un paquet reçu.

2. (I) /IP mobile/ Indice de 32 bits qui identifie une association de sécurité dans une collection d'associations qui sont disponibles entre une paire de nœuds, pour l'application aux messages de protocole IP mobile qu'échangent les nœuds.

$ périmètre de sécurité *(security perimeter)*

(I) Frontière physique ou logique qui est définie pour un domaine ou enclave et au sein de laquelle s'applique une politique de sécurité ou architecture de sécurité particulière. (Voir : interne, externe.)

$ politique de sécurité *(security policy)*

1. (I) Objectif, cours, ou méthode d'action défini pour guider et déterminer les décisions présentes et futures concernant la sécurité dans un système. [NCS03], [RFC3198] (À comparer à : politique de certificat.)

2a. (I) Ensemble de règles de politique (ou de principes) qui précisent comment un système (ou une organisation) fournit les services de sécurité pour protéger les ressources système sensibles et critiques. (Voir : politique de sécurité fondée sur l'identité, règle de politique, politique de sécurité fondée sur la règle, règles de comportement. À comparer à : architecture de sécurité, doctrine de sécurité, mécanisme de sécurité, modèle de sécurité, [RFC1281].)

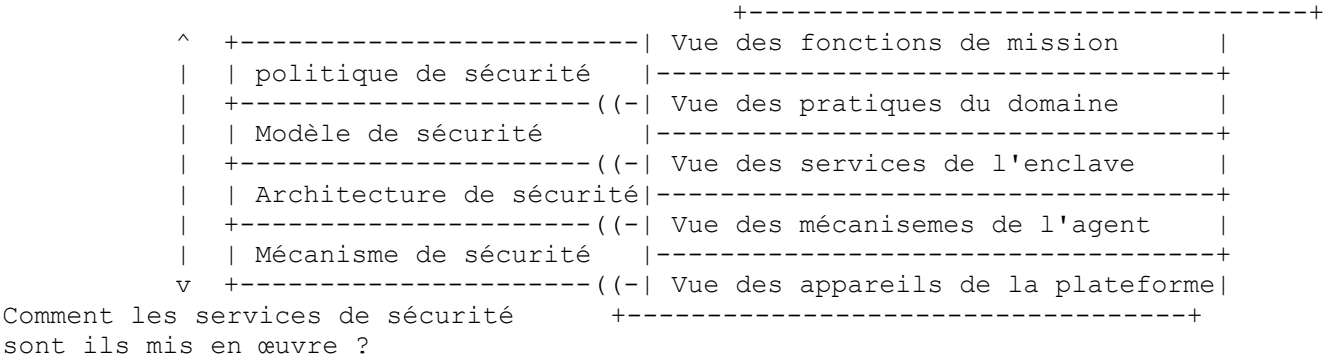
2b. (O) Ensemble de règles pour administrer, gérer, et contrôler l'accès aux ressources du réseau. [RFC3060], [RFC3198]

2c. (O) /X.509/ Ensemble de règles établies par une autorité pour gouverner l'utilisation et le provisionnement de services et facilités de sécurité.

2d. (O) /Critères communs/ Ensemble de règles régulant la gestion et la protection des biens, et distribuées dans un TOE.

Instructions : Ravi Sandhu suggère qu'une politique de sécurité est une des quatre couches du processus d'ingénierie de la sécurité (comme le montre le diagramme suivant). Chaque couche donne une vision différente de la sécurité, allant des services nécessaires à comment les services sont mis en œuvre.

Quels services de sécurité devraient être fournis ?



On suggère que chacune des quatre couches de Sandhu soit une transposition entre deux points de vue qui diffèrent dans leur degré d'abstraction, selon la perspective des divers participants au concept du système, au développement, et aux activités de focntionnement, comme suit :

- Vue des fonctions de mission : perspective d'un utilisateur de ressources système. Déclare les besoins de protection des ressources en fonction des phases de temps et identifie les ressources sensibles et critiques -- réseaux, hôtes, applications, et bases de données. Indépendante des règles et pratiquees utilisées pour réaliser la protection.
- Vue des pratiques du domaine : perspective d'un gestionnaire d'entreprise qui fixe des normes de protection pour les ressources. Fixe les règles et les pratiques pour la protection. Identifie les membres du domaine; c'est-à-dire, les entités (usagers/fournisseurs) et les ressources (y compris les objets de données). Indépendant de la topologie du système. N'est pas obligé d'être hiérarchique.
- Vue des services de l'enclave : perspective d'un concepteur de système qui alloue les fonctions de sécurité aux composants majeurs. Alloue les services de sécurité aux structures topologiques du système et à leur contenu. Indépendante des mécanismes de sécurité. Hiérarchique à travers tous les domaines.
- Vue des mécanismes d'agent : perspective d'un ingénieur système qui spécifie les mécanismes de sécurité pour mettre en œuvre les services de sécurité. Spécifie les mécanismés à utiliser par le protocole, la base de données, et les moteurs d'application. Indépendant du type et du fabricant des plateformes et autres appareils physiques.
- Vue des appareils de la plateforme : perspective d'une description telle que construite du système en fonctionnement. Spécifie exactement comment construire ou assembler le système, et spécifie aussi les procédures de fonctionnement du système.

$ base de données de politique de sécurité (SPD, *Security Policy Database*)

(I) /IPsec/ Dans une mise en œuvre d'IPsec qui fonctionne dans un nœud de réseau, une base de données qui contient des paramètres qui spécifient les politiques établies par un utilisateur ou administrateur pour déterminer quels services IPsec, s'il en est, doivent être fournis aux datagrammes IP envoyés ou reçus par le nœud, et de quelle façon ils sont fournis. Pour chaque datagramme, le SPD spécifie un des trois choix : éliminer le datagramme, appliquer les services IPsec (par exemple,

AH ou ESP) ou outrepasser IPsec. Des SPD entrants et sortants séparés sont nécessaires à cause de la directionnalité des associations de sécurité IPsec. [RFC4301] (À comparer à : SAD.)

$ protocole de sécurité n° 3 (SP3, *Security Protocol 3*)
(O) Protocole [SDNS3] développé par SDNS pour fournir la sécurité de données sans connexion au sommet de la couche 3 de l'OSIRM. (À comparer à : IPsec, NLSP.)

$ protocole de sécurité n° 4 (SP3, *Security Protocol 4*)
(O) Protocole [SDNS4] développé par SDNS pour fournir la sécurité des données sans connexion ou en mode connexion de bout en bout au bas de la couche 4 de l'OSIRM. (Voir : TLSP.)

$ événement en rapport avec la sécurité *(security-relevant event)*
(D) Synonyme de "événement de sécurité".
Terme déconseillé : les IDOC NE DEVRAIENT PAS utiliser ce terme ; il est verbeux.

$ fonction sensible à la sécurité *(security-sensitive function)*
(D) Synonyme de "fonction de sécurité".
Terme déconseillé : les IDOC NE DEVRAIENT PAS utiliser ce terme ; il est verbeux.

$ service de sécurité *(security service)*
1. (I) Service de traitement ou de communication qui est fourni par un système pour assurer une sorte de protection spécifique aux ressources système. (Voir : service de contrôle d'accès, service d'audit, service de disponibilité, service de confidentialité des données, service d'intégrité des données, service d'authentification d'origine des données, service de non répudiation, service d'authentification de l'entité homologue, service d'intégrité du système.)

Instructions : les services de sécurité mettent en œuvre les politiques de sécurité, et sont mis en œuvre par les mécanismes de sécurité.

2. (O) "Service fourni par une couche de systèmes ouverts communicants, [qui] assure une sécurité adéquate des systèmes ou des transferts de données." [I7498-2]

$ situation de sécurité *(security situation)*
(I) /ISAKMP/ Ensemble de toutes les informations pertinentes pour la sécurité (par exemple, adresses réseau, classifications de sécurité, fonctionnement normal ou d'urgence) qui sont nécessaires pour décider des services de sécurité qui sont exigés pour protéger l'association en cours de négociation.

$ cible de sécurité *(security target)*
(N) /Critères communs/ Ensemble des exigences et des spécifications de sécurité à utiliser comme base de l'évaluation d'un TOE identifié.
Instructions : une cible de sécurité (ST) est une déclaration de revendications de sécurité pour un produit ou système de sécurité de technologie de l'information particulier, et elle est la base de l'accord entre les parties quant à la nature de la sécurité que le produit ou système offre. Une ST est parallèle à la structure d'un profil de protection, mais a des éléments supplémentaires qui incluent des informations détaillées spécifiques du produit. Une ST contient une spécification sommaire, qui définit les mesures spécifiques prises dans le produit ou système pour satisfaire les exigences de sécurité.

$ jeton de sécurité *(security token)* (I) Voir : jeton.

$ violation de sécurité *(security violation)*
(I) Acte ou événement qui désobéit ou par ailleurs enfreint une politique de sécurité. (Voir : compromission, pénétration, incident de sécurité.)

$ germe *(seed)* (I) Valeur qui est une entrée d'un générateur de nombres pseudo aléatoires.

$ confidentialité sélective selon le champ *(selective-field confidentiality)*
(I) Service de confidentialité des données qui préserve la confidentialité pour une ou plusieurs parties (c'est-à-dire, champs) de chaque paquet. (Voir : intégrité selon le champ.)
Instructions : le service de confidentialité des données est généralement appliqué à des SDU entières, mais certaines situations peuvent requérir de ne protéger qu'une partie de chaque paquet. Par exemple, lorsque Alice utilise une carte de débit sur un distributeur automatique de billets (ATM, *automatic teller machine*) peut-être que seul son PIN est chiffré pour rester confidentiel lorsque sa demande de transaction est transmise de l'ATM à l'ordinateur de sa banque.
Dans toute situation de fonctionnement, il peut y avoir de nombreuses raisons différentes pour utiliser la confidentialité sélective selon le champ. Dans l'exemple de l'ATM, il y a au moins quatre possibilités : le service peut fournir un mode de

fonctionnement à l'épreuve de l'échec, assurant que la banque peut quand même traiter les transactions (moyennant un certain risque) lorsque le système de chiffrement est défaillant. Il peut rendre les messages plus faciles à travailler quand on fait l'isolement des fautes du système. Il peut éviter les problèmes avec les lois qui interdisent l'exportation de données chiffrées à travers les frontières internationales. Il peut améliorer l'efficacité en réduisant la charge du traitement sur un site informatique central.

$ intégrité sélective selon le champ *(selective-field integrity)*
(I) Service d'intégrité des données qui préserve l'intégrité pour une ou plusieurs parties (c'est-à-dire, champs) de chaque paquet. (Voir : confidentialité selon le champ.)
Instructions : un service d'intégrité des données peut être mis en œuvre dans un protocole pour protéger la partie SDU des paquets, la partie PCI, ou les deux.
- protection de la SDU : lorsque le service est fourni pour les SDU, il est généralement appliqué aux SDU entières, mais il peut être appliqué seulement à des parties des SDU dans certaines situations. Par exemple, un protocole de couche Application IPS pourrait avoir besoin de protéger seulement une partie de chaque paquet, et cela pourrait accélérer le traitement.
- protection de la PCI : pour empêcher l'écoute active, il peut être souhaitable d'appliquer le service d'intégrité des données à la PCI entière, mais certains champs de PCI dans certains protocoles ont besoin d'être modifiables dans le transit. Par exemple, le champ "Durée de vie" dans IPv4 est changé chaque fois qu'un paquet passe à travers un routeur dans la couche Internet. Donc, la valeur que ce champ va avoir lorsque le paquet arrive à sa destination n'est pas prévisible par l'envoyeur et ne peut pas être incluse dans une somme de contrôle calculée par l'envoyeur. (Voir : en-tête d'authentification.)

$ certificat auto signé *(self-signed certificate)*
(I) Certificat de clé publique pour lequel la clé publique liée par le certificat et la clé privée utilisée pour signer le certificat sont des composants de la même paire de clés, qui appartient au signataire. (À comparer à : certificat racine.)
Instructions : dans un certificat auto signé de clé publique X.509, le DN du producteur est le même que le DN du sujet.

$ sécurité sémantique *(semantic security)*
(I) Attribut d'un algorithme de chiffrement qui est une formalisation de la notion que l'algorithme cache non seulement le texte source mais aussi ne révèle aucune information partielle sur le texte source ; c'est-à-dire, tout ce qui est calculable sur le texte source lorsque on donne le texte chiffré, est aussi calculable sans le texte chiffré. (À comparer à : indistinguabilité.)

$ semi formel *(semiformal)*
(I) Exprimé dans un langage de syntaxe restreinte avec une sémantique définie. [CCIB] (À comparer à : formel, informel.)

$ sensible *(sensitive)*
(I) Condition d'une ressource système telle que la perte de certaine propriété spécifiée de cette ressource, comme la confidentialité ou l'intégrité, aurait un effet contraire sur les intérêts ou les affaires de son possesseur ou utilisateur. (Voir : informations sensibles. À comparer à : critique.)

$ informations sensibles compartimentées (SCI, *sensitive compartmented information*)
(O) /Gouvernement des USA/ Informations classifiées concernant ou dérivée de sources de renseignements, de méthodes, ou de processus analytiques, dont il est exigé qu'elles soient traitées selon des systèmes de contrôle formels établis par le Directeur du renseignement central *(Central Intelligence)*. [C4009] (Voir : compartiment, SAP, SCIF. À comparer à : informations collatérales.)

$ facilités pour les informations sensibles compartimentées (SCIF, *sensitive compartmented information facility*)
(O) /Gouvernement des USA/ "Zone accréditée, pièce, groupe de pièces, bâtiments, ou installation ou les SCI peuvent être mémorisées, utilisées, discutées, et/ou traitées." [C4009] (Voir : SCI. À comparer à : clôture blindée.)

$ informations sensibles *(sensitive information)*
1. (I) Informations pour lesquelles (a) la divulgation, (b) l'altération, ou (c) la destruction ou la perte pourrait affecter de façon contraire les intérêts ou les affaires de leur possesseur ou utilisateur. (Voir : confidentialité des données, intégrité des données, sensible. À comparer à : classifié, critique.)
2. (O) /Gouvernement des USA/ Informations pour lesquelles (a) la perte, (b) le mauvais usage, (c) l'accès non autorisé, ou (d) la modification non autorisée pourrait affecter de façon contraire l'intérêt national ou la conduite de programmes fédéraux, ou la protection de la vie privée à laquelle ont droit les individus au titre du Privacy Act de 1974, mais qui n'ont pas été spécifiquement autorisées selon les critères établis par un ordre exécutif ou un Acte du Congrès pour être classifiées dans l'intérêt de la défense nationale ou de la politique étrangère.

Instructions : les systèmes qui ne sont pas des système de la sécurité nationales des U.S.A, mais qui contiennent des informations sensibles du gouvernement fédéral des U.S.A, doivent être protégés selon l'acte sur la sécurité informatique de

1987 (Loi publique 100-235). (Voir : sécurité nationale.)

$ étiquette de sensibilité *(sensitivity label)*
(D) Synonyme de "étiquette de classification".
Terme déconseillé : les IDOC NE DEVRAIENT PAS utiliser ce terme parce que la définition de "sensible" n'implique pas seulement la confidentialité des données, mais aussi l'intégrité des données.

$ niveau de sensibilité *(sensitivity level)*
(D) Synonyme de "niveau de classification".
Terme déconseillé : les IDOC NE DEVRAIENT PAS utiliser ce terme parce que la définition de "sensible" n'implique pas seulement la confidentialité des données, mais aussi l'intégrité des données.

$ séparation des tâches *(separation of duties)*
(I) Pratique consistant à diviser les étapes d'un processus système entre différentes entités individuelles (c'est-à-dire, différents utilisateurs ou différents rôles) afin d'empêcher qu'une seule entité agisse seule et soit capable de subvertir le processus. Usage : autrement dit "séparation de privilège". (Voir : sécurité administrative, contrôle duel.)

$ numéro de série *(serial number)* Voir : numéro de série de certificat.

$ Serpent
(O) Chiffrement de bloc symétrique de 128 bits conçu par Ross Anderson, Eli Biham, et Lars Knudsen comme candidat pour l'AES.

$ serveur *(server)*
(I) Entité système qui fournit un service en réponse aux demandes provenant d'autres entités système appelées clients.

$ unité de données de service (SDU, *service data unit*) (N) Voir : définition secondaire sous "unité de données de protocole".

$ session
1a. (I) /usage informatique/ Période continue, usuellement initiée par une connexion, durant laquelle un usager accède à un système informatique.
1b. (I) /activité informatique/ Ensemble des transactions ou autres activités informatiques qui sont effectuées par ou pour un usager durant une période d'utilisation d'un ordinateur.
2. (I) /contrôle d'accès/ Transposition temporaire d'un principal dans un ou plusieurs rôles. (Voir : contrôle d'accès fondé sur le rôle.)
Instructions : un usager établit une session en tant que principal et active un sous ensemble de rôles auxquels le principal a été affecté. Les autorisations disponibles pour le principal dans la session sont l'union des permissions de tous les rôles activés dans la session. Chaque session est associée à un seul principal et donc, à un seul usager. Un principal peut avoir plusieurs sessions concurrentes et peut activer un ensemble de rôles différents dans chaque session.
3. (I) /réseau informatique/ Association persistante mais (normalement) temporaire entre un agent d'utilisateur (normalement un client) et un second processus (normalement un serveur). L'association peut persister à travers plusieurs échanges de données, incluant plusieurs connexions. (À comparer à : association de sécurité.)

$ clé de session *(session key)*
(I) Dans le contexte du chiffrement symétrique, une clé qui est temporaire ou est utilisée pour une période relativement courte. (Voir : éphémère, KDC, session. À comparer à : clé maîtresse.)
Instructions : une clé de session est utilisés pour une période définie de communication entre deus entités ou composants système, comme pour la durée d'une seule connexion ou ensemble de transactions ; ou la clé est utilisée dans une application qui protège de relativement grandes quantités de données et donc a besoin d'être changée fréquemment.

$ SET(marque déposée) (O) Voir : SET Secure Electronic Transaction(marque déposée).

$ extension privée SET *(SET private extension)*
(O) Une des extensions privées définies par SET pour les certificats X.509. Porte des informations sur la clé racine hachée, le type de certificat, les données marchandes, les exigences de certificat du détenteur de carte, de la prise en charge du chiffrement pour le tunnelage, ou de la prise en charge de message pour les instructions de payement.

$ qualificatif SET *(SET qualifier)*
(O) Qualificatif de politique de certificat qui fournit des informations sur la localisation et le contenu d'une politique de certificat SET.

Instructions : à côté des politiques et des qualificatifs hérités de son propre certificat, chaque CA dans la hiérarchie de certification SET peut ajouter une déclaration qualifiante à la politique racine lorsque la CA produit un certificat. Le qualificatif supplémentaire est une politique de certificat pour cette CA. Chaque politique dans un certificat SET peut avoir ces qualificatifs : (a) un URL où une copie de la déclaration de politique peut se trouver ; (b) une adresse de messagerie électronique où peut se trouver une copie de la déclaration de politique, (c) un résultat de hachage de la déclaration de politique, calculé en utilisant l'algorithme indiqué, et (d) une déclaration présentant toute revendication associée à la production du certificat.

$ SET Secure Electronic Transaction(marque déposée) ou SET(marque déposée)
(N) Protocole développé conjointement par MasterCard International et Visa International et publié comme norme ouverte pour assurer la confidentialité des informations de transaction, l'intégrité des payements et l'authentification des participants à la transaction pour les transactions par carte de payement sur des réseaux non sûrs tels que l'Internet. [SET1] (Voir : acquéreur, marque, détenteur de carte, signature duelle, commerce électronique, IOTP, producteur, marchand, passerelle de payement, tiers.)
Instructions : ce terme et l'acronyme sont des marques commerciales de SETCo. MasterCard et Visa ont annoncé la norme SET le 1er février 1996.

$ SETCo
(O) Abréviation de "SET Secure Electronic Transaction LLC", formé le 19 décembre 1997 par MasterCard et Visa pour la mise en œuvre de la norme SET Secure Electronic Transaction(marque déposée). Un mémorandum d'accord ultérieur a ajouté American Express et JCB Credit Card Company comme copropriétaires de SETCo.

$ SHA, SHA-1, SHA-2 (N) Voir : Algorithme de hachage sécurisé.

$ identité partagée *(shared identity)* (I) Voir : définition secondaire sous "identité".

$ secret partagé *(shared secret)*
(D) Synonyme de "clé de chiffrement" ou "mot de passe".
Utilisation déconseillée : les IDOC qui utilisent ce terme DEVRAIENT en donner une définition parce que le terme est utilisé de nombreuses façons et pourrait facilement être mal compris.

$ clôture blindée *(shielded enclosure)*
(O) "Chambre ou conteneur conçu pour atténuer les radiations électromagnétiques, les signaux acoustiques, ou les émanations." [C4009] (Voir : émanation. À comparer à : SCIF.)

$ titre court *(short title)*
(O) "Combinaison identifiante de lettres et chiffres allouée à certains éléments de matériel COMSEC pour faciliter le traitement, la comptabilité et le contrôle." [C4009] (À comparer à : KMID, titre long.)

$ blinder *(shroud)*
(D) /verbe/ Chiffrer une clé privée, éventuellement de concert avec une politique qui empêche la clé d'être disponible en clair au delà d'un certain périmètre de sécurité bien défini. [PKC12] (Voir : chiffrer. À comparer à : sceller, envelopper.)
Terme déconseillé : les IDOC NE DEVRAIENT PAS utiliser ce terme comme défini ici, la définition duplique la signification d'autres termes standard. À la place, utiliser "chiffrer" ou une autre terminologie spécifique du mécanisme utilisé.

$ signer *(sign)* (I) Créer une signature numérique pour un objet de données. (Voir : signer.)

$ analyse du signal *(signal analysis)*
(I) Obtenir une connaissance indirecte (inférence) de données communiquées par la surveillance et l'analyse d'un signal qui est émis par un système et qui contient les données mais n'est pas destiné à communiquer les données. (Voir : émanation. À comparer à : analyse de trafic.)

$ intelligence du signal *(signal intelligence)*
(I) Science et pratique de l'extraction d'informations à partir des signaux. (Voir : sécurité du signal.)

$ sécurité du signal *(signal security)*
(N) (I) Science et pratique de la protection des signaux. (Voir : cryptologie, sécurité.)
Instructions : le terme "signal" note (a) une communication dans presque toutes les formes et aussi (b) les émanations pour d'autres propos, comme un radar. Sécurité du signal s'oppose à intelligence du signal, et chaque discipline inclut des sous

disciplines opposées comme suit [Kahn] :

Sécurité du signal	Intelligence du signal
1. Sécurité de communication	1. Intelligence de communication
1a. Cryptographie	1a. Cryptanalyse
1b. Sécurité du trafic	1b. Analyse du trafic
1c. Stéganographie	1c. Détection et interception
2. Sécurité électronique	2. Intelligence électronique
2a. Sécurité des émissions	2a. Reconnaissance électronique
2b. Contre-contremesures	2b. Contre-mesures

$ signature
(O) Symbole ou processus adopté ou exécuté par une entité système avec l'intention présente de déclarer qu'un objet de données est authentique. (Voir : signature numérique, signature électronique.)

$ certificat de signature *(signature certificate)*
(I) Certificat de clé publique qui contient une clé publique destinée à être utilisée pour vérifier des signatures numériques, plutôt que pour le chiffrement de données ou pour effectuer d'autres fonctions cryptographiques.
Instructions : un certificat de clé publique X.509 v3 peut avoir une extension "keyUsage" qui indique l'objet pour lequel est destinée la clé publique certifiée. (Voir : profil de certificat.)

$ récépissé signé *(signed receipt)*
(I) Service S/MIME [RFC2634] qui (a) fournit à l'origine d'un message une preuve de livraison du message et (b) permet à l'origine de démontrer à un tiers que le receveur a été capable de vérifier la signature du message d'origine.
Instructions : le récépissé est lié au message d'origine par une signature ; par conséquent, le service ne peut être demandé que pour un message signé. L'envoyeur du récépissé peut aussi facultativement chiffrer le récépissé pour assurer la confidentialité entre l'envoyeur et le receveur du récépissé.

$ signataire *(signer)*
(N) Personne ou organisation qui utilise une clé privée pour signer (c'est-à-dire, créer une signature numérique sur) un objet de données. [DSG]

$ SILS (N) Voir : normes pour la sécurité de LAN/MAN interopérables

$ simple authentification
1. (I) Processus d'authentification qui utilise un mot de passe comme information nécessaire pour vérifier une identité revendiquée par une entité. (À comparer à : authentification forte.)
2. (O) "Authentification au moyen d'arrangements de mots de passe simples." [X509]

$ Authentification simple et couche de sécurité (SASL, *Simple Authentication and Security Layer*)
(I) Spécification Internet [RFC2222], [RFC4422] pour ajouter un service d'authentification aux protocoles en mode connexion. (À comparer à : EAP, GSS-API.)
Instructions : pour utiliser SASL, un protocole comporte une commande pour authentifier un usager auprès d'un serveur et facultativement pour négocier la protection des interactions de protocole ultérieures. La commande désigne un mécanisme de sécurité enregistré. Les mécanismes SASL incluent Kerberos, GSS-API, S/KEY, et d'autres. Certains des protocoles qui utilisent SASL sont IMAP4 et POP3.

$ gestion de clé simple pour les protocoles Internet (SKIP, *Simple Key Management for Internet Protocols*)
(I) Protocole de distribution de clés qui utilise un chiffrement hybride pour porter les clés de session qui sont utilisées pour chiffrer les données dans les paquets IP. (Voir la référence à SKIP dans la [RFC2356].)
Instructions : SKIP a été conçu par Ashar Aziz et Whitfield Diffie de Sun Microsystems et proposé comme protocole standard de gestion de clés pour IPsec, mais IKE a été choisi à la place. Bien que IKE soit obligatoire pour une mise en œuvre de IPsec, l'utilisation de SKIP n'est pas exclue.
SKIP utilise l'algorithme Diffie-Hellman-Merkle (ou pourrait utiliser un autre algorithme d'accord de clés) pour générer une clé de chiffrement de clé à utiliser entre les deux entités. Une clé de session est utilisée avec un algorithme symétrique pour chiffrer les données dans un ou plusieurs paquets IP qui sont à envoyer d'une entité à l'autre. Une KEK symétrique est établie et utilisée pour chiffrer la clé de session, et la clé de session chiffrée est placée dans un en-tête SKIP qui est ajouté à chaque paquet IP qui est chiffré avec cette clé de session.

$ protocole simple de transfert de messagerie (SMTP, *Simple Mail Transfer Protocol*)
(I) Norme de protocole de l'Internet fondé sur TCP, de couche Application (RFC 821) pour déplacer les messages électroniques d'un ordinateur à l'autre.

$ protocole simple de gestion de réseau (SNMP, *Simple Network Management Protocol*)
(I) Norme de protocole de l'Internet (généralement) fondé sur UDP, de couche Application (RFC 3410 à 3418) pour convoyer les informations de gestion entre les composants de système qui agissent comme gestionnaires et agents.

$ infrastructure simple de clé publique (SPKI, *Simple Public Key Infrastructure*)
(I) Ensemble de concepts expérimentaux (RFC 2692, 2693) qui ont été proposés comme solution de remplacement aux concepts normalisés dans PKIX.

$ propriété de sécurité simple *(simple security property)*
(N) /modèle formel/ Propriété d'un système par laquelle un sujet n'a un accès réel à un objet que si l'habilitation du sujet domine la classification de l'objet. Voir : modèle de Bell-LaPadula.

$ guichet unique *(single sign-on)*
1. (I) Sous système d'authentification qui permet à un usager d'accéder à plusieurs composants de système connectés (comme des hôtes séparés sur un réseau) après une seule procédure de connexion sur un des composants. (Voir : Kerberos.)
2. (O) /Liberty Alliance/ Sous système de sécurité qui permet que soit authentifiée l'identité d'un usager chez un fournisseur d'identité -- c'est-à-dire, chez un service qui authentifie et certifie l'identité de l'usager -- et ensuite fait que cette authentification est honorée par les autres fournisseurs de service.

Instructions : un seul sous système de guichet unique exige normalement d'un usager qu'il suive la procédure de connexion une fois au début d'une session, et qu'ensuite durant la session il obtienne de façon transparente l'accès à plusieurs hôtes, applications, ou autres ressources système, protégés séparément, sans autre action de procédure de connexion de la part de l'usager (bien sûr, tant que l'usager ne se déconnecte pas). Un tel sous système a l'avantage de la facilité d'utilisation et de permettre de gérer l'authentification de façon cohérente au niveau de l'entreprise. Un tel sous système présente aussi l'inconvénient d'exiger que tous les composants soumis à l'accès dépendent de la sécurité des mêmes informations d'authentification.

$ identité singulière *(singular identity)* (I) Voir : définition secondaire sous "identité".

$ site
(I) Facilité -- c'est-à-dire, espace physique, pièce, ou bâtiment, avec ses éléments physiques, personnels, administratifs, et autres sauvegardes -- dans laquelle sont effectuées les fonctions système. (Voir : nœud.)

$ situation (I) Voir : situation. de sécurité.

$ SKEME (I) Protocole de distribution de clé à partir duquel des caractéristiques ont été adaptées pour IKE. [SKEME]

$ SKIPJACK
(N) Chiffrement de bloc de type 2, de 64 bits [SKIP], [RFC2773] avec une taille de clé de 80 bits. (Voir : CAPSTONE, CLIPPER, FORTEZZA, algorithme d'échange de clés.)
Instructions : SKIPJACK a été développé par la NSA et ensuite classifié au niveau "Secret" par le U.S. DoD . Le 23 juin 1998, la NSA a annoncé que SKIPJACK avait été déclassifié.

$ créneau *(slot)*
(O) /MISSI/ Une des zones de mémorisation de la carte PC FORTEZZA qui sont chacunes capables de contenir un certificat X.509 plus d'autres données, y compris la clé privée qui est associée à un certificat de clé publique.

$ carte à mémoire *(smart card)*
(I) Appareil de la taille d'une carte de crédit qui contient une ou plusieurs puces de circuits intégrés qui effectuent les fonctions d'un processeur central, de mémoire et d'interface d'entrée/sortie d'ordinateur. (Voir : carte PC, jeton intelligent.)
Usage : ce terme est parfois utilisé de façon assez stricte pour signifier une carte qui se conforme étroitement aux dimensions et apparence de la carte de crédit en plastique produite par les banques et les commerçants. D'autres fois, le terme est utilisé de façon large pour inclure des cartes qui sont plus grandes que des cartes de crédit, en particulier plus épaisses, comme les cartes PC.

$ jeton intelligent *(smart token)*
(I) Appareil qui se conforme à la définition de "carte à mémoire" sauf que plutôt que d'avoir les dimensions standard d'une carte de crédit, le jeton est formaté autrement, comme dans une étiquette de chien de guerre, ou une clé de porte. (Voir : carte à mémoire, jeton cryptographique.)

$ attaque par surcharge *(smurf attack)*
(D) /argot/ Attaque de déni de service qui utilise l'adressage en diffusion IP pour envoyer des paquets de ping ICMP dans l'intention d'inonder un système. (Voir : fraggle attack, inondation ICMP.)
Terme déconseillé : il est vraisemblable que les autres cultures utilisent des métaphores différentes pour ce concept. Donc, pour éviter l'incompréhension entre les nations, les IDOC NE DEVRAIENT PAS utiliser ce terme.
Dérivation : les Smurfs sont une race fictive de petites créatures bleues qui ont été créées par un dessinateur de bande dessinée. Peut-être que l'inventeur de cette attaque pensait qu'une invasion de paquets ping ressemblait à une bande de smurfs. (Voir : Utilisation déconseillée sous "Livre Vert".)
Instructions : l'attaquant envoie des paquets de demande d'écho ICMP ("ping") qui paraissent avoir pour origine non pas la propre adresse IP de l'attaquant, mais l'adresse de l'hôte ou routeur qui et la cible de l'attaque. Chaque paquet est adressé à une adresse de diffusion IP, par exemple, à toutes les adresses IP d'un certain réseau. Donc, chaque demande d'écho qui est envoyée par l'attaquant résulte en l'envoi de nombreuses réponses d'écho à l'adresse cible. Cette attaque peut interrompre le service d'un hôte particulier, chez les hôtes qui dépendent d'un certain routeur, ou d'un réseau entier.

$ sneaker net
(D) /argot/ Processus qui transfère des données entre systèmes seulement de façon manuelle, sous contrôle humain ; c'est-à-dire, un processus de transfert de données qui implique une rupture de continuité.
Terme déconseillé : il est vraisemblable que les autres cultures utilisent des métaphores différentes pour ce concept. Donc, pour éviter l'incompréhension entre les nations, les IDOC NE DEVRAIENT PAS utiliser ce terme.

$ Snefru
(N) Fonction de hachage cryptographique du domaine public (autrement dit "la fonction de hachage sûr de Xerox") conçue par Ralph C. Merkle de Xerox Corporation. Snefru peut produire un résultat de 128 bits ou de 256 bits (c'est-à-dire, un résultat de hachage). [Schn] (Voir : Khafre, Khufu.)

$ renifflage *(sniffing)*
(D) /argot/ Synonyme de "écoute passive", se réfère le plus souvent à la capture et l'examen des paquets de données portés sur un LAN. (Voir : renifflage de mot de passe.)
Terme déconseillé : les IDOC NE DEVRAIENT PAS utiliser ce terme ; il duplique sans nécessité la signification d'un terme qui est mieux établi. (Voir : Utilisation déconseillée sous "Livre Vert".

$ ingénierie sociale *(social engineering)*
(D) Euphémisme pour des méthodes non techniques ou de technologie inférieure, impliquant souvent la tricherie ou la fraude, qui sont utilisées pour attaquer des systèmes d'information. Exemple : hameçonnage .
Terme déconseillé : les IDOC NE DEVRAIENT PAS utiliser ce terme ; il est trop vague. À la place, utiliser un terme spécifique des moyens de l'attaque, par exemple, chantage, corruption, coercition, usurpation d'identité, intimidation, mensonge, ou vol.

$ sécurisé sur Kerberos fondé sur des accréditifs (SOCKS, *Secured Over Credential-based Kerberos*)
(I) Protocole Internet [RFC1928] qui fournit un serveur mandataire généralisé qui permet à des applications client-serveur (par exemple, TELNET, FTP, ou HTTP, fonctionnant sur TCP ou UDP) d'utiliser les services d'un pare-feu.
Instructions : SOCKS est mis en couche en dessous de la couche Application IPS et au dessus de la couche Transport. Lorsque un client à l'intérieur d'un pare-feu souhaite établir une connexion avec un objet qui n'est accessible qu'à travers le pare-feu, il utilise TCP pour se connecter au serveur SOCKS, négocie avec le serveur la méthode d'authentification à utiliser, s'authentifie avec la méthode choisie, et envoie alors une demande relais. Le serveur SOCKS évalue la demande, normalement sur la base des adresses de source et de destination, et établit la connexion appropriée, ou la refuse.

$ tempête logicielle *(soft TEMPEST)*
(O) Utilisation de techniques logicielles pour réduire la fuite d'informations radio fréquences des écrans et claviers d'ordinateur. [Kuhn] (Voir : TEMPEST.)

$ jeton logiciel *(soft token)*
(D) Objet de données qui est utilisé pour le contrôle d'accès ou authentifier une autorisation. (Voir : jeton.)
Terme déconseillé : les IDOC NE DEVRAIENT PAS utiliser ce terme comme défini ici ; la définition duplique la signification d'autres termes standard. À la place, utiliser "certificat d'attribut" ou un autre terme spécifique du mécanisme utilisé.

$ logiciel *(software)*
(I) Programmes d'ordinateur (qui sont mémorisés et exécutés par un matériel informatique) et leurs données associées (qui sont aussi mémorisées dans le matériel) qui peuvent être écrits ou modifiés de façon dynamique pendant l'exécution. (À

comparer à : progiciel.)

$ erreur logicielle *(software error)*
(I) /action de menace/ Voir : définitions secondaires sous "corruption", "exposition", et "incapacitation".

$ authentification de source *(source authentication)*
(D) Synonyme de "authentification de l'origine des données" ou "authentification de l'entité homologue". (Voir : authentification de l'origine des données, authentification de l'entité homologue).
Terme déconseillé : les IDOC NE DEVRAIENT PAS utiliser ce terme parce qu'il est ambigu et, dans l'un et l'autre sens, duplique la signification de termes internationalement normalisés. Si l'intention est d'authentifier le créateur original ou le paqueteur des données reçues, utiliser alors "authentification de l'origine des données". Si l'intention est d'authentifier l'identité de l'envoyeur des données dans l'instance en cours, utiliser alors "authentification de l'entité homologue".

$ intégrité de source *(source integrity)*
(I) Propriété que les données sont dignes de confiance (c'est-à-dire, on peut s'y fier ou leur faire confiance) sur la base de la confiance qu'on peut accorder à ses sources et à la confiance dans les procédures utilisées pour traiter les données dans le système.
Usage : autrement dit intégrité Biba. (Voir : intégrité. À comparer à : intégrité correcte, intégrité des données.)
Instructions : pour cette sorte d'intégrité, il y a des modèles formels de modification non autorisée (voir : modèle Biba) qui complètent logiquement les modèles plus familiers de divulgation non autorisée (voir : modèle de Bell-LaPadula). Dans ces modèles, les objets sont étiquetés pour indiquer la crédibilité des données qu'ils contiennent, et il y a des règles pour le contrôle d'accès qui dépendent des étiquettes.

$ envoi de pourriels *(spam)*
1a. (I) /argot verbe/ Envoyer sans discrimination de messages non sollicités, non désirés, non pertinents ou inappropriés, en particulier d'annonces commerciales en quantités massives.
1b. (I) /argot nom/ Electronic "junk mail". [RFC2635]
Utilisation déconseillée : les IDOC NE DEVRAIENT PAS utiliser ce terme en majuscules, parce que SPAM(marque déposée) est une marque déposée de Hormel Foods Corporation. Hormel dit, "Non n'avons pas d'objection à l'utilisation de ce terme d'argot [spam] pour décrire [des messages électroniques d'annonces non sollicitées], bien que non fassions des objections à l'utilisation de l'image de notre produit en association avec ce terme. Aussi, si le terme doit être utilisé, il DEVRAIT l'être tout en minuscules pour le distinguer de notre marque déposée SPAM, qui DEVRAIT être utilisée tout en majuscules." (Voir : métadonnées.)
Instructions : en volume suffisant, le pourriel peut causer un déni de service. (Voir : inondation.) Selon Hormel, le terme a été adopté par suite d'une saynète des Monty Python dans laquelle un groupe de vikings chantait un chœur de 'SPAM, SPAM, SPAM ...' crescendo, noyant toute autre conversation. Cette chanson est devenue une métaphore pour les messages d'annonce non sollicités qui menacent de couvrir tout autre discours sur l'Internet.

$ programme à accès réservé (SAP, *special access program*)
(O) /Gouvernement des USA/ "Programme sensible, [qui est] approuvé par écrit par un directeur d'agence avec [c'est-à-dire, qui a] une autorité de classification originale de top secret [et] qui impose un besoin de savoir et des contrôles d'accès au delà de ceux normalement fournis pour l'accès aux informations Confidentielles, Secret, ou Top Secret. Le niveau de contrôle se fonde sur la criticité du programme et la menace supposées de renseignement hostile. Le programme peut être un programme d'acquisition, ou un programme de renseignement, ou un programme d'opérations et de soutien." [C4009] (Voir : approbation d'accès formelle, SCI. À comparer à : informations collatérales.)

$ clé éclatée *(split key)*
(I) Clé de chiffrement qui est générée et distribuée comme deux éléments de données séparées ou plus, qui ne portent individuellement aucune connaissance de la clé totale qui résulte de la combinaison des éléments. (Voir : contrôle duel, connaissance éclatée.)

$ connaissance éclatée *(split knowledge)*
1. (I) Technique de sécurité dans laquelle deux entités ou plus détiennent séparément des éléments de données qui ne portent individuellement aucune connaissance des informations qui résultent de la combinaison des éléments. (Voir : contrôle duel, clé éclatée.)
2. (O) "Condition sous laquelle deux entités ou plus ont séparément les composants d'une clé [qui] ne portent individuellement aucune connaissance de la clé source [qui] sera produite lorsque les composants de la clé sont combinés dans le module cryptographique." [FP140]

$ usurpation *(spoof)* (I) /action de menace/ Voir : définition secondaire sous "mascarade".

$ attaque par usurpation *(spoofing attack)* (I) Synonyme de "attaque par mascarade".

$ étalement de spectre *(spread spectrum)*
(N) Technique TRANSEC qui transmet un signal dans une bande passante bien plus large que ce que nécessitent les informations transmises. [F1037] Exemple : saut de fréquence.
Instructions : utilise généralement une structure de signal séquentielle, ressemblant à du brouillage pour étaler le signal des information normalement en bande étroite sur une bande de fréquences relativement large. Le receveur corrèle les signaux pour restituer le signal des informations d'origine. Cette technique diminue les interférence potentielles avec d'autres receveurs, tout en réalisant la confidentialité des données et en augmentant l'immunité des receveurs de spectre étalé aux brouillages et interférences.

$ logiciel espion *(spyware)*
(D) /argot/ Logiciel qu'un intrus a installé subrepticement sur un ordinateur en réseau pour rassembler des données à partir de cet ordinateur et les envoyer à travers le réseau à l'intrus ou autre partie intéressée. (Voir : logique malveillante, cheval de Troie.)
Utilisation déconseillée : les IDOC qui utilisent ce terme DEVRAIENT en donner une définition parce que le terme est utilisé de nombreuses façons et pourrait facilement être mal compris.
Instructions : certains exemples des types de données qui pourraient être collectées par un logiciel espion sont les fichiers d'application, les mots de passe, les adresses de messagerie électronique, les historiques d'usage, et les frappes de touches. Des exemples des motifs de collecte des données sont le chantage, la fraude financière, le vol d'identité, l'espionnage industriel, les études de marché, et le voyeurisme.

$ SSH(marque déposée) (N) Voir : Secure Shell(marque déposée).

$ PIN SSO *(SSO PIN)*
(O) /MISSI/ Un des deux PIN qui contrôlent l'accès aux fonctions et aux données mémorisées d'une carte PC FORTEZZA. La connaissance du PIN SSO permet à l'utilisateur de carte d'effectuer les fonctions FORTEZZA dont l'utilisation est prévue par l'utilisateur final et aussi les fonctions dont l'utilisation est prévue par une CA MISSI. (Voir : PIN d'utilisateur.)

$ ORA de PIN SSO (SORA, *SSO-PIN ORA*)
(O) /MISSI/ RA organisationnelle MISSI qui fonctionne dans un mode dans lequel l'ORA effectue toutes les fonctions de gestion de carte, et donc exige la connaissance du PIN SSO PIN pour les cartes PC FORTEZZA produites à l'utilisateur final.

$ normes d'interopérabilité de la sécurité LAN/MAN (SILS, *Standards for Interoperable LAN/MAN Security*)
1. (N) Comité de normalisation IEEE 802.10. (Voir : [FP191].)
2. (N) Ensemble de normes de l'IEEE qui est en huit parties : (a) Modèle, incluant la gestion de la sécurité, (b) protocole d'échange sûr de données, (c) gestion de clés, (d) [a été incorporé dans (a)], (e) SDE sur Ethernet 2.0, (f) gestion de la sous couche SDE, (g) étiquettes de sécurité SDE, et (h) PICS de conformité de SDE. Les parties b, e, f, g, et h sont incorporées dans la norme IEEE 802.10-1998.

$ propriété étoile *(star property)* (N) Voir : propriété-*.

$ attaque Star Trek *(attack Star Trek)*
(D) /argot/ Attaque qui pénètre un système où aucune attaque n'était parvenue jusqu'alors.
Utilisation déconseillée : les IDOC NE DEVRAIENT PAS utiliser ce terme ; c'est un mot pour les amateurs de "space opera". (Voir : Utilisation déconseillée sous "Livre Vert".)

$ statique *(static)*
(I) /adjectif/ Se réfère à une clé de chiffrement ou autre paramètre qui est d'une relativement longue durée de vie. (À comparer à : éphémère.)

$ stéganographie *(steganography)*
(I) Méthodes pour cacher l'existence d'un message ou d'autres données. C'est différent de la cryptographie, qui cache la signification d'un message mais ne cache pas le message lui-même. Exemples : pour les méthodes classiques, physiques, voir [Kahn] ; pour les méthodes modernes, numériques, voir [John]. (Voir : cryptologie. À comparer à : système de dissimulation, marquage numérique effaçable.)

$ canal de mémorisation *(storage channel)* (I) Voir : canal de mémorisation couvert.

$ clé de mémorisation *(storage key)*
(I) Clé de chiffrement utilisée par un appareil pour protéger des informations qui sont conservées dans l'appareil, par opposition à la protection des informations qui sont transmises entre des appareils. (Voir : jeton cryptographique, copie de jeton. À comparer à : clé de trafic.)

$ chiffrement de flux *(stream cipher)*
(I) Algorithme de chiffrement qui coupe le texte source en un flux d'éléments successifs (normalement des bits) et chiffre le nième élément de texte source avec le nième élément d'un flux de clé parallèle, convertissant ainsi le flux de texte source en un flux de texte chiffré. [Schn] (Voir : chiffrement de bloc.)

$ service d'intégrité de flux *(stream integrity service)*
(I) Service d'intégrité des données qui préserve l'intégrité pour une séquence de paquets de données, incluant à la fois (a) l'intégrité du datagramme bit par bit de chaque paquet individuel dans l'ensemble, et (b) l'intégrité séquentielle paquet par paquet de l'ensemble comme un tout. (Voir : intégrité des données. À comparer à : service d'intégrité de datagramme.)
Instructions : certaines applications d'inter réseau ont seulement besoin de l'intégrité des datagrammes, mais d'autres exigent aussi que le flux entier des paquets soit protégé contre l'insertion, le réarrangement, la suppression, et le retard :
- "Insertion" : la destination reçoit un paquet supplémentaire qui n'a pas été envoyé par la source.
- "Réarrangement" : la destination reçoit des paquets dans un ordre différent de celui dans lequel ils ont été envoyés par la source.
- "Suppression" : un paquet envoyé par la source n'est jamais livré à la destination prévue.
- "Retard" : un paquet est retenu pendant une certaine durée à un relais, entravant et retardant ainsi la livraison normale du paquet entre la source et la destination.

$ force *(strength)*
1. (I) /cryptographie/ Niveau de résistance d'un mécanisme cryptographique aux attaques [RFC3766]. (Voir : entropie, fort, facteur de travail.)
2. (N) /Critères communs/ La "force d'une fonction" est une "qualification d'une fonction de sécurité d'une TOE qui exprime le minimum d'efforts supposés nécessaire pour vaincre un comportement de sécurité attendu par une attaque directe de ses mécanismes de sécurité sous-jacents" : (Voir : fort.)
- de base : "niveau de la force d'une fonction d'une TOE lorsque l'analyse montre que la fonction fournit une protection adéquate contre une rupture fortuite de la sécurité de la TOE par des attaquants possédant un faible potentiel d'attaque."
- moyen : "... contre une rupture directe ou intentionnelle ... par des attaquants possédant un potentiel d'attaque modéré."
- élevé : "... contre une rupture délibérément planifiée ou organisée ... par des attaquants possédant un fort potentiel d'attaque."

$ fort *(strong)*
1. (I) /cryptographie/ Utilisé pour décrire un algorithme de chiffrement qui exigerait une grande quantité de puissance de calcul pour le vaincre. (Voir : force, facteur de travail, clé faible.)
2. (I) /COMPUSEC/ Utilisé pour décrire un mécanisme de sécurité qui serait difficile à vaincre. (Voir : force, facteur de travail.)

$ authentification forte *(strong authentication)*
1. (I) Processus d'authentification qui utilise un mécanisme de sécurité cryptographique -- en particulier des certificats de clé publique -- pour vérifier l'identité revendiquée par une entité. (À comparer à : simple authentification.)
2. (O) "Authentification au moyen d'accréditifs déduits cryptographiquement." [X509]

$ sujet *(subject)*
1a. (I) Processus dans un système informatique qui représente un principal et qui s'exécute avec les privilèges qui ont été accordés à ce principal. (À comparer à : principal, usager.)
1b. (I) /modèle formel/ Entité système qui cause l'écoulement des informations entre les objets ou change l'état du système ; techniquement, une paire processus-domaine. Un sujet peut lui-même être un objet par rapport à un autre sujet ; donc, l'ensemble des sujets dans un système est un sous ensemble de l'ensemble des objets. (Voir : modèle de Bell-LaPadula, objet.)
2. (I) /certificat numérique/ Nom (d'une entité système) qui est lié aux éléments de données dans un certificat numérique ; par exemple, un DN qui est lié à une clé dans un certificat de clé publique. (Voir : X.509.)

$ CA sujette *(subject CA)*
(D) CA qui est le sujet d'un certificat croisé produit par une autre CA. [X509] (Voir : certification croisée.)
Terme déconseillé : les IDOC NE DEVRAIENT PAS utiliser ce terme parce qu'il n'est pas largement connu et pourrait être mal compris. À la place, dire "la CA qui est le sujet du certificat croisé".

$ sous réseau *(subnetwork)*
(N) Terme OSI pour un système de relais de paquets et de liaisons de connexion qui mettent en œuvre la couche 2 ou 3 d'OSIRM pour fournir un service de communication qui interconnecte les systèmes d'extrémité rattachés. Généralement, les relais sont tous du même type (par exemple, des commutateurs de paquets X.25, ou des unités d'interface dans un LAN IEEE 802.3). (Voir : passerelle, internet, routeur.)

$ CA subordonnée (SCA, *subordinate CA*)
1. (I) CA dont le certificat de clé publique est produit par une autre CA (supérieure). (Voir : hiérarchie de certification. À comparer à : certification croisée.)
2. (O) /MISSI/ Quatrième niveau (c'est-à-dire, du bas) d'une hiérarchie de certification MISSI ; une CA MISSI dont le certificat de clé publique est signé par une CA MISSI plutôt que par une PCA MISSI. Une SCA MISSI est l'autorité administrative pour une sous unité d'une organisation, établie lorsque il est souhaitable de répartir organisationnellement ou de décentraliser le service de CA. Le terme se réfère aussi bien au bureau ou rôle d'autorisation qu'à la personne qui tient ce bureau. Une SCA MISSI enregistre les utilisateurs finaux et produit leurs certificats et peut aussi enregistrer des ORA, mais ne peut pas enregistrer d'autres CA. Une SCA produit périodiquement une CRL.

$ DN subordonné *(subordinate DN)*
(I) Un DN X.500 est subordonné à un autre DN X.500 si il commence par un ensemble d'attributs qui sont les mêmes que le second DN entier excepté l'attribut terminal du second DN (qui est généralement le nom d'une CA). Par exemple, le DN <C=FooLand, O=Gov, OU=Treasurer, CN=DukePinchpenny> est subordonné au DN <C=FooLand, O=Gov, CN=KingFooCA>.

$ abonné *(subscriber)*
(I) /PKI/ Usager qui est enregistré dans une PKI et donc peut être désigné dans le champ "sujet" d'un certificat produit par une CA dans cette PKI. (Voir : enregistrement, usager.)
Usage : ce terme est nécessaire pour distinguer les usagers enregistré de deux autres sortes d'usagers de PKI :
- Usagers qui accèdent à la PKI mais ne sont pas identifié chez elle : par exemple, un consommateur d'assertions peut accéder à un répertoire de PKI pour obtenir le certificat d'un tiers. (Voir : accès.)
- Usagers qui n'accèdent pas à la PKI : par exemple, un consommateur d'assertions (voir : utilisateur de certificat) peut utiliser un certificat numérique qui a été obtenu d'une base de données qui ne fait pas partie de la PKI qui a produit le certificat.

$ substitution
1. (I) /cryptographie/ Méthode de chiffrement dont les éléments du texte source conservent leur position séquentielle mais sont remplacés par des éléments de texte chiffré. (À comparer à : transposition.)
2. (I) /action de menace/ Voir : définition secondaire sous "falsification".

$ sous système *(subsystem)*
(I) Collection de composants de système en rapport qui ensemble effectuent une fonction du système ou délivrent un service du système.

$ super chiffrement *(superencryption)*
(I) Opération de chiffrement pour laquelle l'entrée de texte source à transformer est le résultat chiffré d'une opération de chiffrement précédente. (À comparer à : chiffrement hybride.)

$ super utilisateur *(superuser)* (I) /UNIX/ Synonyme de "racine".

$ capacité à survivre *(survivability)*
(I) Capacité d'un système à rester en fonctionnement ou existence en dépit de conditions défavorables, incluant des occurrences naturelles, des actions accidentelles, et des attaques. (À comparer à : disponibilité, fiabilité.)

$ swIPe
(I) Protocole de chiffrement pour IP qui assure la confidentialité, l'intégrité, et l'authentification et peut être utilisé pour la sécurité de bout en bout comme de bond intermédiaire. [Ioan] (À comparer à : IPsec.)
Instructions : le protocole swIPe est un prédécesseur de IP qui n'est concerné que par les mécanismes de chiffrement ; la politique et la gestion de clé sont traitées en dehors du protocole.

$ syllabaire *(syllabary)*
(N) /chiffrement/ Liste de lettres individuelles, combinaisons de lettres, ou de syllabes, avec leurs groupes de code équivalents, utilisés pour épeler les noms propres ou autres mots non usuels qui ne sont pas présents dans le vocabulaire de base (c'est-à-dire, ne sont pas dans le livre de code) d'un code utilisé pour le chiffrement.

$ chiffrement symétrique *(symmetric cryptography)*
(I) Branche de la cryptographie dans laquelle les algorithmes utilisent la même clé pour les deux contreparties de l'opération cryptographique (par exemple, le chiffrement et le déchiffrement). (Voir : chiffrement asymétrique. À comparer à : cryptographie à clé secrète.)
Instructions : le chiffrement symétrique a été utilisé pendant des milliers d'années [Kahn]. Un exemple moderne est AES.
Le chiffrement symétrique présente un inconvénient par rapport au chiffrement asymétrique à l'égard de la distribution de clé. Par exemple, lorsque Alice veut assurer la confidentialité des données qu'elle envoie à Bob, elle chiffre les données avec une clé, et Bob utilise la même clé pour déchiffrer. Cependant, conserver la clé partagé comporte à la fois des coûts et des risques lorsque la clé est distribuée à la fois à Alice et à Bob. (Voir : distribution de clé, gestion de clé.)

$ clé symétrique *(symmetric key)*
(I) Clé de chiffrement qui est utilisée dans un algorithme de chiffrement symétrique. (Voir : chiffrement symétrique.)

$ inondation de SYN *(SYN flood)*
(I) Attaque de déni de service qui envoie un grand nombre de paquets TCP SYN (synchroniser) à un hôte dans l'intention d'interrompre le fonctionnement de cet hôte. (Voir : attaque aveugle, inondation.)
Instructions : cette attaque cherche à exploiter une vulnérabilité de la spécification TCP ou d'une mise en œuvre de TCP. Normalement, deux hôtes utilisent un triple échange de paquets pour établir une connexion TCP : (a) l'hôte 1 demande une connexion en envoyant un paquet SYN à l'hôte 2 ; (b) l'hôte 2 répond par l'envoi d'un paquet SYN-ACK (accusé de réception) à l'hôte 1 ; et (c) l'hôte 1 achève la connexion en envoyant un paquet ACK à l'hôte 2. Pour attaquer l'hôte 2, l'hôte 1 peut envoyer une séries de messages SYN TCP, chacun ayant une adresse de source factice différente. (La [RFC2827] expose comment utiliser le filtrage de paquets pour empêcher que de telles attaques soient lancées depuis l'arrière d'un point d'agrégation d'un fournisseur d'accès Internet.) L'hôte 2 traite chaque SYN comme une demande d'un hôte distinct, répond à chacune avec un SYN-ACK, et attend de recevoir les ACK correspondants. (L'attaquant peut utiliser des adresses de source aléatoires ou injoignables dans les paquets SYN, ou peut utiliser des adresses de source qui appartiennent à des tiers, qui deviennent alors des victimes secondaires.)
Pour chaque SYN-ACK envoyé, le processus TCP dans l'hôte 2 a besoin d'un certain espace mémoire pour mémoriser les informations d'état pendant qu'il attend que l'ACK correspondant soit retourné. Si l'ACK correspondant n'arrive jamais à l'hôte 2, un temporisateur associé au SYN-ACK en attente va finalement arriver à expiration et libérer l'espace. Mais si l'hôte 1 (ou un groupe d'hôtes qui coopèrent) peut rapidement envoyer de nombreux SYN à l'hôte 2, celui-ci va avoir besoin de mémoriser les informations d'état pour de nombreux SYN-ACK en instance et peut arriver à manquer d'espace. Ceci peut empêcher l'hôte 2 de répondre à des demandes de connexion légitimes provenant d'autre hôtes, ou même, si il y a des fautes dans la mise en œuvre TCP de l'hôte 2, de le mettre en panne lorsque l'espace disponible sera épuisé.

$ synchronisation *(synchronization)*
(I) Toute technique par laquelle un processus de déchiffrement receveur atteint un état interne qui correspond au processus d'émission (de chiffrement) c'est-à-dire, qui a le matériel de chiffrement approprié pour traiter le texte chiffré et est correctement initialisé pour le faire.

$ système *(system)*
(I) Synonyme de "système d'information".
Usage : c'est une définition générique, et c'est celle avec laquelle ce terme est utilisé dans le présent glossaire. Cependant, les IDOC qui utilisent le terme, en particulier les IDOC qui sont des spécifications de protocole, DEVRAIENT donner une définition plus spécifique. Aussi, les IDOC qui spécifient des dispositifs, des services, et des assurances de sécurité doivent définir quels composants de système et quelles ressources système sont à l'intérieur du périmètre de sécurité applicable et celles qui sont à l'extérieur. (Voir : architecture de sécurité.)

$ architecture de système *(system architecture)*
(N) Structure des composants d'un système, leurs relations, et les principes et lignes directrices qui gouvernent leur conception et leur évolution dans le temps. [DoD10] (À comparer à : architecture de sécurité.)

$ composant système *(system component)*
1. (I) Collection de ressources système qui (a) forme la partie physique ou logique du système, (b) a les fonctions et interfaces spécifiées, et (c) est traitée (par exemple, par les politiques ou spécifications) comme existant indépendamment des autres parties du système. (Voir : sous-système.)
2. (O) /ITSEC/ Partie identifiable et auto contenue d'une TOE.

Usage : un composant est un terme relatif parce que les composants peuvent être incorporés ; c'est-à-dire, un composant d'un système peut-être une partie d'un autre composant de ce système.
Instructions : les composants peuvent être caractérisés comme suit :
- un "composant physique" a une masse et prend de la place ;

- un "composant logique" est une abstraction utilisée pour gérer et coordonner des aspects de l'environnement physique, et représente normalement un ensemble d'états ou capacités du système.

$ entité système *(system entity)*
(I) Partie active d'un système -- personne, ensemble de personnes (par exemple, une sorte d'organisation) un processus automatique, ou un ensemble de processus (voir : sous système) -- qui a un ensemble spécifique de capacités. (À comparer à : sujet, usager.)

$ à hauteur du système *(system high)*
(I) Le plus haut niveau de sécurité auquel fonctionne, ou est capable de fonctionner un système, à un instant particulier ou dans un environnement particulier. (Voir : mode de sécurité à hauteur du système.)

$ mode de sécurité à hauteur du système *(system-high security mode)*
(I) Mode de fonctionnement d'un système dans lequel tous les utilisateurs qui ont accès au système possèdent toutes les autorisations nécessaires (à la fois en niveau d'habilitation et en approbation formelle d'accès) pour toutes les données traitées par le système, mais certains utilisateurs peuvent ne pas avoir le besoin de savoir pour toutes les données. (Voir : /fonctionnement de système/ sous "mode", approbation formelle d'accès, niveau de protection, niveau d'habilitation.)
Usage : généralement abrégé en "mode de hauteur système". Ce mode a été défini dans la politique de l'U.S. DoD qui s'appliquait à l'accréditation de système, mais ce terme est largement utilisé en dehors du gouvernement.

$ intégrité du système *(system integrity)*
1. (I) Attribut ou qualité "qu'a un système lorsque il peut effectuer sans entrave la fonction à laquelle il est destiné, et libre de toute manipulation non autorisée délibérée ou involontaire." [C4009], [NCS04] (Voir : récupération, service d'intégrité de système.)
2. (D) "Qualité d'un [système d'information] qui reflète la correction et la fiabilité logique du système d'exploitation ; la complétude logique du matériel et du logiciel qui mettent en œuvre les mécanismes de protection, et la cohérence des structures de données et l'occurrence des données mémorisées." [tiré d'une ancienne version de C4009]

Définition déconseillée : les IDOC NE DEVRAIENT PAS utiliser la définition 2 parce qu'elle mélange plusieurs concepts d'une façon potentiellement trompeuse. À la place, les IDOC DEVRAIENT utiliser le terme avec la définition 1 et, selon ce que l'on veut dire, coupler le terme avec des termes supplémentaires, plus spécifiquement descriptifs et informatifs, comme "correction", "fiabilité", et "intégrité des données".

$ service d'intégrité du système *(system integrity service)*
(I) Service de sécurité qui protège les ressources système d'une manière vérifiable contre les changements non autorisés ou accidentels, la perte ou la destruction. (Voir : intégrité du système.)

$ le plus bas du système *(system low)*
(I) Le plus bas niveau de sécurité supporté par un système à un instant particulier ou dans un environnement particulier. (À comparer à : à hauteur du système.)

$ ressource système *(system resource)*
(I) Données contenues dans un système d'information; ou un service fourni par un système, ou une capacité d'un système, comme la puissance de traitement ou la bande passante de communication, ou un élément d'un équipement d'un système (c'est-à-dire, du matériel, progiciel, logiciel ou la documentation) ou une facilité qui héberge les opérations et l'équipement du système. (Voir : composant de système.)

$ officier de sécurité système (SSO, *system security officer*)
(I) Personne responsable de la mise en application ou de l'administration de la politique de sécurité qui s'applique à un système. (À comparer à : gestionnaire, opérateur.)

$ utilisateur du système *(system user)*
(I) Entité système qui consomme un produit ou service fourni par le système, ou qui accède et emploie des ressources système pour produire un produit ou service du système. (Voir : accès, [RFC2504]. À comparer à : utilisateur autorisé, gestionnaire, opérateur, principal, utilisateur privilégié, sujet, abonné, entité système, utilisateur non autorisé.)
Usage : les IDOC qui utilisent ce terme DEVRAIENT en donner une définition parce que le terme est utilisé de nombreuses façons et pourrait facilement être mal compris :
- ce terme se réfère généralement à une entité qui a été autorisée à accéder au système, mais le terme est parfois utilisé sans égard à l'autorisation d'accès.
- ce terme se réfère généralement à une personne vivante qui agit soit personnellement, soit dans un rôle organisationnel. Cependant, le terme peut aussi se référer à un processus automatique sous la forme d'un matériel, d'un logiciel ou

progiciel, à un ensemble de personnes, ou à un ensemble de processus.
- Les IDOC NE DEVRAIENT PAS utiliser ce terme pour se référer à un ensemble mixte contenant à la fois des personnes et des processus. Cette exclusion est destinée à empêcher des situations qui pourraient causer l'interprétation d'une politique de sécurité de deux façons différentes et contradictoires.

Un utilisateur système peut être caractérisé comme direct ou indirect :
- "utilisateur passif" : une entité système qui est (a) en dehors du périmètre de sécurité du système *et* (b) peut recevoir des résultats du système mais ne peut pas lui fournir des entrées ou interagir autrement avec le système.
- "utilisateur actif" : une entité système qui est (a) à l'intérieur du périmètre de sécurité du système *ou* (b) peut fournir des entrées ou interagir autrement avec le système.

$ TACACS+
(I) Protocole fondé sur TCP qui améliore TACACS en séparant les fonctions d'authentification, d'autorisation, et de comptabilité en chiffrent tout le trafic entre le serveur d'accès réseau et le serveur d'authentification. TACACS+ est extensible pour permettre d'utiliser tout mécanisme d'authentification avec les clients TACACS+.

$ falsifier *(tamper)*
(I) Faire une modification non autorisée dans un système qui altère le fonctionnement du système d'une façon qui dégrade les services de sécurité que le système avait l'intention de fournir. (Voir : QUADRANT. À comparer aux définitions secondaires sous "corruption" et "mauvaise utilisation".)

$ évidemment falsifié *(tamper-evident)*
(I) Caractéristique d'un composant de système qui donne la preuve qu'une attaque a été tentée sur ce composant ou système. Usage : implique généralement une preuve physique . (Voir : falsifier.)

$ résistant à la fraude *(tamper-resistant)*
(I) Caractéristique d'un composant de système qui fournit une protection passive contre une attaque. (Voir : falsifier.)
Usage : implique généralement des moyens de protection physiques.

$ falsification *(tampering)*
(I) /action de menace/ Voir : définitions secondaires sous "corruption" et "mauvaise utilisation".

$ cible d'évaluation (TOE, *target of evaluation*)
(N) /Critères communs/ Produit ou système de technologie de l'information qui est le sujet d'une évaluation de sécurité, conjointement avec la documentation administrative et d'utilisation associée au produit. (À comparer à : profil de protection.)
Instructions : les caractéristiques de sécurité de la cible d'évaluation (TOE) sont décrites dans des termes spécifiques par une cible de sécurité correspondante, ou dans des termes plus généraux par un profil de protection. Dans la philosophie des critères communs, il est important qu'une TOE soit évaluée par rapport à l'ensemble spécifique de critères exprimés dans la cible. Cette évaluation consiste en une analyse rigoureuse et des essais effectués par un laboratoire accrédité indépendant. La portée d'une évaluation d'une TOE est établie par l'EAL et d'autres exigences spécifiées dans la cible. Une partie de ce processus est une évaluation de la cible elle-même, pour s'assurer qu'elle est correcte, complète, et cohérente en interne, et peut être utilisée comme base de l'évaluation de la TOE.

$ TCP/IP (I) Synonyme de "suite des protocoles de l'Internet".

$ attaque des larmes *(teardrop attack)*
(D) /argot/ Attaque de déni de service qui envoie des fragments de paquets IP mal formés dans l'intention de causer la défaillance du système de destination.
Terme déconseillé : les IDOC qui utilisent ce terme DEVRAIENT en donner une définition parce que le terme est souvent utilisé de façon imprécise et pourrait facilement être mal compris. (Voir : Utilisation déconseillée sous "Livre Vert".)

$ non répudiation technique *(technical non-repudiation)* (I) Voir : (définition secondaire sous) non-répudiation.

$ sécurité technique *(technical security)*
(I) Mécanismes et procédures de sécurité qui sont mis en œuvre et exécutés dans un matériel informatique, un progiciel ou un logiciel pour fournir une protection automatique d'un système. (Voir : architecture de sécurité. À comparer à : sécurité administrative.)

$ système de nomenclature de sécurité des télécommunications (TSEC, *Telecommunications Security Nomenclature System*)
(O) /Gouvernement des USA/ Terminologie pour désigner les équipements de sécurité des télécommunications. (À

comparer à : TCSEC.)
Instructions : une désignation TSEC comporte les parties suivantes :
- Préfixe "TSEC/" pour les éléments et systèmes, ou suffixe "/TSEC" pour les assemblages. (Souvent omis si le contexte est clair.)
- Première lettre, pour la fonction : "C" système d'équipement COMSEC, "G" objet général, "K" cryptographique, "H" auxiliaire de chiffrement, "M" manufacturé, "N" non cryptographique, "S" objet spécial.
- Seconde lettre, pour le type ou l'objet : "G" génération de clé, "I" transmission de données, "L" conversion littérale, "N" conversion du signal, "O" multi objets, "P" production de matériels, "S" objet spécial, "T" essais ou vérification, "U" télévision, "W" télétype, "X" télécopie, "Y" parole.
- Une troisième lettre facultative n'est utilisée que pour désigner des assemblages, pour le type ou l'objet : "A" en cours, "B" base ou cabinet, "C" combinaison, "D" tiroir ou panneau, "E" bande ou châssis, "F" trame ou casier, "G" générateur de clé, "H" clavier, "I" traducteur ou lecteur, "J" traitement de la parole, "K" calage ou permutation, "L" répéteur, "M" mémoire or stockage, "O" observation, "P" alimentation ou conversion d'énergie, "R" receveur, "S" synchronisation, "T" transmetteur, "U" imprimante, "V" composant COMSEC amovible, "W" programmeur/programmation logique, "X" objet spécial.
- Numéro de modèle, généralement deux ou trois chiffres, alloués à la suite de chaque combinaison de lettres (par exemple, KG-34, KG- 84).
- Suffixe de lettre facultatif, utilisé pour désigner une version. La première version n'a pas de lettre, la version suivante a "A" (par exemple, KG-84, KG- 84A), etc.

$ TELNET
(I) Norme de protocole Internet fondée sur TCP, de couche Application (RFC 854) pour la connexion à distance d'un hôte avec un autre.

$ TEMPEST
1. (N) Nom abrégé pour la technologie et les méthodes de protection contre la compromission des données due aux émanations électromagnétiques provenant des équipements électriques et électroniques. [Army], [Russ] (Voir : espace inspectable, TEMPEST douce, zone de TEMPEST. À comparer à : QUADRANT)
2. (O) /Gouvernement des USA/ "Nom abrégé qui se réfère aux investigations, études, et contrôle des émanations compromettantes provenant des équipement IS." [C4009]

Utilisation déconseillée : les IDOC NE DEVRAIENT PAS utiliser ce terme comme synonyme de "sécurité des émanations électromagnétiques" ; à la place, utiliser EMSEC. Aussi, le terme N'EST PAS un acronyme pour Transient Electromagnetic Pulse Surveillance Technology *(technologie de surveillance des impulsions électromagnétiques transitoires)*.
Instructions : le gouvernement fédéral des USA produit des politiques de sécurité qui (a) établissent des spécifications et des normes pour les techniques de réduction de la force des émanations provenant des systèmes et réduire la capacité de tiers non autorisés à recevoir et faire usage des émanations et (b) établir des règles pour appliquer ces techniques. D'autres nations font probablement de même.

$ zone TEMPEST *(TEMPEST zone)*
(O) "Zone désignée [c'est-à-dire, un volume physique] au sein d'une facilité où les équipements avec les caractéristiques TEMPEST appropriées ... peuvent fonctionner." [C4009] (Voir : sécurité des émanations, TEMPEST. À comparer à : zone de contrôle, espace inspectable.)
Instructions : la force d'un signal électromagnétique décroît en proportion du carré de la distance entre la source et le receveur. Donc, la EMSEC pour les signaux électromagnétiques peut être réalisée par une combinaison de (a) la réduction de la force des émanations à un niveau défini et (b) l'établissement autour de cet équipement d'une zone tampon physique d'une taille appropriée d'où les entités non autorisées sont exclues. En rendrant la zone assez grande, il est possible de limiter la force du signal disponible aux entités en dehors de la zone à un niveau inférieur à celui qui peut être reçu et lu avec les méthodes connues de l'état de l'art. Normalement, le besoin et la taille d'une zone TEMPEST établie par une politique de sécurité dépend non seulement du niveau mesuré du signal émis par l'équipement, mais aussi du niveau de menace perçu dans l'environnement de l'équipement.

$ système de contrôle d'accès par contrôleur d'accès de terminal (TACACS, *Terminal Access Controller Access Control System*)
(I) Protocole d'authentification et de contrôle d'accès fondé sur UDP [RFC1492] dans lequel un serveur d'accès réseau reçoit un identifiant et un mot de passe d'un terminal distant et les passe à un serveur d'authentification séparé pour vérification. (Voir : TACACS+.)
Instructions : TACACS peut fournir un service non seulement pour les serveurs d'accès réseau mais aussi aux routeurs et autres appareils de calcul en réseau via un ou plusieurs serveurs d'authentification centralisés. TACACS était à l'origine développé pour l'ARPANET et a évolué pour être utilisé dans des équipements commerciaux.

$ système de chiffrement exponentiel (TESS, *The Exponential Encryption System*)
(I) Système de mécanismes et fonctions cryptographiques séparés mais coopérants pour un échange sûr authentifié de clés

de chiffrement, la génération de signatures numériques, et la distribution des clés publiques. TESS utilise le chiffrement asymétrique, sur la base de l'exponentiation discrète, et une structure de clés publiques auto certifiées. [RFC1824]

$ vol *(theft)*
(I) /action de menace/ Voir : définitions secondaires sous "interception" et "appropriation illégitime".

$ menace *(threat)*
1a. (I) Potentiel de violation de la sécurité, qui existe lorsque il y a une entité, circonstance, capacité, action, ou événement qui pourrait causer des dommages. (Voir : menace vaine, niveau INFOCON, action de menace, agent de menace, conséquence de menace. À comparer à : attaque, vulnérabilité.)
1b. (N) Toute circonstance ou événement qui a le potentiel d'un effet contraire sur un système à travers un accès non autorisé, la destruction, la divulgation, ou la modification de données, ou le déni de service. [C4009] (Voir : informations sensibles.)
Usage : (a) Fréquemment mal utilisé avec la signification de "action de menace" ou de "vulnérabilité". (b) Dans certains contextes, "menace" est utilisé dans un sens plus étroit pour ne se référer qu'aux menaces intelligentes, par exemple, voir la définition 2 ci-dessous. (c) Dans certains contextes, "menace" est utilisé dans un sens plus large pour couvrir à la fois la définition 1 et d'autres concepts, comme dans la définition 3.
Instructions : une menace est un danger possible qui peut exploiter une vulnérabilité. Donc, une menace peut être ou non intentionnelle :
- "menace intentionnelle" : possibilité d'une attaque par une entité intelligente (par exemple, un craqueur individuel ou une organisation criminelle).
- "menace accidentelle" : possibilité d'erreur ou omission humaine, d'un dysfonctionnement non intentionnel d'un équipement, ou désastre naturel (par exemple, feu, inondation, tremblement de terre, tempête, et autres causes énumérées dans [FP031]).

Les critères communs caractérisent une menace en termes de (a) agent de menace, (b) méthode d'attaque présumée, (c) toutes les vulnérabilités qui sont le fondement de l'attaque, et (d) la ressource système qui est attaquée. Cette caractérisation est en accord avec les définitions de ce glossaire (voir le diagramme sous "attaque").
2. (O) Capacité technique et opérationnelle d'une entité hostile à détecter, exploiter, ou subvertir un système ami et l'intention démontrée, présumée, ou déduite de cette entité à conduire une telle activité.
Instructions : pour être sur le point de lancer une attaque, un adversaire doit avoir (a) un motif d'attaque, (b) une méthode ou la capacité technique de faire l'attaque, et (c) une opportunité d'accéder de façon appropriée au système ciblé.
3. (D) "Indication de l'imminence d'un événement indésirable." [Park]
Définition déconseillée : les IDOC NE DEVRAIENT PAS utiliser ce terme avec la définition 3 parce qu'elle est ambiguë ; la définition était destinée à inclure les trois significations suivantes :
- "menace potentielle" : une possible violation de la sécurité ; c'est-à-dire, la même que la définition 1.
- "menace active" : une expression de l'intention de violer la sécurité. (Le contexte distingue généralement cette signification de la précédente.)
- "menace accomplie" ou "menace actuelle" : c'est une action de menace. Utilisation déconseillée : les IDOC NE DEVRAIENT PAS utiliser le terme "menace" avec cette signification ; à la place, utiliser "action de menace".

$ action de menace *(threat action)*
(I) Réalisation d'une menace, c'est-à-dire, une occurrence dans laquelle la sécurité d'un système est assaillie par suite d'un événement accidentel ou d'un acte intentionnel. (Voir : attaque, menace, conséquence de menace.)
Instructions : une architecture de sécurité complète traite aussi bien des actes intentionnels (c'est-à-dire, des attaques) que des événements accidentels [FP031]. (Voir : diverses sortes d'actions de menace définies sous les quatre sortes de "conséquence de menace".)

$ agent de menace *(threat agent)*
(I) Entité système qui effectue une action de menace, ou un événement qui résulte en une action de menace.

$ analyse de menace *(threat analysis)*
(I) Analyse des actions de menace qui peuvent affecter un système, en soulignant principalement leur probabilité d'occurrence mais aussi en considérant leurs conséquences. Exemple : RFC 3833. (À comparer à : analyse de risque.)

$ conséquence de menace *(threat consequence)*
(I) Violation de la sécurité qui résulte d'une action de menace.
Instructions : les quatre types de base de conséquence de menace sont la "divulgation non autorisée", la "tromperie", "l'interruption", et "l'usurpation". (Voir dans les entrées principales du glossaire pour chacun de ces quatre termes les listes des types d'actions de menace qui peuvent résulter de ces conséquences.)

$ empreinte de pouce *(thumbprint)*

1. (I) Dessin des crêtes papillaires formée sur le bout d'un pouce. (Voir : authentification biométrique, empreinte digitale.)
2. (D) Synonyme de certain type de "résultat de hachage". (Voir : authentification biométrique. À comparer à : empreinte digitale.)

Utilisation déconseillée : les IDOC NE DEVRAIENT PAS utiliser ce terme avec la définition 2 parce que cette définition mélanges les concepts d'une façon potentiellement trompeuse.

$ ticket

(I) Synonyme de "jeton de capacité".

Instructions : un ticket est généralement accordé par un serveur de contrôle d'accès centralisé (agent de délivrance de ticket) pour autoriser l'accès à une ressource système pour un temps limité. Les tickets peuvent être mis en œuvre avec le chiffrement symétrique (voir : Kerberos) ou avec le chiffrement asymétrique (voir : certificat d'attribut).

$ brigades du tigre *(tiger team)*

(O) Groupe d'évaluateurs employés par les gestionnaires d'un système pour effectuer des essais de pénétration sur le système.

Utilisation déconseillée : il est vraisemblable que les autres cultures utilisent des métaphores différentes pour ce concept. Donc, pour éviter l'incompréhension entre les nations, les IDOC NE DEVRAIENT PAS utiliser ce terme. (Voir : Utilisation déconseillée sous "Livre Vert".)

$ horodatage *(time stamp)*

1. (I) /nom/ Par rapport à un objet de données, étiquette ou marquage dans lequel est enregistrée l'heure (courante ou une autre mesure du temps écoulé) à laquelle l'étiquette ou le marquage a été accolé à l'objet de données. (Voir : protocole d'horodatage.)
2. (O) /nom/ "Par rapport à un événement enregistré du réseau, c'est un champ de données dans lequel est enregistrée l'heure (courante ou une autre mesure du temps écoulé) à laquelle l'événement a eu lieu." [A1523]

Instructions : un horodatage peut être utilisé comme preuve pour montrer qu'un objet de données existait (ou qu'un événement s'est produit) à un instant donné ou avant. Par exemple, un horodatage peut être utilisé pour prouver qu'une signature numérique fondée sur une clé privée a été créée alors que le certificat de clé publique correspondant était valide, c'est-à-dire, avant que le certificat ait expiré ou ait été révoqué. L'établissement de cette preuve permettrait au certificat d'être utilisé après son expiration ou révocation, pour vérifier une signature qui a été créée antérieurement. Cette sorte de preuve est requise au titre de la mise en œuvre des services PKI, comme le service de non répudiation, les services de sécurité à long terme, comme l'audit.

$ protocole d'horodatage *(Time-Stamp Protocol)*

(I) Protocole Internet (RFC 3161) qui spécifie comment un client demande et reçoit un horodatage d'un serveur pour un objet de données détenu par le client.

Instructions : le protocole décrit le format (a) d'une demande envoyée à une autorité d'horodatage, et (b) d'une réponse retournée qui contient un horodatage. L'autorité crée l'horodatage en enchaînant (a) une valeur hachée de l'objet de données entrée avec (b) une valeur d'heure UTC et d'autres paramètres (OID de politique, numéro de série, indication de la précision horaire, nom occasionnel, DN de l'autorité, et diverses extensions) et ensuite en signant cet ensemble de données avec la clé privée de l'autorité comme spécifié dans la CMS. Une telle autorité va normalement fonctionner comme service de tiers de confiance, mais d'autres modèles de fonctionnement peuvent être utilisés.

$ canal à temporisation *(timing channel)* (I) Voir : canal à temporisation couverte.

$ TKEY

(I) Mnémonique qui se réfère à un protocole Internet (RFC 2930) pour établir une clé secrète partagée entre un résolveur DNS et un serveur de noms DNS. (Voir : TSIG.)

$ jeton *(token)*

1. (I) /cryptographie/ Voir : jeton cryptographique. (À comparer à : boîtier de protection.)
2. (I) /contrôle d'accès/ Objet utilisé pour contrôler l'accès et qui est passé entre des entités coopérantes dans un protocole qui synchronise l'utilisation d'une ressource partagée. Généralement, l'entité qui détient actuellement le jeton a un accès exclusif à la ressource. (Voir : jeton de capacité.)

Usage : ce terme est très surchargé dans la littérature informatique ; donc, les IDOC NE DEVRAIENT PAS utiliser ce terme avec une autre définition que 1 ou 2.

3a. (D) /authentification/ Objet de données ou appareil physique utilisé pour vérifier une identité dans un processus d'authentification.

3b. (D) /Gouvernement des USA/ Quelque chose que dans un processus d'authentification le déclarant (c'est-à-dire, l'entité qui revendique une identité) possède et contrôle, et utilise pour prouver la revendication durant l 'étape de vérification du processus. [SP63]

Utilisation déconseillée : les IDOC NE DEVRAIENT PAS utiliser ce terme avec les définitions 3a et 3b ; à la place, utiliser les termes plus spécifiquement descriptifs et informatifs que sont "informations d'authentification" ou "jeton cryptographique", selon ce que l'on veut dire.
Le NIST définit quatre types de jetons de revendication pour l'authentification électronique dans les systèmes d'information [SP63]. Les IDOC NE DEVRAIENT PAS utiliser ces quatre termes du NIST ; ils mélangent les concepts d'une façon potentiellement trompeuse et dupliquent la signification de termes mieux établis. Ces quatre termes peuvent être évités en utilisant les termes plus spécifiquement descriptifs qui suivent :

- le "jeton matériel" du NIST : appareil matériel qui contient une clé de chiffrement protégée. (C'est un type de "jeton cryptographique", et la clé est un type "d'informations d'authentification".)
- "jeton d'appareil de mot de passe à utilisation unique" du NIST : appareil matériel personnel qui génère des mots de passe à utilisation unique. (Les mots de passe à utilisation unique sont normalement générés cryptographiquement. Donc, c'est un type de "jeton cryptographique", et la clé est un type "d'informations d'authentification".)
- "jeton logiciel" du NIST : c'est une clé de chiffrement qui est normalement mémorisée sur un disque ou quelque autre support magnétique. (La clé est un type "d'informations d'authentification" ; "clé d'authentification" serait une meilleure description.)
- "jeton de mot de passe" du NIST : valeur de données secrète que mémorisé le déclarant. (C'est un "mot de passe" qui est utilisé comme "informations d'authentification".)

$ sauvegarde de jeton *(token backup)*
(I) Opération de gestion de jeton qui mémorise des informations suffisantes dans une base de données (par exemple, dans une CAW) pour recréer ou restaurer un jeton de sécurité (par exemple, une carte à mémoire) si il est perdu ou endommagé.

$ copie de jeton *(token copy)*
(I) Opération de gestion de jeton qui copie toutes les informations personnelles provenant d'un jeton de sécurité sur un autre. Cependant, à la différence d'une opération de restauration de jeton, le second jeton est initialisé avec ses propres valeurs de sécurité locales différentes comme des PIN et des clé de mémorisation.

$ gestion de jeton *(token management)*
(I) Processus qui inclut l'initialisation de jetons de sécurité (par exemple, "carte à mémoire") le chargement de données dans le jeton, et le contrôle des jetons durant leur durée de vie. Peut inclure d'effectuer des fonctions de gestion de clés et de gestion de certificats, de générer et installer des PIN, de charger des données personnelles d'utilisateur, d'effectuer une sauvegarde de carte, une copie de carte, et des opérations de restauration de carte, et des mises à jour de progiciel.

$ restauration de jeton *(token restore)*
(I) Opération des gestion de jeton qui charge un jeton de sécurité avec des données afin de recréer ((dupliquer) le contenu précédemment détenu par ce jeton ou par un autre . (Voir : récupération.)

$ clé de mémorisation de jeton *(token storage key)*
(I) Clé de chiffrement utilisée pour protéger des données qui sont mémorisées sur un jeton de sécurité.

$ CA sommet *(top CA)*
(I) Synonyme de "racine" dans une hiérarchie de certification. (Voir : ancre de confiance sommet.)

$ spécification de niveau supérieur *(top-level specification)*
(I) "Description non procédurale du comportement d'un système au niveau le plus abstrait ; normalement une spécification fonctionnelle qui omet tous les détails de mise en œuvre." [NCS04] (Voir : spécification formelle de niveau supérieur, Instructions sous "politique de sécurité".)
Instructions : une spécification de niveau supérieur est à un niveau d'abstraction en dessous de "modèle de sécurité" et au-dessus de "architecture de sécurité" (voir : Instructions sous "politique de sécurité").
Une spécification de niveau supérieur peut être descriptive ou formelle :

- "Spécification de niveau supérieur descriptive" : celle qui est écrite dans un langage naturel comme le français ou une notation de dessin informelle.
- "Spécification de niveau supérieur formelle" : celle qui est écrite dans un langage mathématique formel pour permettre de démontrer des théorèmes qui prouvent que la spécification met correctement en œuvre un ensemble d'exigences formelles ou un modèle de sécurité formelle. (Voir : preuve de correction.)

$ retraçage *(traceback)*
(I) Identification de la source d'un paquet de données. (Voir : mascarade, entrelaçage de réseau.)

$ traceur *(tracker)*
(N) Technique d'attaque pour réaliser une divulgation non autorisée à partir d'une base de données statistique. [Denns] (Voir

: Instructions sous "contrôle d'inférence".)

$ analyse de trafic *(traffic analysis)*

1. (I) Obtenir la connaissance d'informations par déduction à partir de caractéristiques observables d'un flux de données, même si les informations ne sont pas directement disponibles (par exemple, lorsque les données sont chiffrées).
   Ces caractéristiques incluent les identités et localisations de la ou des sources et de la ou des destinations du flux, et de la présence, quantité, fréquence, et durée d'occurrence du flux. L'objet de l'analyse peut être les informations dans les SDU, les informations dans la PCI, ou les deux. (Voir : inférence, confidentialité du flux de trafic, écoute. À comparer à : analyse du signal.)
2. (O) "Déduction des informations à partir de l'observation des flux de trafic (présence, absence, quantité, direction, et fréquence)." [I7498-2]

$ analyse de flux de trafic *(traffic-flow analysis)* (I) Synonyme de "analyse de trafic".

$ confidentialité du flux de trafic (TFC, *traffic-flow confidentiality*)

1. (I) Service de confidentialité des données pour protéger contre l'analyse de trafic. (Voir : communications couvertes.)
2. (O) ") Service de confidentialité pour protéger contre l'analyse de trafic." [I7498-2]

Instructions : le souci de la confidentialité implique la divulgation aussi bien directe qu'indirecte des données, et cette dernière inclut l'analyse de trafic. Cependant, les considérations de fonctionnement peuvent rendre la TFC difficile à réaliser. Par exemple, si Alice envoie une idée de produit à Bob dans un message électronique, elle veut la confidentialité des données pour le contenu du message, et elle peut aussi vouloir dissimuler la destination du message pour cacher l'identité de Bob à ses concurrents. Cependant, l'identité du receveur prévu, ou au moins une adresse réseau pour le receveur doit être disponible pour le système de messagerie. Donc, des schémas de transmission complexes peuvent être nécessaires pour dissimuler la destination ultime lorsque le message voyage à travers l'Internet ouvert (voir : acheminement en oignon).

Plus tard, si Alice utilise un ATM durant une visite clandestine pour négocier avec Bob, elle pourrait préférer que sa banque dissimule l'origine de sa transaction, parce que la connaissance de la localisation de l'ATM pourrait permettre à un concurrent de déduire l'identité de Bob. D'un autre côté, la banque peut préférer protéger seulement le PIN d'Alice (voir : confidentialité de champs choisis).

Un service TFC peut être complet ou partiel :

- "TFC complet" : ce type de service dissimule toutes les caractéristiques du trafic.
- "TFC partiel" : ce type de service (a) dissimule certaines des caractéristiques, mais pas toutes ou (b) ne cache pas complètement certaines caractéristiques.

Sur les liaisons de données point à point, la TFC peut être fournie en chiffrant toutes les PDU et aussi en générant un flux de données continu aléatoire pour boucher sans discontinuité tous les trous entre les PDU. Pour un observateur, la liaison paraît alors porter un flux continu de données chiffrées. Dans d'autres cas -- y compris sur des supports partagés ou de diffusion, ou de bout à bout sur un réseau -- seule une TFC partielle est possible, et cela peut exiger une combinaison de techniques. Par exemple, un LAN qui utilise un "accès multiple avec surveillance de signal et détection de collision" (CSMA/CD, *carrier sense multiple access with collision detection* ; autrement dit "l'écoute tout en parlant") pour contrôler l'accès au support, s'appuie sur la détection des intervalles de silence, qui empêche d'utiliser la TFC complète. La TFC partielle peut être fournie sur ce LAN avec des mesures telles que l'ajout de PDU parasites, le bourrage des PDU à une taille constante, ou en chiffrant les adresses juste au dessus de la couche Physique ; mais ces mesures réduisent l'efficacité avec laquelle le LAN peut porter le trafic. À des couches de protocole supérieures, les SDU peuvent être protégées, mais les adresses et d'autres éléments de PCI doivent être visibles aux couches inférieures.

$ clé de trafic *(traffic key)*

(I) Clé de chiffrement utilisée par un appareil pour protéger les informations qui sont transmises entre les appareils, par opposition à la protection des information qui sont conservées dans l'appareil. (À comparer à : clé de mémorisation.)

$ bourrage de trafic *(traffic padding)*

(I) "Génération d'instances parasites de communication, d'unités de données parasites, et/ou de données parasites au sein des unités de données." [I7498-2]

$ propriété de tranquillité *(tranquility property)*

(N) /modèle formel/ Propriété d'un système par laquelle le niveau de sécurité d'un objet ne peut pas changer lorsque cet objet est en cours de traitement par le système. (Voir : modèle de Bell-LaPadula.)

$ transaction

1. (I) Unité d'interaction entre une entité externe et un système, ou entre des composants au sein d'un système, qui implique une série d'actions ou événements du système.
2. (O) "Événement discret entre un usager et des systèmes qui prend en charge un objet d'affaire ou de programmation."

[M0404]
Instructions : pour conserver un état sûr, les transactions doivent être traitées de façon cohérente et fiable. Généralement, elles doivent être conçues comme atomiques, cohérentes, isolées, et durables [Gray] :
- "atomique" : il est garanti quie toutes les actions et les événements qui comprennent la transaction sont achevés avec succès, ou autrement le résultat est comme si aucun n'avait été exécuté.
- "cohérente" : la transaction satisfait les contraintes de correction définies pour les données qui sont traitées.
- "isolée" : si deux transactions sont effectuées concurremment, elles n'interfèrent pas l'une avec l'autre, et tout se passe comme si le système les effectuait une à la fois.
- "durable" : l'état du système et la sémantique de la transaction survivent aux défaillances du système.

$ champ Code de contrôle de transmission (TCC field, *Transmission Control Code field*)
(I) Champ de données qui fournit un moyen pour discriminer les trafics et définir des communautés contrôlées d'intérêt dans l'option de sécurité (type d'option = 130) du format d'en-tête de datagramme IPv4. Les valeurs de TCC sont des trigraphes alphanumériques alloués par le gouvernement des USA comme spécifié dans la RFC 791.

$ protocole de contrôle de transmission (TCP, *Transmission Control Protocol*)
(I) Norme Internet du protocole de couche Transport (RFC 793) qui livre de façon fiable une séquence de datagrammes d'un ordinateur à un autre dans un réseau informatique. (Voir : TCP/IP.)
Instructions : TCP est conçu pour tenir dans une suite de protocoles en couches qui prend en charge les applications inter réseaux. TCP suppose qu'il peut obtenir un service simple mais potentiellement non fiable de datagrammes de bout en bout (comme IP) à partir des protocoles de couche inférieure.

$ sécurité de transmission (TRANSEC, *transmission security*)
(I) Mesures COMSEC qui protègent les communications contre l'interception et l'exploitation par des moyens autres que la cryptanalyse. Exemple : saut de fréquence. (À comparer à : anti-brouillage, confidentialité du flux de trafic.)

$ couche Transport *(Transport Layer)*. Voir : suite de protocoles Internet, OSIRM.

$ sécurité de la couche Transport (TLS, *Transport Layer Security*)
(I) TLS est un protocole Internet [RFC4346] qui se fonde sur, et est très similaire à, SSL version 3.0. (À comparer à : TLSP.)
Instructions : le protocole TLS est mal nommé. Le nom suggère de façon trompeuse que TLS est situé dans la couche Transport de l'IPS, mais TLS est toujours mis en couche au dessus d'un protocole fiable de couche Transport (généralement TCP) et mis en couche soit immédiatement en dessous, soit intégré à un protocole de couche Application (souvent HTTP).

$ protocole de sécurité de la couche Transport (TLSP, *Transport Layer Security Protocol*)
(N) Protocole de chiffrement de bout en bout (ISO 10736) qui fournit des services de sécurité au bas de la couche 4 de l'OSIRM, c'est-à-dire, directement au dessus de la couche 3. (À comparer à : TLS.)
Instructions : TLSP a évolué directement à partir de SP4.

$ mode transport *(transport mode)*
(I) Une des deux façons d'appliquer AH ou ESP pour protéger les paquets de données ; dans ce mode, le protocole IPsec encapsule les paquets (c'est-à-dire, que la protection s'applique aux paquets) d'un protocole de couche Transport IPS (par exemple, TCP, UDP) qui sont normalement portés directement au dessus de IP dans une pile de protocoles IPS. (À comparer à : mode tunnel.)
Instructions : une association de sécurité IPsec en mode transport est toujours entre deux hôtes ; aucune des extrémités n'a de rôle de passerelle de sécurité. Chaque fois qu'une extrémité d'une association de sécurité IPsec est une passerelle de sécurité, l'association est obligée d'être en mode tunnel.

$ transposition
(I) /cryptographie/ Méthode de chiffrement dans laquelle les éléments d'un texte source conservent leur forme d'origine mais subissent certains changements de leur position séquentielle. (À comparer à : substitution.)

$ porte dérobée *(trap door)* (I) Synonyme de "porte de derrière".

$ outrepasser *(trespass)* (I) /action de menace/ Voir : définition secondaire sous "intrusion".

$ Triple algorithme de chiffrement de données *(Triple Data Encryption Algorithm)*
(I) Chiffrement de bloc qui transforme chaque bloc de 64 bits de texte en clair en appliquant trois fois de suite l'algorithme de chiffrement de données (DEA), en utilisant deux ou trois clés différentes pour une longueur de clé efficace de 112 ou

168 bits. [A9052], [SP67]
Exemple : Une variante proposée pour l'ESP d'IPsec utilise une clé de 168 bits, consistant en trois valeurs indépendantes de 56 bits utilisées par le DEA, et une valeur d'initialisation de 64 bits. Chaque datagramme contient une IV pour assurer que chaque datagramme reçu peut être déchiffré même lorsque les autres datagrammes sont abandonnés ou qu'une séquence de datagrammes est réarrangée dans le transit. [RFC1851]

$ triple enveloppe *(triple-wrapped)*
(I) /S-MIME/ Données qui ont été signées avec une signature numérique, puis chiffrées, puis signées à nouveau [RFC2634]

$ cheval de Troie *(Trojan horse)*
(I) Programme informatique qui paraît avoir une fonction utile, mais a aussi une fonction cachée potentiellement malveillante qui évite les mécanismes de sécurité, parfois en exploitant les autorisations légitimes d'une entité de système qui implique le programme. (Voir : logiciel malveillant, logiciel espion. Comparer à bombe logique, virus, ver.)

$ confiance *(trust)*
1. (I) /systèmes d'information/ Sentiment de certitude (parfois fondé sur des évidences trompeuses) que (a) le système ne va pas tomber en panne ou (b) que le système satisfait à ses spécifications (c'est-à-dire, le système fait ce qu'il prétend faire et n'effectue pas de fonctions non désirées). (Voir : niveau de confiance, système de confiance, système digne de confiance. Comparer à assurance.)

Instructions : Les composants d'un système peuvent être groupés en trois classes de confiance [Gass] :
- "de confiance" : Le composant est chargé de mettre en application la politique de sécurité sur les autres composants ; la sécurité du système dépend d'un fonctionnement sans faute du composant. (Voir : processus de confiance.)
- "Bénin" : Le composant n'est pas responsable de la mise en application de la politique de sécurité, mais il a des autorisations sensibles. Il doit être supposé ne pas violer intentionnellement la politique de sécurité, mais les violations de la sécurité sont supposées être accidentelles et probablement ne pas affecter la sécurité globale du système.
- "pas de confiance" : Le composant est de provenance inconnue ou suspecte et doit être traité comme délibérément malveillant. (Voir : logique malveillante.)

2. (I) /PKI/ Une relation entre un utilisateur de certificat et une autorité de certification (CA) dans laquelle l'utilisateur agit conformément à l'hypothèse que la CA ne crée que des certificats numériques valides.

Instructions : "Généralement, une entité est dite 'faire confiance' à une seconde entité lorsque la première entité fait l'hypothèse que la seconde entité va se comporter exactement comme l'attend la première entité. Cette confiance peut ne s'appliquer qu'à une fonction spécifique. Le rôle clé de la confiance dans [X.509] est de décrire la relation entre une entité [c'est-à-dire, un utilisateur de certificat] et une [CA] ; une entité devra être certaine qu'elle peut faire confiance à la CA pour ne créer que des certificats valides et fiables." [X509]

$ ancre de confiance *(trust anchor)*
(I) /PKI/ Un point de confiance établi (généralement fondé sur l'autorité d'une personne, bureau, ou organisation) à partir duquel l'utilisateur de certificat commence la validation d'un chemin de certification. (Voir : ancre de confiance supérieure, validation de chemin, CA d'ancre de confiance, certificat d'ancre de confiance, clé d'ancre de confiance.)
Usage : les IDOC qui utilisent ce terme DEVRAIENT en donner une définition parce qu'il est utilisé de diverses façons dans les IDOC existants et dans la littérature sur la PKI. La littérature utilise presque toujours ce terme dans un sens qui est équivalent à cette définition, mais l'usage diffère souvent par rapport à ce qui constitue le point de confiance.
Instructions : une ancre de confiance peut être définie comme se fondant sur une clé publique, une CA, un certificat de clé publique, ou une combinaison ou variante de :
1. une clé publique comme point de confiance : bien qu'un chemin de certification soit défini comme commençant par une "séquence de certificats de clé publique", la mise en œuvre d'un processus de validation de chemin peut ne pas traiter explicitement un certificat racine comme partie du chemin, mais à la place commencer le processus en utilisant une clé racine de confiance pour vérifier la signature sur un certificat qui a été produit pas la racine.
   Donc, "ancre de confiance" est parfois défini comme juste une clé publique. (Voir : clé racine, clé d'ancre de confiance, clé de confiance.)
2. Une CA comme point de confiance : une clé publique de confiance est juste un des éléments de données nécessaires pour la validation de chemin ; l'algorithme IPS de validation de chemin [RFC3280] a aussi besoin du nom de la CA à laquelle appartient la clé, c'est-à-dire, le DN du producteur du premier certificat X.509 à être validé sur le chemin. (Voir : produire.)
   Donc, "ancre de confiance" est parfois défini comme soit juste une CA (où une clé publique est impliquée) soit comme une CA avec une clé publique spécifiée qui appartient à cette CA. (Voir : racine, CA ancre de confiance, CA de confiance.)
   Exemple : "Une clé publique et le nom d'une [CA] qui est utilisée pour valider le premier certificat dans une séquence de certificats. La clé publique ancre de confiance est utilisée pour vérifier la signature sur un certificat produit par une ancre de confiance [CA]." [SP57]
3. Un certificat de clé publique comme point de confiance : à côté de la clé publique et du nom de la CA de confiance, l'algorithme de validation de chemin a besoin de connaître l'algorithme de signature numérique et tous les paramètres

associés avec lesquels la clé publique est utilisée, et aussi toutes les contraintes qui ont été placées sur l'ensemble des chemins qui peuvent être validés en utilisant la clé. Toutes ces informations sont disponibles à partir du certificat de clé publique de la CA. Donc, "l'ancre de confiance" est parfois définie comme un certificat de clé publique d'une CA. (Voir : certificat racine, certificat d'ancre de confiance, certificat de confiance.)

4. Combinaisons : des combinaisons et variantes des trois premières définitions sont aussi utilisées dans la littérature PKI. Exemple : "informations d'ancre de confiance". La norme IPS pour la validation de chemin [RFC3280] spécifie les informations qui décrivent "une CA qui sert d'ancre de confiance pour le chemin de certification. Les informations de l'ancre de confiance incluent : (a) le nom du producteur de confiance, (b) l'algorithme de la clé publique de confiance, (c) la clé publique de confiance, et (d) facultativement, les paramètres de clé publique de confiance associés à la clé publique. Les informations d'ancre de confiance peuvent être fournies à la procédure de traitement du chemin sous la forme d'un certificat auto signé. Les informations d'ancre de confiance sont de confiance parce qu'elles ont été livrées à la procédure de traitement du chemin par une procédure hors bande digne de confiance. Si l'algorithme de clé publique de confiance exige des paramètres, ceux-ci sont alors fournis avec la clé publique de confiance."

$ CA d'ancre de confiance *(trust anchor CA)*
(I) CA qui est le sujet d'un certificat d'ancre de confiance ou qui établit par ailleurs une clé d'ancre de confiance. (Voir : racine, CA de confiance.)
Instructions : le choix d'une CA comme ancre de confiance est une affaire de politique. Certains des choix possibles incluent (a) la CA supérieure dans une PKI hiérarchique, (b) la CA qui a produit le propre certificat du vérificateur, ou (c) toute autre CA dans un réseau de PKI. Différentes applications peuvent s'appuyer sur différentes ancres de confiance, ou peuvent accepter des chemins qui commencent par tout ensemble d'ancres de confiance. L'algorithme de validation de chemin IPS est le même, sans considération du choix.

$ certificat d'ancre de confiance *(trust anchor certificate)*
(I) Certificat de clé publique qui est utilisé pour fournir la première clé publique dans un chemin de certification. (Voir : certificat racine, ancre de confiance, certificat de confiance.)

$ clé d'ancre de confiance *(trust anchor key)*
(I) Clé publique qui est utilisée comme première clé publique dans un chemin de certification. (Voir : clé racine, ancre de confiance, clé publique de confiance.)

$ informations d'ancre de confiance *(trust anchor information)*
(I) Voir : définition secondaire sous "ancre de confiance".

$ chaîne de confiance *(trust chain)*
(D) Synonyme de "chemin de certification". (Voir : ancre de confiance, certificat de confiance.)
Terme déconseillé : les IDOC NE DEVRAIENT PAS utiliser ce terme, parce qu'il duplique sans nécessité la signification d'un terme normalisé internationalement. Aussi, le terme mélange des concepts d'une façon potentiellement trompeuse. Avoir "confiance" implique des facteurs sans relation avec la simple vérification de signatures et d'effectuer d'autres essais comme spécifié par un algorithme standard pour la validation de chemin (par exemple, la RFC3280). Donc, même si un usager est capable de valider par un algorithme un chemin de certification, il peut n'avoir quand même pas confiance dans une des CA qui a produit des certificats dans ce chemin ou se défier de certains autres aspects de la PKI.

$ PKI de fichier de confiance *(trust-file PKI)*
(I) PKIA non hiérarchique dans laquelle chaque utilisateur de certificat a son propre fichier local (qui est utilisé par le logiciel d'application) d'ancres de confiance, c'est-à-dire, des clés publiques ou des certificats de clé publique que l'usager estime de confiance comme points de départ pour les chemins de certification. (Voir : ancre de confiance, réseau de confiance. À comparer à : PKI hiérarchique, PKI maillée.)
Exemple : des navigateurs populaires sont distribués avec un fichier initial de certificats d'ancre de confiance, qui sont souvent des certificats auto signés. Les utilisateurs peuvent ajouter des certificats au fichier ou en supprimer. Le fichier peut être directement géré par l'usager, ou l'organisation de l'usager peut le gérer à partir d'un serveur centralisé.

$ hiérarchie de confiance *(trust hierarchy)*
(D) Synonyme de "hiérarchie de certification".
Utilisation déconseillée : les IDOC NE DEVRAIENT PAS utiliser ce terme parte qu'il mélange des concepts d'une façon potentiellement trompeuse, et parce que une hiérarchie de confiance pourrait être mise en œuvre d'autres façons. (Voir : confiance, chaîne de confiance, réseau de confiance.)

$ niveau de confiance *(trust level)*
(N) Caractérisation d'un standard de protection de la sécurité à atteindre dans un système d'information. (Voir : Critères communs, TCSEC.)

Instructions : un niveau de confiance ne se fonde pas seulement sur (a) la présence de mécanismes de sécurité, mais aussi sur l'utilisation de (b) discipline d'ingénierie des systèmes pour structurer de façon appropriée le système et (c) l'analyse de la mise en œuvre pour assurer que le système fournit un degré de confiance approprié.

$ de confiance *(trusted)* (I) Voir : définition secondaire sous "confiance".

$ CA de confiance *(trusted CA)*
(I) CA sur laquelle un utilisateur de certificat s'appuie comme produisant des certificats valides ; en particulier une CA qui est utilisée comme CA d'ancre de confiance. (Voir : chemin de certification, racine, CA d'ancre de confiance, validation.)
Instructions : cette confiance est transitive dans la mesure où le permettent les extensions de certificat X.509 ; c'est-à-dire que si une CA de confiance produit un certificat à une autre CA, un usager qui a confiance dans la première CA fera aussi confiance à la seconde si l'usager réussit à valider le chemin de certificats (voir : validation de chemin).

$ certificat de confiance *(trusted certificate)*
(I) Certificat numérique qu'un usager de certificat accepte comme étant valide "a priori", c'est-à-dire, sans vérifier le certificat pour le valider comme certificat final sur un chemin de certification, en particulier un certificat qui est utilisé comme certificat d'ancre de confiance. (Voir : chemin de certification, certificat racine, certificat d'ancre de confiance, PKI de fichier de confiance, validation.)
Instructions : l'acceptation d'un certificat comme étant de confiance est une question de politique et de choix. Généralement, un certificat est accepté comme de confiance parce que l'utilisateur l'a obtenu par des moyens fiables hors bande qui font qu'il croit que le certificat lie précisément le nom de son sujet à la clé publique du sujet ou d'autres valeurs d'attribut. De nombreux choix sont possibles, par exemple, un certificat de clé publique de confiance peut être (a) le certificat racine dans une PKI hiérarchique, (b) le certificat de la CA qui a produit le propre certificat de l'utilisateur dans une PKI maillée, ou (c) un certificat fourni avec une application qui utilise une PKI de fichier de confiance.

$ Critères d'évaluation de système informatique de confiance (TCSEC, *Trusted Computer System Evaluation Criteria*)
(N) Norme pour l'évaluation de la sécurité fournie par les systèmes d'exploitation [CSC1], [DoD1]. Connue sous le nom de "Livre Orange" à cause de la couleur de sa couverture ; premier document de la série Rainbow. (Voir : Critères communs, Utilisation déconseillée sous "Livre Vert", Livre Orange, niveau de confiance, système de confiance. Comparer à TSEC.)
Instructions : TCSEC définit des classes de niveau d'assurance ordonnés hiérarchiquement pour classer les systèmes informatiques. De la meilleure à la plus mauvaise, les classes sont les suivantes :

Division A :	protection assurée.
Au delà de A1	au-delà de la technologie actuelle. (Voir : au-delà de A1.)
Classe A1	conception vérifiée. (Voir : SCOMP.)
Division B :	protection obligatoire
Classe B3	domaines de sécurité.
Classe B2	protection structurée (Voir : Multics.)
Classe B1	protection de sécurité étiquetée
Division C :	protection discrétionnaire
Classe C2	protection d'accès contrôlé.
Classe C1	protection de sécurité discrétionnaire.
Division D :	protection minimale, c'est-à-dire, a été évaluée mais ne satisfait pas aux exigences d'une classe d'évaluation plus élevée.

$ base de calcul de confiance (TCB, *trusted computing base*)
(N) "Totalité des mécanismes de protection au sein d'un système informatique, incluant le matériel, les progiciels et logiciels, dont la combinaison est responsable de l'application d'une politique de sécurité." [NCS04] (Voir : "de confiance" sous "confiance". À comparer à : TPM.)

$ groupe de calcul de confiance (TCG, *Trusted Computing Group*)
(N) Organisation de normalisation industrielle, à but non lucratif, formée pour développer, définir et promouvoir des normes ouvertes pour des technologies de calcul et de sécurité de confiance pour les matériels, y compris les éléments de construction des matériels et les interfaces logicielles, à travers de multiples plateformes, périphériques, et appareils. (Voir : TPM, système de confiance. À comparer à : TSIG.)

$ distribution de confiance *(trusted distribution)*
(I) /COMPUSEC/ "Méthode de confiance pour la distribution des composants de matériels, logiciels, et progiciels de TCB originaux et leurs mises à jour, qui fournit des méthodes pour protéger la TCB contre la modification durant la distribution et pour la détection de tout changement de la TCB qui pourrait survenir." [NCS04] (Voir : signature de code, contrôle de configuration.)

$ clé de confiance *(trusted key)*
(D) Abréviation pour "clé publique de confiance" et aussi pour d'autres types de clés. (Voir : clé racine, clé d'ancre de confiance.)
Utilisation déconseillée : les IDOC DEVRAIENT soit (a) donner une définition de ce terme, soit (b) utiliser un terme différent, moins ambigu. Ce terme est ambigu quand il est employé seul ; par exemple, il pourrait se référer à une clé publique de confiance ou à une clé privée ou à une clé symétrique dont on pense qu'elle est sûre (c'est-à-dire, non compromise).

$ chemin de confiance *(trusted path)*
1a. (I) /COMPUSEC/ Mécanisme par lequel un utilisateur de système informatique peut communiquer directement et fiablement avec la TCB et qui ne peut être activé que par l'usager ou la TCB et ne peut pas être imité par un logiciel qui n'est pas de confiance au sein de l'ordinateur. [NCS04]
1b. (I) /COMSEC/ Mécanisme par lequel une personne ou un processus peut communiquer directement avec un module cryptographique et qui ne peut être activé que par la personne, processus, ou module, et ne peut pas être initié par un logiciel qui n'est pas de confiance au sein du module. [FP140]

$ module de plateforme de confiance (TPM, *Trusted Platform Module*)
(N) Nom d'une spécification, publiée par le TCG, pour un micro contrôleur qui peut mémoriser des informations sécurisées, et c'est aussi le nom général des mises en œuvre de cette spécification. (À comparer à : TCB.)

$ processus de confiance *(trusted process)*
(I) Composant de système qui a des privilèges lui permettant d'affecter l'état de la sécurité du système et qui peut donc, à travers une exécution incorrecte ou malveillante, violer la politique de sécurité du système. (Voir : processus privilégié, système de confiance.)

$ clé publique de confiance *(trusted public key)*
(I) Clé publique sur laquelle s'appuie un usager, en particulier une clé publique produite comme clé d'ancre de confiance. (Voir : chemin de certification, clé racine, clé d'ancre de confiance, validation.)
Instructions : une clé publique de confiance pourrait être (a) la clé racine dans une PKI hiérarchique, (b) la clé de la CA qui a produit le propre certificat de l'usager dans une PKI maillée, ou (c) toute clé acceptée par l'usager dans une PKI de fichier de confiance.

$ récupération de confiance *(trusted recovery)*
(I) Processus qui, après qu'un système a subi une défaillance ou une attaque, restaure le fonctionnement normal du système (ou un état sûr) sans causer de compromission de la sécurité. (Voir : récupération.)

$ sous réseau de confiance *(trusted subnetwork)*
(I) Sous réseau qui contient des hôtes et des routeurs qui se font confiance les uns les autres pour ne pas s'engager dans des attaques actives ou passives. (Il y a aussi l'hypothèse que les canaux de communication sous-jacents, comme les lignes téléphoniques ou un LAN, sont protégées contre l'attaque.)

$ système de confiance *(trusted system)*
1. (I) /système d'information/ Système qui fonctionne comme prévu, selon sa conception et sa politique, qui fait ce qui est demandé -- en dépit des interruptions de l'environnement, des erreurs de l'utilisateur humain et de l'opérateur, et des attaques par des tiers hostiles -- et ne fait rien d'autre [NRC98]. (Voir : niveau de confiance, processus de confiance. À comparer à : digne de confiance.)
2. (N) /sécurité à plusieurs niveaux/ "Un [système de confiance est un] système qui emploie des mesures d'assurance de matériel et logiciel suffisantes pour permettre son utilisation pour un traitement simultané d'une gamme d'informations sensibles ou classifiées." [NCS04] (Voir : mode de sécurité multi niveau.)

$ groupe d'interopérabilité de systèmes de confiance (TSIG, *Trusted Systems Interoperability Group*)
(N) Forum de fabricants d'ordinateurs, d'intégrateurs de systèmes et d'utilisateurs dédié à la promotion de l'interopérabilité de systèmes informatiques de confiance. (Voir : système de confiance. À comparer à : TCG.)

$ système digne de confiance *(trustworthy system)*
1. (I) Système qui non seulement est de confiance, mais aussi garantit cette confiance parce que le comportement du système peut être validé d'une façon convaincante, comme par une analyse formelle ou une relecture du code. (Voir : confiance. À comparer à : de confiance.)
2. (O) /Lignes directrices des signatures numériques/ "Matériel, logiciel, et procédures informatiques qui (a) sont raisonnablement sûrs contre l'intrusion et la mauvaise utilisation, (b) fournissent un niveau raisonnablement fiable de disponibilité, de fiabilité, et de fonctionnement correct; (c) sont raisonnablement adaptés à effectuer les fonctions pour

lesquelles ils sont prévus, et (d) adhèrent aux principes généralement acceptés de sécurité." [DSG]

$ TSIG
1. (N) Voir : groupe d'interopérabilité de système de confiance.
2. (I) Mnémonique (vraisemblablement dérivé de "Transaction SIGnature") qui se réfère à un protocole Internet (RFC2845) pour l'authentification de l'origine des données et l'intégrité des données pour certaines opérations du DNS. (Voir : TKEY.)

$ tunnel
1. (I) Canal de communication créé dans un réseau informatique en encapsulant (c'est-à-dire, en mettant en couches) les paquets de données d'un protocole de communication dans (c'est-à-dire, au dessus) un second protocole qui serait normalement porté au dessus, ou à la même couche que le premier. (Voir : L2TP, mode tunnel, VPN. À comparer à : canal couvert.)

Instructions : le tunnelage peut impliquer presque toute paire de couches de protocole IPS. Par exemple, une connexion TCP entre deux hôtes pourrait être portée au dessus de SMTP (c'est-à-dire, dans les messages SMTP) comme un canal couvert pour s'évader des contrôles d'accès qu'applique une passerelle de sécurité à la couche TCP normale qui est en dessous de SMTP.

Généralement, cependant, un tunnel est une liaison logique point à point -- c'est-à-dire, une connexion de couche 2 OSIRM -- créée par encapsulation du protocole de couche 2 dans un des trois types de protocoles IPS suivants : (a) un protocole de couche Transport IPS (comme TCP), (b) un protocole de couche Réseau ou de couche Internet IPS (comme IP), ou (c) un autre protocole de couche 2. Dans de nombreux cas, l'encapsulation est accomplie avec un protocole intermédiaire supplémentaire (c'est-à-dire, un "protocole de tunnelage", par exemple, L2TP) qui est mis en couche au dessous du protocole tunnelé de couche 2 et au dessus du protocole encapsulant.

Le tunnelage peut aussi être utilisé pour déplacer des données entre des ordinateurs qui utilisent un protocole qui n'est pas pris en charge par le réseau qui les connecte. Le tunnelage peut aussi permettre à un réseau informatique d'utiliser les services d'un second réseau bien que ce second réseau soit un ensemble de liaisons point à point entre les nœuds du premier réseau. (Voir : VPN.)

2. (O) /SET/ Nom d'une extension privée SET qui indique si la CA ou la passerelle de payement accepte de passer des messages chiffrés aux détenteurs de cartes à travers le commerçant. Si il en est ainsi, l'extension fait la liste des OID des algorithmes de chiffrement symétrique qui sont pris en charge.

$ mode tunnel *(tunnel mode)*

(I) Une des deux façons d'appliquer les protocoles IPsec (AH et ESP) pour protéger les paquets de données ; dans ce mode, le protocole IPsec encapsule (c'est-à-dire, la protection s'applique aux) les paquets IP, plutôt que les paquets de protocoles de couche supérieure. (Voir : tunnel. À comparer à : mode transport.)

Instructions : chaque extrémité d'une association de sécurité en mode tunnel peut être un hôte ou une passerelle de sécurité. Chaque fois que l'une ou l'autre extrémité d'une association de sécurité IPsec est une passerelle de sécurité, l'association est obligée d'être en mode tunnel.

$ contrôle par deux personnes *(two-person control)*

(I) Surveillance et contrôle étroits d'un système, d'un processus, ou de matériels (en particulier à l'égard de la cryptographie) à tout instant par un minimum de deux personnes autorisées de façon appropriée, chacune étant capable de détecter les procédures incorrectes et non autorisées par rapport aux tâches à effectuer et chacune étant familiarisée avec les exigences de sécurité établies. (Voir : contrôle duel, zone d'accompagnement obligatoire.)

$ Twofish

(O) Chiffrement symétrique de blocs de 128 bits avec une longueur de clé variable (128, 192, ou 256 bits) développée par Counterpane Labs comme candidat pour l'AES. (Voir : Blowfish.)

$ produit de type 0 *(type 0 product)*

(O) /cryptographie, Gouvernement des USA/ Équipement de cryptographie classifié approuvé par la NSA pour être utilisé (lorsque munie des clés appropriées) dans les matériels de chiffrement électroniques de distribution en vrac.

$ clé de type 1 *(type 1 key)*

(O) /cryptographie, Gouvernement des USA/ "Générée et distribuée sous les auspices de la NSA pour être utilisée dans un appareil cryptographique pour la protection d'informations classifiée et sensibles sur la sécurité nationale." [C4009]

$ produit de type 1 *(type 1 product)*

(O) /cryptographie, Gouvernement des USA/ "Assemblage ou composant d'équipement cryptographique classifié ou certifié par la NSA pour chiffrer et déchiffrer les informations classifiées et sensibles de la sécurité nationale lorsque chiffrées de façon appropriée. Développé en utilisant les processus de traitement établis par la NSA et contenant des

algorithmes approuvés par la NSA. Utilisé pour protéger des systèmes exigeant les mécanismes de protection les plus stricts". [C4009]
Instructions : la définition actuelle de ce terme est moins spécifique que celle d'une version antérieure : "Élément cryptographique classifié ou contrôlé approuvé par la NSA pour sécuriser les informations classifiées et sensibles du gouvernement des USA, lorsqu'elles sont chiffrées de façon appropriée. Le terme se réfère seulement aux produits, et non aux informations, clés, services, ou contrôles. Les produits de type 1 contiennent des algorithmes classifiés par la NSA. Ils sont disponibles pour les utilisateurs du gouvernement des USA, leurs cocontractants, et aux activités financées par le gouvernement fédéral des USA non sujettes aux restrictions d'exportation en accord avec le règlement international sur le trafic des armes." [d'après une version antérieure de C4009] (Voir : ITAR.)

$ clé de type 2 *(type 2 key)*
(O) /cryptographie, Gouvernement des USA/ "Générée et distribuée sous les auspices de la NSA pour être utilisée dans un appareil cryptographique pour la protection d'informations non classifiées de sécurité nationale." [C4009]

$ produit de type 2 *(type 2 product)*
(O) /cryptographie, Gouvernement des USA/ "Équipement cryptographique, assemblé ou de composant certifié par la NSA pour chiffrer et déchiffrer les informations sensibles de la sécurité nationale lorsque chiffrées de façon appropriée. Développé en utilisant les processus de traitement établis par la NSA et contenant des algorithmes approuvés par la NSA. Utilisé pour protéger des systèmes exigeant des mécanismes de protection qui excèdent les meilleures pratiques commerciales incluant des systèmes utilisés pour la protection d'informations non classifiées de sécurité nationale." [C4009]
Instructions : la définition actuelle de ce terme est moins spécifique que celle d'une version antérieure : "Assemblage ou composant d'équipement cryptographique non classifié approuvé par la NSA, pour être utilisé dans les systèmes de sécurité nationale comme définis dans l' U.S.C. Titre 40, Section 1452." [d'après une version antérieure de C4009] (Voir : système de sécurité nationale. À comparer à : EUCI.)

$ clé de type 3 *(type 3 key)*
(O) /cryptographe, Gouvernement des USA/ "Utilisé dans un appareil cryptographique pour la protection d'informations sensibles non classifiées, même si utilisé dans un produit de type 1 ou de type 2." [C4009]

$ produit de type 3 *(type 3 product)*
(O) /cryptographie, Gouvernement des USA/ "Assemblage ou composant d'équipement cryptographique non classifié utilisé, lorsque il est muni de clés appropriées, pour chiffrer ou déchiffrer des informations sensibles non classifiées du gouvernement des USA ou des informations commerciales, et pour protéger des systèmes qui exigent des mécanismes de protection cohérents avec les pratiques commerciales standard. Développé en utilisant les standard commerciaux établis et contenant des algorithmes/modules approuvés par le NIST ou évalués avec succès par le partenariat d'assurance des informations nationales (NIAP, *National Information Assurance Partnership*)." [C4009]

$ clé de type 4 *(type 4 key)*
(O) /cryptographie, Gouvernement des USA/ "Utilisée par un appareil de cryptographie à l'appui de sa fonctionnalité de type 4 ; c'est-à-dire, toute fourniture de clé qui n'a pas l'aval ou la tutelle du gouvernement des USA." [C4009]

$ produit de type 4 *(type 4 product)*
(O) /cryptographie, Gouvernement des USA/ "Assemblage ou composant non évalué d'un équipement commercial de cryptographie que ni la NSA ni le NIST ne certifient pour un usage gouvernemental. Ces produits sont normalement livrés au titre d'offres commerciales et sont en accord avec les pratiques commerciales du fabricant. Ces produits peuvent contenir des algorithmes qui sont la propriété du fabricant, des algorithmes enregistrés par le NIST, ou des algorithmes enregistrés par le NIST et publiés dans une FIPS." [C4009]

$ inondation UDP *(UDP flood)*
(I) Attaque de déni de service qui tire parti de la fonction d'essai UDP d'un système (a) qui génère une série de caractères pour chaque paquet reçu, et de la fonction d'essai UDP d'un autre système (b) qui fait écho à tout caractère qu'il reçoit ; l'attaque connecte (a) à (b) pour causer un flux ininterrompu de données entre les deux systèmes. (Voir : inondation.)

$ divulgation non autorisée *(unauthorized disclosure)*
(I) Circonstance ou événement par lequel une entité obtient l'accès à des informations auxquelles l'entité n'est pas autorisée.
Instructions : Ce type de conséquence de menace peut être causé par les types d'actions de menace suivants : exposition, interception, inférence, et intrusion. Certaines méthodes de protection contre ces conséquences incluent le contrôle d'accès, le contrôle de flux, et le contrôle d'inférence. (Voir : confidentialité des données.)

$ utilisateur non autorisé *(unauthorized user)*

(I) /contrôle d'accès/ Entité système qui accède à des ressources systèmes pour lesquelles elle n'a pas reçu d'autorisation. (Voir : usager. À comparer à : usager autorisé, interne, externe.)
Usage : les IDOC qui utilisent ce terme DEVRAIENT en donner une définition parce que le terme est utilisé de nombreuses façons et pourrait facilement être mal compris.

$ incertitude *(uncertainty)*
(N) Mesure théorique de l'information (normalement déclarée en nombre de bits) de la quantité minimum d'informations du texte source qui a besoin d'être récupérée à partir du texte chiffré pour connaître la totalité du texte source qui a été chiffré. [SP63] (Voir : entropie.)

$ non classifié *(unclassified)* (I) Qui n'est pas classifié. (À comparer à : FOUO.)

$ non chiffré *(unencrypted)* (I) Qui n'est pas chiffré.

$ infalsifiable *(unforgeable)*
(I) /cryptographie/ Propriété d'une structure de données cryptographique (c'est-à-dire, une structure de données qui est définie en utilisant une ou plusieurs fonctions cryptographiques, par exemple, "certificat numérique") qui rend impossible par le calcul de construire (c'est-à-dire, calculer) une valeur non autorisée mais correcte de la structure sans avoir connaissance d'une ou plusieurs clés.
Instructions : cette définition est plus étroite que celle de l'usage du français courant, où "infalsifiable" signifie incapable d'être créé ou dupliqué par fraude. Dans ce sens plus large, n'importe qui peut faire un faux certificat numérique contenant un ensemble quelconque d'éléments de données en générant le certificat à signer et en le signant avec une clé privée quelconque. Mais pour les besoins de PKI, la structure de données falsifiée est invalide si elle n'est pas signée avec la vraie clé privée du producteur prétendu ; donc, la falsification sera détectée lorsque un utilisateur de certificat utilisera la vraie clé publique du producteur prétendu pour vérifier la signature.

$ identifiant de ressource universel (URI, *uniform resource identifier*)
(I) (b) Type d'identifiant formaté (RFC3986) qui encapsule le nom d'un objet Internet, et l'étiquette avec une identification de l'espace de noms, produisant ainsi un membre de l'ensemble universel des noms dans les espaces de noms et d'adresses enregistrés qui se réfèrent aux protocoles ou espaces de noms enregistrés.
Exemple : HTML utilise des URI pour identifier la cible des hyperliens.
Usage : "Un URI peut être classé comme un localisateur (voir : URL), un nom (voir : URN), ou les deux. ... Des instances d'URI provenant de tout schéma peuvent avoir les caractéristiques de noms ou de localisateurs ou les deux, dépendant souvent de la persistance et du soin apporté à l'allocation des identifiants par l'autorité de désignation, plutôt que d'une qualité du schéma." Les IDOC DEVRAIENT "utiliser le terme général 'URI' plutôt que les termes plus restrictifs de 'URL' et 'URN'." (RFC3986)

$ localisateur de ressource universel (URL, *uniform resource locator*)
(I) URI qui décrit la méthode d'accès et la localisation d'un objet de ressource d'information sur l'Internet. (Voir : Usage sous "URI". À comparer à : URN.)
Instructions : le terme d'URL "se réfère au sous ensemble des URI qui, en plus d'identifier une ressource, fournit un moyen de localisation de la ressource en décrivant son principal mécanisme d'accès (par exemple, sa 'localisation' réseau)." (RFC3986) Un URL fournit des instructions explicites sur la façon d'accéder à l'objet désigné. Par exemple, "ftp://bbnarchive.bbn.com/foo/bar/picture/cambridge.zip" est un URL. La partie avant les deux-points spécifie le schéma ou le protocole d'accès, et la partie après les deux points est interprétée conformément à cette méthode d'accès. Généralement, deux barres obliques après les deux-points indiquent le nom d'hôte d'un serveur (écrit comme un nom de domaine). Dans un URL FTP ou HTTP, le nom d'hôte est suivi par le nom de chemin d'un fichier sur le serveur. La dernière partie (facultative) d'un URL peut être un fragment d'identifiant qui indique une position dans le fichier, ou une chaîne d'interrogation.

$ nom de ressource universel (URN, *uniform resource name*)
(I) URI qui a les propriétés d'un nom. (Voir : Usage sous "URI". À comparer à : URL.)
Instructions : le terme URN "a été utilisé historiquement pour se référer à la fois aux URI sous le schéma "urn" (RFC2141), qui sont obligés de rester uniques au monde et persistants même lorsque la ressource cesse d'exister ou devient indisponible, et à tout autre URI qui a les propriétés d'un nom." (RFC3986)

$ pas de confiance *(untrusted)* (I) Voir : définition secondaire sous "confiance".

$ processus qui n'est pas de confiance *(untrusted process)*
1. (I) Composant système qui n'est pas capable d'affecter l'état de sécurité du système par une opération incorrecte ou malveillante. Exemple : un composant qui a son fonctionnement confiné par un noyau de sécurité. (Voir : processus de

confiance.)
2. (I) Composant système qui (a) n'a pas été évalué ou examiné par rapport à l'adhésion à une politique de sécurité spécifiée et donc , (b) doit être supposé contenir une logique qui pourrait tenter de circonvenir la sécurité du système.

$ mise à jour *(update)* Voir : "mise à jour de certificat" et "mise à jour de clé".

$ mise à niveau *(upgrade)*
(I) /sécurité des données/ Augmentation du niveau de classification de données sans changer les informations contenues dans les données. (Voir : classifier, dégrader, reclassifier.)

$ utilisateur *(user)*
Voir : utilisateur système.
Usage : les IDOC qui utilisent de terme DEVRAIENT en donner une définition parce qu'il est utilisé de nombreuses façons et pourrait facilement être mal compris.

$ service d'authentification d'utilisateur *(user authentication service)*
(I) Service de sécurité qui vérifie l'identité revendiquée par une entité qui tente d'accéder au système. (Voir : authentification, usager.)

$ protocole de datagramme d'utilisateur (UDP, *User Datagram Protocol*)
(I) Norme de protocole de l'Internet, de couche Transport (RFC0768) qui livre une séquence de datagrammes d'un ordinateur à un autre dans un réseau informatique. (Voir : inondation UPD.)
Instructions : UDP suppose que IP est le protocole sous-jacent. UDP permet aux programmes d'application d'envoyer des données en mode transaction aux autres programmes avec un mécanisme minimal de protocole. UDP ne fournit pas de livraison fiable, de contrôle de flux, de séquençage, ou d'autres garanties de service de bout en bout que fournit TCP.

$ identifiant d'utilisateur *(user identifier)* (I) Voir : identifiant.

$ identité d'utilisateur *(user identity)* (I) Voir : identité.

$ PIN d'utilisateur *(user PIN)*
(O) /MISSI/ Un des deux PIN qui contrôlent l'accès aux fonctions et aux données mémorisées d'une carte PC FORTEZZA. La connaissance du PIN d'utilisateur permet à un utilisateur de carte d'effectuer les fonctions FORTEZZA qui sont destinées à être utilisées par un utilisateur final. (Voir : PIN. À comparer à : PIN SSO.)

$ ORA de PIN d'utilisateur (UORA, *user-PIN ORA*)
(O) /MISSI/ RA organisationnel MISSI qui opère dans un mode dans lequel l'ORA n'effectue que le sous ensemble des fonctions de gestion de carte qui est possible avec la connaissance du PIN d'utilisateur pour une carte PC FORTEZZA. (Voir : ORA sans PIN, ORA de PIN SSO.)

$ usurpation
(I) Circonstance ou événement qui résulte en le contrôle des services ou fonctions d'un système par une entité non autorisée. Ce type de conséquence de menace peut être causé par les types d'actions de menace suivants : appropriation délictueuse, mauvaise utilisation. (Voir : contrôle d'accès.)

$ heure UTC *(UTCTime)*
(N) Le type de données ASN.1 « UTCTime » contient une date calendaire (AAMMJJ) et une heure à une précision de une minute (HHMM) ou d'une seconde (HHMMSS), où l'heure est soit (a) le temps coordonné universel, soit (b) l'heure locale suivie par un décalage qui permet de calculer le temps coordonné universel. (Voir : Temps coordonné universel. À comparer à : Temps généralisé.)
Usage : si on se soucie des siècles ou des millénaires, on a probablement besoin du type de données GeneralizedTime plutôt que de UTCTime.

$ certificat v1 *(v1 certificate)*
(N) Abréviation qui se réfère de façon ambiguë soit à un « certificat de clé publique X.509 en format version 1 » soit à un « certificat d'attribut X.509 en format version 1 ».
Utilisation déconseillée : les IDOC PEUVENT utiliser ce terme comme abréviation de « certificat de clé publique X.509 version 1 », mais seulement après avoir utilisé le terme complet la première fois. Autrement, le terme est ambigu, parce que X.509 spécifie à la fois les certificats de clé publique v1 et les certificats d'attribut v1. (Voir : certificat d'attribut X.509, certificat de clé publique X.509.)

$ CRL v1 *(v1 CRL)*
(N) Abréviation de « CRL X.509 en format version 1 ».
Usage : les IDOC PEUVENT utiliser cette abréviation, mais DEVRAIENT utiliser le terme complet à sa première occurrence et définir l'abréviation à ce moment là.

$ certificat v2 *(v2 certificate)*
(N) Abréviation de « certificat de clé publique X.509 en format version 2 ».
Usage : les IDOC PEUVENT utiliser cette abréviation, mais DEVRAIENT utiliser le terme complet à sa première occurrence et définir l'abréviation à ce moment là.

$ CRL v2 *(v2 CRL)*
(N) Abréviation de « CRL X.509 en format version 2 ».
Usage : les IDOC PEUVENT utiliser cette abréviation, mais DEVRAIENT utiliser le terme complet à sa première occurrence et définir l'abréviation à ce moment là.

$ certificat v3 *(v3 certificate)*
(N) Abréviation de « certificat de clé publique X.509 en format version 3 ».
Usage : les IDOC PEUVENT utiliser cette abréviation, mais DEVRAIENT utiliser le terme complet à sa première occurrence et définir l'abréviation à ce moment là.

$ certificat valide *(valid certificate)*
1. (I) Certificat numérique qui peut être validé avec succès. (Voir : valider, vérifier.)
2. (I) Certificat numérique pour lequel on peut se fier au lien des éléments de données.

$ signature valide *(valid signature)*
(D) Synonyme de « signature vérifiée ».
Terme déconseillé : les IDOC NE DEVRAIT PAS utiliser ce synonyme. Le présent glossaire recommande de dire « valider le certificat » et « vérifier la signature » ; donc, il serait incohérent de dire qu'une signature est « valide ». (Voir : valider, vérifier.)

$ valider *(validate)*
1. (I) Établir la justesse ou la correction d'une construction. Exemple : validation de certificat. (Voir : valider vs. vérifier.)
2. (I) Approuver officiellement quelque chose, parfois en relation avec un standard. Exemple : le NIST valide la conformité des modules cryptographiques avec [FP140].

$ valider ou vérifier *(validate vs. verify)*
Usage : s'assurer de la cohérence et de l'alignement avec l'usage du français ordinaire, les IDOC DEVRAIENT se conformer aux deux règles suivantes :
- Règle 1 : utiliser "valider" pour se référer à un processus destiné à établir la justesse ou la correction d'une construction (par exemple, "validation de certificat"). (Voir : valider.)
- Règle 2 : utiliser "vérifier" pour se référer à un processus destiné à essayer ou prouver la vérité ou la précision d'un fait ou d'une valeur (par exemple, "authentifier"). (Voir : vérifier.)

Instructions : la communauté de la sécurité de l'Internet utilise parfois ces deux termes de façon incohérente, en particulier dans un contexte de PKI. Le plus souvent cependant, on dit "vérifier la signature" mais on dit "valider le certificat". C'est-à-dire, on "vérifie" des vérités atomiques mais on "valide" des structures de données, des relations, et des systèmes qui sont composés de ou dépendent d'éléments vérifiés. Cet usage a une base en latin :
Le mot "valide" est dérivé d'un mot latin qui signifie "bien portant". Donc, valider signifie vérifier qu'une construction est juste. Par exemple, un utilisateur de certificat valide un certificat de clé publique pour établir la confiance dans le lien que le certificat affirme entre une identité et une clé. Cela peut inclure de vérifier divers aspects de la construction du certificat, comme de vérifier la signature numérique sur le certificat en effectuant des calculs, de vérifier que l'heurs courante est dans la période de validité du certificat, et de valider un chemin de certification impliquant des certificats supplémentaires.
Le mot "vérifier" est dérivé d'un mot latin qui signifie "vrai". Donc, vérifier signifie rechercher la vérité d'une assertion en examinant les preuves ou en effectuant des essais. Par exemple, pour vérifier une identité, un processus d'authentification examine les informations d'identification qui sont présentées ou générées. Pour valider un certificat, un utilisateur de certificat vérifie la signature numérique sur le certificat en effectuant des calculs, vérifie que l'heure courante est dans la période de validité du certificat, et peut avoir besoin de valider un chemin de certification qui implique des certificats supplémentaires.

$ validation (I) Voir : valider ou vérifier.

$ période de validité *(validity period)*
(I) /PKI/ Élément de données, dans un certificat numérique, qui spécifie la période de temps pendant laquelle le lien entre les éléments de données (en particulier entre le nom du sujet et la valeur de clé publique dans un certificat de clé publique) est valide, sauf si le certificat apparaît sur une CRL ou si la clé apparaît sur une CKL. (Voir : cryptopériode, durée de vie de clé.)

$ réseau à valeur ajoutée (VAN, *value-added network*)
(I) Réseau ou sous réseau informatique (généralement une entreprise commerciale) qui transmet, reçoit, et mémorise des transactions d'EDI au nom de ses utilisateurs.
Instructions : un VAN peut aussi fournir des services additionnels, allant de la traduction de format d'EDI à la conversion d'EDI en télécopie, jusqu'à des systèmes d'affaires intégrés.

$ vérification *(verification)*
1. (I) /authentification/ Processus d'examen d'informations pour établir la vérité d'un fait ou valeur revendiqué. (Voir : valider vs. vérifier, vérifier. À comparer à : authentification.)
2. (N) /COMPUSEC/ Processus de comparaison de deux niveaux de spécification de système pour une correspondance appropriée, comme de comparer un modèle de sécurité avec une spécification de niveau supérieur, une spécification de niveau supérieur avec le code source, ou le code source avec le code d'objet. [NCS04]

$ conception vérifiée *(verified design)* (O) Voir : TCSEC classe A1.

$ vérifier *(verify)*
(I) Faire des essais pour prouver ou prouver la vérité ou l'exactitude d'un fait ou d'une valeur. (Voir : valider vs. vérifier, vérification. À comparer à : authentifier.)

$ effectuer un contrôle de sécurité *(vet)*
(I) /verbe/ Examiner ou évaluer attentivement. (À comparer à : authentifier, preuve d'identité, valider, vérifier.)

$ violation Voir : violation de la sécurité.

$ réseau privé virtuel (VPN, *virtual private network*)
(I) Réseau informatique à utilisation restreinte, logique (c'est-à-dire, artificiel ou simulé) qui est construit à partir des ressources système d'un réseau relativement public, physique (c'est-à-dire, réel) (par exemple, l'Internet) souvent en utilisant le chiffrement (localisé chez les hôtes ou les passerelles) et souvent en tunnelant les liaisons du réseau virtuel à travers le réseau réel. (Voir : tunnel.)
Instructions : un VPN est généralement moins coûteux à la construction et en fonctionnement qu'un réseau réel dédié, parce que le réseau virtuel partage les coûts des ressources système avec les autres utilisateurs du réseau réel sous-jacent. Par exemple, si une corporation a des LAN sur plusieurs sites différents, chacun connecté à l'Internet par un pare-feu, la corporation pourrait créer un VPN en utilisant des tunnels cryptés pour se connecter de pare-feu à pare-feu à travers l'Internet.

$ virus
(I) Section de logiciel (généralement malveillant) informatique auto-réplicative (et généralement cachée) qui se propage en infectant -- c'est-à-dire, en insérant une copie de lui-même et en s'incorporant -- dans un autre programme. Un virus ne peut pas fonctionner par lui-même, il requiert que son programme hôte fonctionne pour rendre le virus actif.

$ Visa Cash
(O) Système de monnaie électronique fondé sur une carte à mémoire qui incorpore de la cryptographie et peut être utilisé pour faire des payements via l'Internet. (Voir : IOTP.)

$ support volatile *(volatile media)*
(I) Support de mémorisation qui exige une alimentation en énergie externe pour garder des informations mémorisées. (À comparer à : support non volatile, stockage permanent.)

$ vulnérabilité *(vulnerability)*
(I) Faute ou faiblesse dans la conception, la mise en œuvre, ou le fonctionnement et la gestion d'un système, qui pourrait être exploitée pour violer la politique de sécurité du système. (Voir : durcir.)
Instructions : un système peut avoir trois types de vulnérabilités : (a) des vulnérabilités dans la conception ou la spécification, (b) des vulnérabilités dans la mise en œuvre, et (c) des vulnérabilités dans le fonctionnement et la gestion. La plupart des systèmes ont une ou plusieurs vulnérabilités, mais cela ne signifie pas que les systèmes soient trop fautifs pour

être utilisés. Toute menace ne résulte pas en une attaque, et toute attaque ne réussit pas. Le succès dépend du degré de vulnérabilité, de la force des attaques, et de l'efficacité des contre-mesures utilisées. Si les attaques nécessaires pour exploiter une vulnérabilité sont très difficiles à mettre en place, la vulnérabilité peut être tolérable. Si le bénéfice perçu par un attaquant est faible, même une vulnérabilité facile à exploiter peut être tolérable. Cependant, si les attaques sont bien comprises et faciles à faire, et si le système vulnérable est employé par une large gamme d'utilisateurs, il est alors vraisemblable que quelqu'un trouvera un motif pour lancer une attaque.

$ W3
(D) Synonyme de WWW.
Abréviation déconseillée : cette abréviation pourrait être confondue avec le W3C ; utiliser "WWW" à la place.

$ war dialer
(I) /argot/ Programme informatique qui compose automatiquement une série de numéros de téléphone pour trouver des lignes connectées à des systèmes d'ordinateurs, et qui catalogue ces numéros afin qu'un craqueur puisse essayer de casser les systèmes.
Utilisation déconseillée : les IDOC qui utilisent de terme DEVRAIENT en donner une définition parce que le terme pourrait être une source de confusion pour les lecteurs étrangers.

$ Accord Wassenaar *(Wassenaar Arrangement)*
(N) L'accord Wassenaar sur le contrôle de l'exportation des armes conventionnelles et les biens et technologies à double utilisation est un accord multilatéral mondial approuvé par 33 pays en juillet 1996 pour contribuer à la sécurité et la stabilité régionale et internationale, par la promotion de l'échange d'informations concernant les transferts d'armes et éléments à double usage, et une plus grande responsabilité à leur égard, empêchant ainsi les accumulations déstabilisantes. (Voir : Règles internationales sur le trafic d'armes.)
Instructions : l'accord a commencé son fonctionnement en septembre 1996 avec son siège à Vienne. Les pays participants étaient l'Argentine, l'Australie, l'Autriche, la Belgique, la Bulgarie, le Canada, la République Tchèque, le Danemark, la Finlande, la France, l'Allemagne, la Grèce, la Hongrie, L'Irlande, l'Italie, le Japon, le Luxembourg, Les Pays-Bas, la Nouvelle Zélande, la Norvège, la Pologne, le Portugal, La République de Corée, la Roumanie, la Fédération de Russie, la Slovaquie, l'Espagne, la Suède, la Suisse, la Turquie, l'Ukraine, le Royaume-Uni, et les États Unis d'Amérique.
Les pays participants cherchent à travers leurs politiques nationales à assurer que les transferts ne contribuent pas au développement ou à l'amélioration des capacités militaires qui saperaient les objectifs de l'accord, et ne sont pas détournés pour soutenir de telles capacités. Les pays maintiennent un contrôle effectif des exportations des éléments figurant sur les listes objet de l'accord, qui sont revues périodiquement pour tenir compte des développements technologiques et de l'expérience accumulée. Par la transparence et des échanges de vues et d'informations, les fournisseurs d'armes et d'éléments à double usage peuvent développer une compréhension commune des risques associés à leurs transferts et vérifier leur portée pour coordonner les politiques de contrôle nationales pour combattre ces risques. Les membres fournissent des notification semestrielles des transferts d'armes, couvrant sept catégories dérivées du registre des armes conventionnelles des Nations Unies. Les membres rapportent aussi les transferts ou refus de transferts de certains éléments à double usage contrôlés. Cependant, la décision de transférer ou de refuser de transférer tout élément est de la seule responsabilité de chaque pays participant. Toutes les mesures prises par rapport à l'accord sont en conformité avec la législation et les politiques nationales et sont mises en œuvre à la discrétion de chaque pays.

$ marquage effaçable *(watermarking)* Voir : marquage numérique effaçable.

$ clé faible *(weak key)*
(I) Dans le contexte d'un algorithme cryptographique particulier, une valeur de clé qui fournit une faible sécurité. (Voir : fort.)
Exemple : le DEA a quatre "clés faibles" [Schn] pour lesquelles le chiffrement produit le même résultat que le déchiffrement. Il a aussi dix paires de "clé semi faibles" [Schn] (autrement dit "de clés duales" [FP074]) pour lesquelles le chiffrement avec une clé de la paire produit le même résultat que le déchiffrement avec l'autre clé.

$ la toile, la Toile *(web, Web)*
1. (I) /en minuscules/ Les IDOC NE DEVRAIENT PAS mettre en majuscule la "toile" lorsque ils utilisent le terme (généralement comme adjectif) pour se référer de façon générique à la technologie -- comme dans les navigateurs de la toile, les serveurs de la toile, HTTP, et HTML --qui est utilisés sur la Toile ou des réseaux similaires.
2. (I) /en majuscules/ Les IDOC DEVRAIENT mettre la "Toile" en majuscules lorsque ils utilisent le terme (comme nom ou comme adjectif) pour se référer spécifiquement à la Toile mondiale. (De même, voir : internet.)

Usage : les IDOC NE DEVRAIENT PAS utiliser "toile" ou "Toile" d'une façon qui pourrait faire confondre ces définitions avec la "toile de confiance" de PGP. Lorsque on utilise Toile comme une abréviation pour la "Toile mondiale", les IDOC DEVRAIENT développer complètement le terme à sa première instance d'usage.

$ toile de confiance *(web of trust)*
(D) /PGP/ Architecture de PKI dans laquelle chaque utilisateur de certificat définit sa ou ses propres ancres de confiance en s'appuyant sur ces relations personnelles. (Voir : ancre de confiance. À comparer à : PKI hiérarchique, PKI maillée.)
Utilisation déconseillée : les IDOC NE DEVRAIENT PAS utiliser ce terme sauf par référence à PGP. Ce terme mélange des concepts d'une façon potentiellement trompeuse, par exemple, cette architecture ne dépend pas de la technologie de la Toile mondiale. À la place de ce terme, les IDOC PEUVENT utiliser "PKI de fichier de confiance". (Voir : toile, Toile).
Instructions : ce type d'architecture n'inclut généralement pas de répertoire public de certificats. À la place, chaque utilisateur de certificat construit son propre répertoire privé de clés publiques de confiance en portant des jugements personnels sur sa capacité à faire confiance à certaines personnes pour détenir convenablement des clés certifiées d'autres personnes. C'est de cet ensemble de relations de personne à personne que l'architecture tire son nom.

$ serveur de la Toile *(web server)*
(I) Processus logiciel qui fonctionne sur un ordinateur hôte connecté à un réseau et qui répond aux demandes HTTP faites par les navigateurs de la Toile clients.

$ confidentialité câblée équivalente (WEP, *Wired Equivalent Privacy*)
(N) Protocole cryptographique qui est défini dans la norme IEEE 802.11 et encapsule les paquets sur des LAN sans fils.
Usage : autrement dit "protocole d'équivalence câblée".
Instructions : la conception de WEP, qui utilise RC4 pour chiffrer à la fois le texte source et un CRC, a été démontrée fautive de nombreuses façons, et elle a aussi souvent souffert de mises en œuvre et de gestion fautives.

$ écoute *(wiretapping)*
(I) Attaque qui intercepte et accède aux informations contenues dans un flux de données dans un système de communication. (Voir : écoute active, chiffrement de bout en bout, écoute passive, définition secondaire sous "interception".)
Usage : bien que le terme se réfère à l'origine à faire une connexion mécanique à un conducteur électrique qui relie deux nœuds, il est maintenant utilisé pour se référer à l'accession à des informations à partir de toutes sortes de supports utilisés pour une liaison ou même à partir d'un nœud, comme d'une passerelle ou d'un commutateur de sous réseau.
Instructions : l'écoute peut être caractérisée selon l'intention :
- "l'écoute active" tente d'altérer les données ou d'affecter autrement le flux ;
- "l'écoute passive" tente seulement d'observer le flux de données et d'obtenir la connaissance des informations qu'il contient.

$ facteur de travail *(work factor)*
1a. (I) /COMPUSEC/ Quantité estimée d'efforts ou de temps qu'on peut s'attendre que doive dépenser un intrus potentiel pour pénétrer un système, ou vaincre une contre-mesure particulière, quand on utilise des quantités spécifiées d'expertise et de ressources. (Voir : force brute, impossible, force.)
1b. (I) /cryptographie/ Quantité estimée de puissance de calcul et de temps nécessaire pour casser un système cryptographique. (Voir : force brute, impossible, force.)

$ Toile mondiale *(World Wide Web "the Web", WWW)*
(N) Collection mondiale, fondée sur l'hypermédia, d'informations et services qui est disponible sur les serveurs Internet et à laquelle accèdent les navigateurs qui utilisent le protocole de transfert hypertexte et d'autres mécanismes de restitution d'informations. (Voir : la toile, la Toile, [RFC2084].)

$ consortium de la Toile Mondiale (W3C, *World Wide Web Consortium*)
(N) Créé en octobre 1994 pour développer et normaliser des protocoles pour promouvoir l'évolution et l'interopérabilité de la Toile, et qui comporte maintenant des centaines d'organisations membres (entreprises commerciales, agences gouvernementales, universités, et autres).
Instructions : les recommandations du W3C sont développées selon un processus similaire à celui des normes publiées par les autres organisations, comme l'IETF. Le chemin de la recommandation W3 (c'est-à-dire, la voie de la normalisation) a quatre niveaux de maturité croissante : document de travail, recommandation candidate, recommandation proposée, et recommandation W3C. Les recommandations W3C sont similaires aux normes publiées par les autres organisations. (À comparer à : norme de l'Internet, ISO.)

$ ver *(worm)*
(I) Programme informatique qui peut fonctionner de façon indépendante, peut propager une version fonctionnelle complète de lui-même sur d'autre hôtes d'un réseau, et peut consommer de façon destructives des ressources système. (Voir : code mobile, ver de Morris, virus.)

$ envelopper *(wrap)*

1. (N) Utiliser la cryptographie pour assurer un service de confidentialité des données pour du matériel de chiffrement. (Voir : chiffrer, algorithme d'enveloppe, clé d'enveloppe. À comparer à : sceller, blinder.)
2. (D) Utiliser la cryptographie pour fournir un service de confidentialité des données pour les données en général.

Utilisation déconseillée : les IDOC NE DEVRAIENT PAS utiliser ce terme avec la définition 2 parce que cela duplique la signification du terme largement compris de "chiffrer".

$ algorithme d'enveloppe *(wrapping algorithm)*
(N) Algorithme de chiffrement qui est spécifiquement destiné à l'utilisation par des clés de chiffrement. (Voir : KEK, envelopper.)

$ clé d'enveloppe *(wrapping key)*
(N) Synonyme de "KEK". (Voir : chiffrer. À comparer à : sceller, blinder.)

$ écrire *(write)*
(I) /modèle de sécurité/ Opération système qui cause un flux d'informations d'un sujet à un objet. (Voir : mode d'accès. À comparer à : lire.)

$ X.400
(N) Recommandation de l'UIT-T [X400] qui est une partie d'une norme multiparties conjointe UIT-T/ISO (X.400-X.421) qui définit les systèmes de traitement de message. (L'équivalent ISO est l'IS 10021, parties 1-7.) (Voir : systèmes de traitement de message.)

$ X.500
(N) Recommandation de l'UIT-T [X500] qui est une partie d'une norme multiparties conjointe UIT-T/ISO (X.500-X.525) qui définit l'annuaire X.500, une collection conceptuelle de systèmes qui fournissent des capacités de répertoire répartis pour les entités, processus, applications, et services OSI. (l'équivalent ISO est l'IS 9594-1 et les normes qui s'y rapportent, IS 9594-x.) (Voir : répertoire vs. Annuaire, X.509.)
Instructions : l'annuaire X.500 est structuré comme une arborescence (l'arbre des informations d'annuaire) et les informations sont mémorisées dans les entrées de l'annuaire. Chaque entrée est une collection d'informations sur un objet, et chaque objet a un DN. Une entrée d'annuaire est composée d'attributs, ayant chacun un type et une ou plusieurs valeurs. Par exemple, si une PKI utilise l'annuaire pour distribuer des certificats, le certificat de clé publique X.509 d'un utilisateur final est alors normalement mémorisé comme valeur d'un attribut de type "userCertificate" dans l'entrée d'annuaire qui a le DN qui est le sujet du certificat.

$ X.509
(N) Recommandation de l'UIT-T [X509] qui définit un cadre pour fournir et prendre en charge l'authentification de l'origine des données et l'authentification de l'entité homologue, incluant les formats pour les certificats de clé publique X.509, les certificats d'attribut X.509, et les CRL X.509. (L'équivalent ISO est l'IS 9498-4.) (Voir : X.500.)
Instructions : X.509 décrit deux "niveaux" d'authentification: "l'authentification simple" et "l'authentification forte". Elle recommande que "bien que l'authentification simple offre une protection limitée contre l'accès non autorisé, seule l'authentification forte devrait être utilisée comme base de la fourniture de services sûrs."

$ certificat d'attribut X.509 *(X.509 attribute certificate)*
(N) Certificat d'attribut dans le format de version 1 (v1) défini par X.509. (La désignation v1 pour un certificat d'attribut X.509 est disjointe de la désignation v1 pour un certificat de clé publique X.509, et de la désignation v1 pour une CRL X.509.)
Instructions : un certificat d'attribut X.509 a un champ "subject", mais le certificat d'attribut est une structure de données séparée de celle d'un certificat de clé publique de sujet. Un sujet peut avoir plusieurs certificats d'attribut associés à chacun de ses certificats de clé publique, et un certificat d'attribut peut être produit par une CA différente de celle qui a produit le certificat de clé publique associée.
Un certificat d'attribut X.509 contient une séquence d'éléments de données et a une signature numérique qui est calculée à partir de cette séquence. À côté de la signature, un certificat d'attribut contient des éléments 1 à 9 cités ci-dessous :

1. version	identifie v1.
2. subject	est un des suivants :
2a. baseCertificateID	producteur et numéro de série d'un certificat de clé publique X.509.
2b. subjectName	DN du sujet.
3. issuer	DN du producteur (la CA qui a signé).
4. signature	OID de l'algorithme qui a signé le certificat.
5. serialNumber	numéro de série du certificat ; un entier alloué par le producteur.
6. attCertValidityPeriod	période de validité ; une paire de valeurs de UTCTime : "pas avant" et "pas après".
7. attributes	séquence d'attributs décrivant le sujet.

8. issuerUniqueId	facultatif, quand un DN n'est pas suffisant.
9. extensions	facultatif.

$ certificat X.509 *(X.509 certificate)*
(N) Synonyme de "certificat de clé publique X.509".
Usage : les IDOC PEUVENT utiliser ce terme comme abréviation de "certificat de clé publique X.509", mais seulement après avoir utilisé le terme complet la première fois. Autrement, le terme est ambigu, parce que X.509 spécifie aussi bien les certificats de clé publique que les certificats d'attribut. (Voir : certificat d'attribut X.509, certificat de clé publique X.509.)
Utilisation déconseillée : les IDOC NE DEVRAIENT PAS utiliser ce terme comme abréviation de "certificat d'attribut X.509", parce que le terme est beaucoup plus couramment utilisé pour signifier "certificat de clé publique X.509" et donc, il sera vraisemblablement mal compris.

$ liste de révocation de certificats X.509 (CRL, *X.509 certificate revocation list*)
(N) Une CRL dans un des formats définis par X.509 -- version 1 (v1) ou version 2 (v2). (Les désignations v1 et v2 pour une CRL X.509 sont disjointes des désignations v1 et v2 pour un certificat de clé publique X.509, et de la désignation v1 pour un certificat d'attribut X.509.) (Voir : révocation de certificat.)
Usage : les IDOC NE DEVRAIENT PAS se référer à une CRL X.509 comme à un certificat numérique ; cependant, noter qu'une CRL X.509 ne satisfait pas à la définition du présent glossaire de "certificat numérique". C'est-à-dire que, comme un certificat numérique, une CRL X.509 fait une assertion et est signée par une CA. Mais au lieu de lier une clé ou d'autres attributs à un sujet, une CRL X.509 affirme que certains certificats X.509 produits précédemment ont été révoqués.
Instructions : une CRL X.509 contient une séquence d'éléments de données et a une signature numérique calculée sur cette séquence. À côté de la signature, v1 et v2 contiennent des éléments 2 à 6b cités ci-dessous. La version 2 contient l'élément 1 et peut facultativement contenir 6c et 7.

1. version	facultatif. Si présent, identifie v2.
2. signature	OID de l'algorithme qui a signé la CRL.
3. issuer	DN du producteur (la CA qui a signé).
4. thisUpdate	valeur d'UTCTime.
5. nextUpdate	valeur d'UTCTime.
6. revokedCertificates	triplet de 6a, 6b, et (facultatif) 6c :
6a. userCertificate	numéro de série d'un certificat.
6b. revocationDate	valeur d'UTCTime de la date de révocation.
6c. crlEntryExtensions	facultatif.
7. crlExtensions	facultatif.

$ certificat de clé publique X.509 *(X.509 public-key certificate)*
(N) Certificat de clé publique dans un des formats définis par X.509 -- version 1 (v1), version 2 (v2), ou version 3 (v3). (Les désignations v1 et v2 pour un certificat de clé publique X.509 sont disjointes de la désignation v1 et v2 pour une CRL X.509, et de la désignation v1 pour un certificat d'attribut X.509.)
Instructions : un certificat de clé publique X.509 contient une séquence d'éléments de données et a une signature numérique calculée sur cette séquence. À côté de la signature, les trois versions contiennent toutes les éléments 1 à 7 cités ci-dessous. Seuls les certificats v2 et v3 peuvent aussi contenir les éléments 8 et 9, et seul v3 peut contenir l'élément 10.

1. version	Identifie v1, v2, ou v3.
2. serialNumber	Numéro de série de certificat, un entier alloué par le producteur.
3. signature	OID de l'algorithme qui a été utilisé pour signer le certificat.
4. issuer	DN du producteur (la CA qui a signé).
5. validity	Période de validité, paire de valeurs de UTCTime : "pas avant" et "pas après".
6. subject	DN de l'entité qui possède la clé publique.
7. subjectPublicKeyInfo	Valeur de la clé publique et OID de l'algorithme.
8. issuerUniqueIdentifier	Défini pour v2, v3, facultatif.
9. subjectUniqueIdentifier	Défini pour v2, v3, facultatif.
10. extensions	Défini seulement pour v3, facultatif.

$ X9 (N) Voir : "Comité de normalisation accrédité X9" sous "ANSI".

$ signature XML *(XML-Signature)*
(N) Recommandation du W3C (c'est-à-dire, norme approuvée) qui spécifie la syntaxe XML et les règles de traitement pour créer et représenter les signatures numériques (fondées sur le chiffrement asymétrique) qui peut être appliquée à tout contenu numérique (c'est-à-dire, tout objet de données) y compris à d'autre matériel XML.

$ Livre Jaune *(Yellow Book)*

(D) /argot/ Synonyme de "Exigences de sécurité informatique : Guide d'application des critères d'évaluation de système informatique de confiance du ministère U.S. de la Défense dans des environnements spécifiques" [CSC3] (Voir : "première loi" sous les "Lois de Courtney".)
Terme déconseillé : les IDOC NE DEVRAIENT PAS utiliser ce terme comme synonyme de ce document ou tout autre document. À la place, utiliser le nom complet approprié du document ou, dans les références suivantes, une abréviation conventionnelle. (Voir : Utilisation déconseillée sous "Livre Vert", Série Arc-en-ciel.)

$ preuve à connaissance zéro *(zero-knowledge proof)*
(I) /cryptographie/ Protocole de preuve de possession par lequel une entité système peut prouver à une autre entité la possession de certaines informations, sans révéler ces informations. (Voir : protocole de preuve de possession.)

$ zéroïser
1. (I) Synonyme de "écraser". (Voir : assainir.) Usage : Particulièrement à l'égard de l'écrasement de clés qui sont mémorisées dans un module cryptographique.
2. (O) Écraser des données mémorisées électroniquement en altérant le contenu de la mémorisation des données de façon à empêcher la récupération des données. [FP140]
3. (O) "Retirer ou éliminer la clé d'un équipement cryptographique ou appareil de remplissage." [C4009]

Usage : la phrase "zéroïser l'appareil" est normalement utilisée pour dire écraser toutes les clé mémorisées dans l'appareil, mais signifie parfois d'écraser tout le matériel de clé dans l'appareil, ou toutes les informations cryptographiques dans l'appareil, ou même toutes les informations sensibles dans l'appareil.

$ zombie
(I) /argot/ Ordinateur hôte de l'Internet qui a été subrepticement pénétré par un intrus qui a installé un logiciel démon malveillant pour obliger l'hôte à fonctionner comme complice d'attaques d'autres hôtes, en particulier dans des attaques réparties qui tentent un déni de service par inondation.
Utilisation déconseillée : d'autres cultures utilisent vraisemblablement des métaphores différentes (comme "robot") pour ce concept, et certains utilisent ce terme pour des concepts différents. Donc, pour éviter une incompréhension entre les nations, les IDOC NE DEVRAIENT PAS utiliser ce terme. À la place, utiliser "ordinateur compromis, coopté" ou autre terminologie explicitement descriptive. (Voir : Utilisation déconseillée sous "Livre Vert".)

$ zone de contrôle (O) /EMSEC/ Synonyme pour "espace inspectable". [C4009] (Voir : TEMPEST.)

5. Considérations pour la sécurité

Le présent document définit principalement des termes dans le domaine de la sécurité et recommande la façon de les utiliser. Il donne aussi des informations didactiques limitées sur les aspects de sécurité des protocoles de l'Internet, mais il ne décrit pas en détail les faiblesses ou les menaces de protocoles spécifique, pas plus qu'il ne décrit les détails des mécanismes qui protègent des protocoles spécifiques.

6. Référence normatives

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997.

7. Références informatives

Ce glossaire se concentre sur le processus de normalisation de l'Internet. Cet ensemble de références met l'accent sur les documents de normalisation internationale, gouvernementale, et industrielle. Certaines RFC qui sont particulièrement pertinentes pour la sécurité de l'Internet sont mentionnées dans les entrées du glossaire entre crochets (par exemple, "[RFC1457]" dans l'entrée pour "étiquette de sécurité") et figurent ici ; d'autres RFC sont mentionnées entre parenthèses (par exemple, "(RFC 959)" dans l'entrée pour "Protocole de transport de fichier") mais ne figurent pas ici.

[A1523] American National Standards Institute, "American National Standard Telecom Glossary", ANSI T1.523-2001.

[A3092] ---, "American National Standard Data Encryption Algorithm", ANSI X3.92-1981, 30 décembre 1980.

[A9009] ---, "Financial Institution Message Authentication (Wholesale)", ANSI X9.9-1986, 15 août 1986.

[A9017] ---, "Financial Institution Key Management (Wholesale)", X9.17, 4 avril 1985. (Définit les procédures pour la

gestion manuelle et automatisée des matériaux de clé et utilise DES pour la fourniture de la gestion de clé pour divers environnements de fonctionnement.)

[A9042] ---, "Public key Cryptography for the Financial Service Industry: Agreement of Symmetric Keys Using Diffie-Hellman and MQV Algorithms", X9.42, 29 janvier 1999. (Voir : Diffie-Hellman-Merkle.)

[A9052] ---, "Triple Data Encryption Algorithm Modes of Operation", X9.52-1998, approuvé ANSI le 9 novembre 1998.

[A9062] ---, "Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)", X9.62-1998, approuvé ANSI le 7 janvier 1999.

[A9063] ---, "Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography", X9.63-2001.

[ACM] Association for Computing Machinery, "Communications of the ACM", juillet 1998 avec M. Yeung, "Digital Watermarking"; N. Memom and P. Wong, "Protecting Digital Media Content" ; et S. Craver, B.-L. Yeo, and M. Yeung, "Technical Trials and Legal Tribulations".

[Ande] Anderson, J., "Computer Security Technology Planning Study", ESD-TR-73-51, Vols. I and II, USAF Electronics Systems Div., Bedford, MA, octobre 1972. (Disponible sous AD-758206/772806, National Technical Information Service, Springfield, VA.)

[ANSI] American National Standards Institute, "Role Based Access Control", Secretariat, Information Technology Industry Council, BSR INCITS 359, projet, 10 novembre 2003.

[Army] U.S. Army Corps of Engineers, "Electromagnetic Pulse (EMP) and Tempest Protection for Facilities", EP 1110-3-2, 31 décembre 1990.

[B1822] Bolt Baranek and Newman Inc., "Appendix H: Interfacing a Host to a Private Line Interface", dans "Specifications for the Interconnection of a Host and an IMP", BBN Report n° 1822, révisé, décembre 1983.

[B4799] ---, "A History of the Arpanet: The First Decade", BBN Report n° 4799, avril 1981.

[Bell] Bell, D. and L. LaPadula, "Secure Computer Systems: Mathematical Foundations and Model", M74-244, The MITRE Corporation, Bedford, MA, mai 1973. (Disponible sous AD-771543, National Technical Information Service, Springfield, VA.)

[Biba] K. Biba, "Integrity Considerations for Secure Computer Systems", ESD-TR-76-372, USAF Electronic Systems Division, Bedford, MA, avril 1977.

[BN89] Brewer, D. and M. Nash, "The Chinese wall politique de sécurité", dans "Proceedings of IEEE Symposium on Security and Privacy", mai 1989, pp. 205-214.

[BS7799] British Standards Institution, "Information Security Management, Part 1: Code of Practice for Information Security Management", BS 7799-1:1999, 15 mai 1999.

---, "Information Security Management, Part 2: Specification for Information Security Management Systems", BS 7799- 2:1999, 15 mai 1999.

[C4009] Committee on National Security Systems (Gouvernement des USA), "National Information Assurance (IA) Glossary", CNSS Instruction n° 4009, révisé en juin 2006.

[CCIB] Critères communs Implementation Board, "Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model", version 2.0, CCIB-98-026, mai 1998.

[Chau] D. Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms", dans "Communications of the ACM", vol. 24, n° 2, février 1981, pp. 84-88.

[Cheh] Cheheyl, M., Gasser, M., Huff, G., and J. Millen, "Verifying Security", dans "ACM Computing Surveys", vol. 13,

n° 3, septembre 1981, pp. 279-339.

[Chris] Chrissis, M. et al, 1993. "SW-CMM [Capability Maturity Model for Software Version", Release 3.0, Software Engineering Institute, Carnegie Mellon University, août 1996.

[CIPSO] Trusted Systems Interoperability Working Group, "Common IP Security Option", version 2.3, 9 mars 1993.

[Clark] Clark, D. and D. Wilson, "A Comparison of Commercial and Military computer Security Policies", in "Proceedings of the IEEE Symposium on Security and Privacy", avril 1987, pp. 184-194.

[Cons] NSA, "Consistency Instruction Manual for Development of US Government Protection Profiles for Use in Basic Robustness Environments", Release 2.0, 1 mars 2004

[CORBA] Object Management Group, Inc., "CORBAservices: Common Object Service Specification", décembre 1998.

[CSC1] U.S. DoD Computer Security Center, "Department of Defense Trusted Computer System Evaluation Criteria", CSC-STD-001-83, 15 août 1983. (Remplacé par [DoD1].)

[CSC2] ---, "Department of Defense Password Management Guideline", CSC-STD-002-85, 12 avril 1985.

[CSC3] ---, "Computer Security Requirements: Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments", CSC-STD-003-85, 25 juin 1985.

[CSOR] U.S. Department of Commerce, "General Procedures for Registering Computer Security Objects", National Institute of Standards Interagency Report 5308, décembre 1993.

[Daem] Daemen, J. and V. Rijmen, "Rijndael, the advanced encryption standard", dans "Dr. Dobb's Journal", vol. 26, n° 3, mars 2001, pp. 137-139.

[DC6/9] Director of Central Intelligence, "Physical Security Standards for Sensitive Compartmented Information Facilities", DCI Directive 6/9, 18 novembre 2002.

[Denn] Denning, D., "A Lattice Model of Secure Information Flow", dans "Communications of the ACM", vol. 19, n°5, mai 1976, pp. 236-243.

[Denns] Denning, D. and P. Denning, "Data Security", dans "ACM Computing Surveys", vol. 11, n° 3, septembre 1979, pp. 27-249.

[DH76] Diffie, W. and M. Hellman, "New Directions in Cryptography", dans "IEEE Transactions on Information Theory", vol. IT-22, n° 6, novembre 1976, pp. 644-654. (Voir : Diffie-Hellman-Merkle.)

[DoD1] U.S. DoD, "Department of Defense Trusted Computer System Evaluation Criteria", DoD 5200.28-STD, 26 décembre 1985. (Remplace [CSC1].) (Remplacé par DoD Directive 8500.1.)

[DoD4] ---, "NSA Key Recovery Assessment Criteria", 8 June 1998. [DoD5] ---, Directive 5200.1, "DoD Information Security Program", 13 décembre 1996.

[DoD6] ---, "Department of Defense Technical Architecture Framework for Information Management, Volume 6: Department of Defense (DoD) Goal Security Architecture", Defense Information Systems Agency, Center for Standards, version 3.0, 15 avril 1996.

[DoD7] ---, "X.509 Certificate Policy for the United States Department of Defense", version 7, 18 décembre 2002. (Remplacé par [DoD9].)

[DoD9] ---, "X.509 Certificate Policy for the United States Department of Defense", version 9, 9 février 2005.

[DoD10] ---, "DoD Architecture Framework, Version 1: Deskbook", 9 février 2004.

[DSG] American Bar Association, "Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Secure Electronic Commerce", Chicago, IL, 1 août 1996. (Voir : [PAG].)

[ElGa] El Gamal, T., "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms", dans "IEEE Transactions on Information Theory", vol. IT-31, n° 4, 1985, pp. 469-472.

[EMV1] Europay International S.A., MasterCard International Incorporated, and Visa International Service Association, "EMV '96 Integrated Circuit Card Specification for Payment Systems", version 3.1.1, 31 mai 1998.

[EMV2] ---, "EMV '96 Integrated Circuit Card Terminal Specification for Payment Systems", version 3.1.1, 31 mai 1998.

[EMV3] ---, "EMV '96 Integrated Circuit Card Application Specification for Payment Systems", version 3.1.1, 31 mai 1998.

[F1037] U.S. General Services Administration, "Glossary of Telecommunications Terms", FED STD 1037C, 7 août 1996.

[For94] Ford, W., "Computer Communications Security: Principles, Standard Protocols and Techniques", ISBN 0-13-799453-2, 1994.

[For97] --- and M. Baum, "Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption", ISBN 0-13-476342-4, 1994.

[FP001] U.S. Department of Commerce, "Code for Information Interchange", Federal Information Processing Standards Publication (FIPS PUB) 1, 1 novembre 1968.

[FP031] ---, "Guidelines for Automatic Data Processing Physical Security and Risk Management", FIPS PUB 31, juin 1974.

[FP039] ---, "Glossary for Computer Systems Security", FIPS PUB 39, 15 février 1976.

[FP041] ---, "Computer Security Guidelines for Implementing the Privacy Act of 1974", FIPS PUB 41, 30 mai 1975.

[FP046] ---, "Data Encryption Standard (DES)", FIPS PUB 46-3, 25 octobre 1999.

[FP074] ---, "Data Encryption Standard (DES)", FIPS PUB 46-3, 25 octobre 1999.

[FP081] ---, "DES Modes of Operation", FIPS PUB 81, 2 décembre 1980.

[FP087] ---, "Guidelines for ADP Contingency Planning", FIPS PUB 87, 27 mars 1981.

[FP102] ---, "Guideline for Computer Security Certification and Accreditation", FIPS PUB 102, 27 septembre 1983.

[FP113] ---, "Computer Data Authentication", FIPS PUB 113, 30 mai 1985.

[FP140] ---, "Security Requirements for Cryptographic Modules", FIPS PUB 140-2, 25 mai 2001 ; avec la notice de changement n° 4, 3 décembre 2002.

[FP151] ---, "Portable Operating System Interface (POSIX) -- System Application Program Interface [C Language]", FIPS PUB 151-2, 12 mai 1993

[FP180] ---, "Secure Hash Standard", FIPS PUB 180-2, août 2000 ; avec la notice de changement n° 1, 25 février 2004.

[FP185] ---, "Escrowed Encryption Standard", FIPS PUB 185, 9 février 1994.

[FP186] ---, "Digital Signature Standard (DSS)", FIPS PUB 186-2, 27 juin 2000 ; avec la notice de changement n° 1, 5 octobre 2001.

[FP188] ---, "Standard Security Label for Information Transfer", FIPS PUB 188, 6 septembre 1994.

[FP191] ---, "Guideline for the Analysis of Local Area Network Security", FIPS PUB 191, 9 novembre 1994.

[FP197] ---, "Advanced Encryption Standard", FIPS PUB 197, 26 novembre 2001.

[FP199] ---, "Standards for Security Categorization of Federal Information and Information Systems ", FIPS PUB 199, décembre 2003.

[FPKI] ---, "Public Key Infrastructure (PKI) Technical Specifications: Part A -- Technical Concept of Operations", NIST, 4 septembre 1998.

[Gass] Gasser, M., "Building a Secure Computer System", Van Nostrand Reinhold Company, New York, 1988, ISBN 0-442-23022-2.

[Gray] Gray, J. and A. Reuter, "Transaction Processing: Concepts and Techniques", Morgan Kaufmann Publishers, Inc., 1993.

[Hafn] Hafner, K. and M. Lyon, "Where Wizards Stay Up Late: The Origins of the Internet", Simon & Schuster, New York, 1996.

[Huff] Huff, G., "Trusted Computer Systems -- Glossary", MTR 8201, The MITRE Corporation, mars 1981.

[I3166] International Standards Organization, "Codes for the Representation of Names of Countries and Their Subdivisions, Part 1: Country Codes", ISO 3166-1:1997.

---, "Codes for the Representation of Names of Countries and Their Subdivisions, Part 2: Country Subdivision Codes", ISO/DIS 3166-2.

---, "Codes for the Representation of Names of Countries and Their Subdivisions, Part 3: Codes for Formerly Used Names of Countries", ISO/DIS 3166-3.

[I7498-1] ---, "Information Processing Systems -- Open Systems Interconnection Reference Model, [Part 1:] Basic Reference Model", ISO/IEC 7498-1. (Équivalent à la Recommandation UIT-T X.200.)

[I7498-2] ---, "Information Processing Systems -- Open Systems Interconnection Reference Model, Part 2: Security Architecture", ISO/IEC 7499-2.

[I7498-4] ---, "Information Processing Systems -- Open Systems Interconnection Reference Model, Part 4: Management Framework", ISO/IEC 7498-4.

[I7812] ---, "Identification cards -- Identification of Issuers, Part 1: Numbering System", ISO/IEC 7812-1:1993

---, "Identification cards -- Identification of Issuers, Part 2: Application and Registration Procedures", ISO/IEC 7812-2:1993.

[I8073] ---, "Information Processing Systems -- Open Systems Interconnection, Transport Protocol Specification", ISO IS 8073.

[I8327] ---, "Information Processing Systems -- Open Systems Interconnection, Session Protocol Specification", ISO IS 8327.

[I8473] ---, "Information Processing Systems -- Open Systems Interconnection, Protocol for Providing the Connectionless Network Service", ISO IS 8473.

[I8802-2] ---, "Information Processing Systems -- Local Area Networks, Part 2: Logical Link Control", ISO IS 8802-2. (Équivalent à IEEE 802.2.)

[I8802-3] ---, "Information Processing Systems -- Local Area Networks, Part 3: Carrier Sense Multiple Access with

Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications", ISO IS 8802-3. (Équivalent à IEEE 802.3.)

[I8823] ---, "Information Processing Systems -- Open Systems Interconnection -- Connection-Oriented Presentation Protocol Specification", ISO IS 8823.

[I9945] "Portable Operating System Interface for Computer Environments", ISO/IEC 9945-1: 1990.

[IATF] NSA, "Information Assurance Technical Framework", Release 3, NSA, septembre 2000. (Voir : IATF.)

[IDSAN] ---, "Intrusion Detection System Analyzer Protection Profile", version 1.1, NSA, 10 décembre 2001.

[IDSSC]---, "Intrusion Detection System Scanner Protection Profile", version 1.1, NSA, 10 décembre 2001.

[IDSSE]---, "Intrusion Detection System Sensor Protection Profile", version 1.1, NSA, 10 décembre 2001.

[IDSSY] ---, "Intrusion Detection System", version 1.4, NSA, 4 février 2002.

[Ioan] Ioannidis, J. and M. Blaze, "The Architecture and Implementation of Network Layer Security in UNIX", in "UNIX Security IV Symposium", octobre 1993, pp. 29-39.

[ITSEC]"Information Technology Security Evaluation Criteria (ITSEC): Harmonised Criteria of France, Germany, the Netherlands, and the United Kingdom", version 1.2, U.K. Department of Trade and Industry, juin 1991.

[JP1] U.S. DoD, "Department of Defense Dictionary of Military and Associated Terms", Joint Publication 1-02, tel qu'amendé au 13 juin 2007.

[John] Johnson, N. and S. Jajodia, "Exploring Steganography; Seeing the Unseen", in "IEEE Computer", février 1998, pp. 26-34.

[Kahn] Kahn, D., "The Codebreakers: The Story of Secret Writing", The Macmillan Company, New York, 1967.

[Knut] Knuth, D., Chapter 3 ("Random Numbers") of Volume 2 ("Seminumerical Algorithms") of "The Art of Computer Programming", Addison-Wesley, Reading, MA, 1969.

[Kuhn] Kuhn, M. and R. Anderson, "Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations", dans David Aucsmith, éd., "Information Hiding, Second International Workshop, IH'98", Portland, Oregon, USA, 15-17 avril 1998, LNCS 1525, Springer-Verlag, ISBN 3-540-65386-4, pp. 124-142.

[Land] Landwehr, C., "Formal Models for Computer Security", in "ACM Computing Surveys", vol. 13, n° 3, septembre 1981, pp. 247-278.

[Larm] Larmouth, J., "ASN.1 Complete", Open System Solutions, 1999 (ouvrage gratuit).

[M0404] U.S. Office of Management and Budget, "E-Authentication Guidance for Federal Agencies", Memorandum M-04-04, 16 décembre 2003.

[Mene] Menezes, A. et al, "Some Key Agreement Protocols Providing Implicit Authentication", dans "The 2nd Workshop on Selected Areas in Cryptography", 1995.

[Moor] Moore, A. et al, "Attack Modeling for Information Security and Survivability", Carnegie Mellon University / Software Engineering Institute, CMU/SEI-2001-TN-001, mars 2001.

[Murr] Murray, W., "Courtney'Laws of Security", dans "Infosecurity News", mars/avril 1993, p. 65.

[N4001] National Security Telecommunications and Information System Security Committee, "Controlled Cryptographic Items", NSTISSI n° 4001, 25 mars 1985.

[N4006] ---, "Controlled Cryptographic Items", NSTISSI n° 4006, 2 décembre 1991.

[N7003] ---, "Protective Distribution Systems", NSTISSI n° 7003, 13 décembre 1996.

[NCS01] National Computer Security Center, "A Guide to Understanding Audit in Trusted Systems", NCSC-TG-001, 1 juin 1988. (Voir : Rainbow Series.)

[NCS03] ---, "Information System politique de sécurité Guideline", I942-TR-003, version 1, juillet 1994. (Voir : Rainbow Series.)

[NCS04] ---, "Glossary of Computer Security Terms", NCSC-TG-004, version 1, 21 octobre 1988. (Voir : Rainbow Series.)

[NCS05] ---, "Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria", NCSC-TG-005, version 1, 31 juillet 1987. (Voir : Rainbow Series.)

[NCS25] --, "A Guide to Understanding Data Remanence in Automated Information Systems", NCSC-TG-025, version 2, septembre 1991. (Voir : Rainbow Series.)

[NCSSG] National Computer Security Center, "COMPUSECese: Computer Security Glossary", NCSC-WA-001-85, Edition 1, 1 octobre 1985. (Voir : Rainbow Series.)

[NRC91] National Research Council, "Computers At Risk: Safe Computing in the Information Age", National Academy Press, 1991.

[NRC98] Schneider, F., ed., "Trust in Cyberspace", National Research Council, National Academy of Sciences, 1998.

[Padl] Padlipsky, M., "The Elements of Networking Style", 1985, ISBN 0-13-268111-0.

[PAG] American Bar Association, "PKI Assessment Guidelines", version 1.0, 10 mai 2002. (Voir : [DSG].)

[Park] Parker, D., "Computer Security Management", ISBN 0-8359-0905-0, 1981

[Perr] Perrine, T. et al, "An Overview of the Kernelized Secure Operating System (KSOS)", dans "Proceedings of the 7th DoD/NBS Computer Security Conference", 24-26 septembre 1984.

[PGP] Garfinkel, S.. "PGP: Pretty Good Privacy", O'Reilly & Associates, Inc., Sebastopol, CA, 1995.

[PKCS] Kaliski Jr., B., "An Overview of the PKCS Standards", RSA Data Security, Inc., 3 juin 1991.

[PKC05] RSA Laboratories, "PKCS #5: Password-Based Encryption Standard ", version 1.5, 1 novembre 1993. (Voir : RFC2898.)

[PKC07] ---, "PKCS #7: Cryptographic Message Syntax Standard", version 1.5, 1 novembre 1993. (Voir : RFC2315.)

[PKC10] ---, "PKCS #10: Certification Request Syntax Standard", version 1.0, 1 novembre 1993.

[PKC11] ---, "PKCS #11: Cryptographic Token Interface Standard", version 1.0, 28 avril 1995.

[PKC12] ---, "PKCS #12: Personal Information Exchange Syntax", version 1.0, 24 juin 1995.

[RFC1108] S. Kent, "Options de sécurité du Ministère US de la défense pour le protocole Internet", novembre 1991. *(Historique)*

[RFC1135] J. Reynolds, "Helminthiasis de l'Internet", décembre 1989

[RFC1208] O. Jacobsen et D. Lynch, "Glossaire des termes de réseautage", mars 1991. *(Info)*

[RFC1281] R. Pethia, S. Crocker et B. Fraser, "Lignes directrices pour un fonctionnement sécurisé de l'Internet", nov. 1991. *(Info.)*

[RFC1319] B. Kaliski, "Algorithme de résumé de message MD2", avril 1992. *(Historique, Information)*

[RFC1320] R. Rivest, "Algorithme de résumé de message MD4", avril 1992. *(Historique, Information)*

[RFC1321] R. Rivest, "Algorithme de résumé de message MD5", avril 1992. *(Information)*

[RFC1334] B. Lloyd et W. Simpson, "Protocoles d'authentification PPP", octobre 1992. *(Remplacé par 1994)*

[RFC1413] M. St. Johns, "Protocole d'identification", février 1993. *(P.S.)*

[RFC1421] J. Linn, "Amélioration de la confidentialité pour la messagerie électronique Internet : Partie I : Chiffrement de message et procédures d'authentification", février 1993. *(Historique)*

[RFC1422] S. Kent, "Amélioration de la confidentialité pour la messagerie électronique Internet : Partie II – Gestion de clés fondée sur le certificat", février 1993. *(Historique)*

[RFC1455] D. Eastlake, "Type de service Sécurité de la liaison physique", mai 1993. *(Exp., remplacée par 2474)*

[RFC1457] R. Housley, "Cadre des étiquettes de sécurité pour l'Internet", mai 1993. *(Information)*

[RFC1492] C. Finseth, "Un protocole de contrôle d'accès , parfois appelé TACACS", juillet 1993. *(Information)*

[RFC1507] C. Kaufman, "DASS : Service de sécurité à authentification répartie", septembre1993. *(Expérimentale)*

[RFC1731] J. Myers, "Mécanismes d'authentification IMAP4", décembre 1994.*(P.S.)*

[RFC1734] J. Myers, "Commande POP3 AUTHentification", décembre 1994. *(P.S., remplacée par la* RFC5034)

[RFC1760] N. Haller, "Système S/KEY de mot de passe à utilisation unique", février 1995. *(Information)*

[RFC1824] H. Danisch, "Système de sécurité exponentielle TESS : un protocole cryptographique fondé sur l'identité pour les échanges de clé authentifiés (Rapport E.I.S.S. 1995/4)", août 1995. *(Information)*

[RFC1828] P. Metzger et W. Simpson, "Authentification IP avec du MD5 à clés", août 1995. *(Historique)*

[RFC1829] P. Karn, P. Metzger et W. Simpson, "Transformation ESP DES-CBC", août 1995. *(P.S.)*

[RFC1848] S. Crocker, N. Freed, J. Galvin et S. Murphy, "Services de sécurité d'objet MIME", octobre 1995.

[RFC1851] P. Karn, P. Metzger et W. Simpson, "Transformation ESP de triple DES", septembre 1995.

[RFC1928] M. Leech, M. Ganis, Y. Lee, R. Kuris, D. Koblas et L. Jones, "Protocole SOCKS version 5",

mars 1996.

[RFC1958] B. Carpenter, éd., "Principes de l'architecture de l'Internet", juin 1996. (*MàJ par* RFC3439) *(Information)*

[RFC1983] G. Malkin, "Glossaire des utilisateurs de l'Internet", FYI 18, août 1996.

[RFC1994] W. Simpson, "Protocole d'authentification par mise en cause de la prise de contact en PPP (CHAP)", août 1996.

[RFC2078] J. Linn, "Interface générique de programme d'application de service de sécurité, version 2", janvier 1997. *((Obsolète, voir la* RFC2743)

[RFC2084] G. Bossert, S. Cooper et W. Drummond, "Considérations sur la sécurité des transactions sur la Toile", janvier 1997.

[RFC2104] H. Krawczyk, M. Bellare et R. Canetti, "HMAC : Hachage de clés pour l'authentification de message", février 1997.

[RFC2144] C. Adams, "L'algorithme de chiffrement CAST-128", mai 1997. *(Information)*

[RFC2179] A. Gwinn, "Sécurité du réseau pour manifestations commerciales", juillet 1997. *(Information)*

[RFC2195] J. Klensin et autres, "Extension IMAP/POP AUTHorize pour mise au défi/réponse simple", septembre 1997. *(P.S.)*

[RFC2196] B. Fraser, "Manuel de la sécurité des sites", septembre 1997. (FYI0008) *(Information)*

[RFC2202] P. Cheng et R. Glenn, "Cas d'essai pour HMAC-MD5 et HMAC-SHA-1", septembre 1997. *(Information)*

[RFC2222] J. Myers, "Authentification simple et couche de sécurité (SASL)", octobre 1997. (*Obsolète, voir* RFC4422, RFC4752) (*MàJ par* RFC2444) *(P.S.)*

[RFC2289] N. Haller, C. Metz, P. Nesser, M. Straw, "Système de mot de passe à utilisation unique", février 1998. (STD0061)

[RFC2323] A. Ramos, "Lignes directrices d'identification et de sécurité de l'IETF", 1er avril 1998. *(Information)*
(Intended for humorous entertainment -- "please laugh loud and hard" -- and does not contain serious security information.)

[RFC2350] N. Brownlee, E. Guttman, "Attentes pour la réponse à un incident de sécurité informatique", juin 1998. (BCP0021)

[RFC2356] G. Montenegro, V. Gupta, "Traversée de pare-feu SKIP de Sun pour IP mobile", juin 1998. *(Information)*

[RFC2401] S. Kent et R. Atkinson, "Architecture de sécurité pour le protocole Internet", novembre 1998. (*Obsolète, voir* RFC4301)

[RFC2402] S. Kent et R. Atkinson, "En-tête d'authentification IP", novembre 1998. (*Obsolète, voir* RFC4302, 4305)

[RFC2403] C. Madson, R. Glenn, "Utilisation de HMAC-MD5-96 au sein d'ESP et d'AH", novembre 1998. *(P.S.)*

[RFC2404] C. Madson, R. Glenn, "Utilisation de HMAC-SHA-1-96 au sein d'ESP et d'AH", novembre 1998. *(P.S.)*

[RFC2405] C. Madson et N. Doraswamy, "Algorithme de chiffrement ESP DES-CBC avec IV explicite", novembre 1998.

[RFC2406] S. Kent et R. Atkinson, "Encapsulation de charge utile de sécurité IP (ESP)", novembre 1998. *(Obsolète, voir* RFC4303)

[RFC2407] D. Piper, "Le domaine d'interprétation de sécurité IP de l'Internet pour ISAKMP", novembre 1998. *(Obsolète, voir 4306)*

[RFC2408] D. Maughan, M. Schertler, M. Schneider et J. Turner, "Association de sécurité Internet et protocole de gestion de clés (ISAKMP)", novembre 1998. *(Obsolète, voir la* RFC4306)

[RFC2410] R. Glenn, S. Kent, "L'algorithme de chiffrement NULL et son utilisation avec IPsec", novembre 1998. *(P.S.)*

[RFC2412] H. Orman, "Protocole OAKLEY de détermination de clés", novembre 1998. *(Information)*

[RFC2451] R. Pereira, R. Adams, "Algorithmes de chiffrement ESP en mode CBC", novembre 1998. *(P.S.)*

[RFC2504] E. Guttman, L. Leong, G. Malkin, "Manuel de sécurité de l'utilisateur", février 1999. (FYI0034) *(Information)*

[RFC2560] M. Myers, R. Ankney, A. Malpani, S. Galperin et C. Adams, "Protocole d'état de certificat en ligne d'infrastructure de clé publique X.509 pour l'Internet - OCSP", juin 1999. *(P.S.) (Remplacée par* RFC6960)

[RFC2612] C. Adams, J. Gilchrist, "Algorithme de chiffrement CAST-256", juin 1999. *(Information)*

[RFC2628] V. Smyslov, "Interface de programme d'application pour cryptographie simple (Crypto API)", juin 1999. *(Information)*

[RFC2631] E. Rescorla, "Méthode d'accord de clé Diffie-Hellman", juin 1999. *(P.S.)*

[RFC2634] P. Hoffman, éd., "Services de sécurité améliorés pour S/MIME", juin 1999. (*MàJ par* RFC5035) *(P.S.)*

[RFC2635] S. Hambridge, A. Lunde, "NE VOMISSEZ PAS – Ensemble de lignes directrices pour les envois en masse de messagerie non sollicités (pourriels*)", juin 1999. (FYI0035) *(Information)*

[RFC2660] E. Rescorla, A. Schiffman, "Protocole de transfert HyperText sécurisé", août 1999. *(Expérimentale)*

[RFC2743] J. Linn, "Interface générique de programme d'application de service de sécurité, version 2, mise à jour 1", janvier 2000. (*MàJ par* RFC5554)

[RFC2773] R. Housley, P. Yee, W. Nace, "Chiffrement avec KEA et SKIPJACK", février 2000.

(Expérimentale)

[RFC2801] D. Burdett, "Protocole Internet du commerce ouvert - IOTP version 1.0", avril 2000. *(Information)*

[RFC2827] P. Ferguson, D. Senie, "Filtrage d'entrée de réseau : Combattre les attaques de déni de service qui utilisent l'usurpation d'adresse de source IP", mai 2000. (*MàJ par* RFC3704) (BCP0038)

[RFC2865] C. Rigney et autres, "Service d'authentification à distance de l'utilisateur appelant (RADIUS)", juin 2000. (*MàJ par* RFC2868, RFC3575, RFC5080) *(D.S.)*

[RFC3060] B. Moore et autres, "Spécification du modèle d'information de cœur de politique -- version 1", février 2001. (*MàJ par* RFC3460) *(P.S.)*

[RFC3198] A. Westerinen et autres, "Terminologie pour la gestion fondée sur la politique", novembre 2001. *(Information)*

[RFC3280] R. Housley, W. Polk, W. Ford et D. Solo, "Profil de certificat d'infrastructure de clé publique X.509 et de liste de révocation de certificat (CRL) pour l'Internet", avril 2002. *(Obsolète, voir* RFC5280)

[RFC3547] M. Baugher, B. Weis, T. Hardjono et H. Harney, "Le domaine d'interprétation de groupe", juillet 2003. *(Obsolète, voir la* RFC6407)

[RFC3552] E. Rescorla, B. Korver, "Lignes directrices pour la rédaction d'une section de considérations sur la sécurité dans les RFC", juillet 2003. (BCP0072)

[RFC3647] S. Chokhani, W. Ford, R. Sabett, C. Merrill, S. Wu,"Cadre pour la politique de certificats d'infrastructure de clés publiques X.509 sur Internet et pour les pratiques de certification", novembre 2003. *(Information)*

[RFC3739] S. Santesson, M. Nystrom, T. Polk, "Infrastructure de clés publiques X.509 pour l'Internet : profil de certificats qualifiés", mars 2004. *(P.S.)*

[RFC3740] T. Hardjono et B. Weis, "Architecture de sécurité de groupe de diffusion groupée", mars 2004.

[RFC3748] B. Aboba et autres, "Protocole extensible d'authentification ", juin 2004. *(P.S., MàJ par* RFC5247)

[RFC3766] H. Orman, P. Hoffman, "Détermination de la force des clés publiques utilisées pour l'échange de clés symétriques", avril 2004. (BCP0086)

[RFC3820] S. Tuecke et autres, "Profil de certificat de mandataire d'infrastructure de clé publique X.509 (PKI) pour l'Internet", juin 2004. *(P.S.)*

[RFC3851] B. Ramsdell, "Spécification du message d'extensions de messagerie Internet multi-objets/sécurisé (S/MIME) version 3.1", juillet 2004. *(Remplacée par* RFC5751)

[RFC3871] G. Jones, éd., "Exigences de fonctionnement de la sécurité pour l'infrastructure de réseau IP des grands fournisseurs de service Internet (ISP)", septembre 2004. *(Information)*

[RFC4033] R. Arends, R. Austein, M. Larson, D. Massey et S. Rose, "Introduction et exigences pour la

sécurité du DNS", mars 2005.

[RFC4034] R. Arends et autres, "Enregistrements de ressources pour les extensions de sécurité au DNS", mars 2005.

[RFC4035] R. Arends et autres, "Modifications du protocole pour les extensions de sécurité du DNS", mars 2005.

[RFC4086] D. Eastlake 3rd, J. Schiller, S. Crocker, "Exigences d'aléa pour la sécurité", juin 2005. (*Remplace* RFC1750) (BCP0106)

[RFC4120] C. Neuman et autres, "Service Kerberos d'authentification de réseau (V5)", juillet 2005. (*MàJ par* RFC4537, RFC5021, RFC6649)

[RFC4158] M. Cooper et autres, "Infrastructure de clés publiques X.509 pour l'Internet : construction du chemin de certification", septembre 2005. *(Information)*

[RFC4210] C. Adams et autres, "Protocole de gestion de certificat (CMP) d'infrastructure de clé publique X.509 pour l'Internet", septembre 2005. (*MàJ par la* RFC6712) *(P.S.)*

[RFC4301] S. Kent et K. Seo, "Architecture de sécurité pour le protocole Internet", décembre 2005. *(P.S.) (Remplace la RFC2401)*

[RFC4302] S. Kent, "En-tête d'authentification IP", décembre 2005. *(P.S.)*

[RFC4303] S. Kent, "Encapsulation de charge utile de sécurité dans IP (ESP)", décembre 2005. (Remplace RFC2406) *(P.S.)*

[RFC4306] C. Kaufman, "Protocole d'échange de clés sur Internet (IKEv2)", décembre 2005. *(Obsolète, voir la* RFC5996)

[RFC4346] T. Dierks et E. Rescorla, "Protocole de sécurité de la couche Transport (TLS) version 1.1", avril 2006.

[RFC4422] A. Melnikov et K. Zeilenga, éd, "Authentification simple et couche de sécurité (SASL)", juin 2006. *(P.S.)*

[Raym] Raymond, E., ed., "The On-Line Hacker Jargon File", version 4.0.0, 24 juillet 1996. (voir la dernière version à : http://www.catb.org/~esr/jargon. Aussi, "The New Hacker's Dictionary", 3rd edition, MIT Press, septembre 1996, ISBN 0-262-68092-0.)

[Roge] Rogers, H., "An Overview of the CANEWARE Program", dans "Proceedings of the 10th National Computer Security Conference", NIST et NCSC, septembre 1987.

[RSA78] Rivest, R., A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", dans "Communications of the ACM", vol. 21, n° 2, février 1978, pp. 120-126.

[RSCG] NSA, "Router Security Configuration Guide: Principles and Guidance for Secure Configuration of IP Routers, with Detailed Instructions for Cisco Systems Routers", version 1.1c, C4-040R-02, 15 décembrz 2005, disponible à http://www.nsa.gov/snac/routers/C4-040R-02.pdf .

[Russ] Russell, D. et al, Chapter 10 ("TEMPEST") of "Computer Security Basics", ISBN 0-937175-71-4, 1991.

[SAML] Organization for the Advancement of Structured Information Standards (OASIS), "Assertions and Protocol for

the OASIS Security Assertion Markup Language (SAML)", version 1.1, 2 septembre 2003.

[Sand] Sandhu, R. et al, "Role-Based Access Control Models", dans "IEEE Computer", vol. 29, n° 2, février 1996, pp. 38-47.

[Schn] Schneier, B., "Applied Cryptography Second Edition", John Wiley & Sons, Inc., New York, 1996.

[SDNS3] U.S. DoD, NSA, "Secure Data Network Systems, Security Protocol 3 (SP3)", document SDN.301, Revision 1.5, 15 mai 1989.

[SDNS4] ---, "Secure Data Network Systems, Security Protocol 4 (SP4)", document SDN.401, Revision 1.2, 12 juillet 1988.

[SDNS7] ---, "Secure Data Network Systems, Message Security Protocol (MSP)", SDN.701, Revision 4.0, 7 juin 1996, avec "Corrections to Message Security Protocol, SDN.701, Rev 4.0, 96-06-07", 30 août 1996.

[SET1] MasterCard and Visa, "SET Secure Electronic Transaction Specification, Book 1: Business Description", version 1.0, 31 mai 1997.

[SET2] ---, "SET Secure Electronic Transaction Specification, Book 2: Programmer's Guide", version 1.0, 31 mai 1997.

[SKEME] Krawczyk, H., "SKEME: A Versatile Secure Key Exchange Mechanism for Internet", dans "Proceedings of the 1996 Symposium on Network and Distributed Systems Security".

[SKIP] "SKIPJACK and KEA Algorithm Specifications", version 2.0, 22 mai 1998, et "Clarification to the SKIPJACK Algorithm Specification", 9 mai 2002 (disponible auprès du NIST Computer Security Resource Center).

[SP12] NIST, "An Introduction to Computer Security: The NIST Handbook", Special Publication 800-12.

[SP14] Swanson, M. et al (NIST), "Generally Accepted Principles and Practices for Security Information Technology Systems", Special Publication 800-14, septembre 1996.

[SP15] Burr, W. et al (NIST), "Minimum Interoperability Specification for PKI Components (MISPC), Version 1", Special Publication 800-15, septembre 1997.

[SP22] Rukhin, A. et al (NIST), "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications", Special Publication 800-15, 15 mai 2001.

[SP27] Stoneburner, G. et al (NIST), "Engineering Principles for Information Technology Security (A Baseline for Achieving Security)", Special Publication 800-27 Rev A, juin 2004.

[SP28] Jansen, W. (NIST), "Guidelines on Active Content and Mobile Code", Special Publication 800-28, octobre 2001.

[SP30] Stoneburner, G. et al (NIST), "Risk Management Guide for Information Technology Systems", Special Publication 800-30, octobre 2001.

[SP31] Bace, R. et al (NIST), "Intrusion Detection Systems", Special Publication 800-31.

[SP32] Kuhn, D. (NIST), "Introduction to Public Key Technology and the Federal PKI Infrastructure ", Special Publication 800-32, 26 février 2001.

[SP33] Stoneburner, G. (NIST), "Underlying Technical Models for Information Technology Security", Special Publication 800-33, décembre 2001.

[SP37] Ross, R. et al (NIST), "Guide for the Security Certification and Accreditation of Federal Information Systems", Special Publication 800-37, mai 2004.

[SP38A] Dworkin, M. (NIST), "Recommendation for Block Cipher Modes of Operation: Methods and Techniques",

Special Publication 800-38A, édition 2001, décembre 2001.

[SP38B] ---, "Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication", Special Publication 800-38B, mai 2005.

[SP38C] ---, "Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality", Special Publication 800-38C, mai 2004.

[SP41] Wack, J. et al (NIST), "Guidelines on Firewalls and Firewall Policy", Special Publication 800-41, janvier 2002.

[SP42] ---, "Guideline on Network Security Testing", Special Publication 800-42, octobre 2003.

[SP56] NIST, "Recommendations on Key Establishment Schemes", Draft 2.0, Special Publication 800-63, janvier 2003.

[SP57] ---, "Recommendation for Key Management", Part 1 "General Guideline" and Part 2 "Best Practices for Key Management Organization", Special Publication 800-57, DRAFT, janvier 2003.

[SP61] Grance, T. et al (NIST), "Computer Security Incident Handling Guide", Special Publication 800-57, janvier 2003.

[SP63] Burr, W. et al (NIST), "Electronic Authentication Guideline", Special Publication 800-63, juin 2004

[SP67] Barker, W. (NIST), "Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher", Special Publication 800-67, mai 2004

[Stal] Stallings, W., "Local Networks", 1987, ISBN 0-02-415520-9.

[Stei] Steiner, J. et al, "Kerberos: An Authentication Service for Open Network Systems", in "Usenix Conference Proceedings", février 1988.

[Weis] Weissman, C., "Blacker: Security for the DDN: Examples of A1 Security Engineering Trades", dans "Symposium on Security and Privacy", IEEE Computer Society Press, mai 1992, pp. 286-292.

[X400] Union Internationale des Télécommunications – Secteur de la normalisation des Télécommunications (ancienneemnt "CCITT"), Recommendation X.400, "Message Handling Services: Message Handling System and Service Overview".

[X419] ---, "Message Handling Systems: Protocol Specifications", Recommandation UIT-T X.419. (équivalente à ISO 10021-6).

[X420] ---, "Message Handling Systems: Interpersonal Messaging System", Recommandation UIT-T X.420. (équivalente à ISO 10021-7).

[X500] --, Recommandation UIT-T X.500, "Information Technology -- Open Systems Interconnection -- The Directory: Overview of Concepts, Models, and Services". (équivalente à ISO 9594-1.)

[X501] ---, Recommandation UIT-T X.501, "Information Technology -- Open Systems Interconnection -- The Directory: Models".

[X509] ---, Recommandation UIT-T X.509, "Information Technology -- Open Systems Interconnection -- The Directory: Authentication Framework", COM 7-250-E Revision 1, 23 February 2001. (équivalente à ISO 9594-8.)

[X519] ---, Recommandation UIT-T X.519, "Information Technology -- Open Systems Interconnection -- The Directory: Protocol Specifications".

[X520] ---, Recommandation UIT-T X.520, "Information Technology -- Open Systems Interconnection -- The Directory: Selected Attribute Types".

[X680] ---, Recommandation UIT-T X.680, "Information Technology -- Abstract Syntax Notation One (ASN.1) -- Specification of Basic Notation", 15 novembre 1994. (équivalente à ISO/IEC 8824-1.)

[X690] ---, Recommandation UIT-T X.690, "Information Technology -- ASN.1 Encoding Rules -- Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)", 15 novembre 1994. (équivalente à ISO/IEC 8825-1.)

7. Remerciements

George Huff a eu une bonne idée ! [Huff]

Adresse de l'auteur

Dr. Robert W. Shirey
3516 N. Kensington St.
Arlington, Virginia 22207-1328
USA

mél : rwshirey4949@verizon.net

Déclaration complète de droits de reproduction

Remerciement

Le financement de la fonction d'édition des RFC est actuellement fourni par l'activité de soutien administratif (IASA) de l'IETF.