Groupe de travail Réseau
Request for Comments : 3788
Catégorie : En cours de normalisation
Traduction Claude Brière de L'Isle

J. Loughney, Nokia Research Center
M. Tuexen, Univ. of Applied Sciences Muenster
J. Pastor-Balbas, Ericsson Espana S.A.

juin 2004

Considérations sur la sécurité des protocoles de transport de signalisation(SIGTRAN)

Résumé
Le présent document discute comment la sécurité de la couche Transport (TLS, *Transport Layer Security*) et IPsec peuvent être utilisés pour sécuriser la communication pour les protocoles SIGTRAN. Le principal objectif est de recommander les moyens de sécurité qu'un nœud SIGTRAN doit au minimum mettre en œuvre afin d'assurer la sécurité de communication. La prise en charge d'IPsec est obligatoire pour tous les nœuds qui gèrent des protocoles SIGTRAN. La prise en charge de TLS est facultative.

Table des Matières

1. Introduction....1
1.1 Généralités....1
1.2 Abréviations....2
2. Convention....2
3. Sécurité dans les réseaux de téléphonie....2
4. Menaces et objectifs....3
5. Utilisation d'IPsec....3
6. Utilisation de TLS....4
7. Prise en charge de IPsec et TLS....5
8. Considérations d'homologue à homologue....5
9. Considérations sur la sécurité....6
10. Considérations relatives à l'IANA....6
11. Remerciements....6
12. Références....6
12.1 Références normatives....6
12.2 Références pour information....6
13. Adresse des auteurs....7
14. Déclaration complète de droits de reproduction....7

1. Introduction

1.1 Généralités

Les protocoles SIGTRAN sont conçus pour porter les messages de signalisation pour les services de téléphonie. Ces protocoles sont utilisés entre :

- o les locaux d'abonnés et les équipements du fournisseur de service en cas de couche d'adaptation d'utilisateur RNIS Q.921 (IUA) [RFC3057].
- o les seuls équipements de fournisseur de service. C'est le cas pour la couche d'adaptation d'utilisateur MTP2 du système de signalisation n° 7 (M2UA) [RFC3331], la couche d'adaptation d'utilisateur MTP2 d'homologue à homologue du système de signalisation n° 7 (M2PA) [RFC4165], la couche d'adaptation d'utilisateur MTP3 du système de signalisation n° 7 (M3UA) [RFC3332] et la couche d'adaptation d'utilisateur SCCP du système de signalisation n° 7 (SUA) [RFC3868]. Les

transporteurs peuvent être différents et peuvent utiliser d'autres fournisseurs de réseau de transport.

Les exigences de sécurité pour ces situations peuvent être différentes.

Les protocoles SIGTRAN impliquent les besoins de sécurité de plusieurs parties, les utilisateurs finaux des services, les fournisseurs de service et les applications concernées. Des exigences de sécurité supplémentaires peuvent découler des règlements locaux. Bien qu'il y ait un certain recouvrement des besoins de sécurité, toute solution de sécurité devrait satisfaire les besoins de toutes les différentes parties.

Les protocoles SIGTRAN supposent que les messages sont sécurisés en utilisant IPsec ou TLS.

1.2 Abréviations

Le présent document utilise les abréviations suivantes :

ASP *(Application Server Process)* : processus de serveur d'application
CA *(Certification Authority) :* autorité de certification
DOI *(Domain of Interpretation)* : domaine d'interprétation
ESP *(encapsulating security payload)* : encapsulation de charge utile de sécurité
FQDN *(fully qualified, fully-qualified domain name)* : nom de domaine complet
IPsec *(Internet Protocol SECurity)* = sécurité du protocole Internet
IKE *(Internet Key Exchange)* = (protocole d')échange de clé Internet
ISDN *(Integrated Services Digital Network)* : RNIS, réseau numérique à intégration de services
IUA *(ISDN Q.921 User Adaptation Layer)* : couche d'adaptation d'utilisateur RNIS Q.921
M2PA *(SS7 MTP2 Peer-to-Peer User Adaptation Layer)* : couche d'adaptation d'utilisateur MTP2 d'homologue à homologue du SS7
M2UA *(SS7 MTP2 User Adaptation Layer)*:= couche d'adaptation d'utilisateur MTP2 du SS7
M3UA *(SS7 MTP3 User Adaptation Layer)* : couche d'adaptation d'utilisateur MTP3 du SS7
PKI *(Public-Key Infrastructure)* : infrastructure de clés publiques
SA *(Security Association)* : association de sécurité
SCTP *(Stream Control Transmission Protocol)* : protocole de transmission des commandes de flux
SS7 *(Signaling System No. 7)* : système de signalisation numéro 7
SUA (SS7 SCCP User Adaptation Layer) :sous système adaptation d'utilisateur SCCP du SS7
TLS (Transport Layer Security) : sécurité de la couche transport

2. Convention

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119].

3. Sécurité dans les réseaux de téléphonie

La sécurité dans les réseaux téléphoniques se fonde principalement sur le principe du réseau fermé. Deux protocoles principaux sont utilisés : les protocoles d'accès (RNIS et autres) sont utilisés pour la signalisation dans le réseau d'accès et la pile de protocoles du système de signalisation n° 7 dans le cœur de réseau.

Comme les réseaux SS7 sont souvent physiquement distants et/ou inaccessiblee à l'utilisateur, on suppose qu'ils sont protégés contre les utilisateurs malveillants. L'équipement est souvent sous clé. Aux frontières de réseaux entre les réseaux SS7, le filtrage de paquets est utilisé. Les utilisateurs finaux ne sont pas directement connectés aux réseaux SS7.

Les protocoles d'accès sont utilisés pour la signalisation d'utilisateur final. Les protocoles de signalisation d'utilisateur final sont traduits en protocoles fondés sur le SS7 par les commutateurs téléphoniques gérés par les opérateurs de réseau.

Les autorités réglementaires exigent souvent que les commutateurs SS7 aient des connexions avec des commutateurs SS7 différents pour se conformer aux spécifications d'essai nationales et/ou internationales.

Il n'y a pas de façon standard d'utiliser les technologies de chiffrement pour assurer la confidentialité ou d'utiliser des technologies d'authentification.

La présente description s'applique aux réseaux de téléphonie gérés par un seul opérateur, et aussi à plusieurs réseaux de téléphonie connectés et gérés par des opérateurs différents.

4. Menaces et objectifs

Les menaces contre l'Internet peuvent être divisées en deux types principaux. Le premier est appelé "attaque passive". Cela se produit chaque fois que l'attaquant lit des paquets sur le réseau mais ne les écrit pas. Des exemples de telles attaques incluent des violations de la confidentialité, le reniflage de mot de passe et les attaques cryptographiques hors ligne, entre autres. Le second type de menace est appelé "attaque active". Dans ce cas, l'attaquant écrit aussi des données au réseau. Des exemples de cette attaque incluent les attaques en répétition, l'insertion de message, la suppression de message, la modification de message ou les attaques par interposition, entre autres.

En général, les protocoles Internet ont les objectifs de sécurité suivants :
- o sécurité de communication :
  - * authentification des homologues
  - * intégrité du transport des données d'utilisateur
  - * confidentialité des données d'usager
  - * protection contre la répétition
- o non répudiation
- o sécurité du système, évitement de :
  - * l'utilisation non autorisée
  - * l'utilisation inappropriée
  - * déni de service

La sécurité de la communication est obligatoire dans certains scénarios de réseau pour empêcher les attaques malveillantes. Le principal objectif du présent document est de recommander les moyens de sécurité minimum qu'un nœud SIGTRAN doit mettre en œuvre pour réaliser une communication sécurisée. À cette fin, nous allons explorer les différentes options de sécurité existantes concernant la communication.

Tous les protocoles SIGTRAN utilisent le protocole de transmission de commande de flux (SCTP, *Stream Control Transmission Protocol*) défini dans la [RFC2960] et la [RFC3309] comme son protocole de transport. SCTP fournit certains dispositifs de sécurité relatifs au transport, comme la résistance contre :
- o les attaques aveugles de déni de service comme :
  - * l'inondation
  - * l'usurpation d'identité
  - * la monopolisation inappropriée des services.

Il n'y a pas de solution toute faite, à taille unique, pour la sécurité.

Lorsque un réseau utilisant des protocoles SIGTRAN implique plus d'une partie, il peut n'être pas raisonnable de s'attendre à ce que toutes les parties aient mis en œuvre la sécurité d'une manière suffisante. La sécurité de bout en bout devrait être le but ; donc, il est recommandé que IPsec ou TLS soit utilisé pour assurer la confidentialité de la charge utile de l'utilisateur. Consulter la [RFC2401] pour plus d'informations sur la configuration des services IPsec.

5. Utilisation d'IPsec

Cette section n'est pertinente que pour les nœuds SIGTRAN qui utilisent IPsec pour sécuriser la communication entre des nœuds SIGTRAN.

Tous les nœuds SIGTRAN qui utilisent IPsec DOIVENT mettre en œuvre IPsec ESP [RFC2406] en mode transport avec les algorithmes de chiffrement non nul et d'authentification pour assurer l'authentification par paquet, la protection de l'intégrité et de la confidentialité, et DOIVENT mettre en œuvre les mécanismes de protection contre la répétition de IPsec. Dans les scénarios où la protection de la couche IP est nécessaire, ESP en mode tunnel DEVRAIT être utilisé. Un chiffrement non nul devrait être utilisé avec IPsec ESP.

Tous les nœuds SIGTRAN DOIVENT prendre en charge IKE pour l'authentification de l'homologue, la négociation des associations de sécurité, et la gestion de clés, en utilisant le DOI IPsec [RFC2407]. Les mises en œuvre de IPsec DOIVENT prendre en charge l'authentification de l'homologue en utilisant une clé pré partagée, et PEUVENT prendre en charge

l'authentification de l'homologue fondée sur un certificat en utilisant des signatures numériques. L'authentification de l'homologue en utilisant les méthodes de chiffrement à clé publique mentionnées aux paragraphes 5.2 et 5.3 de la [RFC2409] NE DEVRAIT PAS être utilisée.

Les mises en œuvre conformes DOIVENT prendre en charge le mode principal et le mode agressif de IKE. Pour le mode transport, lorsque des clés pré partagées sont utilisées pour l'authentification, le mode IKE agressif DEVRAIT être utilisé, et le mode principal IKE NE DEVRAIT PAS être utilisé. Lorsque des signatures numériques sont utilisées pour l'authentification, le mode principal ou le mode agressif IKE PEUT être utilisé. Lors de l'utilisation de ESP en mode tunnel, le mode principal IKE PEUT être utilisé pour créer une association ISAKMP avec la protection d'identité durant la phase 1.

Lorsque des signatures numériques sont utilisées pour réaliser l'authentification, une négociation IKE DEVRAIT utiliser une ou des charges utiles de demande de certificat IKE pour spécifier l'autorité (ou les autorités) de certification qui est de confiance conformément à la politique locale. Les négociateurs IKE DEVRAIENT utiliser les vérifications pertinentes de révocation de certificat avant d'accepter un certificat PKI à utiliser dans les procédures d'authentification IKE. Voir dans la [RFC3280] la révocation de certificat et la [RFC2560] pour la vérification en ligne.

Les échanges en mode rapide de phase 2 utilisés pour négocier la protection des sessions SIGTRAN DOIVENT explicitement porter les champs de charge utile d'identité (IDci et IDcr). Le DOI fournit plusieurs types de données d'identification. Cependant, lorsque elles sont utilisées dans des mises en œuvre conformes, chaque charge utile d'ID DOIT porter une seule adresse IP et un seul numéro d'accès non à zéro, et NE DOIT PAS utiliser les formats de sous réseau IP ou de gamme d'adresses IP. Cela permet que l'association de sécurité de phase 2 corresponde aux connexions spécifiques TCP et SCTP.

Comme le matériel d'accélération IPsec ne peut être capable de traiter qu'un nombre limité de SA actives IKE de phase 2, des messages de suppression de phase 2 peuvent être envoyés pour les SA inactives comme moyen de garder à un minimum le nombre de SA actives de phase 2. La réception d'un message IKE Phase 2 delete NE DEVRAIT PAS être interprété comme une raison pour supprimer une session SIGTRAN. Il est préférable de laisser la connexion ouverte, par qui une autre SA IKE Phase 2 sera construite pour la protéger si du trafic supplémentaire est envoyé. Cela évite d'avoir à continuellement ouvrir et fermer les connexions.

On devrait noter que SCTP prend en charge des hôtes multi rattachement et il en résulte le besoin d'avoir plusieurs associations de sécurité pour une association SCTP. Cet inconvénient de IPsec a été traité dans la [RFC3554]. Aussi les mises en œuvre de IPsec utilisées par les nœuds SIGTRAN DEVRAIENT prendre en charge le dispositif IPsec décrit dans la [RFC3554].

6. Utilisation de TLS

Cette section n'est pertinente que pour les nœuds SIGTRAN qui utilisent TLS pour sécuriser la communication entre des nœuds SIGTRAN.

Un nœud SIGTRAN qui initie une association SCTP avec un autre nœud SIGTRAN agit comme un client TLS selon la [RFC2246], et un nœud SIGTRAN qui accepte une connexion agit comme un serveur TLS. Les homologues SIGTRAN qui mettent en œuvre TLS pour la sécurité DOIVENT s'authentifier mutuellement au titre de l'établissement de la session TLS. Afin d'assurer l'authentification mutuelle, le nœud SIGTRAN qui agit comme serveur TLS doit demander un certificat au nœud SIGTRAN qui agit comme client TLS, et le nœud SIGTRAN qui agit comme client TLS DOIT être prêt à fournir un certificat à la demande.

La [RFC3436] exige la prise en charge de la suite de chiffrement TLS_RSA_WITH_AES_128_CBC_SHA. Les nœuds SIGTRAN PEUVENT négocier d'autres suites de chiffrement TLS.

TLS DOIT être utilisé sur tous les flux bidirectionnels. D'autres flux unidirectionnels NE DOIVENT PAS être utilisés.

On devrait aussi noter qu'une mise en œuvre SCTP utilisée pour TLS sur SCTP DOIT prendre en charge la fragmentation des données d'utilisateur et pourrait aussi avoir besoin de prendre en charge l'API de livraison partielle. Cela tient même si tous les messages SIGTRAN sont petits. De plus, le dispositif de 'livraison désordonnée' de SCTP ne peut pas être utilisé en conjonction avec TLS. Voir plus de détails dans la [RFC3436].

Parce que TLS ne protège que la charge utile, l'en-tête SCTP et tous les tronçons de contrôle ne sont pas protégés. Cela peut être utilisé pour des attaques de déni de service. C'est un problème général de sécurité posé à la couche transport.

Les protocoles SIGTRAN utilisent le même numéro d'accès SCTP et identifiant de protocole de charge utile lorsque ils fonctionnent avec TLS. Une procédure de mise à niveau de session doit être utilisée pour initier la communication fondée sur TLS.

Cette procédure de mise à niveau de session devrait se présenter comme ceci :

- Si un ASP a été configuré à utiliser TLS, il envoie un message STARTTLS sur le flux 0 et lance un temporisateur T_TLS. C'est le premier message envoyé et l'ASP n'envoie pas d'autre message de couche d'adaptation jusqu'à ce que la communication fondée sur TLS ait été établie.

- Si l'homologue ne prend pas en charge TLS, il renvoie un message ERROR indiquant un type de message non pris en charge. Dans ce cas, l'association SCTP est terminée et il est fait rapport à la couche de gestion que l'homologue ne prend pas TLS en charge.

- Si l'homologue prend en charge TLS, il renvoie un message STARTTLS_ACK. Le client commence alors la communication fondée sur TLS.

- Si T_TLS arrive à expiration sans obtenir aucune des réponses ci-dessus, l'association se termine et l'échec est rapporté à la couche de gestion.

Toutes les couches d'adaptation SIGTRAN partagent un format de message commun. Le message STARTTLS consiste en un en-tête commun qui utilise seulement la classe de message 10 et le type de message 1. Le message STARTTLS_ACK utilise la même classe de message 10 et le type de message 2. Aucun message ne contient de paramètres.

En utilisant cette procédure, il est possible qu'un attaquant interposé fasse une attaque de déni de service en indiquant que l'homologue ne prend pas en charge TLS. Mais cette sorte d'attaque est toujours possible pour un attaquant interposé.

7. Prise en charge de IPsec et TLS

Si le contenu des messages de protocole SIGTRAN doit être protégé, IPsec ESP ou TLS peut être utilisé. Dans les deux cas de IPsec ESP en mode transport et de TLS, les informations d'en-tête IP ne sont ni chiffrées ni protégées. Si IPsec ESP est choisi, les informations de contrôle SCTP sont chiffrées et protégées tandis que dans la solution fondée sur TLS, les informations de contrôle SCTP ne sont pas chiffrées et sont seulement protégées par les procédures SCTP.

En général, IPsec et TLS ont tous deux assez de mécanismes pour sécuriser les communications SIGTRAN.

Donc, afin d'avoir un modèle sûr qui fonctionne aussitôt que possible, on fait la recommandation suivante : un nœud SIGTRAN DOIT prendre en charge IPsec et PEUT prendre en charge TLS.

8. Considérations d'homologue à homologue

M2PA, M3UA et SUA prennent en charge le modèle d'homologue à homologue comme généralisation du modèle client-serveur qui est pris en charge par IUA et M2UA. Un nœud SIGTRAN fonctionnant sur M2PA, M3UA ou SUA et travaillant en mode d'homologue à homologue est appelé un homologue SIGTRAN.

Comme avec tout protocole d'homologue à homologue, une configuration appropriée du modèle de confiance au sein d'un homologue est essentielle pour la sécurité. Lorsque des certificats sont utilisés, il est nécessaire de configurer les ancres de confiance pour l'homologue. Ces ancres de confiance vont probablement être uniques pour l'usage de SIGTRAN et distinctes des ancres de confiance qui pourraient être de confiance pour d'autres besoins tels que la navigation sur la Toile. En général, on s'attend à ce que ces ancres de confiance soient configurées de façon à refléter les relations d'affaires entre l'organisation qui héberge l'homologue et les autres organisations. Par suite, un homologue ne va normalement pas être configuré pour permettre la connexité avec un homologue arbitraire. Lorsque les homologues d'authentification de certificat ne peuvent pas être connus à l'avance, la découverte d'homologues peut être nécessaire.

Noter qu'IPsec est considérablement moins souple que TLS lorsque il s'agit de configurer des ancres de confiance. Comme l'utilisation d'identifiants d'accès est interdite dans IKE phase 1, il n'est pas possible de configurer de façon univoque des ancres de confiance qui soient de confiance pour chaque application individuelle au sein d'IPsec ; la même politique doit être utilisée pour toutes les applications. Cela implique, par exemple, qu'une ancre de confiance qui est de confiance pour l'utiliser avec un protocole SIGTRAN doit aussi être de confiance pour protéger d'autres protocoles (par exemple SNMP). Ces restrictions sont au mieux étranges.

Lorsque on utilise l'authentification par clés pré partagées avec IPsec pour protéger une communication fondée sur SIGTRAN,

les clés uniques pré partagées sont configurées avec des homologues qui sont identifiés par leur adresse IP (en mode principal) ou éventuellement leur FQDN (mode agressif). Par suite, il est nécessaire que l'ensemble des homologues soit connu à l'avance. Donc, la découverte d'homologues est normalement inutile.

Ce qui suit est destiné à donner des lignes directrices sur ce problème.

Il est recommandé que les homologues SIGTRAN utilisent le même mécanisme de sécurité (IPsec ou TLS) à travers toutes les sessions avec d'autres homologues SIGTRAN. Une utilisation incohérente des mécanismes de sécurité peut résulter en l'utilisation redondante des mécanismes de sécurité (par exemple, TLS sur IPsec) ou pire, de potentielles vulnérabilités. Lorsque IPsec est utilisé avec un protocole SIGTRAN, une politique normale de sécurité pour le trafic sortant est "Initier IPsec, de moi à tous, accès de destination P" ; pour le trafic entrant, la politique serait "Exiger IPsec, de tous à moi, accès de destination P". Ici, P note un des numéros d'accès enregistrés pour un protocole SIGTRAN.

Cette politique cause l'utilisation de IPsec chaque fois qu'un homologue SIGTRAN initie une session avec un autre homologue SIGTRAN, et elle est exigée chaque fois qu'une session SIGTRAN entrante se produit. Cette politique est séduisante, car elle n'exige pas que la politique soit établie pour chaque homologue ou modifiée dynamiquement chaque fois qu'une nouvelle session SIGTRAN est créée ; une SA IPsec est automatiquement créée sur la base d'une simple politique statique. Comme les extensions IPsec ne sont normalement pas disponibles sur les API de prise sur la plupart des plateformes, une fonction de politique IPsec dépend de la mise en œuvre, l'utilisation d'une simple politique statique est souvent le chemin le plus simple pour activer IPsec avec un homologue SIGTRAN.

Si IPsec est utilisé pour sécuriser une session SIGTRAN d'homologue à homologue, la politique IPsec DEVRAIT être établie pour exiger la protection d'IPsec pour les connexions entrantes, et pour initier la protection d'IPsec pour les connexions sortantes. Cela peut être accompli via l'utilisation d'une politique de filtres entrants et sortants.

9. Considérations sur la sécurité

Le présent document expose l'usage de IPsec et de TLS pour sécuriser le trafic SIGTRAN.

10. Considérations relatives à l'IANA

La classe de message 12 a été réservée dans le registre des allocations de couche d'adaptation d'utilisateur de signalisation. Pour cette classe de messages, le type de message 1 a été réservé pour le message STARTTLS, et le type de message 2 pour le messages STARTTLS_ACK.

11. Remerciements

Les auteurs tiennent à remercier B. Aboba, K. Morneault et beaucoup d'autres pour leurs précieux commentaires et suggestions.

12. Références

12.1 Références normatives

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997.

12.2 Références pour information

[RFC2246] T. Dierks et C. Allen, "Protocole TLS version 1.0", janvier 1999.

[RFC2401] S. Kent et R. Atkinson, "Architecture de sécurité pour le protocole Internet", novembre 1998. (*Obsolète, voir RFC4301*)

[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* RFC4306)

[RFC2409] D. Harkins et D. Carrel, "L'échange de clés Internet (IKE)", novembre 1998. *(Obsolète, voir la* RFC4306)

[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)

[RFC2960] R. Stewart et autres, "Protocole de transmission de commandes de flux", octobre 2000. (*Obsolète, voir* RFC4960) *(P.S.)*

[RFC3057] K. Morneault et autres, "Couche d'adaptation RNIS Q.921-utilisateur", février 2001. (*Obsolète, voir* RFC4233) (*MàJ par* RFC3807) *(P.S.)*

[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)

[RFC3309] J. Stone, R. Stewart, D. Otis, "Changement de somme de contrôle du protocole de transmission de commandes de flux (SCTP)". septembre 2002. (*Obsolète, voir* RFC4960) *(P.S.)*

[RFC3331] K. Morneault et autres, "Sous-système de transfert de message (SSTM2) du système de signalisation n° 7 (SS7) – Couche d'adaptation d'usager", septembre 2002. *(P.S.)*

[RFC3332] G. Sidebottom et autres, "Sous-système de transfert de message (SSTM3) du système de signalisation n° 7 (SS7) - Couche d'adaptation d'usager (M3UA)", septembre 2002. (*Obsolète, voir* RFC4666) *(P.S.)*

[RFC3436] A. Jungmaier, E. Rescorla, M. Tuexen, "Sécurité de la couche Transport sur le protocole de transmission de contrôle de flux", décembre 2002. *(P.S.)*

[RFC3554] S. Bellovin et autres, "Utilisation du protocole de transmission de commandes de flux (SCTP) avec IPsec", juillet 2003. *(P.S.)*

[RFC3868] J. Loughney et autres, "Couche d'adaptation d'utilisateur du sous-ensemble de contrôle de connexion de signalisation (SUA)", octobre 2004. *(P.S.)*

[RFC4165] T. George et autres, "Sous-système n° 2 de transfert de messages (SSTM2) du système de signalisation n° 7 (SS7) – Couche d'adaptation d'homologue à homologue d'utilisateur (M2PA)", septembre 2005. *(P.S.)*

13. Adresse des auteurs

John Loughney
Nokia Research Center
PO Box 407
FIN-00045 Nokia Group
Suomi
mél : john.loughney@nokia.com

Michael Tuexen (editor)
Univ. of Applied Sciences Muenster
Stegerwaldstr. 39
48565 Steinfurt
Deutchland
mél : tuexen@fh-muenster.de

Javier Pastor-Balbas
Ericsson Espana S.A.
Via de los Poblados, 13
28033 Madrid
España
mél : j.javier.pastor@ericsson.com

14. Déclaration complète de droits de reproduction

FORCE déclinent toutes garanties, exprimées ou implicites, y compris mais non limitées à toute garantie que l'utilisation des informations ci-encloses ne violent aucun droit ou aucune garantie implicite de commercialisation ou d'aptitude à un objet particulier.

Propriété intellectuelle

L'IETF ne prend pas position sur la validité et la portée de tout droit de propriété intellectuelle ou autres droits qui pourraient être revendiqués au titre de la mise en œuvre ou l'utilisation de la technologie décrite dans le présent document ou sur la mesure dans laquelle toute licence sur de tels droits pourrait être ou n'être pas disponible ; pas plus qu'elle ne prétend avoir accompli aucun effort pour identifier de tels droits. Les informations sur les procédures de l'ISOC au sujet des droits dans les documents de l'ISOC figurent dans les BCP 78 et BCP 79.

Des copies des dépôts d'IPR faites au secrétariat de l'IETF et toutes assurances de disponibilité de licences, ou le résultat de tentatives faites pour obtenir une licence ou permission générale d'utilisation de tels droits de propriété par ceux qui mettent en œuvre ou utilisent la présente spécification peuvent être obtenues sur le répertoire en ligne des IPR de l'IETF à http://www.ietf.org/ipr .

L'IETF invite toute partie intéressée à porter son attention sur tous copyrights, licences ou applications de licence, ou autres droits de propriété qui pourraient couvrir les technologies qui peuvent être nécessaires pour mettre en œuvre la présente norme. Prière d'adresser les informations à l'IETF à ietf- ipr@ietf.org .

Remerciement
Le financement de la fonction d'édition des RFC est actuellement fourni par l'Internet Society.