Guide de déploiement DNSSEC pour les ccTLD

Bureau du directeur de la technologie de l'ICANN

Yazid Akanho et Paul Muchene
OCTO-029
12 novembre 2021

ICANN

TABLE DES MATIERES

Le présent guide fait partie de la série de documents publiés par le Bureau du directeur de la technologie (OCTO) de l'ICANN. Vous trouverez sur la page des publications de l'OCTO une liste des documents de la série. Si vous avez des questions ou des suggestions par rapport à ces documents, veuillez les envoyer à octo@icann.org.

Ce guide vient en appui à l'objectif stratégique de l'ICANN qui vise à améliorer la responsabilité partagée du maintien de la sécurité et de la stabilité du système des noms de domaine (DNS) par le biais du renforcement de la coordination du DNS en partenariat avec les parties prenantes concernées. L'objectif stratégique de l'ICANN concerne le renforcement de la sécurité du DNS et du système des serveurs racine du DNS (RSS).

1 Introduction

Au cours de ces dernières années, la sécurité est devenue un enjeu majeur sur Internet. En ce qui concerne le système des noms de domaine (DNS), plusieurs protocoles de sécurité ont été proposés et développés au fil des années, dont les extensions de sécurité du système de noms de domaine (DNSSEC), qui figurent parmi les plus importants. Les extensions de sécurité DNSSEC aident à sécuriser les réponses du DNS en ajoutant une authentification de l'origine des données et une protection de leur intégrité.

La première signature DNSSEC de la zone racine du DNS gérée par l'ICANN remonte à juillet 2010. Au moment de la publication de ce guide, tous les domaines génériques de premier niveau (gTLD) sont signés DNSSEC, en partie en raison d'obligations contractuelles avec l'ICANN. En revanche, seuls environ 60 % des domaines de premier niveau géographiques (ccTLD) sont signés. L'une des raisons susceptibles d'expliquer cette tendance au niveau des ccTLD est le manque de visibilité des gestionnaires de ccTLD dans le processus de sécurisation de leurs zones avec DNSSEC.

C'est pourquoi le Bureau du directeur de la technologie (OCTO) de l'ICANN publie le présent guide, destiné à aider les opérateurs de registres ccTLD à mieux s'approprier le processus de signature de leurs zones à l'aide de DNSSEC. Ce guide n'aborde pas un deuxième aspect de DNSSEC, à savoir la validation qui intervient principalement du côté des résolveurs récursifs du DNS, situés généralement au niveau des fournisseurs d'accès à Internet (FAI), des opérateurs les plus importants de services informatiques publics dans le nuage, ou des réseaux d'entreprise.

1.1 À qui s'adresse le présent document

Le présent guide vise principalement à fournir aux gestionnaires de registres ccTLD, à leur personnel et à leurs parties prenantes, en particulier les bureaux d'enregistrement, les titulaires de noms de domaine et autres, un aperçu des extensions de sécurité DNSSEC et de la façon dont ces extensions peuvent être mises en œuvre par un registre pour la signature de zone. Le présent document ne rentre pas dans les détails de la configuration technique. Il s'agit d'un guide pour obtenir des connaissances de base sur le protocole DNSSEC, ainsi que sur les prérequis et les considérations liées à son déploiement pour la signature de zones d'un ccTLD.

Même si vous exploitez déjà un TLD signé DNSSEC, le présent document pourrait vous aider à identifier des points à améliorer, tels que les meilleures pratiques actuelles en matière d'algorithmes ou la documentation appropriée du service DNS global. Si vous êtes un opérateur de ccTLD ou si vous administrez des zones sous un ccTLD signé, ce guide peut vous aider à faire vos premiers pas. Même si l'ensemble des opérateurs de gTLD ont déjà signé leurs zones, ils pourraient également tirer des enseignements des meilleures pratiques opérationnelles en matière de DNSSEC décrites dans le présent document et les utiliser comme référence pour sensibiliser leurs bureaux d'enregistrement et titulaires de noms de domaine à DNSSEC.

Il existe une multitude de documents portant sur les aspects théoriques, techniques et opérationnels de DNSSEC, dont plusieurs sont cités en référence dans ce guide. Les lecteurs sont donc invités à les examiner s'ils souhaitent approfondir leurs connaissances ou leur compréhension d'autres aspects liés à DNSSEC.

2 DNSSEC et son utilité pour le DNS

Le système des noms de domaine (DNS) est un système de nommage hiérarchique, distribué et décentralisé propre à l'Internet. À l'instar d'un annuaire téléphonique qui traduit des noms en numéros de téléphone, le DNS aide à convertir les informations relatives aux noms de domaine en adresses IP et vice versa. On considère que le DNS est un service essentiel pour le fonctionnement de l'Internet, mais il n'a pas initialement été conçu avec des mécanismes solides de sécurité garantissant l'intégrité et l'authenticité de ses données. Au fil des années, un certain nombre de vulnérabilités menaçant la fiabilité et la crédibilité du DNS ont été détectées. DNSSEC aide à y remédier.

Les extensions DNSSEC sont principalement définies et décrites dans trois documents de normes Internet : le RFC 4033, *Introduction et exigences pour la sécurité du DNS* ; le RFC 4034, *Enregistrements de ressource pour les extensions de sécurité du DNS ;* et le RFC 4035, *Modifications de protocole pour les extensions de sécurité du DNS*. DNSSEC utilise la cryptographie à clé publique (la génération de paires de clés publiques et privées) pour apporter au DNS des mécanismes permettant d'authentifier l'origine des données, de contrôler leur intégrité, d'effectuer des vérifications et d'authentifier des dénis d'existence. Plus précisément, il ajoute au DNS des signatures numériques et un nouvel ensemble de types d'enregistrement de ressources et de bits d'en-tête de message (flags ou fanions) qui peuvent être utilisés pour vérifier les réponses DNS provenant d'une zone signée. Il convient de noter que DNSSEC ne chiffre pas les données des messages du DNS et n'assure donc pas la confidentialité.

Une fois qu'un domaine est signé avec DNSSEC, des signatures numériques sont générées par l'administrateur de zone à l'aide d'une clé privée et publiées sous la forme de signatures d'enregistrements de ressource (RRSIG) dans le fichier de zone en tant que données de zone du domaine. Lorsqu'un résolveur récursif à capacité de sécurité, également connu sous le nom de résolveur validant, envoie une requête DNS à un serveur faisant autorité pour le domaine signé, la réponse DNS contient l'enregistrement de ressource en clair (en format non chiffré), et sa signature numérique associée. Le résolveur utilise alors la signature numérique qu'il a reçue afin de valider sa réponse DNS. Pour ce faire, le résolveur validant demande également d'autres informations de DNSSEC, telles que la clé publique qui est stockée dans l'enregistrement DNSKEY et publiée par l'administrateur du domaine dans les données de zone.

3 Prérequis et exigences pour le déploiement de DNSSEC

3.1 Documentation du système existant

Étant donné le rôle fondamental que joue le DNS sur l'Internet et la nécessité d'empêcher en tout temps des interruptions de service, il est important de tenir à jour la documentation qui décrit l'infrastructure, les opérations et les processus du DNS. De plus, DNSSEC ajoute un certain degré de complexité à l'infrastructure et aux opérations DNS existantes. Par conséquent, maintenir une documentation à jour est un élément essentiel pour disposer d'une image claire du système existant à des fins de référence. Cela garantit également la continuité

opérationnelle en cas de renouvellement du personnel ou de mises à niveau des infrastructures.

Nous recommandons que la documentation résume deux aspects principaux : les politiques de gouvernance du ccTLD ainsi que les aspects opérationnels et techniques du service.

En outre, il est souhaitable que la documentation contienne le plus d'informations possible, à l'exception de données sensibles ou confidentielles telles que des noms d'utilisateur et des mots de passe qui pourraient être utilisés pour mener des attaques à l'encontre du registre.

Les aspects liés à la gouvernance de la documentation peuvent concerner les questions suivantes :

- Aperçu général et structure du ccTLD.
- Modèle(s) d'enregistrement : 3R (« *registry, registrar, and registrant* » [opérateur de registre, bureau d'enregistrement et titulaire de nom de domaine]), 2R (« *registry and registrant* » [opérateur de registre et titulaire de nom de domaine]) ou autres modèles.
- Contacts techniques et administratifs de l'opérateur de registre.
- Ressources humaines, rôles, responsabilités et coordonnées des personnes intervenant dans le processus de prise de décisions techniques de l'opérateur de registre.
- Liste des bureaux d'enregistrement avec leurs coordonnées respectives.

Les aspects techniques et opérationnels de la documentation peuvent concerner les questions suivantes :

- Nombre de serveurs de noms (NS) primaires et secondaires faisant autorité avec leurs adresses IP respectives ; coordonnées des TLD (téléphones et adresses électroniques) ; protocoles utilisés entre l'opérateur de registre et les bureaux d'enregistrement tels que le protocole d'avitaillement extensible (EPP – Extensible Provisioning Protocol) ; les logiciels et le matériel permettant la mise en œuvre des fonctions du registre, dont la base de données du registre ; le protocole d'accès aux données d'enregistrement des noms de domaine (RDAP – Registration Data Access Protocol) et/ou les serveurs WHOIS ; entre autres éléments d'information techniques.
- Accès utilisateur et inventaire de privilèges uniquement disponibles pour un nombre limité de personnes autorisées.
- Sauvegardes et procédures de restauration.
- Sécurité : accès physique, gestion des journaux, contrôles d'accès, gestion des mots de passe, pare-feux, intégrité du fichier de zone et sécurité du transfert de zone, pour n'en citer que quelques-uns.
- Systèmes de supervision : matériel, logiciels, synchronisation de zone (entre NS).
- Stratégie de maintenance.
- Plan de continuité des opérations et de reprise après catastrophe.

3.2 Audit de l'infrastructure existante

Comme indiqué précédemment, le déploiement de DNSSEC ajoute un degré de complexité à l'infrastructure et aux opérations existantes du DNS. Par conséquent, une bonne pratique de sécurité consiste à mener un audit de l'infrastructure, des opérations et des processus du système actuel par une partie externe ou interne possédant les compétences et l'autonomie requises pour identifier et partager les vulnérabilités et les insuffisances détectées. Il est

essentiel de corriger les défauts du système actuel avant ou parallèlement à la signature de la zone. Ce faisant, on réduit le risque de perte de contrôle après la mise en œuvre de DNSSEC.

3.3 Rédiger une politique DNSSEC et une déclaration de pratiques DNSSEC

3.3.1. Qu'est-ce qu'une politique DNSSEC et une déclaration de pratiques DNSSEC ?

Plusieurs éléments doivent être pris en compte et des paramètres doivent être définis lors de la signature d'un domaine, par exemple les algorithmes de signature DNSSEC, la taille des clés, la période de validité de la signature et la fréquence de mise à jour de la signature. Dans le cas d'une zone ayant un grand nombre de délégations, une bonne pratique consiste à documenter intégralement et à tenir à jour les ensembles de paramètres applicables à la zone et à les mettre à la disposition du public. De ce fait, deux concepts doivent ici être pris en compte :

- La **politique DNSSEC** (DP) : elle définit les exigences et les normes en matière de sécurité qui doivent être mises en œuvre pour une zone signée DNSSEC. La DP sert de fondement à l'audit, à l'accréditation ou à l'évaluation d'une entité, par exemple un opérateur de registre. Chaque entité peut être évaluée par rapport à une ou à plusieurs DP qu'elle prétend mettre en œuvre. En résumé, la DP énonce ce qui doit être fait.
- La **déclaration de pratiques DNSSEC** (DPS) : il s'agit d'un document répertoriant les pratiques opérationnelles qui peut venir appuyer et compléter la politique DNSSEC (s'il y en a une). Elle précise comment un opérateur de zone et, le cas échéant, ses partenaires dans la gestion d'une zone, doivent mettre en œuvre des procédures et des contrôles afin de satisfaire aux exigences de la DP applicable. À la différence d'une DP, la DPS indique ce qui est réellement fait.

Une DP énonce des principes généraux alors qu'une DPS donne une description des procédures et des contrôles, ce qui en fait un document plus détaillé qu'une DP. D'autre part, la DP est en règle générale rédigée par une autorité politique (un gestionnaire de TLD ou une autorité de régulation) et peut s'appliquer à une ou à plusieurs zones dans la hiérarchie du DNS, alors qu'une déclaration de pratiques (DPS) propre à une seule zone est rédigée par l'opérateur de zone qui décrit la façon dont il satisfait aux exigences d'une politique ou d'un ensemble de politiques spécifiques.

Par exemple, dans le cas où le contact administratif et le contact technique d'un ccTLD sont des entités différentes, le contact administratif peut publier une politique posant les normes et les exigences à suivre tout en imposant également au contact technique de publier une déclaration de pratiques détaillant comment ces normes et ces exigences seront appliquées.

Autrement, un opérateur ou un gestionnaire de zone qui n'est pas soumis à une politique externe peut publier une DPS.

La publication d'une DPS vaut surtout pour des entités exploitant une zone qui contient un nombre significatif de délégations, comme un TLD. La publication d'une DPS permet d'assurer un niveau de transparence qui renforce la confiance de la communauté dans les opérations du TLD, mais comme indiqué précédemment, une DPS ne doit pas contenir d'informations opérationnelles sensibles.

Le RFC 6841, *Cadre pour les politiques DNSSEC et les déclarations de pratiques DNSSEC,* est un document permettant d'acquérir des connaissances approfondies sur un vaste ensemble d'éléments dont un opérateur de TLD doit tenir compte lorsqu'il définit une DP et/ou une DPS.

3.3.2 Comment rédiger une DP et une DPS

La rédaction d'une DPS constitue une étape importante du processus qui aboutit à la signature d'un ccTLD. La DPS peut être brève et simple ou longue et complexe, mais dans tous les cas elle doit aider les personnes à comprendre le cadre de fonctionnement des extensions DNSSEC et à faire confiance au processus de signature du ccTLD.

Le tableau suivant est un résumé de l'ensemble des huit composants du RFC 6841 qui pourraient être pris en considération lors de la rédaction d'une DP ou d'une DPS. Il n'est pas obligatoire de mettre en œuvre tous les composants du RFC 6841, et vous êtes donc libre de choisir les (sous-)composants les mieux adaptés à vos besoins.

Titre	Description	Sous-composants
Introduction	Identifie et présente l'ensemble des dispositions, et indique les types d'entités et d'applications auxquelles la politique ou la déclaration de pratiques s'adresse.	• Aperçu • Nom et identification du document • Parties intéressées et conditions d'application • Administration
Publication et référentiels	Décrit les obligations auxquelles doit se soumettre une entité pour publier des informations concernant ses pratiques, les clés publiques, le statut actuel de ces clés ainsi que les référentiels dans lesquels les informations sont conservées.	• Référentiels • Publication de clés publiques
Besoins opérationnels	Décrit les besoins opérationnels liés à l'exploitation d'une zone signée DNSSEC.	• Signification des noms de domaine • Identification et authentification d'un gestionnaire de zone enfant • Collecte et publication d'enregistrements de ressource DS (signataire de délégation) • Méthode pour prouver la possession et les droits de propriété de la clé privée • Suppression d'un enregistrement DS

Emplacement, gestion et contrôles opérationnels	Décrit les mesures de sécurité non techniques, c'est-à-dire les contrôles physiques ainsi que les contrôles des procédures et du personnel permettant de réaliser en toute sécurité les fonctions liées à DNSSEC. Ces contrôles comprennent l'accès physique, la gestion des clés, la reprise après catastrophe, l'audit et l'archivage. Ces mesures de sécurité non techniques sont essentielles pour faire confiance aux signatures générées par DNSSEC.	● Contrôles physiques ● Contrôles des procédures ● Contrôles du personnel ● Procédures de journalisation d'audits ● Compromission et reprise d'activité après catastrophe ● Cessation des activités du registre
Mesures de sécurité techniques	Définit les mesures de sécurité prises afin d'assurer la gestion des clés cryptographiques et des données d'activation, par exemple des codes PIN, des mots de passe ou des portions de clés détenues manuellement relatives aux opérations DNSSEC.	● Génération de paires de clés et installation ● Protection de la clé privée et contrôles des modules cryptographiques ● Données d'activation
Signature de zone	Couvre tous les aspects liés à la signature de zone, dont la spécification cryptographique des clés de signature, le schéma de signature, la méthodologie de roulement de clé et la signature de zone elle-même. Les zones enfants et autres parties de confiance peuvent dépendre des informations de cette section pour comprendre les données attendues dans la zone signée et déterminer leur propre comportement.	● Longueur des clés, types de clés et algorithmes ● Dénis d'existence authentifiés ● Format de signature ● Roulement de clé ● Durée de vie de la signature et fréquence de la resignature
Audit de conformité	Décrit comment les audits doivent être menés par l'opérateur de zone et éventuellement par d'autres entités concernées.	● Fréquence d'un audit de conformité d'une entité ● Identité/qualifications de l'auditeur ● Éléments faisant l'objet de l'audit ● Mesures faisant suite à l'audit

Dispositions légales	Indique la juridiction sous laquelle le registre est exploité et fournit des références par rapport à tout contrat associé en vigueur. La section Dispositions légales peut fournir des informations sur des implications identifiées en matière de données privées personnellement identifiables.	• Mention de la juridiction compétente • Obligations contractuelles et conformité aux lois et règlements nationaux, transnationaux ou internationaux • Protection des données et traitement des données personnellement identifiables

Des composants supplémentaires peuvent être ajoutés à ce cadre afin de répondre aux besoins spécifiques d'un ccTLD. Des exemples de déclarations de pratiques DNSSEC sont disponibles dans l'Annexe A du présent guide.

3.3.3 Sélection d'algorithmes cryptographiques pour une zone

Le domaine de la cryptographie évolue en permanence. De nouveaux algorithmes remplacent les algorithmes existants lorsqu'il est déterminé qu'ils sont moins sécurisés qu'auparavant. C'est pourquoi les modalités et les préconisations en matière de mise en œuvre des algorithmes sont régulièrement mises à jour afin de tenir compte des nouvelles réalités.

La mise en œuvre de DNSSEC comporte le choix d'un algorithme cryptographique adéquat. Au moment de la publication du présent guide, le RFC 8624, *Exigences et lignes directrices d'utilisation et de mise en œuvre d'algorithmes pour DNSSEC*, fournit à la fois des directives pour la mise en œuvre des algorithmes et des spécifications par rapport aux paramètres de signature requis pour DNSSEC.

Le tableau suivant recense une partie des recommandations (liste non exhaustive) tirées du RFC 8624. Les opérateurs individuels peuvent faire le choix d'adapter ces recommandations à leurs besoins spécifiques.

Objet	**Recommandation**
Algorithme DNSKEY	L'**algorithme 13 (ECDSAP256SHA256)** est cryptographiquement puissant et son utilisation est actuellement recommandée pour les nouveaux déploiements de DNSSEC en raison de ses clés plus courtes et de sa taille de signature, qui permettent d'obtenir des paquets DNS plus petits. Toutefois, l'**algorithme 8 (RSASHA256)** peut également être utilisé car il est largement déployé et a

	été l'algorithme par défaut pendant un certain nombre d'années en raison de sa puissance cryptographique.
Algorithmes pour les enregistrements de ressource de signataire de délégation (DS)	L'algorithme SHA-256, largement utilisé, est un puissant algorithme de hachage recommandé pour l'enregistrement DS dans les déploiements nouveaux et existants.
Algorithme de sécurité de DNSSEC (composé de l'algorithme cryptographique et de l'algorithme de hachage)	Actuellement, on recommande d'utiliser l'algorithme 13 (ECDSAP256SHA256). Sinon, il est également possible d'utiliser l'algorithme 8 (RSASHA256).
Taille de clé pour la clé de signature de zone (ZSK) et la clé de signature de clé (KSK)	L'algorithme 13 (ECDSAP256SHA256) générera toujours des clés de 256 bits. La taille de clé de l'algorithme 8 (RSASHA256) peut être définie entre 2048 et 4096 bits.
Période de validité de la ZSK et de la KSK	Il n'existe pas de bonne méthode d'évaluation des besoins individuels dans la mesure où les opérateurs ajustent les périodes de validité de clé en se fondant sur leurs expériences précédentes. Plusieurs opérateurs utilisent la ZSK pendant un à trois mois, et la KSK d'un à cinq ans avant de procéder à un roulement.
Stockage de clés privées	Machines hors ligne, non connectées au réseau, sécurisées d'un point de vue physique, telles que les modules matériels de sécurité (HSM).

Remarque : plus la taille des clés augmentera, plus la taille des enregistrements RRSIG et DNSKEY sera importante, ce qui comportera un risque accru de débordement de paquets DNS UDP. En outre, le temps nécessaire pour valider et créer des signatures d'enregistrement de ressources (RRSIG) augmente avec des clés plus grandes. Évitez donc d'accroître inutilement la taille des clés.

3.3.4 Déni d'existence : NSEC ou NSEC3

Le déni d'existence ou la preuve qu'un élément n'existe pas est un mécanisme qui permet d'indiquer à un résolveur qu'un nom de domaine donné n'existe pas (NXDOMAIN). Inversement, un nom de domaine existe mais ne possède pas l'enregistrement de ressource spécifique (NODATA) demandé. L'authentification de déni d'existence utilise la cryptographie pour signer une réponse négative. Avec DNSSEC, cela est rendu possible soit via NSEC (Next Secure) soit via NSEC3 (Next Secure v3).

NSEC est utilisé pour décrire un intervalle entre des noms. Il indique indirectement à un résolveur quels noms n'existent pas dans une zone en fournissant, dans l'ordre canonique, le

nom précédent et le nom suivant. Ce mécanisme mis en œuvre dans NSEC constitue la base du déni d'existence authentifié avec DNSSEC et se trouve confronté à deux problèmes :

- Les enregistrements NSEC sont exposés aux attaques de parcours de zone (*zone walking*), et cette vulnérabilité peut permettre à un attaquant de traverser tous les noms d'une zone. Il est donc possible de reconstruire l'ensemble de la zone en contournant ainsi toute tentative de blocage de transfert de zone configuré par l'administrateur.

- Le deuxième problème auquel est confronté NSEC dans une zone centrée sur la délégation, telle qu'un TLD, est que tous les noms de cette zone ont un enregistrement NSEC et leur RRSIG associée, ce qui a pour effet défavorable une augmentation de la taille de la zone signée. Les contraintes générées par cette augmentation pourraient avoir un impact négatif sur les performances des serveurs DNS faisant autorité, par exemple en limitant les ressources de stockage matériel ou en rallongeant la durée d'exécution des transferts de zone.

En revanche, NSEC3 réduit le risque d'attaque de parcours de zone propre au NSEC grâce au hachage de noms de domaine, avec la possibilité de les renforcer à l'aide d'une fonction de salage (salt). De plus, grâce à une fonction spécifique dénommée « opt-out», les noms de domaine non signés délégués dans une zone (délégations non sécurisées) n'ont pas besoin d'un enregistrement NSEC3 et donc n'en obtiennent pas. Cela implique que lorsque la fonction « opt-out » est activée dans une zone TLD, NSEC3 ne peut prouver ou nier l'existence des domaines non signés enregistrés sous le TLD concerné. Toutefois, l'un des inconvénients de NSEC3 est que les réponses DNS sont plus volumineuses que celles de NSEC.

Il n'existe pas de bonne réponse unique lorsqu'il s'agit de choisir entre NSEC et NSEC3. Si l'on préfère utiliser NSEC3 afin d'éviter les attaques de parcours de zone, il est généralement recommandé de mettre en œuvre NSEC3 sans itérations supplémentaires et avec un sel (salt) vide. Toutefois, pour les plus petites zones, l'utilisation d'enregistrements NSEC3 avec la fonction « opt-out » n'est pas recommandée. Pour les zones très grandes et faiblement signées, dans lesquelles la majorité des enregistrements constituent des délégations non sécurisées, la fonction « opt-out » de NSEC3 pourrait être utilisée. Outre ces considérations, il est plus facile de corriger les problèmes de NSEC que ceux de NSEC3.

3.4 Participation des bureaux d'enregistrement

Il est vivement recommandé de faire participer les bureaux d'enregistrement dès les premières étapes de la signature d'un ccTLD. Non seulement parce qu'ils font office d'intermédiaires entre l'opérateur de registre et les titulaires de noms de domaine, mais aussi parce que le déploiement de DNSSEC au niveau du ccTLD constitue le point de départ pour sécuriser l'espace de noms de ce ccTLD. Une fois le ccTLD signé, les détenteurs de noms de domaine de second niveau peuvent commencer à sécuriser leurs domaines respectifs. Les bureaux d'enregistrement devront être en mesure de collecter un nouveau type d'enregistrement auprès de ces titulaires de noms de domaine de second niveau ou de niveau suivant et de les envoyer à l'opérateur de registre. Ce nouveau type d'enregistrement est appelé signataire de délégation (DS – Delegation signer).

D'un point de vue technique, le DS est un hachage de la clé de signature de clé (KSK) et aide à établir la chaîne de confiance entre une zone parent et une zone enfant dans l'espace de noms du DNS. Le fait de disposer de l'enregistrement DS dans la zone parent crée une liaison

sécurisée qu'un attaquant externe devrait surmonter pour falsifier les données de la clé dans la zone enfant.

En règle générale, le ccTLD partage son enregistrement DS avec l'Autorité chargée de la gestion de l'adressage sur Internet (IANA) à des fins de publication dans la zone racine. Les titulaires et les administrateurs de noms de domaine sous le ccTLD partagent leurs enregistrements DS avec le ccTLD directement ou via un bureau d'enregistrement. Ici, les bureaux d'enregistrement ont deux rôles importants à jouer :

- **Fournir une interface ou un mécanisme sécurisé et fiable de collecte des enregistrements DS** auprès des titulaires de noms de domaine. Si une telle interface ou un tel mécanisme n'existe pas encore, les bureaux d'enregistrement souhaitant proposer la fonctionnalité DNSSEC à leurs titulaires de noms de domaine devraient travailler dès que possible à implémenter une telle interface. Il n'y a pas de méthode normalisée pour transférer l'enregistrement DS entre le client et le bureau d'enregistrement. Les bureaux d'enregistrement disposent de différents mécanismes allant de simples interfaces web à différentes API.
- **Communiquer le DS à l'opérateur de registre.** Il est recommandé d'utiliser une solution automatisée pour la publication du DS dans la zone parent au lieu de procéder à une intervention manuelle. Dans le modèle opérateur de registre-bureau d'enregistrement, il est possible d'utiliser les extensions DNSSEC de EPP pour le transfert de jeux d'enregistrements de ressources DS (RRsets) et éventuellement des RRsets DNSKEY. Dans tous les cas, des tests doivent être effectués entre l'opérateur de ccTLD et les bureaux d'enregistrement afin de garantir la faisabilité des nouvelles transactions à l'aide de l'infrastructure existante.

Un autre mécanisme permettant à une zone enfant de gérer automatiquement le DS avec sa zone parent consiste à utiliser un RRset CDS (DS de zone enfant) ou CDNSKEY (DNSKEY de zone enfant) si la zone parent dispose d'une politique d'acceptation de ces enregistrements. Ils peuvent être utilisés dans les trois cas suivants :

- Publication initiale du DS.
- Roulement de clé.
- Retour à l'état d'insécurité.

Autrement dit, CDS/CDNSKEY est une instruction donnée à la zone parent pour modifier le RRset de ressources DS si le CDS/CDNSKEY et le DS sont différents. Le RFC 8078, *Gestion des enregistrements du DNS provenant du parent via CDS/CDNSKEY,* apporte davantage de précisions sur la gestion automatisée des enregistrements DS entre la zone enfant et la zone parent.

Enfin, faire participer les bureaux d'enregistrement dès le début du processus leur permet également de bénéficier des programmes de formation pratique DNSSEC dispensés par l'ICANN et ses partenaires au sein de la communauté Internet.

4 Chronogramme

Il n'existe pas de chronogramme spécifique pour le déploiement de DNSSEC. Le déploiement peut prendre des semaines, des mois ou des années selon différents facteurs. Toutefois, afin d'éviter une trop longue durée de mise en œuvre, tenez compte des suggestions suivantes :

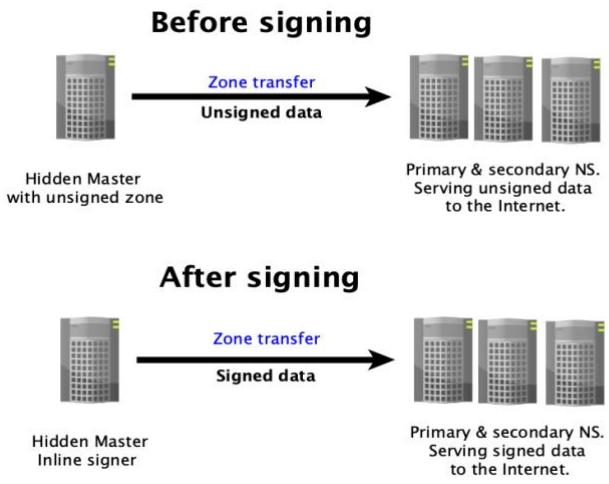
- Définissez le processus comme un projet, avec une date de début précise, une date de fin prévue et des étapes à franchir. De plus, nommez un chef de projet ou un responsable technique doté de ressources adéquates.
- Identifiez, communiquez et collaborez avec les parties prenantes, dont le(s) régulateur(s), les bureaux d'enregistrement, les parties techniques et administratives, les prestataires, le(s) opérateur(s) de services back-end ou toute autre partie. Une communication satisfaisante entre les différentes parties prenantes du ccTLD doit également être assurée.
- Identifiez et gérez correctement les risques.

5 Scénarios de déploiement de DNSSEC

Que vous décidiez de gérer la zone uniquement avec vos propres ressources et infrastructures ou en engageant un prestataire tel qu'un opérateur de services back-end, il est fort probable que l'architecture de déploiement technique corresponde à l'un des deux principaux scénarios décrits par la suite.

5.1 Signature en ligne par serveur primaire (serveur primaire caché)

Dans cette configuration, un serveur de nom primaire caché, inconnu sur Internet, dessert la zone avec un ensemble de serveurs DNS faisant autorité, généralement un serveur primaire public et un certain nombre de serveurs secondaires. Un serveur de nom primaire caché ne constitue pas une exigence spécifique pour DNSSEC. Il s'agit plutôt d'une bonne pratique préconisée pour le DNS, qui consiste à avoir un serveur de noms hors ligne (non connecté à Internet) faisant autorité, inaccessible et inconnu du public, où l'on peut effectuer toutes les mises à jour de zone. Ce serveur doit également mettre en place des procédures plus strictes en matière de sécurité et d'audit. L'architecture ressemble à la figure suivante :

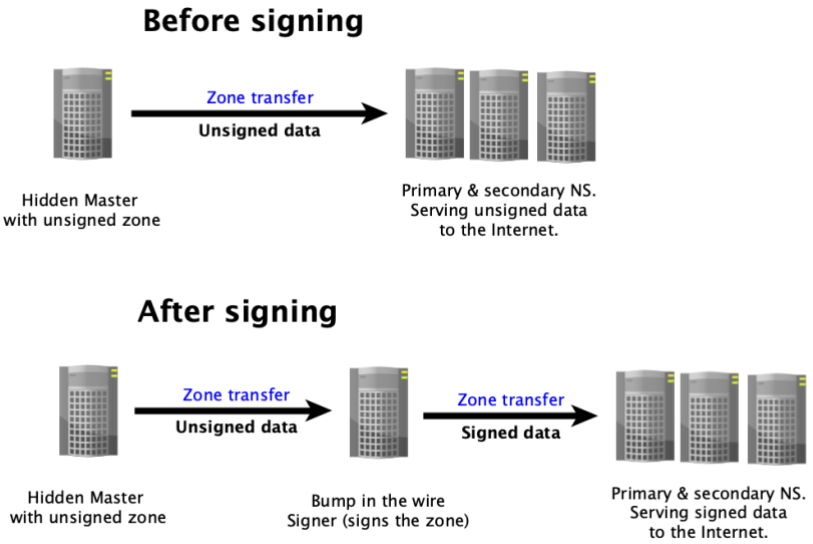


Ce serveur primaire caché sera configuré de sorte à reconnaître les clés créées et à les utiliser pour générer et charger une zone signée, en fonction des spécifications du logiciel DNS qu'il exécute. Une fois terminé, la version signée du fichier de zone sera transférée et synchronisée avec l'ensemble des serveurs de noms publics faisant autorité sur le domaine.

Outre les changements de configuration dans le serveur de nom primaire caché, aucun autre changement de configuration ou de logiciel ne doit être effectué pour mettre en œuvre cette architecture.

5.2 Signature en ligne par serveur « bump-in-the-wire »

Dans cette configuration, un nouveau serveur de nom, le serveur signataire, est inséré dans l'architecture existante et placé entre le serveur primaire caché et les serveurs de nom publics desservant la zone sur Internet. Ce nouveau serveur agit comme un dispositif « bump-in-the-wire (BITW) ». Il prend le fichier de zone non signé du serveur primaire caché, signe les données et envoie le fichier de zone signé afin qu'il soit distribué aux serveurs de nom publics du domaine.



À cette fin, les étapes suivantes peuvent être envisagées :

1. Le serveur primaire caché ne doit pas être indiqué dans le RRset de ressource de serveur de nom (NS) pour le domaine afin d'éviter de recevoir des réponses contradictoires, c'est-à-dire des réponses non signées du serveur primaire caché et des réponses signées des autres serveurs de noms.
2. La configuration du serveur primaire caché doit être mise à jour afin de permettre uniquement au signataire d'effectuer un transfert de zone.
3. Le signataire utilise le fichier de zone non signé reçu du serveur primaire caché et une clé privée afin de signer les enregistrements de ressources. Enfin, il distribue le fichier

de zone signé aux serveurs de noms primaire et secondaires via des mécanismes de transfert de zone.

4. La configuration des serveurs de noms doit également être mise à jour en conséquence afin de recevoir des transferts de zone uniquement du signataire.

Indépendamment du scénario de déploiement, il est recommandé de procéder à la vérification de la zone signée avant de la distribuer à l'ensemble des serveurs. Cet exercice de vérification peut être mené sur le nom de domaine à l'aide d'outils en ligne tels que ceux décrits à la section 10 du présent document. Une autre bonne pratique consiste à effectuer plusieurs requêtes visant à rechercher des signatures d'enregistrements de ressources DNSSEC et des dates d'expiration de signature, entre autres paramètres, dans chacune des zones administrées. Prévoyez d'inclure ces tests dans le processus de validation de votre déploiement.

Pour résumer, procédons à une comparaison des étapes dans la chaîne de production de zone entre le DNS normal et DNSSEC :

- **DNS normal** : Créer → Valider → Publier → Surveiller
- **Avec DNSSEC** : Créer → Valider → Signer → Valider → Publier → Surveiller

6 Signature d'un TLD

Comme pour tout autre changement majeur, il est vivement recommandé de mener une étape de test rigoureuse avant de planifier un déploiement dans le système de production. Dans le cas de DNSSEC, cette étape est d'autant plus nécessaire que de nouveaux changements sont introduits dans la zone. Les étapes décrites ci-dessous donnent un aperçu général de la signature d'une zone TLD mais, selon votre environnement et vos besoins spécifiques, vous pourriez être amené à les ajuster.

Dans certains cas, la signature de l'ensemble du fichier de zone en une seule fois pourrait s'avérer inadéquate pour les grands ccTLD. À la place, il serait plus sûr d'adopter une approche progressive pour la signature de la zone. D'autres ccTLD peuvent également choisir, dans un premier temps, de signer une zone enfant sur un banc d'essai, avant d'ajouter un enregistrement DS dans la zone parent. Il s'agit d'un test préparatoire avant de signer réellement la zone du ccTLD.

Dans tous les cas, pour réussir le processus de signature, il est judicieux de faire preuve de prudence en adoptant des plans de déploiement et de test adéquats, accompagnés d'une méthodologie de validation stricte.

1. Déployez et configurez un environnement de test (banc d'essai) DNSSEC. En fonction du modèle de déploiement, le banc d'essai peut contenir les éléments suivants :
   - Un serveur test de signature, c'est à dire un serveur de nom (NS test) capable de signer un fichier de zone. Le serveur doit être en mesure soit de générer les clés de signature soit de recevoir les clés générées à partir d'un serveur différent ou d'un module matériel de sécurité (HSM), de signer la zone et de distribuer le fichier de zone signé, entre autres fonctions.
   - Un serveur de nom secondaire de test faisant autorité recevra la zone signée et la desservira.

- Un résolveur de test doit être configuré afin d'effectuer des validations DNSSEC au niveau local pour la zone signée.

2. Copiez le fichier de zone non signé du serveur primaire caché dans le serveur test de signature. La distribution du fichier de zone non signé au système test de signature peut être automatisée par la suite lors de l'étape de test.
3. Générez les clés KSK et ZSK. Il est recommandé de générer les clés à partir du système de signature. Stockez la KSK dans un HSM ou hors ligne et utilisez-la uniquement pour signer les enregistrements de ressources DNSKEY.
4. Signez la zone et publiez-la dans le ou les serveurs de noms secondaires de test.
5. Générez et importez les DS en tant que clés de confiance dans le résolveur de test. Dans le monde réel, le DS ne sera pas distribué aux résolveurs récursifs du monde entier directement par les administrateurs de TLD ; il sera envoyé à l'IANA à des fins de publication dans la zone racine. Les résolveurs récursifs validants à travers le monde chercheront alors à obtenir le DS correspondant à ce TLD à partir de la zone racine.
6. Mettez en place des tests d'acceptance utilisateur (UAT) basés sur des scénarios de test définis. Les tests doivent porter sur des aspects tels que la récupération des clés et des signatures, la vérification de l'expiration des signatures, le délai et la taille des réponses aux requêtes. Effectuer la validation DNSSEC entre autres tâches.
7. Si le processus de signature de test est automatisé, portez une attention particulière à l'expiration de la signature et à la génération automatique des nouvelles signatures. Sinon, vous devez effectuer des roulements manuels jusqu'à l'automatisation du processus de test de signature.
8. Procédez au roulement de la ZSK et de la KSK. Pour un roulement de la KSK, générez le nouveau DS et simulez le partage avec la zone parent en l'ajoutant au résolveur de test à des fins de validation locale. En fonction de différents paramètres de temps tels que la période de validité de la clé dans l'environnement de test, vous devrez supprimer l'ancien DS du résolveur de test et l'ancienne KSK de la zone afin de procéder au roulement de la KSK.
9. Effectuez plusieurs nouveaux tests et peaufinez les étapes 1 à 8.
10. Une fois que vous maîtrisez la méthodologie de test, concentrez-vous sur la préparation à la mise en production, le choix de l'environnement adéquat et du scénario de déploiement : signature en ligne par serveur bump-in-the-wire (BITW) ou signature en ligne par serveur primaire caché. Menez un nouveau test d'acceptance utilisateur (UAT) afin de confirmer que l'ensemble des serveurs de noms de domaine faisant autorité desservent correctement la zone et ses enregistrements de ressources DNSSEC correspondants.
11. Enfin, publiez le DS dans la zone racine en respectant les directives relatives à la gestion des délégations pour les TLD, telles que définies par l'IANA à l'adresse suivante : https://www.iana.org/domains/root/manage. Une fois le DS ajouté à la zone racine, le monde entier est informé que le ccTLD est signé DNSSEC et que tous les résolveurs récursifs à capacité de sécurité doivent procéder à une validation DNSSEC à partir des enregistrements DNS provenant de cette zone. Il est vivement recommandé d'utiliser un outil tel que https://dnsviz.net/ (voir la section 10 pour plus détails) pour valider réellement la chaîne de confiance DNSSEC de la zone.
12. Une fois le ccTLD « officiellement signé », prévoyez de donner aux bureaux d'enregistrement la possibilité de publier les enregistrements DS des titulaires de noms de domaine dans le registre afin que la chaîne de confiance soit efficace.

7 Roulement de clé et d'algorithme

Lorsqu'une zone est sécurisée avec DNSSEC, le gestionnaire de zone doit être prêt à remplacer (ou « rouler ») périodiquement les clés utilisées pour sécuriser la zone, que ce soit pour des raisons de sécurité, opérationnelles ou en cas d'urgence. Pour mettre en œuvre un roulement de clé ou d'algorithme, il faut introduire de nouvelles clés et supprimer les anciennes clés de la zone. Il est essentiel de garder à l'esprit que les données publiées pour une zone se trouvent dans différents caches de résolveurs. Ignorer les données susceptibles de se trouver dans les caches pourrait entraîner une interruption du service pour les clients. Prenons comme exemple des données de zone signées avec une ancienne clé, validées par un résolveur qui n'a pas l'ancienne clé de zone dans son cache. Si l'ancienne clé ne se trouve plus dans la zone actuelle, la validation échouera et les données de zone correspondantes seront considérées fausses.

De la même manière, si un résolveur essaie de valider des données qui sont signées avec une nouvelle clé alors que l'ancienne clé se trouve toujours dans le cache du résolveur, les données seront également considérées fausses. Il existe différents types de techniques de roulement de clés et d'algorithmes, telles que celles décrites dans le RFC 6781, *Pratiques du fonctionnement de DNSSEC, Version 2* et le RFC 7583, *Considérations sur le délai de retour à zéro des clés dans DNSSEC*. Parmi des exemples de ces techniques on peut citer : *la prépublication, le roulement de la ZSK à double RRSIG, la double KSK, le double DS et le double RRset*, entre autres.

Dans le cas spécifique où un roulement de clé d'urgence est nécessaire en raison d'un risque de compromission d'une paire de clés ZSK ou KSK, il est conseillé d'avoir déjà mis en place une procédure documentée.

7.1 Roulement de ZSK

Lors d'un roulement de ZSK, il est essentiel de garantir que tout résolveur validant ayant en cache une signature donnée puisse avoir également accès à la ZSK valide correspondante. Le RFC 6781, *Pratiques du fonctionnement de DNSSEC, Version 2* présente trois méthodes pour le roulement d'une ZSK : la prépublication, la double signature et la double RRSIG.

Dans le présent document, nous nous contenterons de décrire la méthode de prépublication, car elle permet de réduire considérablement les tailles de la zone et des réponses pendant toute la durée du processus de roulement. Avec cette méthode, la nouvelle ZSK est introduite dans le RRset DNSKEY, après un délai permettant de s'assurer que tout RRset DNSKEY mis en cache contient bien les deux clés. La zone est alors signée à l'aide de la nouvelle ZSK et les anciennes signatures sont supprimées. Enfin, lorsque toutes les signatures créées avec l'ancienne ZSK ont expiré dans les caches, l'ancienne clé est supprimée. Les étapes suivantes décrivent le processus.

1. La nouvelle ZSK A est introduite dans la zone et figure dans le RRset DNSKEY, mais elle ne sera pas tout de suite utilisée pour signer les enregistrements dans la zone. Les KSK actuellement actives resignent le RRset DNSKEY, qui est alors resigné avec les KSK actuellement actives. À ce stade, la nouvelle ZSK est dite publiée.
2. Après un certain temps, la ZSK A est prête à signer des enregistrements dans la zone. Cette période correspond au délai de propagation de la zone auquel s'ajoute la durée de vie des enregistrements DNSKEY dans la zone. En d'autres termes, il s'agit du temps

maximum d'expiration des enregistrements DNSKEY existant dans les caches. La ZSK A devient active et commence réellement à signer des enregistrements pour la zone.

3. La ZSK A continuera à signer et à rafraîchir des enregistrements pour la zone jusqu'au jour où une nouvelle ZSK B devra être publiée. Le délai de publication de la clé B dépend du temps d'activation de A et de la durée de vie de la ZSK définie pour la zone dans la politique relative à la gestion des clés. La ZSK B est prête et peut être utilisée pour signer des enregistrements, mais la ZSK A est toujours active.
4. Lorsque la durée de vie de la ZSK arrive à sa fin pour la clé A, elle est retirée. La clé B devient active et est utilisée pour signer la zone. Toutefois, la clé retirée doit être conservée dans la zone un certain temps (on parle d' « intervalle de retrait ») afin de permettre aux RRSIG générées à l'aide de cette clé de continuer à être validées par les résolveurs. L'intervalle de retrait correspond au temps requis pour que l'ensemble des RRsets existants soient resignés avec la clé B, auquel s'ajoutent le délai de propagation de la zone ainsi que le TTL de toutes les RRSIG créées avec l'ancienne clé dans la zone.
5. Après un certain temps, les signatures créées avec la clé retirée disparaissent des caches des résolveurs et l'ancienne clé est déclarée morte.
6. Une fois l'ancienne clé morte, elle peut être supprimée du RRset DNSKEY, qui doit être resigné avec la KSK actuelle de la zone. À ce stade, la clé A est déclarée supprimée.
7. Après un certain temps, une nouvelle clé sera publiée, et l'intégralité du processus sera répété.

7.2 Roulement de KSK

Lors d'un roulement de KSK, le principal défi consiste à faire en sorte qu'une KSK de confiance existe en tout temps dans la zone, y compris pendant le processus de roulement. Le RFC 6781, *Pratiques du fonctionnement de DNSSEC, Version 2* présente également trois méthodes pour le roulement d'une KSK : la double KSK, la double signature et le double RRset. La méthode du double RRset est la plus efficace des trois, étant donné que les nouveaux enregistrements DS et les RRsets DNSKEY se propagent en parallèle.

Avec cette méthode, les nouveaux enregistrements DNSKEY et DS sont publiés simultanément dans les zones adéquates. Lorsqu'un délai suffisant a permis aux anciens RRsets DNSKEY et DS d'expirer dans les caches, ils sont supprimés de leurs zones respectives. Les étapes de roulement sont les suivantes :

1. Les enregistrements DS et DNSKEY se trouvent dans leurs zones respectives. Leur KSK A correspondante est active et sécurise la zone.
2. Lorsque la durée de vie de la KSK A actuelle est proche de son terme, une nouvelle KSK B est introduite dans la zone et utilisée pour signer le RRset DNSKEY. Le DS de la KSK B est envoyé à la zone parent à des fins de publication dans ladite zone (parente).
3. La zone parent peut procéder à la vérification du nouveau DS et ensuite le publier dans la zone parent.
4. Au bout d'un certain temps, le nouveau DS ou DNSKEY s'est déjà propagé dans les caches des résolveurs validants. À ce moment, la KSK A est supprimée de la zone.
5. Ultérieurement, les enregistrements DS et DNSKEY associés à la KSK A sont également supprimés.
6. Après un certain temps, une nouvelle clé sera publiée, et l'intégralité du processus sera répété.

8 Autres considérations liées aux zones signées

Il convient de tenir compte des éléments suivants lors de la préparation d'une stratégie de déploiement DNSSEC :

- **Définition d'un programme de renforcement des capacités**. Identifiez et participez à des ateliers, à des séminaires web, à des formations pratiques et à d'autres activités de renforcement des capacités vous permettant d'accroître vos connaissances et de développer de nouvelles compétences en matière de DNSSEC. L'équipe de l'ICANN chargée de la relation avec la communauté technique dispense des formations, telles que des ateliers sur DNSSEC, qui se tiennent généralement lors des réunions de l'ICANN.
  - Outre l'ICANN, le Network Startup Resource Center (NSRC), l'Internet Society et les registres Internet régionaux (RIR) proposent également des activités liées à DNSSEC.
  - Enfin, la participation à des forums, à des séminaires web et à des ateliers où des opérateurs chevronnés discutent avec des nouveaux venus des déploiements actuels et futurs de DNSSEC, est un bon moyen de renforcer vos connaissances concernant les pratiques opérationnelles de DNSSEC.
- **Abonnement aux listes de diffusion de NOG**. Ces listes constituent d'intéressants forums pour discuter et partager de l'expertise et des expériences techniques ainsi que pour chercher à obtenir du soutien et de l'aide sur des questions d'ordre technique. Prenez ces listes comme une véritable communauté qui pourrait vous aider lorsque vous en aurez besoin.
- **Génération et gestion de clés.** Les modules matériels de sécurité (HSM) constituent généralement un bon moyen de générer et de stocker des clés privées. Toutefois, les coûts liés à l'achat, à la sécurisation et à l'entretien des HSM doivent être pris en compte. Selon leurs fonctions, les coûts liés aux HSM peuvent varier de quelques centaines à quelques milliers de dollars. Les HSM peuvent également ajouter des frais généraux de formation, dans la mesure où tout nouveau matériel comporte son lot de défis. L'utilisation de HSM constitue une bonne pratique mais il ne s'agit pas de la seule méthode de génération de clés. Une autre possibilité intéressante consiste à générer, à stocker et à utiliser des clés privées dans une machine hors ligne, non connectée au réseau, sécurisée d'un point de vue physique. Le RFC 6781, *Pratiques du fonctionnement de DNSSEC, Version 2* donne de plus amples informations sur la génération et la gestion de clés.
- **Considérations liées au temps**. DNSSEC introduit la notion de temps absolu dans le DNS. Les signatures DNSSEC ont une période de validité allant de leur date de création à leur date d'expiration, après quoi la signature est considérée comme invalide et les données signées comme fausses. Il est critique de bien gérer les délais afin que les signatures soient générées avec la bonne période de validité. Imaginez une zone signée dont la période de validité de signature a expiré ; cela entraînerait un échec de la validation du côté du résolveur. Ainsi, il est vivement recommandé de configurer le serveur Network Time Protocol (NTP, protocole de temps réseau) afin de conserver une référence de temps précise. D'autres éléments doivent également être pris en compte tels que le temps de vie (TTL) minimum et maximum de la zone, la période de

publication de signature et la période de validité de signature, tels qu'ils sont décrits dans le RFC 6781, *Pratiques du fonctionnement de DNSSEC, Version 2*.

- **Exigences relatives aux logiciels, au matériel et au réseau**. Il existe aujourd'hui des implémentations de DNSSEC dans des solutions commerciales et open source telles que Berkeley Internet Name Domain (BIND), PowerDNS, NLnet Labs Name Server Daemon (NSD) et Knot DNS. OpenDNSSEC est une solution de signature largement utilisée étant donné qu'elle automatise le processus de gestion des clés DNSSEC et de la signature de zones. Si votre plan consiste à déployer DNSSEC dans un serveur faisant autorité, vous devrez générer les clés de signature cryptographique dans le système. Le temps requis pour générer les clés dépend de la source de génération de nombres aléatoires (entropie) dans le système. Des systèmes tels que des machines virtuelles dotées d'une entropie insuffisante peuvent prendre beaucoup plus de temps à générer des clés.
  - Les ressources matérielles, telles que le CPU, le stockage du système et la mémoire, sont autant d'éléments à prendre en compte aussi pour d'éventuelles optimisations. Cela est dû au fait que l'activation DNSSEC augmente le stockage du système, l'usage de la mémoire et la charge du CPU, en partie à cause de la génération et de la signature de clés. Une zone signée s'accompagne toujours d'une augmentation substantielle de la taille du fichier de zone.
  - En ce qui concerne les politiques de sécurité du réseau, vérifiez que les règles régissant les pare-feux et les listes de contrôle d'accès (ACL), par exemple, autorisent à la fois de grands paquets DNS UDP et le DNS sur TCP port 53. De plus, le mécanisme d'extension pour le DNS (EDNS0) doit être activé dans les serveurs DNS et dans la configuration du réseau, respectivement.

9 Suppression de la signature du TLD si nécessaire

Comme bien d'autres choses dans ce monde, DNSSEC n'est pas à l'abri de problèmes. Lorsque l'on en rajoute à la complexité du DNS, cela augmente la probabilité de pannes ou de défaillances. Par exemple, la KSK et/ou la ZSK peuvent être perdues ou compromises. Un incident matériel ou logiciel imprévu pourrait empêcher la signature et la distribution d'une zone et, par conséquent, ne pas lui permettre d'être correctement desservie.

Dans le pire des cas, il est peut-être préférable de supprimer la signature de la zone pour régler toute défaillance et bogue avant de procéder à une nouvelle signature. Toutefois, la suppression de la signature d'un domaine comporte des risques liés au retour à l'état non sécurisé.

La présence d'un enregistrement DS dans la zone parent permet de savoir si une zone est signée ou non. S'il n'y a pas d'enregistrement DS, la chaîne de confiance n'est pas assurée. Par conséquent, revenir à un état non signé est techniquement aussi facile que de supprimer tous les enregistrements DS d'une zone parent. Dans le cas d'un ccTLD, cela implique de demander à l'IANA de supprimer le(s) enregistrement(s) DS correspondant(s) de la zone racine.

Une fois tous les problèmes réglés, l'opérateur de TLD doit envisager la génération de nouvelles clés et la resignature de la zone. En outre, l'opérateur doit s'assurer que la zone nouvellement signée est bien distribuée et disponible dans tous les serveurs de noms avant de

publier un nouvel enregistrement DS dans la zone racine. Une fois le DS publié par l'IANA, l'ensemble du réseau Internet est informé que la zone TLD a de nouveau été signée et que les résolveurs validants vérifieront tous les enregistrements de ressources desservis par cette zone.

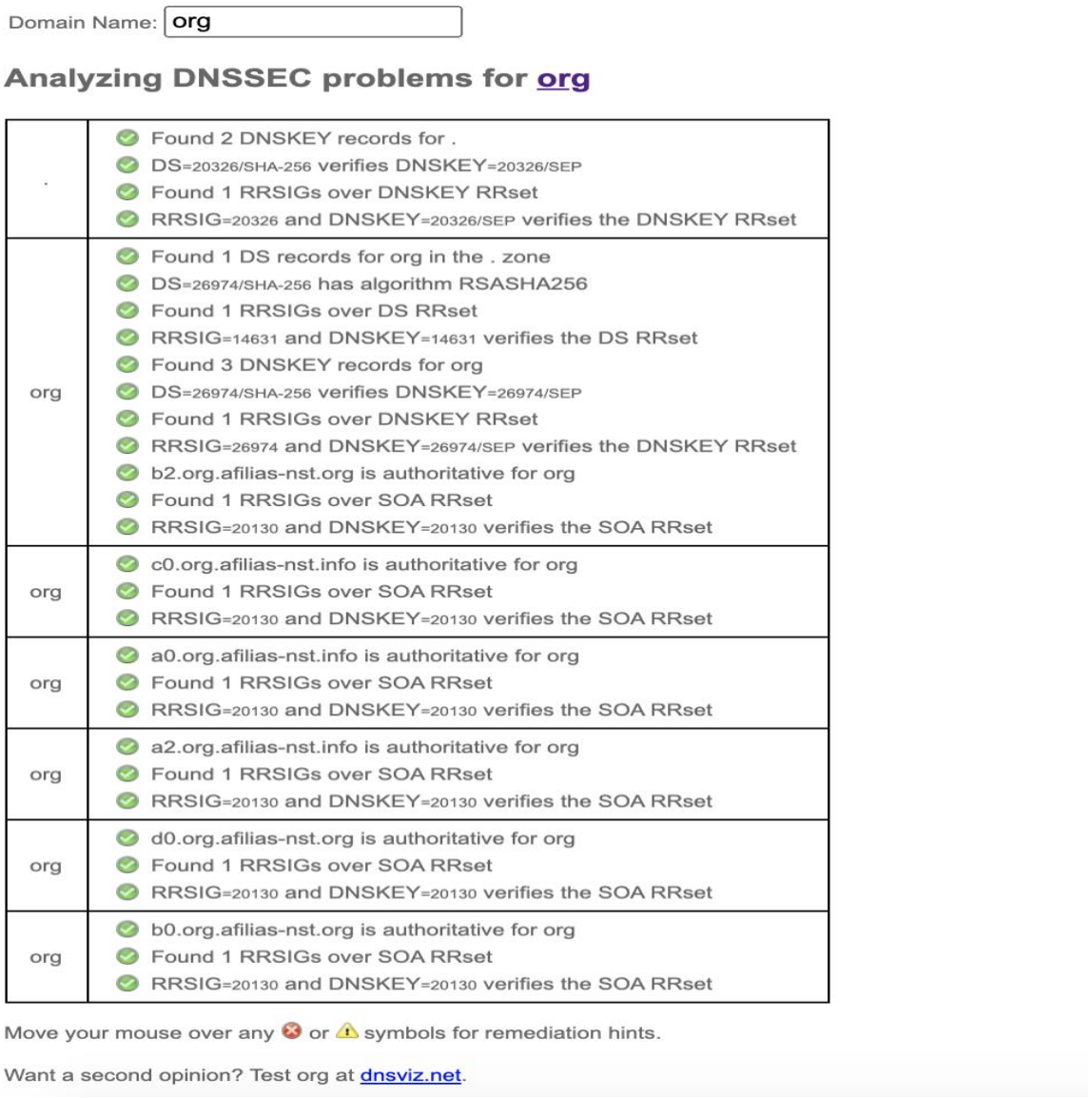
10 Outils DNSSEC pratiques

Les outils suivants peuvent être utiles pour régler des problèmes relatifs aux extensions DNSSEC.

10.1 Débogueur DNSSEC de Verisign

Ce débogueur DNSSEC, disponible sur https://dnssec-debugger.verisignlabs.com/, est un outil web qui permet de s'assurer que la « *chaîne de confiance* » est intacte pour un nom de domaine donné ayant des extensions DNSSEC activées. Il propose une validation des noms de domaine étape par étape et signale les problèmes rencontrés.

Voici un exemple des résultats obtenus à partir de cet outil :



Domain Name: org

Analyzing DNSSEC problems for org

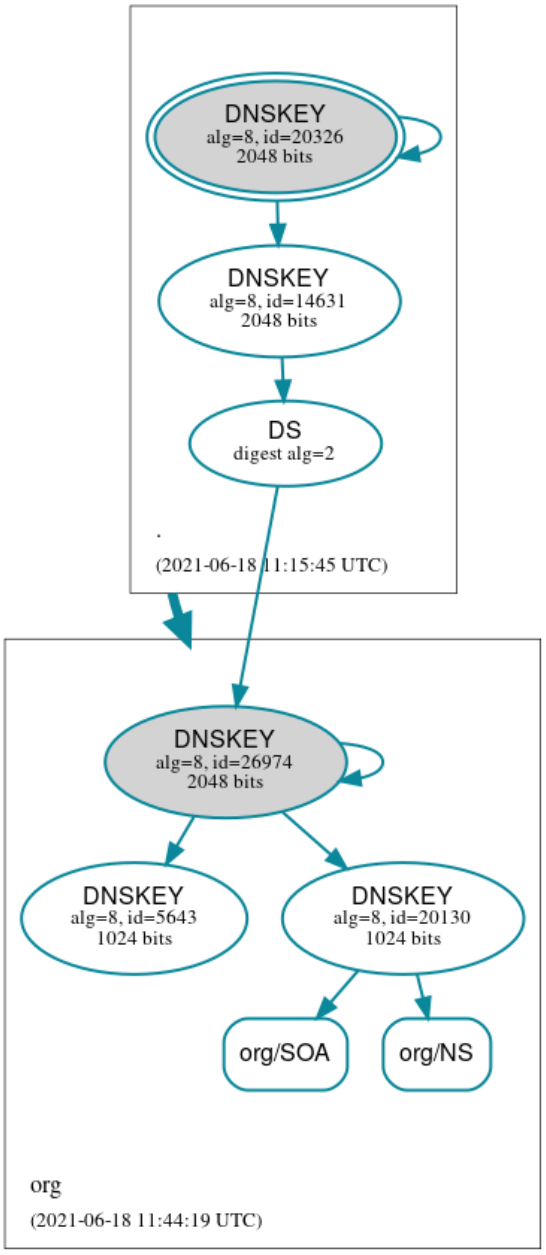
.	Found 2 DNSKEY records for . DS=20326/SHA-256 verifies DNSKEY=20326/SEP Found 1 RRSIGs over DNSKEY RRset RRSIG=20326 and DNSKEY=20326/SEP verifies the DNSKEY RRset
org	Found 1 DS records for org in the . zone DS=26974/SHA-256 has algorithm RSASHA256 Found 1 RRSIGs over DS RRset RRSIG=14631 and DNSKEY=14631 verifies the DS RRset Found 3 DNSKEY records for org DS=26974/SHA-256 verifies DNSKEY=26974/SEP Found 1 RRSIGs over DNSKEY RRset RRSIG=26974 and DNSKEY=26974/SEP verifies the DNSKEY RRset b2.org.afilias-nst.org is authoritative for org Found 1 RRSIGs over SOA RRset RRSIG=20130 and DNSKEY=20130 verifies the SOA RRset
org	c0.org.afilias-nst.info is authoritative for org Found 1 RRSIGs over SOA RRset RRSIG=20130 and DNSKEY=20130 verifies the SOA RRset
org	a0.org.afilias-nst.info is authoritative for org Found 1 RRSIGs over SOA RRset RRSIG=20130 and DNSKEY=20130 verifies the SOA RRset
org	a2.org.afilias-nst.info is authoritative for org Found 1 RRSIGs over SOA RRset RRSIG=20130 and DNSKEY=20130 verifies the SOA RRset
org	d0.org.afilias-nst.org is authoritative for org Found 1 RRSIGs over SOA RRset RRSIG=20130 and DNSKEY=20130 verifies the SOA RRset
org	b0.org.afilias-nst.org is authoritative for org Found 1 RRSIGs over SOA RRset RRSIG=20130 and DNSKEY=20130 verifies the SOA RRset

Move your mouse over any ⊗ or ⚠ symbols for remediation hints.

Want a second opinion? Test org at dnsviz.net.

10.2 DNSVIZ

DNSViz (https://dnsviz.net) est un outil permettant de visualiser l'état d'une zone DNS. Il fournit une analyse visuelle de la chaîne d'authentification DNSSEC pour un nom de domaine et son chemin de résolution dans l'espace de noms du DNS. Il dresse également une liste des erreurs de configuration détectées par l'outil. Vous trouverez ci-dessous un aperçu de la zone .ORG :



11 Conclusion

Les extensions DNSSEC constituent un protocole robuste qui garantit l'authentification et l'intégrité des données du DNS. La signature d'un nom de domaine avec DNSSEC change beaucoup de choses au niveau opérationnel car elle introduit de nouveaux concepts et tâches qui n'existaient pas avec le DNS normal.

Le présent document est un guide destiné à aider les opérateurs de registre de ccTLD et toute autre partie à comprendre les tenants et les aboutissants de la signature d'un ccTLD. Il y a

beaucoup à dire sur DNSSEC. Le présent document couvre certains des aspects les plus importants à prendre en compte pour le déploiement de DNSSEC.

Comme toute autre solution de sécurité, il est recommandé de suivre un processus approprié et de bien se préparer pour éviter tout risque de panne. Toutes les parties doivent évaluer leur propre environnement et les menaces et vulnérabilités associées afin de déterminer le niveau de risque qu'elles sont prêtes à accepter si elles déploient DNSSEC pour protéger leur zone et les domaines qui s'y trouvent.

Essentiellement, des efforts coordonnés et une collaboration active de toutes les parties prenantes restent la clé du succès pour le déploiement de DNSSEC.

A Exemple de politiques DNSSEC et de déclarations de pratiques DNSSEC

- Cadre de politiques DNSSEC et déclaration de pratiques DNSSEC de ZACR, version 001, septembre 2016, ZACR : https://www.registry.net.za/downloads/u/zacr-dps-signed.pdf
- Déclaration de pratiques DNSSEC pour .fr, version 1.2, juin 2013, Afnic : https://www.afnic.fr/wp-media/uploads/2020/12/dps-english-fr.pdf
- Déclaration de pratiques DNSSEC de CIRA pour .CA, version 1.5, août 2016, CIRA : https://www.cira.ca/cira-dnssec-practice-statement-ca
- Déclaration de pratiques DNSSEC pour la zone JP (DPS de JP), version 1.4, octobre 2015, JPRS : https://jprs.jp/doc/dnssec/jp-dps-eng.v1.4.html
- Déclaration de pratiques DNSSEC de Verisign pour la zone TLD/GTLD, version 1.8, décembre 2019, Verisign Inc. : https://www.verisign.com/assets/20191111_CTLD_VerisignDNSSECPracticeStatement_v1.8_finalized.pdf. La liste de zones auxquelles ce document s'applique est disponible à l'adresse suivante : https://www.verisign.com/assets/20190430-Verisign-Operated-TLD-GTLD-Zones-v1.04-Converted.pdf

B Exemple de zone non signée et signée

B.1 Zone non signée

```
example.                  86400  IN     SOA    a.nic.dns.blablabla.
hostmaster.dns.blablabla. (
                 2017072300 ; serial
                 1800       ; refresh (30 minutes)
                 900        ; retry (15 minutes)
                 2419200    ; expire (4 weeks)
                 300        ; minimum (5 minutes)
                 )

example.                  86400  IN     NS     a.nic.dns.blablabla.
example.                  86400  IN     NS     b.nic.dns.blablabla.
example.                  86400  IN     NS     d.nic.dns.blablabla.
```

```
example.                    86400   IN      NS      e.nic.dns.blablabla.
example.                    86400   IN      NS      f.nic.dns.blablabla.
aaa.example.                86400   IN      NS      ns1.reg.zzzz.
aaa.example.                86400   IN      NS      ns2.reg.zzzz.
bbb.example.                86400   IN      NS      ns1.reg.zzzz.
bbb.example.                86400   IN      NS      ns2.reg.zzzz.
ccc.example.                86400   IN      NS      ns1.reg.zzzz.
ccc.example.                86400   IN      NS      ns2.reg.zzzz.
ddd.example.                86400   IN      NS      ns3-l2.nic.zzzz.
```

B.2 Zone signée

```
example.                    86400   IN      SOA     a.nic.dns.blablabla.
hostmaster.dns.blablabla. (
                2017072305 ; serial
                1800       ; refresh (30 minutes)
                900        ; retry (15 minutes)
                2419200    ; expire (4 weeks)
                300        ; minimum (5 minutes)
                )

example.                    86400   IN      RRSIG   SOA 8 1 86400 20170724231821
20170618015310 660 example. nQ8H8StSRDoQgzwBNQ0k9+E1LGrV0tsCinoB6KxcyuHfGT4ehWsj5JI6
N01WpXqy/q1S/XlhqtjVoiti4zSOwIjFlSloug3W09eJnH9biwmb6U8B
JQoHf3edGvZtWNZdtcOKY1CFBI2ApceFn8KOYvT0qzpygOlF5lMrJvnO J5c=
exemple.                    86400   IN      NS      a.nic.dns.blablabla.
exemple.                    86400   IN      NS      b.nic.dns.blablabla.
exemple.                    86400   IN      NS      d.nic.dns.blablabla.
exemple.                    86400   IN      NS      e.nic.dns.blablabla.
exemple.                    86400   IN      NS      f.nic.dns.blablabla.
exemple.                    86400   IN      RRSIG   NS 8 1 86400 20170730192856
20170617025305 660 example. KNaF2jTPuCGq5FIzspbJL+TDBx/6z01E7+tkkzYRNh0xAKDnutcfb1It
D7XrNWPEbXsaafFyZ/M5DaDGzTzsVNm1h9h3md6o0vZNH07q8nmm+fYX
do8sx9aFxCgl9NsmG0cyrBbVnyrPKxDlAx69HJCh0kBb7PFKhr1hpnYY xGA=
example.                    86400   IN      DNSKEY 256 3 8
AwEAAasHjitdDurpevNLojD4Sp3609P+C9uOTR42DJel0NSSva/x38Ba
7gs0b4Q+tmKPI5cmxDhECiUfdzaRRA8vxPZK8x5LL/V1WZ5q6egFmH4x
eLxWaxlftFotev/T8kVe7jZUk7Hh3x7LPgGLajpjNNFELj42Xe6XBkkN 9FY1lQkB
example.                    86400   IN      DNSKEY 257 3 8
AwEAAY6HLDY5M5kjlrjVV9HQyWUkkrYZ2eB8KeJjUMN9qDM6FsA57pbS
5tmbGV1zxxqGon0pO7HYV06GZIgFOLBqDvgGsnKDQ5A2iktYNuSmTh+w
fd8ixgbYigtoBMBnNeqFozMK58c1yf7amui2cCOg9ibGZMpLQvjKOSyV
Jnlh0l8e3OE7Ul1GEa39XpVez2wkjImhsG0e7KAZPlFjEUpvwie8HEQV
jz3PK7Zr6SZVLLyet0rnN3prCHfvhNh6DycN/rt6/PopLvPQM8SaW+u8
zn6Z4S4AoTPTxKm5udzb7mWf7lT83PAbOvLu/WIRY6nqye+4SkJsrmjI xnLdk/Q54E8=
example.                    86400   IN      RRSIG   DNSKEY 8 1 86400 20170703000000
20170613000000 54322 example. B2riGYos+/q5RqXVBQKrrkVUuruDBH8ANNa8J6sMHUjf0MPZOuICd2kZ
PlAGMpZpp8LoaRoG2zaTVILZ8Vhi90FsyLsZVpPooAvmKlTFOrWoJoPo
XScLhb3ISRLOzKEnyLt5Ds3TxuabHLPlf8jpTXaHMFZCzYYtTJJQb+M3
BLeK+Lx4uCwU1pvxNkuR9StKa5tJquByIZCWZsSx5nKWPyrsGLtFJKrg
DXe8XlA8LxeER69OQgSZ1VXvK8Kd4p3wyvzUHCcsPYZzebxHXPqDrYB7
BU7eqsDUjCfThqbkC0Ju7koHROYRjGdoY/4f6nDOJEOICIFEgEDHJg2t w1nENQ==
example.                    0       IN      NSEC3PARAM 1 0 3 00FF
example.                    0       IN      RRSIG   NSEC3PARAM 8 1 0 20170716213640
20170606005304 660 example. a6Mp1NjW2/nnn+5i98AWzVrOX0yUvu/urP1cqY6zZjISReZOSLx6aorJ
```

```
lM9Nnx1fNVr2COtD71UVJI7kFUC5jVbmAitWdHHH/zyzK6WyyaN5Nsaf
cKW0Su8lLkctCHiqpKmuhOhnK1Dqmigx8YhyhPbN5nCzoST6lcnNjtV0 TwQ=
aaa.example.          86400  IN     NS     ns1.reg.zzzz.
aaa.example.          86400  IN     NS     ns2.reg.zzzz.
bbb.example.          86400  IN     NS     ns1.reg.zzzz.
bbb.example.          86400  IN     NS     ns2.reg.zzzz.
ccc.example.          86400  IN     NS     ns1.reg.zzzz.
ccc.example.          86400  IN     NS     ns2.reg.zzzz.
ddd.example.          86400  IN     NS     ns3-l2.nic.zzzz.
0KPQJ71AL5RHRST9HM8LEFLK0I0QN5N7.example.      3600 IN       NSEC3 1 1 3 00FF
464L7A368JEOCPKU9G34B9RQADEPKA14 NS DS RRSIG
0KPQJ71AL5RHRST9HM8LEFLK0I0QN5N7.example.      3600 IN       RRSIG NSEC3 8 2 3600
20170703210235 20170602012306 660 example.
H+qdaHqnAgUa66VSKmMmfKWopeZQM0ridMUN2YN4rncHeWD8b0yA6O6N
hLF/ojpZoGrQN+G+p4SWJVb/pj2CkLk00E2AhloXXV0KaQIzUwPVNm7p
J9es7ohi5ErGtM1ClLpGggz05qNWboejbrXtS8TFdoTtn6Z2Omk4RNmj hG0=
464L7A368JEOCPKU9G34B9RQADEPKA14.example.      3600 IN       NSEC3 1 1 3 00FF
MLTMB5J4Q7T5R3GJBSBTMVD2LBMFU3KA NS DS RRSIG
464L7A368JEOCPKU9G34B9RQADEPKA14.example.      3600 IN       RRSIG NSEC3 8 2 3600
20170715005821 20170610062309 660 example.
dk6WScB3zmJYig0w8LxFXoc9vj1leqFRBlET4YAVVmeAwcGf0ixa41T+
pKKcMHbXDsw+PHYZHaRLmA9lEgs+4lJMdA3fRroNSXyV2usHMdFaKUoG
UZKehVGdgrBRx4vx+o4w1ztdumY6MsD0ART6IrhUbr+cvGHAlxNSviCI BbE=
MLTMB5J4Q7T5R3GJBSBTMVD2LBMFU3KA.example.      3600 IN       NSEC3 1 1 3 00FF
0KPQJ71AL5RHRST9HM8LEFLK0I0QN5N7 NS SOA RRSIG DNSKEY NSEC3PARAM
MLTMB5J4Q7T5R3GJBSBTMVD2LBMFU3KA.example.      3600 IN       RRSIG NSEC3 8 2 3600
20170706043605 20170604225320 660 example.
Ndq6p+Y8ztlgNN1vH12o5rxxh7QM8GLY3E1FPCX4h7N4RtnuoPpvEpsl
/K4XQ1p/8Uehe6Izg0BpvQ7A256/+UW3lkwlonR7UaOX/+gkEdxuxlC/
41nX5fI9G5QFrV7H8B7ezlVF/uLz4nXyH4mzz496x4iTMEoHfoAdMinL C7A=
exemple.                    86400  IN     SOA    a.nic.dns.blablabla.
hostmaster.dns.blablabla. 2017072305 86400 14400 2592000 3600
```

C Liste de contrôle pour le déploiement de DNSSEC

C.1 Lancement et préparation

- ❑ Définir le déploiement de DNSSEC comme un projet.

  Gérer l'ensemble du processus comme un projet, avec une date de début, une date de fin prévue et des livrables précis en adoptant une approche de gestion de projet.

- ❑ Documenter le système existant.

  Documentation à jour décrivant le système et les processus utilisés.

- ❑ Procéder à un audit de l'infrastructure existante.

  Corriger tous les défauts du système actuel avant le déploiement de DNSSEC.

- ❑ Faire participer les parties prenantes.

  Les préparer afin qu'elles comprennent le déploiement de DNSSEC et qu'elles y soient prêtes.

❑ Définir et suivre un plan de formation.

Transmettre à votre personnel et à vos parties prenantes les connaissances et compétences nécessaires au déploiement de DNSSEC.

C.2 Déploiement et suivi

❑ Rédiger une DP ou une DPS.

Publier le cadre opérationnel de DNSSEC applicable à la zone.

❑ Rédiger un plan de déploiement de DNSSEC.

Documenter la stratégie globale du déploiement ainsi que ses étapes. Plusieurs points de la liste de contrôle peuvent être abordés dans ce document.

❑ Rédiger et valider les processus et les procédures opérationnelles de DNSSEC.

Documenter les procédures suivant vos besoins et votre environnement.

❑ Choisir un scénario de déploiement de DNSSEC.

Identifier le modèle de mise en œuvre de DNSSEC.

❑ Identifier et acheter du nouveau matériel et de nouveaux équipements.

Acheter du nouveau matériel et de nouveaux équipements.

❑ Sélectionner les paramètres de signature DNSSEC.

Attribuer des valeurs à un ensemble de paramètres de DNSSEC.

❑ Créer un banc d'essai pour DNSSEC.

Rédiger, exécuter et valider des tests pour la signature de zone afin de vous familiariser avec les processus et les opérations de DNSSEC.

❑ Préparer le lancement et prévoir une solution de repli.

Préparer et documenter le lancement dans l'environnement de production ainsi que les procédures de suivi et de repli.

❑ Lancement et suivi.

Mettre en œuvre et surveiller la signature DNSSEC dans l'environnement de production.

❑ Prévoir la publication du DS des titulaires de noms de domaine.

Promouvoir DNSSEC, se préparer à recevoir et à traiter les enregistrements DS des sous-domaines.

❑ Publier le DS des titulaires de noms de domaine.

Annoncer les DS des sous-domaines dans la zone du ccTLD.

❑ Documenter les enseignements tirés.

Compiler les enseignements et les expériences glanés lors de chaque étape du processus.

D Lectures complémentaires

- *Major DNSSEC Outages and Validation Failures* (Principales pannes et échecs de validation DNSSEC), IANIX : https://ianix.com/pub/dnssec-outages.html
- *DNSSEC: The long and bumpy road of algorithm deployment* (La longue route semée d'embûches du déploiement des algorithmes), APNIC, https://blog.apnic.net/2020/12/01/dnssec-the-long-and-bumpy-road-of-algorithm-deployment/
- *DNSSEC Infrastructure Audit Framework* (Cadre pour l'audit de l'infrastructure de DNSSEC), NLnet Labs, https://nlnetlabs.nl/downloads/publications/dns-audit-framework-1.0.pdf
- *Root DNSSEC information* (Informations DNSSEC de la racine), IANA, https://www.iana.org/dnssec
- *Frequently Asked Questions about DNSSEC* (*Foire aux questions concernant DNSSEC*), SIDN, https://www.sidn.nl/en/faq/dnssec
- RFC 6781, *Pratiques du fonctionnement de DNSSEC, Version 2,* https://www.rfc-editor.org/rfc/rfc6781.html
- *RFC 6841, Cadre pour les politiques DNSSEC et les déclarations de pratiques DNSSEC,* https://www.rfc-editor.org/rfc/rfc6841.html
- *RFC 8078, Gestion des enregistrements du DNS provenant du parent via CDS/CDNSKEY,* https://www.rfc-editor.org/rfc/rfc8078.html
- *RFC 8624, Exigences et lignes directrices d'utilisation et de mise en œuvre d'algorithmes pour DNSSEC,* https://www.rfc-editor.org/rfc/rfc8624.html