Plan de roulement de la KSK de la zone racine

Rapport préliminaire de l'équipe de conception - Mis à jour le 4 août 2015

1 Aperçu

L'ICANN prépare un plan pour mener à bien le roulement de la clé de signature de clé (KSK) des DNSSEC dans la zone racine. L'ICANN planifie l'opération de roulement en tant qu'opérateur des fonctions IANA, en coopération avec les autres partenaires de la gestion de la zone racine (RZM). Les partenaires sont Verisign, en tant que mainteneur de la zone racine et l'Agence nationale des télécommunications et de l'information des États-Unis (NTIA) comme administrateur de la zone racine.[1]

Le roulement de la KSK de la zone racine fait référence à la modification de la clé qui a été utilisée depuis 2010 lorsque la zone racine a été signée pour la première fois conformément à la définition des extensions de sécurité du système des noms de domaine (DNSSEC)[2]. Changer la clé veut dire générer une nouvelle composante cryptographique secrète et distribuer une nouvelle composante publique. La distribution adéquate de la nouvelle composante publique est l'aspect le plus critique de l'opération de roulement des clés.

Ce document, mis à disposition pour consultation publique, est un rapport préliminaire sur les délibérations d'une équipe de conception qui se compose d'un groupe d'experts bénévoles recrutés dans le DNS et les DNSSEC, ainsi qu'entre les partenaires de la gestion de la zone racine. Il s'agit d'un document préliminaire qui sera modifié en tenant compte des contributions de la communauté Internet au cours de la période de consultation publique de l'ICANN et de la poursuite des délibérations. Un rapport final sera publié suite aux débats qui auront lieu.

2 Table des matières

[1] Ce plan préliminaire est élaboré conformément à, et / ou compte tenu de la structure actuelle de gestion de la zone racine tel que cela est établi dans le contrat des fonctions IANA et le contrat de coopération entre la NTIA et Verisign. L'équipe de conception et les partenaires de la RZM reconnaissent que les efforts de transition de la supervision de l'IANA en cours peuvent avoir des répercussions sur le plan de roulement de la KSK et l'implication de la NTIA dans de futurs processus. Toutefois, les détails techniques et les considérations sont tout à fait indépendants de l'effort de transition et de son résultat final.

[2] Voir RFC 4033, RFC 4034 et RFC 4035

3 Résumé analytique

L'ICANN, en tant qu'opérateur des fonctions IANA, en collaboration avec Verisign comme le mainteneur de la zone racine et de la NTIA (Agence nationale des télécommunications et de l'information des États-Unis) connus comme les partenaires de gestion de la zone racine (RZM), a cherché à élaborer un plan de roulement pour la clé de signature de clé (KSK) de la zone racine.

Conformément aux DNSSEC, la KSK de la zone racine est utilisée pour signer l'ensemble des enregistrements de ressources DNSKEY de la zone racine. Cet ensemble comprend la clé de signature de zone (ZSK), qui est utilisée pour signer tous les autres ensembles d'enregistrements de ressources (RRsets) dans la zone racine. Le roulement de la KSK de la zone racine fait référence à la modification de la clé qui a été utilisée depuis 2010 (lorsque la zone racine a été signée pour la première fois conformément aux DNSSEC). Changer la clé veut dire générer une nouvelle composante cryptographique secrète et distribuer une nouvelle composante publique. La distribution adéquate de la nouvelle composante publique est l'aspect le plus critique du roulement des clés.

En décembre 2014, l'ICANN a fait un appel à bénévoles de la communauté pour participer avec les partenaires de la RZM dans une équipe de conception afin de développer le plan de roulement de la KSK de la zone racine, tel que présenté dans ce document. Le résultat de ce travail est un ensemble de recommandations techniques et opérationnelles destinées à orienter les partenaires de la RZM dans la production d'un plan détaillé de mise en œuvre pour l'exécution du premier roulement de la KSK de la zone racine. Ce document devrait être examiné comme un plan préliminaire destiné à fournir les résultats attendus.

3.1 Terminologie du DNS

Ce document porte sur des détails techniques du DNS et des DNSSEC. Afin que les définitions des termes relatifs aux DNSSEC (jargon) soient facilement accessibles, les définitions de certaines questions importantes sont incluses Tableau 1 ci-dessous.

Terme	Abréviation	Explication
Ensembles d'enregistrements de ressources	RRSet	Une unité de données stockées dans le DNS, la plus petite unité qui est signée par une clé DNSSEC
Clé de signature de clé	KSK	Une paire de clés publique-privée[3] dont le rôle est de produire une signature vérifiable de l'ensemble de clés en cours d'utilisation dans une zone DNS. Ce rôle est spécial parce que les DNSSEC exigent que ce genre de clé publique soit distribué à l'extérieur du protocole DNS
Clé de signature de zone	ZSK	Une paire de clés publique-privée dont le rôle est de produire des signature pour tous les autres ensembles de données dans une zone DNS. Cette clé n'est pas distribuée en dehors du protocole DNS
DNSKEY RRset		L'ensemble des clés utilisées dans une zone, y compris les rôles de la KSK et de la ZSK, un ensemble d'enregistrements de ressources DNSKEY
Roulement de la clé		Le fait de changer d'une clé cryptographique à une autre de façon harmonieuse
Validateur (DNSSEC)		Logiciel qui effectue les vérifications de sécurité sur les réponses des DNSSEC, y compris la vérification des signatures sur les données en une seule étape
Ancres de confiance		Une KSK stockée publiquement qui a la confiance absolue d'un validateur
Mises à jour automatisées des ancres de confiance des DNSSEC	RFC 5011	Une méthode pour mettre à jour automatiquement les ancres de confiance dans un validateur

[3] Ferguson, Niels; Schneier, Bruce (2003). *Practical Cryptography*. Wiley. ISBN 0-471-22357-3.

Terme	Abréviation	Explication
Double-signature		L'inclusion de deux signatures pour un RRset, normalement l'ancienne et la nouvelle clé impliquées dans un roulement. Usuellement une signature est suffisante pour un RRset
Comité consultatif du système des serveurs racine	RSSAC	Mandaté par les statuts constitutifs de l'ICANN, le RSSAC fournit des conseils à la communauté de l'ICANN au sujet du système des serveurs racine
Mécanismes d'extension pour le DNS	EDNS ou EDNS(0)	Actuellement défini dans le RFC 6891, l'EDNS fournit un moyen d'étendre ou d'élargir le format original du protocole DNS. EDNS(0) se réfère à la première série d'extensions
Enregistrement de ressources pour l'entrée relative à la signature de délégation	DS	Enregistrement des DNSSEC indiquant la KSK en cours d'utilisation par une sous-délégation (ou pour la zone racine, la KSK d'un domaine de premier niveau)
Réponse négative	NSEC ou NSEC3	Ensemble d'enregistrements de ressource définis par les DNSSEC utilisé pour indiquer l'inexistence de données pour la question posée
Déclaration de pratiques des DNSSEC	DPS	Un document décrivant les particularités du traitement des DNSSEC pour une zone.
Cérémonies de clés		Événements dans lesquels la clé privée est utilisée, à l'intérieur d'un module matériel de sécurité (HSM), pour générer des signatures. Un processus formel est utilisé lorsqu'il est souhaitable que des témoins observent les pratiques.

Tableau 1. Terminologie du DNS et des DNSSEC

3.2 Autres termes de sécurité

Terme	Abréviation	Explication
OpenPGP	OpenPGP	Un moyen de gestion de clés publiques-privées. RFC 4880 : *Format de message OpenPGP*
Normes de syntaxe du message cryptographique	PKCS#7	RFC 2315 : *PKCS #7 : Syntaxe du message cryptographique - Version 1.5*
L'annuaire - cadre général des certificats de clé publique et d'attribut	X.509	Norme ITU-T pour la gestion de clés publiques-privées. Recommandation ITU-T X.509 | ISO/IEC 9594-8
Requête de signature de clé	KSR	Une structure de données contenant les requêtes de signature de clés, plus précisément des ensembles DNSKEY qui doivent être signés par la KSK
Réponse avec des clés signées	SKR	Une structure de données contenant les signatures de clés générées privées, plus précisément les signatures KSK pour les ensembles DNSKEY

Tableau 2. Autres termes de sécurité

3.3 Autres termes de réseau

D'autres termes utilisés qui devraient être définis pour le grand public

Terme	Abréviation	Explication
Protocole de datagramme utilisateur	UDP	Un protocole de transport sans contexte, le meilleur pour envoyer des données à travers l'Internet

Terme	Abréviation	Explication
Protocole de contrôle de transmissions	TCP	Protocole de transport orienté vers la connexion, avec l'ordre des octets garantis pour l'envoi de données sur Internet
Unité de transfert maximale	MTU	Le nombre maximal d'octets qui peut être acheminé sur une partie de l'Internet. Path MTU se réfère à la MTU minimale de toutes les parties utilisées dans un voyage de bout en bout à travers l'Internet

Tableau 3. Autres termes de réseau

3.4 Sommaire des recommandations

Recommandation 1 : le roulement de la KSK de la zone racine devrait suivre la procédure décrite dans la RFC 5011 pour mettre à jour les ancres de confiance lors du roulement de la clé de signature de clé.

Recommandation 2 : l'ICANN devrait identifier les principaux fournisseurs de logiciels DNS et travailler en étroite collaboration avec eux afin de formaliser le processus et ainsi assurer que la distribution de l'ancre de confiance à travers des canaux spécifiques du fournisseur soit fiable et sécurisée.

Recommandation 3 : l'ICANN devrait identifier les intégrateurs clés du système du DNS et travailler en étroite collaboration avec eux afin de formaliser le processus et ainsi assurer que la distribution de l'ancre de confiance à travers des canaux spécifiques de l'intégrateur soit fiable et sécurisée.

Recommandation 4 : l'ICANN devrait jouer un rôle actif dans la promotion des authentifications de l'ancre de confiance de la zone racine, y compris mettre en évidence l'information publiée sur le site Web de l'IANA de l'ICANN.

Recommandation 5 : le roulement de la KSK de la zone racine ne devrait nécessiter aucune modification de fond à la gestion et au processus d'utilisation de la KSK existante afin de maintenir les normes élevées de transparence y associées.

Recommandation 6 : toutes les modifications apportées aux RRsets DNSKEY de la zone racine doivent être alignées avec l'intervalle de 10 jours décrit au DPS de l'opérateur KSK.

Recommandation 7 : l'algorithme existant et la taille de clé pour la KSK entrante pour le premier roulement de la KSK de la zone racine devraient être maintenus.

Recommandation 8 : le choix de l'algorithme et la taille de la clé devraient être revus pour les futurs roulements de la KSK de la zone racine.

Recommandation 9 : l'ICANN, en collaboration avec les partenaires de la RZM, doit concevoir et exécuter un plan de communication pour sensibiliser la population sur le roulement de la KSK de la zone racine, y compris la sensibilisation de la communauté technique mondiale par le biais de réunions techniques appropriées et de « partenaires de distribution » tels que ceux mentionnés dans ce document.

Recommandation 10 : l'ICANN devrait demander au RSSAC de coordonner une révision détaillée du calendrier pour la période de roulement de la KSK avant qu'il soit publié et devrait tenir compte des demandes de modification raisonnables à ce calendrier, au cas où un opérateur de serveur racine identifierait des raisons opérationnelles pour ce faire.

Recommandation 11 : l'ICANN devrait coordonner son travail avec le RSSAC et les partenaires de la RZM pour assurer que des canaux de communication en temps réel soient utilisés afin d'assurer la bonne sensibilisation opérationnelle du système des serveurs racines pour chaque modification de la zone racine qui implique l'ajout ou la suppression d'une KSK.

Recommandation 12 : l'ICANN devrait coordonner avec le RSSAC la demande aux opérateurs du serveur racine de collecter des données qui informeront les analyses subséquentes et aideront à caractériser l'impact opérationnel du roulement de la KSK, et que les plans et les produits de cette collecte de données soient publiés pour qu'ils soient analysés par une tierce partie.

Recommandation 13 : les partenaires de la RZM devraient s'assurer que toute augmentation future de la taille de la ZSK soit soigneusement coordonnée avec les roulements de la KSK, puisque les deux exercices ne sont pas simultanés.

Recommandation 14 : pour réduire le temps de récupération en raison de problèmes impliquant la KSK entrante, une SKR générée uniquement par la KSK en place devrait être obtenue en parallèle avec la SKR générée par la KSK entrante.

Recommandation 15 : les partenaires de la RZM devraient élaborer et documenter le processus d'utiliser le SKR généré par la KSK en place.

3.5 Public cible

Ce document est destiné à un public technique et en particulier à un public connaissant bien les protocoles DNS et DNSSEC, les aspects opérationnels du DNS, et les processus associés à l'utilisation des DNSSEC dans la zone racine.

3.6 Portée du document

Ce document a pour but d'encadrer et de fournir un ensemble de recommandations visant à guider les partenaires de la RZM dans leur élaboration d'un plan de mise en œuvre détaillé pour le roulement de la KSK de la zone racine.

4 Histoire abrégée

4.1 Déploiement des DNSSEC dans la zone racine

En 2009, les partenaires de la RZM ont collaboré[4] au déploiement des DNSSEC dans la zone racine, qui a abouti à la première publication d'une zone raine signée pouvant être validée en juillet 2010. La KSK de la zone racine actuellement utilisée a été générée lors de la première cérémonie KSK qui s'est tenue dans une structure de gestion de clés (KMF) gérée par l'ICANN à Culpeper, Virginie, États-Unis. Les matériaux clés ont été transportés suite à une deuxième KMF de l'ICANN à El Segundo, Californie, États-Unis et, une fois vérifié que le transport avait été fait en toute sécurité, la partie publique de la KSK a été publiée dans la zone racine et comme ancres de confiance.

Les exigences pour générer et maintenir la KSK de la zone racine, ainsi que les responsabilités respectives de chacun des partenaires de la RZM, ont été précisées par la NTIA[5]. Les procédures par lesquelles ces exigences ont été remplies par le mainteneur de la zone racine et l'opérateur des fonctions IANA ont été publiées dans des déclarations de politique et pratiques des DNSSEC (DPS)[6].

Le contrat des fonctions IANA entre la NTIA et l'ICANN a été modifié en juillet 2010 pour y inclure les responsabilités liées à la gestion de la KSK de la zone racine, et

[4] Les détails du déploiement des DNSSEC dans la zone racine sont publiés sur http://www.root-dnssec.org/
[5] « Exigences en matière de test et de mise en œuvre pour le déploiement initial des DNSSEC dans la zone racine autoritaire » 29 octobre 2009, http://www.ntia.doc.gov/files/ntia/publications/dnssec_requirements_102909.pdf
[6] https://www.iana.org/dnssec, https://www.verisigninc.com/en_US/repository/index.xhtml

ces exigences ont été reportées dans les révisions subséquentes de ce contrat[7]. L'accord de coopération entre la NTIA et Verisign a été également modifié en juillet 2010 pour refléter les responsabilités de l'opérateur de la KSK de la zone racine de Verisign.[8]

Le contrat des fonctions IANA exige à l'ICANN d'effectuer un roulement de la KSK de la zone racine, mais ne spécifie ni un calendrier détaillé ni un plan de mise en œuvre. Le DPS de l'opérateur de la KSK de la zone racine contient cette déclaration, et précise une exigence pour un roulement dans la section 6.5 :

« Chaque clé de signature de clé de la zone racine (RZ KSK) est programmée pour être reportée à travers une cérémonie de clé selon les besoins, ou après 5 ans d'opération ».

4.2 Commentaires publics sur le plan de roulement de la KSK de la zone racine

Le 8 mars 2013, l'ICANN a ouvert une période de consultation publique pour recevoir des commentaires au sujet de l'exécution d'un roulement de la KSK de la zone racine[9]. Des réponses de six organisations et de 15 personnes ont été reçues. Dans son résumé des réponses[10], l'ICANN a identifié sept recommandations à en tenir compte par partenaires de la RZM :

1. il faudrait établir une série d'essais et de mesures, avec un banc d'essai, avant de s'embarquer dans un roulement de la KSK suivant le RFC 5011. Des voies de communication doivent être établies au cours des étapes d'essai ainsi que des méthodes pour l'évaluation du succès.
2. le roulement de la KSK doit être effectué aussitôt que possible, en mettant l'accent sur la préparation.
3. les mesures et la surveillance sont les principaux modes clés qui doivent être mis en place pour mesurer l'impact [technique et sur l'utilisateur final] d'un roulement de la KSK.
4. le roulement de la KSK devrait avoir lieu régulièrement.
5. les notifications aux groupes de parties prenantes multiples et divers devraient se faire avant le roulement de la KSK, l'avis devant être envoyé suffisamment à l'avance.

[7] http://www.ntia.doc.gov/page/iana-functions-purchase-order
[8] http://www.ntia.doc.gov/files/ntia/publications/amendment31_07062010.pdf
[9] https://www.icann.org/public-comments/root-zone-consultation-2013-03-08-en
[10] https://www.icann.org/en/system/files/files/report-comments-root-zone-consultation-08apr14-en.pdf

6. il est nécessaire de mener une enquête plus approfondie sur la stabilité opérationnelle, les roulements de la KSK répétés et [la probabilité et l'impact] la non-conformité avec le RFC 5011.

4.3 Discussion préliminaire sur le roulement de la KSK de la zone racine en 2013

Les partenaires de la RZM ont convoqué à une réunion fin juillet 2013 pour discuter des options pour rouler la KSK de la zone racine. L'équipe a identifié le besoin de réaliser une procédure de roulement des clés en étapes distinctes sur une période de temps prudente, les avantages de la sensibilisation de la communauté et la notion d'un calendrier de roulement RFC5011 modifié avec une révocation retardée. Ces principes de haut niveau ont été présentés pendant la réunion du groupe de travail des opérations du DNS (DNSOP) à l'IETF 87[11].

4.4 Avis du SSAC sur le roulement des clés DNSSEC dans la zone racine

En novembre 2013, le Comité consultatif sur la sécurité et la stabilité de l'ICANN (SSAC) a publié le SAC063[12], concernant le roulement de la KSK. Le rapport portait sur les risques encourus ainsi que l'état du code de base à ce moment-là (mises en œuvre du DNS à code source ouvert en particulier). Le rapport recommande d'entreprendre une action de communication pour faire connaître le roulement de la clé de la KSK de la zone racine, d'encourager des tests pour collecter et analyser les comportements du résolveur, de créer des paramètres des niveaux acceptables de « rupture » dans un roulement des clés de la KSK de la zone racine, de définir les mesures de restauration en cas d'excès de « rupture » et de collecter des informations pour informer les futurs exercices de roulement de clés de ce genre.

Le rapport du SSAC a signalé trois thèmes qui sont abordés plus loin dans ce document. Tout d'abord, une estimation grossière de 1,1 % de ceux s'appuyant sur le DNS utilisant les DNSSEC pourraient être négativement affectés même par un roulement des clés de la KSK de la zone racine bien géré. Deuxièmement, l'état du support pour les mises à jour automatisées des ancres de confiance des DNSSEC, également connu comme RFC 5011, est présent mais imprévisible. Et, troisièmement, que la taille des réponses DNS résulte inquiétante lorsqu'elle se rapporte à l'apparition de la fragmentation sous-jacente des paquets UDP et le retour à des requêtes TCP.

[11] http://www.ietf.org/proceedings/87/slides/slides-87-dnsop-6.pdf
[12] https://www.icann.org/en/system/files/files/sac-063-en.pdf

4.5 L'ICANN convoque l'équipe de conception du roulement de la KSK de la racine

En décembre 2014, l'ICANN a fait un appel à bénévoles de la communauté pour participer avec les partenaires de la RZM dans une équipe de conception afin de développer le plan de roulement de la KSK de la zone racine, tel que présenté dans ce document.

5 Description de haut niveau du roulement d'une KSK

Le plan de juillet 2013, qui n'est pas très éloigné des plans pour rouler n'importe quelle autre KSK, suit les étapes suivantes :

1) la génération d'une paire de clés entrantes de la KSK (publique et privée).

2) la clé publique de la KSK entrante est placée dans la zone racine et/ou mise à disposition des parties qui l'utilisent.

3) dans une déviation par rapport à d'autres zones, la nouvelle clé publique de la KSK de la zone racine se trouve dans un état où elle devient acceptée par toutes les parties concernées ce qui est en effet la prochaine KSK. En plus d'être acceptée passivement, la nouvelle clé publique de la KSK de la zone racine est rendue disponible sur divers supports électroniques et non électroniques pour permettre aux opérateurs et aux développeurs du résolveur qui ont des serveurs ne supportant pas le RFC 5011 d'avoir le temps suffisant d'inclure la nouvelle ancre de confiance dans leurs systèmes et produits. (Pour les « autres zones », cette étape est remplacée par informer le titulaire de l'enregistrement DS qu'il y a une KSK entrante.)

4) le processus de signature passe d'utiliser la clé privée de titulaires de la KSK à la clé privée de la KSK entrante.

5) la KSK entrante est maintenant dans un état de transition car les signatures générées par le titulaire de la KSK en place expirent ou autrement disparaissent de la vue opérationnelle.

6) la clé publique de la KSK en place est supprimée de la zone racine (sans révocation).

7) dans une autre déviation des opérations normales, la KSK de la zone racine en place est réintroduite dans le but de signaler qu'elle est révoquée conformément aux lignes directrices du RFC 5011. Cette étape distincte est conçue pour

s'adapter aux opérations de la ZSK, y compris les roulements de cette clé sans surdimensionner les réponses du DNS pour le jeu de clés complet de la zone racine.

6 Approche de l'équipe de conception

L'équipe de conception a examiné plusieurs aspects d'un roulement de la KSK de la zone racine et a produit des recommandations de chaque domaine d'étude pour guider l'élaboration d'un plan de mise en œuvre par les partenaires de zone racine.

- Considérations opérationnelles : l'impact sur les utilisateurs finaux de l'Internet et les opérateurs des systèmes DNS, et les services utilisés par ces utilisateurs finaux
- Considérations sur le protocole : dans la mesure où ils existent, les éléments de protocole documentés sont suffisants pour accueillir un roulement de la KSK de la zone racine
- Impact sur la gestion de la KSK de la zone racine : l'impact sur les processus impliqués dans la gestion de la KSK par l'opérateur des fonctions IANA
- Considérations cryptographiques : assurer que le système dans son ensemble a la puissance cryptographique suffisante
- La communication et la coordination avec toutes les parties concernées

Chacun de ces points est abordé individuellement dans les sections qui suivent. Une solution de roulement technique détaillée est également fournie pour illustrer comment les recommandations pourraient être suivies et censées être le point de départ pour les partenaires de la RZM au fur et à mesure de la finalisation de leur plan de mise en œuvre.

6.1 Considérations opérationnelles

L'impact sur les utilisateurs finaux de l'Internet et sur les opérateurs des systèmes DNS devraient se produire au cours des deux étapes ci-dessus. Lorsque la clé publique de la KSK entrante est ajoutée à la zone racine, la taille de la réponse pour l'ensemble DNSKEY de la racine augmentera. Lorsque la clé privée de la KSK en place ne générera plus de signatures, la validation utilisant cette clé publique ne fonctionnera plus tel que prévu.

Avec une réponse élargie au DNSKEY, il se peut que la fragmentation de paquets UDP se produise avec des résultats légèrement différents sur IPv4 et IPv6. Il y a déjà des composantes Internet qui considèrent les fragments anormaux qui sont

filtrés. Pour le DNS, qui ne maintient aucun état concernant les réponses envoyées, signifie qu'un client pourrait ne pas obtenir la réponse attendue. Il y a aussi le potentiel pour qu'une plus large réponse UDP dépasse la taille de la charge transportée spécifiée de la requête du DNS, augmentant ainsi le niveau des réponses tronquées et la nouvelle requête ultérieure en utilisant TCP.

Une fois que la KSK en place ne signe plus la clé de signature de clé de la zone, avec l'implication que la KSK entrante génère des signatures, un validateur DNSSEC avec seulement la KSK en place configurée comme une ancre de confiance échouera pour valider les réponses signées des DNSSEC. Le validateur « échouera, puis se fermera », ce qui signifie qu'il considèrera toutes les réponses DNS signées comme invalides.

Un client final qui utilise exclusivement des résolveurs de validation qui ne parviennent pas à interpréter la KSK entrante, ou qui ne parviennent pas à recevoir les réponses plus larges pendant le processus de roulement de la clé ne pourra valider aucune des réponses DNS signées. Cela apparaîtra pour le client final comme une forme de panne d'Internet, où les noms de domaine ne sont pas susceptibles d'être résolus. Lorsque des situations similaires se sont produites auparavant, l'effet secondaire a été une augmentation des appels aux centres de soutien à la clientèle, ce qui impose une charge supplémentaire pour le soutien à la clientèle et sur les rôles de gestion opérationnelle des FSI.

L'ICANN devrait prévoir des communications en vue d'être coordonnée avec l'introduction de la KSK entrante, ainsi que l'échange de la génération de signatures de la KSK en place à la KSK entrante (voir recommandation 8).

6.2 Considérations concernant le protocole

6.2.1 Configuration de l'ancre de confiance de la zone racine

Il existe deux types de configurations d'ancre de confiance à en tenir compte :

- ancres de confiance pour les résolveurs de validation en ligne
- ancres de confiance dans les dispositifs ou systèmes qui sont hors ligne pendant le roulement et mis en ligne plus tard

Les résolveurs de validation en ligne peuvent utiliser des *Mises à jour automatisées des ancres de confiance de la sécurité du DNS (DNSSEC)* comme décrit dans le RFC 5011, si le logiciel DNS utilisé prend en charge ce mécanisme et s'il est configuré pour utiliser ce mécanisme afin de mettre à jour la clé de signature de clé de la zone racine.

Les résolveurs de validation en ligne qui sont incapables ou refusent d'utiliser les mises à jour automatisées des ancres de confiance de la sécurité du DNS devront être mis à jour manuellement pendant le roulement de la clé de signature de clé. La mise à jour manuelle devrait suivre le délai du mécanisme du RFC 5011 – la nouvelle ancre de confiance doit être ajoutée à la configuration de ce résolveur de validation dans la période de PUBLICATION du roulement (voir la Section 11 pour plus de détails), et l'ancre de confiance en place ne doit pas être supprimée avant que la zone racine soit signée avec la KSK entrante de la zone racine. Par ailleurs, pour suivre une pratique opérationnelle prudente, l'ancre de confiance en place ne devrait pas être retirée avant que la KSK en place de la zone racine soit révoquée. Les mécanismes pour récupérer la nouvelle ancre de confiance sont les mêmes que pour les dispositifs en mode hors ligne décrits ci-dessous.

Recommandation 1 : le roulement de la KSK de la zone racine devrait suivre la procédure décrite dans la RFC 5011 pour mettre à jour les ancres de confiance lors du roulement de la clé de signature de clé.

Les dispositifs qui sont hors ligne durant le roulement de la KSK de la zone racine devront être mis à jour manuellement s'ils sont mis en ligne une fois que le roulement est terminé. Essentiellement, ces dispositifs doivent être soumis à la méthode du « bootstrap »comme s'ils venaient d'être installées.

Plus généralement, le processus par lequel n'importe quel dispositif se prépare pour effectuer la validation des DNSSEC devrait suivre une approche qui réduit la possibilité d'utiliser une ancre de confiance inappropriée. Des conseils généraux pour ces dispositifs sont actuellement distribués dans un document préliminaire d'Internet, intitulé « Publication de l'ancre de confiance des DNSSEC pour la zone racine » au sein de l'IETF[13]. Mais il est nécessaire de faire une analyse plus approfondie afin d'arriver à un document de consensus stable qui donne des avis aux responsables de la mise en œuvre.

L'équipe de conception soutient la discussion de la communauté et l'examen du document préliminaire d'Internet au sein de l'IETF, dans le but de publier une spécification stable, évaluée par des pairs dans les séries du RFC.

Il y a plusieurs cas d'utilisation de la récupération des ancres de confiance actualisées, qui sont abordés brièvement ci-dessous.

[13] http://tools.ietf.org/html/draft-jabley-dnsop-validator-bootstrap-00

6.2.1.1 Poursuite des débats sur le RFC 5011

Le texte précédent fait allusion aux résolveurs qui « ne peuvent ou ne veulent pas » dépendre de l'approche du RFC 5011. Cette section est destinée à fournir des renseignements généraux sur cette phrase.

L'esprit du jalon de futur ajout du RFC 5011 est important. Le jalon est inclus afin d'empêcher qu'une clé faussement présentée soit acceptée. Autrement dit, si une entité veut présenter une KSK fausse, elle devrait avoir du succès en publiant la clé. Dans ce cas, la véritable autorité sera en mesure de rejeter la fausse clé avant qu'elle devienne fiable.

La résistance des résolveurs au RFC 5011 ne repose pas sur des questions liées à la conception du mécanisme de mise à jour. Plutôt, la résistance s'enracine dans quelques réalités opérationnelles. La gestion de la configuration est une question majeure lorsque l'on opère une flotte de serveurs et dépend de l'« ouverture vers l'extérieur » des fichiers de configuration gérés. Le mécanisme de mise à jour du RFC 5011 va à l'encontre de cela, avec la flotte de machines configurées apprenant de nouvelles données, s'écartant de la configuration centralisée.

Dans cet esprit, les grands opérateurs auront un processus manuel en place, un processus qui utilisera divers mécanismes automatisés. Un système automatisé peut être un outil qui suit le mécanisme de mise à jour du RFC 5011. Dans une brève enquête informelle, les grands opérateurs pourront compter sur un sondage de la nouvelle KSK de la zone racine de différentes manières, y compris la communication humaine pour établir la confiance. C'est la raison pour laquelle des solutions alternatives au RFC 5011 sont proposées.

En étudiant plus profondément l'opérationnalisation du RFC 5011, quelques lacunes ont été identifiées. La première implique la vérification à distance d'un processus réussi du RFC 5011. La deuxième implique la possibilité de tester les déploiements à la lumière du futur jalon d'ajout.

Ce qui est nécessaire c'est un moyen pour que les ancres de confiance utilisées dans un résolveur soient connues par la source de confiance. Compte tenu de l'arrière-plan de la surveillance généralisée, l'intention est de ne pas connaître la configuration et les capacités spécifiques du résolveur, mais tout d'abord il faut confirmer que le processus du RFC 5011 a été bien suivi et avoir une idée de quand il est acceptable de s'engager avec la KSK entrante de la zone racine.

Il a également été identifié qu'il est nécessaire d'accélérer la possibilité d'effectuer un test fonctionnel, un qui montre les étapes du RFC 5011 bien que n'adhérant pas au modèle de sécurité requis. Plus précisément, les outils doivent pouvoir substituer

le futur jalon d'ajout spécifié pour permettre un réglage plus court au cours des essais. Il est souhaitable de fournir un mécanisme de « test sécurisé » pour s'assurer que le futur jalon d'ajout de test n'est pas utilisé dans la production. Il s'agit d'une suggestion adressée aux développeurs d'outils et aux fournisseurs de logiciels DNS.

6.2.1.2 Autres formats d'ancres de confiance

Depuis la signature initiale de la zone racine, l'ICANN a mis à disposition l'ancre de confiance dans des formats non DNS via un site Web[14]. Ces ancres de confiance fournissent un chemin non-critique pour distribuer et recevoir l'ancre de confiance de la zone racine, c'est-à-dire un moyen en dehors des opérations du DNS. (Le site Web nécessite accéder aux DNS pour arriver aux fichiers). Compte tenu de l'examen du chemin non critique, de nouvelles ancres de confiance peuvent être distribuées. À un certain moment dans l'avenir, il est possible d'ajouter des ancres de confiance de différents algorithmes cryptographiques des DNSSEC[15] pour mettre l'accent sur les nouvelles capacités requises. Cela peut aussi être un moyen pour le peuplement des résolveurs avant un roulement déclenché d'urgence.

6.2.1.3 Fournisseurs de logiciels pour le DNS

Le fournisseur peut assembler les ancres de confiance au logiciel du DNS (logiciel open source ou propriétaire/commercial). Le fournisseur du logiciel devra émettre une nouvelle version de l'ensemble de l'ancre de confiance pour garder le logiciel actuel.

Il est important que les ancres de confiance distribuées de cette manière soient authentiques et tirent profit de tout mécanisme de vérification existant pour assurer l'intégrité du logiciel sur un système utilisé dans la phase initiale ou finale (end-system). Les fournisseurs de logiciels requièrent une méthode robuste et efficace pour s'assurer que les ancres de confiance qu'ils distribuent avec leur logiciel sont authentiques, étant donné que l'impact de la distribution des clés non authentiques est potentiellement important, notamment si elles sont signées avec des clés de signature de code dans le cadre de la stratégie de mise à jour du logiciel du fournisseur.

Recommandation 2 : l'ICANN devrait identifier les principaux fournisseurs de logiciels DNS et travailler en étroite collaboration avec eux afin de formaliser

[14] https://www.iana.org/dnssec/files
[15] https://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xhtml#dns-sec-alg-numbers-1

le processus et ainsi assurer que la distribution de l'ancre de confiance à travers des canaux spécifiques du fournisseur soit fiable et sécurisée.

6.2.1.4 Intégrateurs de systèmes

Une méthode de distribuer les ancres de confiance des DNSSEC se fait par l'intégrateur de systèmes, par exemple, un mainteneur de paquets ou un fournisseur de systèmes d'exploitation. Dans ce cas, l'intégrateur de systèmes fournira les paquets mis à jour pour toutes les copies des ancres de confiance dans le système. Il y a des efforts dans plusieurs distributions de Linux pour fournir un paquet avec une copie officielle de l'ancre de confiance.

Recommandation 3 : l'ICANN devrait identifier les intégrateurs clés du système du DNS et travailler en étroite collaboration avec eux afin de formaliser le processus et ainsi assurer que la distribution de l'ancre de confiance à travers des canaux spécifiques de l'intégrateur soit fiable et sécurisée.

6.2.1.5 Administrateurs du système

Les administrateurs des systèmes peuvent télécharger manuellement les ancres de confiance des DNSSEC du site de Web de l'IANA de l'ICANN pendant l'installation ou la mise à jour du logiciel. Les ancres de confiance de la zone racine actuelles sont fournies par l'opérateur des fonctions IANA sur un site Web dédié[16] pour plus d'informations se rapportant aux DNSSEC dans la zone racine. Déterminer l'authenticité des ancres de confiance téléchargées est essentiel pour établir la confiance dans les DNSSEC. Pour supporter la vérification de l'authenticité, différents types de signatures numériques, sous forme de OpenPGP, PKCS #7 et un certificat X.509 contenant la clé racine sont également publiés sur le même site dédié.

Bien qu'il soit extrêmement important de déterminer l'authenticité, ce fait est souvent négligé et sous-spécifié. Lorsque les processus pour supporter les preuves d'authenticité ont été rendus disponibles pour révision publique, le volume des commentaires de fond a été faible. Cela sape les efforts visant à soutenir adéquatement l'authenticité. Il semble possible qu'une révision supplémentaire (avec des modifications compatibles avec les versions précédentes, le cas échéant) soit justifiée. Comme mentionné plus haut, l'équipe de conception soutient la discussion de la communauté et la révision du document préliminaire d'Internet intitulé « *Publication de l'ancre de confiance des DNSSEC pour la zone racine* » au

[16] Répertoriés à https://www.iana.org/dnssec/files

sein de l'IETF (cité ci-dessus), dans le but de publier une spécification stable, évaluée par des pairs dans les séries du RFC.

D'autre part, les récupérations observées dans les signatures numériques de support à l'authentification suggèrent que peu de parties, voire aucune, ont fait usage des signatures numériques. Gagner la confiance ne se fait pas tout simplement en fournissant des signatures numériques, cela vient plutôt de la promotion active.

Recommandation 4 : l'ICANN devrait jouer un rôle actif dans la promotion des authentifications de l'ancre de confiance de la zone racine, y compris la mise en évidence de l'information publiée sur le site Web de l'IANA de l'ICANN.

6.3 Impact sur la gestion de la KSK de la zone racine

Comme décrit dans la *Déclaration de pratiques des DNSSEC pour l'opérateur de la KSK de la zone racine*, l'opérateur de la KSK de la zone racine signe chacun des DNSKEY RRsets de la zone racine au moyen d'une demande de signature de clé (KSR) fournie par l'opérateur de la zone de signature de clé (ZSK) de la zone racine. Il en résulte une SKR contenant un ensemble de DNSKEY RRsets signés fournis au mainteneur de la zone racine.

Ces processus sont bien documentés et, dans le cas des actions qui ont lieu lors des cérémonies KSK, font l'objet de la vérification externe des comptes et de l'observation généralisée ; l'équipe de conception estime que cela est très avantageux pour éviter toute modification de fond aux processus à la suite du roulement de la KSK afin d'éviter l'interruption d'un processus qui est, dans sa forme actuelle, déjà bien compris.

Recommandation 5 : le roulement de la KSK de la zone racine ne devrait nécessiter aucune modification de fond aux processus existants afin de maintenir les normes élevées de transparence y associées.

Chaque KSR couvre un cycle de temps d'un trimestre (trois mois ou à peu près 90 jours) et est divisé en 9 intervalles de 10 jours chacun. Si le cycle de temps dépasse les 90 jours, le dernier intervalle du cycle est élargi pour combler la période. Pour cette raison, toutes les modifications apportées au DNSKEY RRset de la zone racine, par exemple, l'ajout et / ou la suppression de clés tel que requis par un roulement de clé, doivent être alignés sur ces périodes de 10 jours pour minimiser tout changement de fond dans les processus utilisés pour publier une zone racine signée.

Recommandation 6 : toutes les modifications apportées aux RRsets DNSKEY de la zone racine doivent être alignées avec l'intervalle de 10 jours décrit au DPS de l'opérateur KSK.

Avec les périodes standards, la taille de la réponse du paquet DNSKEY RRset de la racine augmente avec le premier et le dernier intervalle dans chaque cycle de temps. Le premier intervalle contient les ZSK publiées après le cycle de temps précédent, alors que le dernier intervalle contient la ZSK prépubliée pour le prochain cycle de temps.

Pour minimiser les questions relatives à la plus grande taille des réponses du DNS, il est souhaitable de planifier un roulement capable de faire en sorte que la taille de réponse DNSKEY RRset soit aussi petite que possible. Un examen détaillé des problèmes liés à la taille de la réponse, accompagné de recommandations, apparaît plus loin dans ce document. Un calendrier de roulement de la KSK de la zone racine conçu à partir des considérations susmentionnées est également inclus ultérieurement dans ce document.

6.4 Considérations cryptographiques

L'équipe de conception a examiné la question de savoir s'il y a eu des motifs impérieux pour envisager un changement dans la taille de la clé ou de l'algorithme pour la KSK. Un motif impérieux pourrait découler de questions concernant la force cryptographique de la taille de la clé ou de l'algorithme choisis.

Avec la publication initiale du SP 800-57, partie 1 (*recommandation pour la gestion des clés*) en 2005, l'Institut national des normes et de la technologie des États-Unis (NIST) a annoncé l'intention de soulever les forces cryptographiques minimales. Toutefois, dans les cinq années écoulées entre la publication et la date de finalisation proposée. les techniques de factorisation n'ont pas progressé aussi rapidement que prévu. Rien ne suggère que l'utilisation de clés plus longues pour la KSK de la zone racine soit urgente.

6.4.1 Cryptographie des corps finis

La clé asymétrique RSA 2048 bits est considérée comme équivalente à la clé symétrique de 103 bits dans le rapport annuel de ECRYPT II 2012 sur les algorithmes et les tailles des clés[17]. Ce même rapport recommande d'utiliser au moins 96 bits de sécurité pour une protection portant sur environ 10 ans. *Recommandation pour la gestion de clés-Partie 1* du NIST : *La révision générale*

[17] http://www.ecrypt.eu.org/ecrypt2/documents/D.SPA.20.pdf

3[18]considère que la clé RSA de 2048 bits est équivalente aux 112 bits de sécurité et considère que cette force est acceptable pour être utilisée de 2014 a 2030. L'Agence nationale française de la sécurité des systèmes d'information (ANSII) *Référentiel Général de Sécurité*[19] considère également que l'utilisation de la clé RSA de 2048 bits sera sûre jusqu'en 2030.

Le contenu signé dans la zone racine est généralement de courte durée puisque les périodes de signature DNSKEY sont mesurées en jours (~ 15 jours), et l'équipe de conception est d'avis que la clé RSA de 2048 bits devrait être sûre pour une nouvelle période de cinq ans, à moins qu'il existe une importante percée technologique dans le grand domaine de factorisation de chiffres.

6.4.2 Courbes elliptiques et cryptographie

Une autre option d'algorithme disponible pour les DNSSEC est l'algorithme de signature numérique à courbe elliptique (ECDSA) défini dans le RFC 6605[20]. L'ECDSA possède certaines propriétés qui rendent souhaitable d'utiliser un algorithme de clé de signature de clé de la zone racine. Les clés sont bien plus petites, tout en gardant une force équivalente à celle des clés RSA. Les estimations actuelles établissent que l'ECDSA avec la courbe P-256 a une force équivalente approximative à RSA avec des clés de 3072 bits (NIST) ou de 3248 bits (ECRYPT II). Toutefois, l'algorithme n'a été normalisé pour l'utilisation des DNSSEC que très récemment – le RFC 6605 a été publié en 2012 – et les mesures décrites plus loin dans ce document ont observé que le soutien pour ECDSA dans les validateurs n'est pas aussi répandu que le soutien pour le RSA (voir la section 7 – Considérations opérationnelles).

Le *Crypto Forum Research Group* (GRFC) de l'IETF travaille également sur un nouveau RFC sur les *« courbes elliptiques pour la sécurité »* qui ajoute de nouvelles courbes elliptiques de sécurité, et il exprime également quelques inquiétudes de sa communauté cryptographique sur la génération et les faiblesses potentielles des courbes utilisées par l'ECDSA. Il est souhaitable de laisser que le CFRG termine le travail sur le document avant de passer à un nouvel algorithme à courbe elliptique pour signer la zone racine.

6.4.3 Conclusion

Sur la base des orientations décrites ci-dessus, l'équipe de conception a constaté qu'il n'y a aucun besoin pressant de changer ni l'algorithme ni la taille de la KSK de la clé RSA de 2048 bits. L'équipe de conception a aussi appris de la mise en œuvre

[18] http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_part1_rev3_general.pdf
[19] http://www.ssi.gouv.fr/uploads/2015/01/RGS_v-2-0_B1.pdf
[20] https://tools.ietf.org/html/rfc6605

du résolveur de validation du DNS qui nécessite que la zone racine soit signée par tous les algorithmes correspondant aux ancres de confiance configurées et, en conséquence, le roulement vers un algorithme différent nécessiterait une approche différente de celle utilisée pour le roulement de la KSK. Cela fournit plus de motivation pratique pour éviter un changement de l'algorithme en ce moment. L'équipe de conception a contacté le fournisseur au sujet de la question et des exigences du fournisseur, et elle s'attend à ce que cela sera assoupli pour les futurs roulements de la KSK non programmés.

Pour ces raisons, la KSK entrante pour le premier roulement de la KSK devrait être une clé RSA de 2048 bits, mais des changements dans l'algorithme et / ou la longueur de la clé peuvent mériter d'être considérés pour les roulements ultérieurs de la KSK.

Recommandation 7 : l'équipe de conception recommande que l'algorithme existant et la taille de clé pour la KSK entrante pour le premier roulement de la KSK de la zone racine devraient être maintenus.

Recommandation 8 : le choix de l'algorithme et la taille de la clé devraient être revus pour les futurs roulements de la KSK de la zone racine.

6.5 Coordination et communication

6.5.1 Coordination avec la communauté technique et les partenaires de distribution

L'ICANN doit concevoir et exécuter un plan de communication pour sensibiliser sur le roulement de la KSK de la zone racine. La sensibilisation devrait se faire au sein de forums techniques tels que ceux au cours desquels le déploiement des DNSSEC dans la zone racine a été présenté.

Le terme « partenaires de distribution » signifie les organisations externes qui facilitent l'utilisation des DNSSEC indépendamment de la gestion de la zone racine. Ces partenaires « distribuent » la valeur de signer la zone racine des partenaires de la RZM dans l'Internet public mondial.

Les partenaires de distribution sont divisés en trois grands domaines. Tout d'abord les facilitateurs, ceux qui mettent en œuvre le logiciel de validation des DNSSEC, traitant, entre autres, la mise en œuvre du RFC 5011. Ensuite les distributeurs de logiciels et de systèmes qui incluent le logiciel de validation des DNSSEC, principalement concerné par la distribution de copies de la KSK de la zone racine. Troisièmement, les opérateurs des DNSSEC qui valident les systèmes qui utilisent la KSK de la zone racine.

Dans le but de faciliter la communication, l'équipe de conception recommande que pour chaque partenaire de distribution, le cas échéant, un contact devrait être gardé au fichier, et des mises à jour sur le roulement de la KSK seront données à ces contacts. Cette liste de contacts n'est pas censée être exclusive ou pouvant échanger du matériel qui n'est pas autrement accessible au public. La liste de contacts est censée donner une idée de la prise de conscience des étapes dans le roulement de la KSK de la zone racine. La liste devrait, toutefois, rester fermée pour permettre aux partenaires de distribution de gérer la prise de conscience de leur information de contact sélectionnée.

Recommandation 9 : l'ICANN, en collaboration avec les partenaires de la RZM, doit concevoir et exécuter un plan de communication pour sensibiliser la population sur le roulement de la KSK de la zone racine, y compris la sensibilisation de la communauté technique mondiale par le biais de réunions techniques appropriées et de « partenaires de distribution » tels que ceux mentionnés dans ce document.

6.5.2 Coordination avec les opérateurs de serveurs racine

Tout changement structurel dans le contenu de la zone racine a le potentiel d'affecter le comportement opérationnel des serveurs racine individuels. L'approvisionnement initial des adresses IPv6 (AAAA) dans la zone racine et la mise en œuvre ultérieure des DNSSEC sont des exemples de modifications apportées à partir de la consultation et d'une coordination étroite avec les opérateurs des serveurs racine, puisque ces modifications ont déclenché des changements dans les modes de requête. Par conséquent, la prudence avec les infrastructures essentielles exige une approche conservatrice à tout changement ~~dans le~~au cas où il y aurait des conséquences inattendues qui pourraient dégrader la performance du système de serveurs racine dans son ensemble.

Les expériences menées dans le cadre de la préparation du présent document suggèrent qu'un roulement de la KSK ne causerait aucun effet nuisible ; cependant, comme avec les exemples précédents de changements structurels mentionnés ci-dessus, il est recommandé d'adopter une approche conservatrice.

L'équipe de conception suggère que les opérateurs de serveurs racine individuels pourraient traiter des événements particuliers pendant la période de roulement de la KSK comme un événement opérationnel planifié important, en publiant des avis de statut publics et en coordination avec d'autres opérateurs de serveurs racine en utilisant les moyens habituels utilisés pour de tels événements en temps réel. Ces événements devraient inclure la période immédiate à l'ajout d'une nouvelle KSK

entrante à l'apex DNSKEY RRSet de la zone racine et l'élimination de la KSK sortante du même RRSet.

L'équipe de conception suggère que les moyens de communication en temps réel entre les opérateurs de serveurs racine individuels et l'ICANN et entre l'ICANN et les autres partenaires de la gestion de la zone racine soient exercés de la même manière autour des mêmes événements pour assurer que tout effet attendu puisse être identifié et partagé sans tarder.

Un calendrier détaillé pour la période de roulement de la KSK devrait être examiné par les opérateurs de serveurs racine, avant d'être finalisé et publié afin de garantir qu'il n'est pas incompatible avec tous les autres plans qui pourraient réduire la capacité d'un opérateur de serveur racine individuel d'offrir le niveau souhaité de couverture opérationnelle. Des efforts devraient être consacrés à l'ajustement du calendrier de roulement pour éviter des conflits opérationnels autant que possible.

Recommandation 10 : l'ICANN devrait demander au RSSAC de coordonner une révision détaillée du calendrier pour la période de roulement de la KSK avant qu'il soit publié et devrait tenir compte des demandes de modification raisonnables à ce calendrier, au cas où un opérateur de serveur racine identifierait des raisons opérationnelles pour ce faire.

Recommandation 11 : l'ICANN devrait coordonner son travail avec le RSSAC et les partenaires de la RZM pour assurer que des canaux de communication en temps réel soient utilisés afin d'assurer la bonne sensibilisation opérationnelle du système des serveurs racines pour chaque modification de la zone racine qui implique l'ajout ou la suppression d'une KSK.

Il est possible de comprendre l'impact opérationnel d'un roulement de la KSK sur les validateurs et sur les serveurs racine eux-mêmes à travers la collecte de données par les opérateurs de serveurs racine au cours du roulement de la KSK. Étant donné que le système de serveurs racine est diversifié tant dans l'architecture que dans la distribution autour de l'Internet, il est entendu que les possibilités de collecte de données dans la durée par les opérateurs de serveurs racine individuels impliquera diverses limitations qui sont difficiles à caractériser de façon succincte pour l'ensemble du système. Il est également entendu que les capacités de collecte de données de référence existent déjà pour satisfaire aux exigences tactiques des conditions de surveillance du service en temps réel, tel que le roulement de la KSK.

Lorsque les DNSSEC ~~a~~ont initialement été déployées dans la zone racine, un exercice de collecte de données considérable a été effectué et les données qui en ont résulté se sont avérées utiles pour l'analyse hors ligne de la réaction du DNS dans son ensemble aux changements structurels en cours dans la zone racine, y

compris une analyse par des tierces parties, facilitée par DNS-OARC[21]. Un exercice similaire est garanti pour le premier roulement de la KSK.

Recommandation 12 : l'ICANN devrait coordonner avec le RSSAC la demande aux opérateurs du serveur racine de collecter des données qui informeront les analyses subséquentes et aideront à caractériser l'impact opérationnel du roulement de la KSK, et que les plans et les produits de cette collecte de données soient publiés pour qu'ils soient analysés par une tierce partie.

6.5.3 Coordination entre l'opérateur de la KSK et l'opérateur de la ZSK

La responsabilité de la gestion de la KSK et de la ZSK de la zone racine est attribuée séparément à l'opérateur des fonctions IANA et au mainteneur de la zone racine, respectivement. Les deux rôles sont gérés séparément.

La ZSK de la zone racine ~~Zone~~ est actuellement une clé RSA de 1024 bits, tel que spécifié dans le DPS du mainteneur de la ZSK[22]. Il est possible que le mainteneur de la zone racine augmente la taille de la clé ZSK dans l'avenir.

La ZSK est roulée régulièrement tous les 90 jours, et il est prévu que cela continue comme d'habitude au cours de la période de roulement de la KSK ; vu que la période de roulement de la KSK devrait être supérieure à 90 jours, il y aura des périodes au cours desquelles le DNSKEY RRSet de l'apex de la zone racine pourrait contenir quatre clés suivant le plan final.

L'augmentation de la taille de la ZSK lors du roulement d'une clé pourrait déclencher un comportement différent dans les validateurs pendant une partie de la période de roulement de la KSK, étant donné que les tailles de réponse augmenteront avec la taille de la ZSK. Cela pourrait compliquer les travaux d'identification, compréhension et atténuation des problèmes opérationnels qui pourraient surgir.

Toute décision relative à la taille de la ZSK est en dehors de la portée du présent document. Cependant, nous recommandons que l'ICANN coordonne avec le mainteneur de la zone racine pour assurer que toute augmentation future de la taille de la ZSK soit soigneusement coordonnée avec les roulements de la KSK, afin que les deux exercices ne soient pas effectués simultanément.

Recommandation 13 : les partenaires de la RZM devraient s'assurer que toute augmentation future de la taille de la ZSK soit soigneusement coordonnée

[21] https://www.dns-oarc.net
[22] http://www.verisigninc.com/assets/dps-zsk-operator-1527.pdf

avec les roulements de la KSK, puisque les deux exercices ne sont pas simultanés.

7 Incidence sur les résolveurs de validation

7.1 Considérations ~~de~~ sur la taille des paquets

Le DNS est censé fonctionner sur les protocoles de transport UDP et TCP. L'UDP a été préféré lors de la conception du protocole DNS en raison de la surcharge inférieure de l'UDP par rapport au TCP, en particulier pour le maintien de la connec~~t~~xion entre États sur un serveur. Cependant, ce choix de protocole implique des limitations. Dans la définition originale du DNS, RFC 1035, les réponses de l'UDP se limitaient à 512 octets. La limite de 512 octets est observée dans le logiciel utilisé aujourd'hui, qui soit respecte ou fait respecter cette limite.

Le mécanisme d'extension pour le DNS, EDNS(0), défini à l'origine dans un RFC publié en août 1999 [RFC 2671, mis à jour par le RFC 6891] permet à un demandeur de DNS d'informer le serveur DNS qu'il peut traiter des réponses UDP supérieures à 512 octets. Le demandeur envoie la taille maximale de sa charge UDP (pas la taille des paquets IP mais la taille des messages DNS) dans la requête et le serveur doit répondre avec une réponse UDP où la charge DNS n'est pas plus grande que la taille de la mémoire tampon spécifiée. Si cela n'est pas possible, le serveur définit le bout tronqué de la réponse comme indice que la troncation s'est produite. Si la réponse tronquée inclut un message DNS valide, le demandeur peut choisir d'utiliser la réponse tronquée. Dans le cas contraire, le demandeur ouvre une session TCP sur le serveur et répète la requête sur TCP.

Les systèmes DNS qui utilisent DNSSEC doivent signaler leur capacité de le faire à l'aide de l'indicateur DO (DNSSEC OK) dans le pseudo-en-tête EDNS. Étant donné que l'impact opérationnel considéré dans le présent document est entièrement centré sur des systèmes qui sont compatibles avec les DNSSEC, les systèmes concernés ont la capacité EDNS(0) (parce que les DNSSEC requiert le support EDNS(0)) et ne sont donc pas limités à 512 octets.

Un client peut initier une transaction en TCP, mais le comportement habituel des demandeurs consiste à initier la transaction en UDP et utiliser le bout tronqué dans une réponse pour indiquer que le demandeur devrait utiliser le protocole TCP pour la requête.

La fragmentation des paquets UDP est traitée différemment dans IPv4 et IPv6. Lorsqu'un paquet est trop grand pour le moyen de transmission de paquets IP sous-jacent, le paquet IP peut être fragmenté. Dans ce cas, les fragments de traçage

utilisent le même directeur du niveau IP (y compris le champ de numéro du protocole UDP), mais excluent spécifiquement la pseudo-en-tête UDP dans les fragments de traçage. En IPv4, l'expéditeur d'origine ou tout autre routeur intermédiaire, peut fragmenter un paquet IP, à moins que l'indicateur *Don't Fragment (Ne pas fragmenter)* IP soit défini. Dans IPv6 seul l'expéditeur d'origine peut fragmenter un paquet IP. Si un routeur intermédiaire ne peut pas transférer un paquet à l'interface de transmission suivante, en IPv6 le routeur générera un paquet de diagnostique ICMPv6 avec la taille MTU de l'interface de transmission suivante et la première partie du paquet, et transférera ces informations à l'expéditeur du paquet.

L'utilisation de l'UDP ne requiert pas que l'expéditeur maintienne un tampon des données non reconnues ; par conséquent, l'expéditeur IPv6 ne peut pas retransmettre les données originales lors de la réception de ce message. Les données empiriques semblent suggérer qu'une réponse commune de nombreuses mises en œuvre de l'IPv6 génèrent une entrée d'hôte dans le tableau de transfert IPv6 locale, et enregistrent les MTU reçus dans ce tableau pour certains délais du caché définis localement. Cela implique que toute tentative ultérieure visant à envoyer un paquet UDP d'IPv6 vers cette destination utilisera cette valeur MTU pour déterminer comment fragmenter le paquet sortant.

7.1.1 L'expérience de la mesure

Une expérience a été conçue et mise en place pour reproduire l'environnement de la situation dans le serveur racine afin d'évaluer l'impact que les grandes tailles de paquets pourrait avoir sur les résolveurs et les utilisateurs.

Ceci a été réalisé en utilisant une plateforme de publicité en ligne qui a déclenché dans les résolveurs DNS une série de requêtes uniques envoyées à un serveur de noms autoritaire configuré pour répondre aux requêtes de deux zones avec des tailles de réponse différentes. On croit que les résolveurs qui envoient la requête au serveur de noms autoritaire dans cet essai sont pour la plupart les mêmes qui devraient envoyer une requête à la zone racine.

Pour vérifier si un résolveur pourrait recevoir une réponse de grande taille, la publicité envoyait une requête sur un nom de domaine cible. Le nom de domaine cible lui-même renverrait une réponse de taille normale. Mais afin d'envoyer la réponse cible, le résolveur devait d'abord recevoir une réponse intermédiaire de grande taille ~~d'abord~~. Si le résolveur réussissait à demander l'information du nom de domaine cible, l'essai montrerait que le résolveur pourrait traiter la réponse intermédiaire de grande taille.

L'essai a également impliqué la récupération d'un objet ~~web~~ Web du serveur ~~web~~ Web de l'expérience, ce qui permettait à l'expérience de faire correspondre les adresses utilisées dans la récupération ~~web~~ Web (l'adresse IP de l'utilisateur final) aux adresses utilisées par les résolveurs de noms à travers l'envoi de la requête DNS.

Dans cet essai, une réponse DNS de 1444 octets a été utilisée.

7.1.2 Résultats des essais

Dans une période de 5 jours au cours de mai 2015, 7 260 000 ~~de~~ systèmes finaux ont récupéré avec succès un petit dossier de contrôle ; parmi ceux-ci, 7 170 000 ~~de~~ systèmes ont récupéré avec succès le dossier d'essai. Entre les deux, environ 90 000 utilisateurs, soit 1 % de l'ensemble d'essai, n'a pas pu récupérer le dossier d'essai DNS de 1444 octets.

Ces systèmes finaux ont utilisé approximativement 83 000 adresses IP différentes des résolveurs DNS. Parmi eux, 94 % des résolveurs ont obtenu avec succès le dossier de contrôle et le dossier d'essai. Des 4251 résolveurs qui ont récupéré le dossier de contrôle mais n'ont pas pu récupérer le dossier d'essai, 3396 résolveurs utilisent l'extension EDNS(0) avec le bout DNSSEC OK, qui a déclenché la réaction de 1444 octets. Parmi ces résolveurs qui ont échoué, 3110 ont été observés une seule fois au cours de l'expérience, alors que 826 résolveurs ont échoué plus d'une fois. Cela implique que 1 % des résolveurs essayés dans cette expérience n'a pas pu récupérer une réponse de grande taille deux ou plusieurs fois, alors que 3 % des résolveurs qui n'ont pas pu récupérer la réponse de grande taille n'ont été essayés qu'une seule fois, ce qui est insuffisant pour conclure avec certitude qu'ils échoueraient systématiquement avec les réponses de grande taille. Ce 1 % des résolveurs qui ont échoué systématiquement deux ou plusieurs fois a été utilisé par un peu moins de 3000 systèmes finaux, soit 0,04 % de la population du système final essayée.

5237 résolveurs utilisaient des adresses IPv6 dans cet essai (6 % du total), tandis que 830 de ces résolveurs n'ont pas pu récupérer le dossier d'essai (21 % des résolveurs défaillants). Ces données suggèrent un problème potentiel avec certains résolveurs IPv6 ainsi qu'avec leur capacité de traiter de grandes tailles de MTU.

En termes de mesure de la variation dans la charge de la requête avec des réponses plus grandes, le nom de contrôle (avec une taille de réponse de 93 octets) a reçu 16 400 000 ~~de~~ requêtes et 475 requêtes ont été observées à l'aide du protocole TCP. Le nom de l'essai (avec une taille de réponse de 1444 octets) a reçu 18 600 000 ~~de~~ requêtes et 1 200 000 de ces requêtes ont été faites sur TCP, soit environ 6,5 % du total des requêtes sur le nom de l'essai. Il existe une différence

dans le nombre total de requêtes envoyées au dossier de contrôle par rapport au nombre total de requêtes envoyées au dossier d'essai. La différence peut s'expliquer par les résolveurs qui répondent à des réponses tronquées reçues pour le dossier d'essai en envoyant une autre requête sur TCP. Ce résultat se correspond assez bien avec la distribution des tailles des mémoires tampon d'UDP offertes dans les extensions EDNS(0) des requêtes UDP. Au moment de servir des réponses de plus grande taille, un serveur faisant autorité peut anticiper une charge plus élevée de la requête et une proportion majeure de requêtes sur TCP.

7.1.3 Conclusion

Environ 1 % des résolveurs DNS qui définissent l'indicateur de DNSSEC OK dans leurs requêtes semble être incapable de recevoir une réponse DNS de 1444 octets (les facteurs d'incertitude expérimentale signifient que le maximum associé à cette valeur est le 6 % du total des résolveurs). Au sein de cet ensemble de résolveurs, les résolveurs qui utilisent IPv6 comme protocole de transport sont représentés de façon disproportionnée. Il est possible que ce taux d'échec ~~se doiv~~soit dû~~e~~ à la présence de diverses formes de middleware d'interception de DNS, ou dans le cas de l'IPv6, à une mauvaise manipulation potentielle des messages ICMP6 *Packet Too Big (paquet trop grand)*, mais la nature exacte de l'échec ne peut pas être établie à partir de cette méthodologie expérimentale.

Les résolveurs qui ne reçoivent pas les réponses desservent une très faible proportion des utilisateurs. Le nombre d'utilisateurs qui utilisent des résolveurs DNS qui sont systématiquement incapables de résoudre un nom DNS lorsque les réponses DNS sont de cette taille semble être 0,04 % du total des utilisateurs (les facteurs d'incertitude expérimentale impliquent que le maximum correspondant à cette valeur est ~~l~~de 1% du total des utilisateurs).

Ces expériences ont réalisé des essais pour une réponse DNS de 1444 octets. Il est à noter que d'autres parties du DNS fournissent déjà des réponses sensiblement plus grandes que la taille évaluée ici et que ces tailles de réponse ne semblent pas susciter l'attention du public ou des commentaires visibles. Par exemple, en date du 6 juin 2015 une requête DNSKEY comparable pour le nom .org a généré une réponse de 1625 octets contenant deux clés de signature de clé RSA de 2048 bit, deux clés de signature de zone RSA de 1024 bit et trois signatures : une pour chaque clé de signature de clé et une pour une des clés de signature de zone. Tout résolveur de validation qui soit incapable de recevoir des réponses DNS aussi grandes serait incapable de valider la signature soit du dossier DS ou du dossier NSEC03 (qui sont utilisés pour signaler l'absence d'un dossier DS) pour chaque délégation dans la zone .org, ce qui provoquerait dans la pratique des échecs de résolution DNS pour les délégations dans .org.

L'équipe de conception n'est pas consciente d'aucun problème opérationnel que pourraient éprouver les titulaires de noms de domaine dans .org en vertu de la taille des paquets de réponse DNS DNSKEY du nom .org. Même si l'on tient compte du très petit nombre de zones signées dans .org, cette absence de rapports opérationnels sur l'échec de la résolution de noms de domaine dans .org indiquerait qu'il est peu probable que la taille de réponse se présente comme un problème opérationnel important pour le roulement de la KSK de la zone racine.

Une différence à noter entre le cas d'essai et la situation de .org est que seulement les résolveurs qui effectuent une validation enverront des requêtes pour le RRset DNSKEY de grande taille. Dans le cas d'essai, tous les résolveurs qui indiquent DNSSEC OK tenteraient de récupérer la réponse de grande taille. Tel que décrit à ~~l'article~~la section 8.2, il semble que moins de 30 % des résolveurs qui indiquent DNSSEC OK dans la requête d'origine effectuent par la suite la validation de la réponse. Il est possible que les opérateurs de résolveurs qui ont initié la validation aient été plus diligents au moment d'identifier et de corriger les problèmes liés au réseau qui peuvent les empêcher de récupérer les paquets de réponse de grande taille, car ces résolveurs seraient plus susceptibles d'éprouver de tels problèmes. D'autres résolveurs qui ne feraient pas la validation ne rencontreraient des paquets de réponse de grande taille que dans des circonstances relativement rares, et ils pourraient ne pas être au courant de telles limitations qui leurs sont imposées par l'environnement de leurs réseaux.

Il est raisonnable de déduire que la grande majorité de ceux qui n'ont pas réussi à recevoir la réponse de grande taille dans les essais ne sont pas des résolveurs de validation, qui ne seraient pas affectés par l'augmentation de la taille du dossier de ressources DNSKEY de la zone racine.

En résumé, ces essais indiquent que moins de 0,04 % des utilisateurs peut être affecté par une taille de réponse plus grande lors d'un roulement de la KSK de la zone racine, mais cela est une estimation avec un facteur d'incertitude élevé, et les observations connexes tirées des TLD avec de grands ensembles de clés sembleraient indiquer que cette limite est un maximum de l'impact potentiel de la réponse de plus grande taille.[23]

7.2 Comportement de validation des DNSSEC

Il y a trois aspects du comportement de validation des DNSSEC à mesurer. Le premier est la récupération des signatures numériques des DNSSEC (qui indiquent

[23] Plus de détails sur l'expérience et les résultats sont disponibles sur http://www.potaroo.net/ispcol/2015-05/ksk.html.

DNSSEC OK pour les options EDNS(0) de la requête), le deuxième est la fonction de validation où une chaîne de confiance est créée à partir de la clé racine pour le nom en cours de validation, et le troisième est si la configuration de la résolution du nom de l'utilisateur acceptera un échec de validation des DNSSEC comme un échec définitif ou si la requête sera envoyée à un autre résolveur.

7.2.1 Résultats des tests

À l'aide de l'expérience décrite ci-dessus (Section 7.1.1), en mai 2015 il a été observé qu'entre 85 % et 90 % des utilisateurs transmettent leurs requêtes à des résolveurs où les requêtes qui en résultent, observées dans un serveur de noms autoritaire pour un nom non mis en caché, ont l'option EDNS(0) incluse dans la requête et ont également l'indicateur DNSSEC OK.

Environ 24 % de la population d'utilisateurs mesurée a effectué des requêtes ultérieures qui montrent que le résolveur validait la réponse à l'aide des DNSSEC en suivant la chaîne de signatures de verrouillage, ce qui soutient la hiérarchie de délégation des noms vers la KSK de la zone racine.

Environ 11 % de la population d'utilisateurs mesurée correspond aux utilisateurs finaux qui répondent à un échec de validation des DNSSEC de la communication précédente en envoyant la requête à un résolveur différent qui n'effectue pas de validation des DNSSEC.

Cela fait penser que tout changement dans les procédures de validation des DNSSEC a l'impact potentiel d'environ un quart de la population d'utilisateurs de l'Internet.

Parmi eux, une peu moins de la moitié de ces utilisateurs interprètent déjà l'échec de validation des DNSSEC (signalé par SERVFAIL) comme un signal pour présenter la même requête à un autre résolveur qui n'effectue pas de validation des DNSSEC. Pour ce 11 % des utilisateurs de l'Internet le changement de la KSKS de la zone racine pourrait potentiellement impliquer un échec de validation de la KSK de la zone racine non reconnu, mais ces utilisateurs ont démontré qu'ils interprètent déjà SERVFAIL en utilisant un autre résolveur. Le résultat pourrait impliquer potentiellement plus de temps pour la résolution des noms avec la signature des DNSSEC, mais n'entraînerait point une incapacité de résoudre le nom.

Le 13 % restant des utilisateurs qui ne reviennent pas à un résolveur non-validant face à une réponse SERVFAIL est potentiellement à risque d'être incapable de résoudre un nom avec la signature des DNSSEC, si les résolveurs utilisés par l'utilisateur sont incapables de suivre les signaux fournis par le processus de roulement de clés du RFC 5011.

7.2.2 Conclusion

Il n'est pas possible d'utiliser ce procédé de mesure pour vérifier si les résolveurs sont capables de suivre un processus RFC 5011 pour récupérer automatiquement une nouvelle valeur de la KSK de la zone racine. Le mieux que l'on puisse faire ici est de quantifier les utilisateurs qui utilisent les résolveurs qui valident les DNSSEC et par conséquent utiliser les résolveurs qui vont soit soutenir le RFC 5011 soit avoir besoin d'interventions manuelles pour charger la nouvelle KSKS de la zone racine au bon moment.

~~Approximativement~~ Environ 24 % des utilisateurs utilise des résolveurs qui effectuent une validation des DNSSEC et sera donc potentiellement affecté par un roulement de la KSK de la zone racine. Un échec de validation affichera la réponse SERVFAIL, et 11 % de tous les utilisateurs utilisent un ensemble de résolveurs pour lesquels la réponse SERVFAIL d'un résolveur provoquera la résolution de la requête par un résolveur non-validant. Cela implique que 13 % des utilisateurs peut être affecté par un roulement de la KSK de la zone racine si leur résolveur n'est pas à jour avec le RFC 5011 et si l'administrateur du résolveur ne charge pas la nouvelle KSK de la zone racine au moment opportun.

Cependant, beaucoup de ces utilisateurs utilisent un des plus grands services de résolveurs qui valident DNSSEC qui sont censés être à jour avec le RFC 5011 (par exemple les résolveurs DNS de Comcast), c'est-à-dire que 13 % est une limite maximale des utilisateurs qui peuvent être affectés ~~ainsi~~de cette manière.

8 Essais

Il existe deux éléments liés aux essais. L'un est l'activité de mesurer l'impact du roulement de la KSK sur les opérations générales de l'Internet aux fins d'évaluer le niveau de l'impact négatif qui pourrait interrompre l'opération. L'autre est l'activité liée à la préparation des parties de confiance pour l'opération, y compris les ressources d'essai de l'auto-évaluation. Ces auto-évaluations peuvent être effectuées par des partenaires de distribution qui développent du logiciel et/ou par les opérateurs qui déploient des parcs de serveurs, ou toute autre personne intéressée.

8.1 Essai de l'impact

Les essais effectués pour d'autres parties du présent rapport qui mesurent le succès de la validation ont mis en évidence une certaine réaction aux échecs de validation des DNSSEC. Il a été identifié, à l'aide de preuves, que certaines requêtes commencent par les DNSSEC, puis « basculent » au DNS. L'augmentation (ou la

réduction) de cette pratique à mesure que la KSK est mise en place peut être un moyen pour évaluer les dommages. Ces « dommages » peuvent autrement passer inaperçus, mais pourraient être une mesure utile lors de l'observation de l'impact des opérations de roulement de la clé de la KSK dans la zone racine. Les utilisateurs (derrière l'écran) ne détectent probablement pas cela et par conséquent n'ouvriront jamais un dossier avec le service de support technique du fournisseur du service.

Les essais qui détectent cela devaient être exécutés de manière périodique (tous les mois) désormais jusqu'à la fin (réussie ou non) de l'opération de roulement de la clé de la KSK dans la zone racine. Avant le roulement, les essais nous donneront une base de référence permettant de faire des comparaisons.

Outre les essais automatisés, le contact avec les partenaires de distribution pendant le roulement de la clé de la KSK dans la zone racine est nécessaire pour fournir des informations explicites, en temps réel ou presque. Il s'agit d'un facteur de motivation pour fournir un préavis aux parties affectées, éviter des délais lorsque le personnel manque de capacité, et privilégie les heures auxquelles les contacts peuvent facilement être établis.

8.2 Installations d'auto-évaluation

Quant à la possibilité de permettre aux parties de confiance de s'auto-évaluer, il devrait y avoir une plate-forme d'essai qui réplique la plate-forme opérationnelle à un rythme de roulement accéléré. En plus d'avoir des serveurs qui exécutent le RFC 5011 à un rythme accéléré avec des zones racine signées fausses, les ancres de confiance dans « d'autres structures de données » devraient être présents dans les noms des mêmes chemins d'accès. Cela encouragerait l'élaboration de meilleurs outils, tels que les outils pour aider à vérifier une clé, les outils pour découvrir ce qu'un validateur contient (pour la consommation locale ou distante).

Ceci peut collaborer avec la sensibilisation au sujet de nouveaux algorithmes à travers l'ajout et l'élimination des clés de différents paramètres.

Le temps est important. Il est nécessaire d'aller plus vite que le temps réel pour pouvoir observer raisonnablement le processus. Mais le temps réel est également bénéfique pour réduire les effets des essais.

Et finalement, la fidélité au système de la racine doit être adressée. Il faut également considérer si l'ensemble de la zone racine est utilisé ou pas comme une zone ou comme des données fausses représentatives.

Il existe certains exemples actuels de ces bancs d'essai[24, 25] qui peuvent être utilisés comme modèles pour les futurs essais.

8.3 Logiciel du mainteneur de la KSK et de la ZSK et mise à l'essai de l'interopérabilité des modifications du processus

Étant donné que le processus de roulement de la KSK nécessite des modifications aux calendriers, aux processus et éventuellement au logiciel existants qui soutiennent les opérations de la KSK, il est nécessaire d'effectuer des essais approfondis de ces changements avant le début du roulement, y compris sans s'y limiter à la génération de clés, la génération du RRset DNSKEY signé, la validation des DNSSEC, l'échange KSR/SKR, les mécanismes de secours et les répétitions de la cérémonie de la clé.

9 Mise en œuvre

Le processus de roulement de clés proposé a commencé rapidement en juillet 2013 et a dès lors été contrôlé et peaufiné. Le processus décrit ici devrait être considéré comme un projet et pourrait être amélioré davantage par les partenaires de RZM avant sa mise en œuvre.

Le processus a été divisé en trois étapes :

1) publication de la KSK entrante de la zone racine
2) changement de signature ; adoption de la KSK entrante de la zone racine (« le roulement »)
3) révocation de la KSK en place dans la zone racine.

La révocation de la KSK en place dans la zone racine est délibérément retardée afin de permettre une restauration, au cas où il y ~~avait~~ aurait des problèmes avec la KSK entrante de la zone racine après avoir retiré la KSK en place dans la zone racine. Le processus vise à se conformer avec le RFC 5011, avec des fenêtres étendues permettant d'ajouter la KSK entrante et de révoquer la KSK en place. Ce processus permet explicitement l'option de reporter la révocation de la KSK en place dans la zone racine pour une durée indéterminée. En cas d'observation de problèmes imprévus dans le processus de roulement qui requièrent un changement au processus de roulement de clés planifié, ceci permet d'agir.

La Figure 1 ci-dessous montre un aperçu des trois trimestres au cours desquels le processus a lieu. Notez que la numérotation des trimestres se fait par rapport au début du processus et n'est pas liée à un calendrier. Par exemple, « trimestre 1 » et

[24] http://keyroll.systems/
[25] http://icksk.dnssek.info/fauxroot.html

« QT1 » ne signifient pas nécessairement de janvier à mars. La KSK entrante est notée comme « KSK-NEW », tandis que la KSK en place apparaît comme « KSK-2010 ».

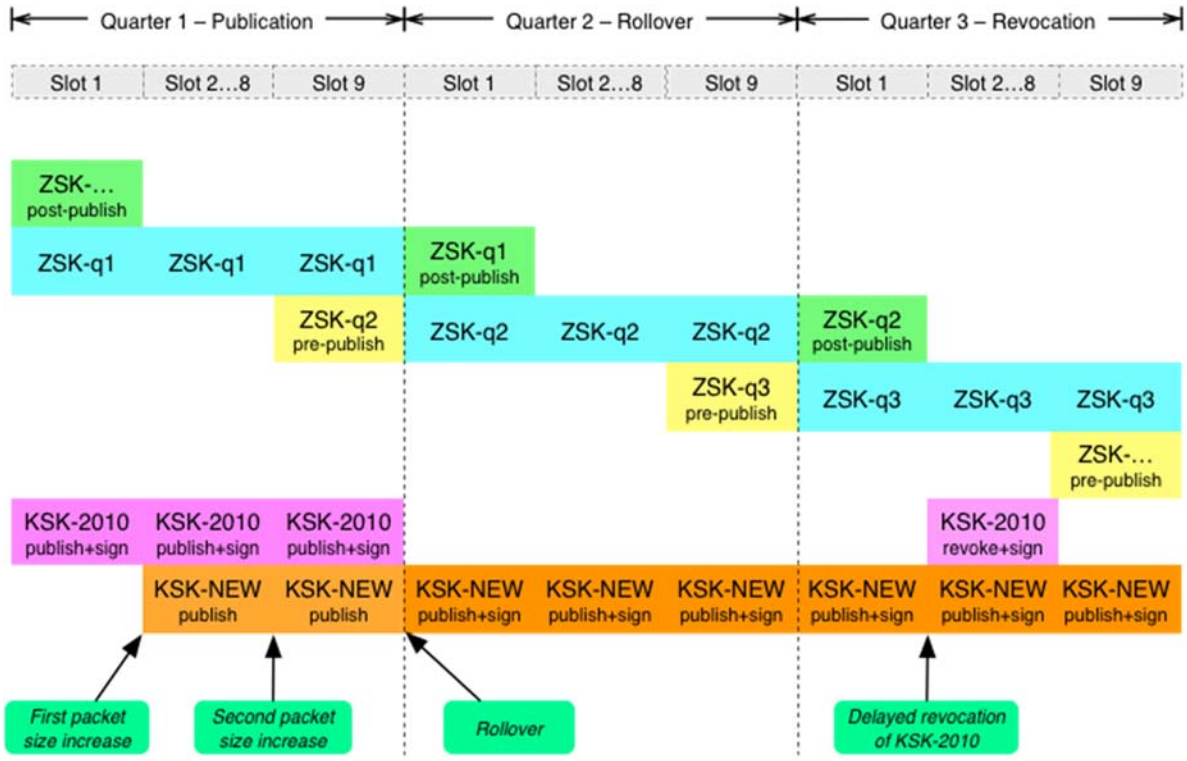

Figure 1. Calendrier de roulement

9.1 Publication de la KSK entrante

La KSK entrante est ajoutée au RRset DNSKEY dans l'intervalle 2 du QT1, mais n'est pas encore utilisée pour signer. Il s'agit d'une étape de publication provisoire pour que la KSK entrante puisse être captée par les validateurs compatibles avec le RFC 5011. La KSK entrante est publiée (et signée par la KSK en place) dans la zone racine pour une période totale de 80 jours avant d'être utilisée pour signer. Les ancres de confiance configurées manuellement sont censées être mises à jour pour inclure la KSK entrante avant ou pendant cette période de temps.

Un roulement compatible avec le RFC 5011 exige la publication d'une nouvelle clé pendant une période minimale de 30 jours (« ajouter une période de réservation »). Si la période de publication de 80 jours proposée est jugée insuffisamment longue, il est possible d'insérer un ou plusieurs trimestres de publication supplémentaires avant de rouler la clé.

Au cours du trimestre de publication de la KSK entrante, les résolveurs de validation des DNSSEC verront la taille du paquet d'une réponse à une requête au RRset

DENSKEY de la zone racine (taille du paquet de réponse) augmenter de 736 octets à 1011 octets. (Cette augmentation théorique se base sur la comparaison de la taille d'une réponse DNS à ce stade si aucun roulement de clé n'était en cours par rapport à la taille au cours du processus de roulement de clés). Dans le dernier intervalle du QT1, pendant le roulement de la ZSK, la taille du paquet de réponse est passée de 833 octets à 1158 octets.

9.2 Roulement à la KSK entrante

Une fois que la KSK entrante a été introduite, elle est utilisée pour signer le RRset DNSKEY commençant dans l'intervalle 1 du QT2. Ce trimestre est comme les autres, sauf que tous les RRsets DNSKEY sont signés avec (exclusivement) la KSK entrante. Le RRset DNSKEY ne serait signé par les KSK entrante et sortante que pendant la période de révocation facultative décrite ci-dessous.

9.3 Révocation de la KSK en place

Si la KSK en place est révoquée tel que décrit dans le RFC 5011, la KSK en place est publiée avec le bout concernant la révocation et signée par les KSK entrante et en place à la fois.

La révocation de la KSK en place est facultative. Si la révocation est souhaitée, la publication de la KSK en place révoquée est effectuée de l'intervalle 2 du QT3 jusqu'à l'intervalle 8 du QT3.

Lors d'une révocation, la taille du paquet de réponse augmente de 736 octets à 1297 octets.

9.4 Impact de la taille du paquet de réponse

Un objectif souhaité est d'éviter la fragmentation UDP autant que possible, et ci-dessous se trouvent quelques contraintes de la taille de réponse pertinente :

Taille	Seuil
512 octets	La taille minimale de la charge de DNS qui doit être soutenue par le DNS
1232 octets	La taille maximale de la charge de DNS d'un paquet DNS UDP IPv6 non-fragmentable
1452 octets	La taille maximale de la charge de DNS d'un paquet DNS UDP Ethernet IPv6 non-fragmenté
1472 octets	La taille maximale de la charge de DNS d'un paquet DNS UDP

	Ethernet IPv4 non-fragmenté

Tableau 4. Seuils de la taille des paquets

Les résultats des essais présentés précédemment indiquent des problèmes potentiels avec certains résolveurs IPv6 et avec leur traitement des réponses de grande taille. La principale contrainte de taille est donc le seuil d'un paquet DNS UDP IPv6 non-fragmentable, ce qui implique une taille de paquet de réponse DNSKEY maximale de 1232 octets.

Ce premier seuil est atteint uniquement pendant l'étape de révocation optionnelle, pendant laquelle la KSK de la zone racine doit être réintroduite et signalée par le bout de révocation . Pour la pleine conformité avec le RFC 5011, il est obligatoire de double-signer le RRset DNSKEY avec la KSK entrante de la zone racine et la KSK en place dans la zone racine pendant l'étape de révocation. La double signature du RRset impliquera une taille de réponse supérieure à 1232 octets.

Le plus grand paquet de réponse unique pour la zone racine est le RRset DNSKEY signé. Le tableau ci-dessous donne un aperçu de la taille du paquet de réponse DNSKEY pendant le roulement proposé, ainsi qu'une comparaison avec la taille des paquets de réponse en cas de non-roulement.

Moment	DNSKEY pendant le roulement	RRSIG pendant le roulement	Taille de réponse DNSKEY pendant le roulement	Taille de réponse DNSKEY pendant le non-roulement
QT1 intervalle 1	1x KSK + 2xZSK	1x KSK	883 octets	883 octets
QT1 intervalles 2 … 8	2x KSK + 1xZSK	1x KSK	1011 octets	736 octets
QT1 intervalle 9	2x KSK + 2xZSK	1x KSK	1158 octets	883 octets
QT2 intervalle 1	1x KSK + 2xZSK	1x KSK	883 octets	883 octets
QT2 intervalles 2... 8	1x KSK + 1xZSK	1x KSK	736 octets	736 octets
TQ2 intervalle	1x KSK + 2xZSK	1x KSK	883 octets	883 octets

9				
TQ3 intervalle 1	1x KSK + 2xZSK	1x KSK	883 octets	883 octets
TQ3 intervalles 2... 8	2x KSK + 2xZSK	2x KSK	1297 octets	736 octets
TQ3 intervalle 9	1x KSK + 2xZSK	1x KSK	883 octets	883 octets

Tableau 5. Taille des paquets lors du roulement

(Le codage en couleurs dans le tableau ci-dessus correspond au graphique ci-dessous).

Les risques associés avec l'évitement de la révocation de la clé sortante n'ont pas été discutés en profondeur, mais l'étape de révocation peut être considérée facultative à ~~cette étape~~ce stade. Une option pourrait être de mettre à jour le RFC 5011 à cet égard et de ne pas exiger la double signature pour révoquer une clé sortante. Cette révision aurait les avantages supplémentaires qu'une clé perdue ou endommagée pourrait être révoquée. Le fait de ne pas devoir signer doublement avec la clé sortante pourrait également faciliter les roulements de clés futurs, les variations de l'algorithme et les changements de la longueur des clés. Toutefois, en raison du temps pour redéfinir, publier, développer et distribuer un code et de le mettre en œuvre dans les opérations, cette option n'est pas jugée réalisable pour ce roulement de la clé KSK.

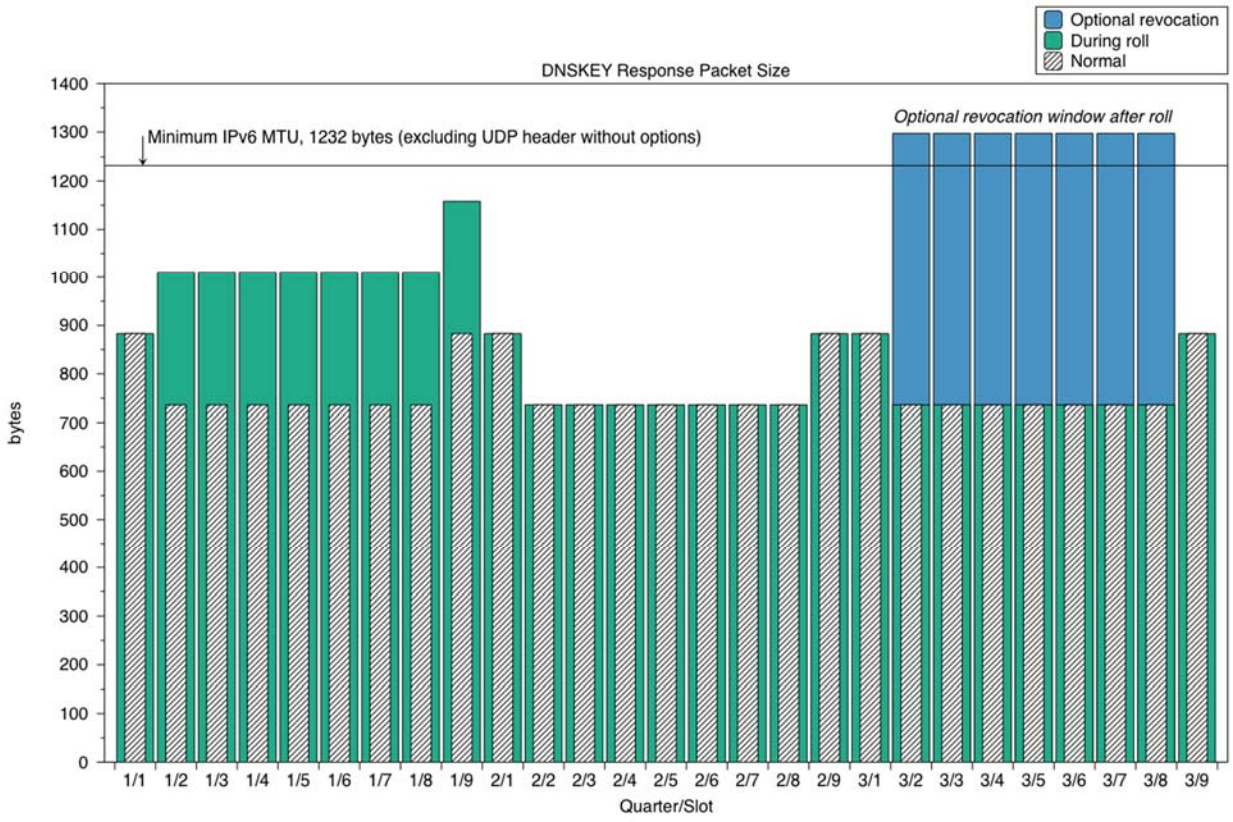

Figure 2. Tailles des paquets de réponse DNSKEY

9.5 Déploiement du serveur racine par le serveur racine

L'introduction des DNSSEC en 2010 s'est produite individuellement pour chaque serveur racine. Une version préliminaire de la zone de signature des DNSSEC est apparue sur un serveur en janvier 2010, sur un autre serveur racine en février, sur deux autres serveurs racine en mars et ainsi de suite. L'objectif était de permettre aux serveurs récursifs (ou à tout ce qui envoyait des requêtes vers les serveurs racine) d'essayer les DNSSEC d'abord et de revenir en arrière si les réponses n'étaient pas acceptables.

Cette stratégie a été proposée pour le roulement de la KSK de la zone racine mais a rapidement été rejetée pour un nombre de raisons. Dans le but d'atténuer les problèmes liés à la nouvelle KSK de la zone racine et à la capacité de mesurer l'adoption de la nouvelle ancre de confiance au fil du temps, les réalités suivantes constituaient des obstacles.

Face à l'échec de validation des DNSSEC, la réaction du serveur de validation récursif varie selon l'outil. Certains outils sont connus comme étant très agressifs en cas de nouvelle tentative, d'autres ne le sont pas tellement, et d'autres encore ne s'y intéressent même pas.

~~Il est su de tous~~Tout le monde sait qu'il n'est pas pratique de détecter si un serveur récursif (ou toute autre source de requêtes) a pris la décision explicite de préférer un serveur racine plutôt qu'un autre. Dans des circonstances normales le suivi des sources de requête sur les serveurs racine est insuffisant pour détecter les serveurs récursifs qui préfèrent un serveur racine pas dessus un autre. La collecte annuelle de DITL[26] par DNS-OARC s'effectue pendant une courte période de temps, est très ambitieuse et n'a encore jamais réussi à couvrir l'ensemble des serveurs racine en même temps à aucun moment.

Une autre considération est le laps de temps disponible pour introduire progressivement la nouvelle ancre de confiance. Les trimestres en dehors d'une ZSK de la zona racine ne durent que 70 jours. L'ajout de la KSK entrante (au premier serveur) nécessite 40 jours, ce qui ne laisse que 30 jours de plus pour terminer la tâche dans une période de roulement de la ZSK. Le déploiement incrémentiel original s'étendait pendant plus de 4 mois.

10 Restauration

~~Dans le~~Au cas où il y aurait de graves problèmes détectés après l'introduction des RRsets DNSKEY de la KSK entrante, les RRsets DNSKEY signés uniquement par la KSK en place devraient être prêts pour le déploiement. Ces RRsets sont en format *Signed Key Response* (SKR) et peuvent être produits en utilisant les mêmes cérémonies des clés KSK de la zone racine que la non restauration des RRsets. Les critères pour une telle restauration doivent être développés davantage par les partenaires de la RZM.

Recommandation 14 : ~~Pour réduire le temps de récupération en raison de problèmes impliquant la KSK entrante, une SKR générée uniquement par la KSK en place devrait être obtenue en parallèle avec la SKR générée par la KSK entrante. YYY~~pour réduire le temps de récupération en raison de problèmes impliquant la KSK entrante, une SKR générée uniquement par la KSK en place devrait être obtenue en parallèle avec la SKR générée par la KSK entrante.

Recommandation 15 : les partenaires de la RZM devraient élaborer et documenter le processus d'utiliser le SKR généré par la KSK en place.

Les SKR de restauration contenant des RRsets DNSKEY doivent être préparées pour tous les trimestres du processus. Au cours du ~~Q~~T1 et ~~Q~~T2, la restauration SKR se compose de DNSKEY RRsets avec la KSK en place et la ou les ZSK(s) en place, signées par la KSK en place. La KSK entrante est omise. Au cours du ~~Q~~T3, la

[26] https://www.dns-oarc.net/ditl/2011

restauration SKR se compose de DNSKEY RRsets avec la KSK entrante et la ou les ZSK(s) en place, signées par la KSK entrante. La KSK en place révoquée est omise.

Seuils

Les essais à la date du déploiement des DNSSEC indiquent que ces essais ont une marge d'erreur d'environ 5 %. Ceci est interprété comme signifiant que toute déclaration relative à un montant de dommages devra reconnaître que 5 % de la population (personnes ou serveurs récursifs, selon la manière de mesurer) peuvent subir une dégradation des performances no~~t~~n détectée. Sur cette base, une mesure spécifique définissante n'est pas considérée comme la bonne réponse à la définition d'un déclencheur de la restauration.

En outre, on ne sait pas quels sont les dommages possibles. Il pourrait s'agir d'un déploiement errant, d'une partie du code errante, d'une procédure errante ou d'un acte aléatoire de l'Internet. Pour cette raison, le premier pas est le maintien de contact avec les partenaires de distribution et l'ouverture des moyens pour le signalement des problèmes, le tout utilisé avec du bon sens pour savoir réagir aux rapports.

Outre la gravité et la propagation des dommages, il n'est pas clair, car il existe beaucoup de cas, si la restauration provoquerait plus de dégâts que la continuation en atténuant les problèmes à mesure qu'ils seront détectés.

11 Quand ?

Compte tenu de l'environnement opérationnel existant, il y a quatre jours dans l'année civile auxquels une nouvelle KSK de la zone racine peut assumer le contrôle. Il s'agit des premiers jours des trimestres, soit le premier janvier, avril, juillet et octobre. Le choix d'une date précise pour le changement ~~se compose~~ dépend de ce qui est raisonnable sur le plan opérationnel, et de ce qui est compatible avec les discussions en cours concernant la transition de l'IANA.[27]

Sur le plan opérationnel, « raisonnable » implique que les dates concernées devraient éviter les weekends, les congés ayant une incidence sur les horaires de travail, et les horaires auxquels le personnel fonctionne sur une ~~mince~~ faible marge. Compte tenu de la nécessité d'aligner trois dates avec une audience mondiale, on ne peut pas tout respecter. Pour compliquer davantage le défi~~davantage~~, en 2016 et 2017 chaque trimestre commencera un vendredi, samedi ou dimanche. Aucun trimestre ne commencera un autre jour de la semaine jusqu'en 2018. (Le quatrième

[27] http://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions

trimestre de 2015 commence le jeudi 1er octobre, mais il n'existera pas de plan en place et il y aura encore moins d'essais achevés pour pouvoir effectuer un roulement de clés ~~en cette date~~ce jour-là.

Un impact non technique est la transition de la supervision des fonctions IANA qui est prévue. Cela rend impraticable la recommandation d'une date spécifique en ce moment.

12 Analyse des risques

12.1 Risques liés à une préparation insuffisante

Description	Impact	Probabilité	Atténuation
Le roulement d'une KSK avec le même algorithme, hachage et taille ne sera pas suffisant aux yeux des parties prenantes	Faible	Peu probable	Planifier un autre roulement une fois que le premier sera complet ; en cas de nécessité d'autres paramètres, les changer
Les opérateurs de réseau ne seront pas au courant du changement (c.-à-d. le NoC recevra des dossiers et doit donc savoir comment réagir)	Modérée	Probable	Dans le plan de communications ; focalisation sur l'opérateur
Les opérateurs de réseau~~x~~ et les développeurs de logiciels (ou « aucun partenaire de distribution ») n'auront pas (accès à) des environnements d'essai adéquats	Modérée	Probable	Mise en place d'un banc d'essai RFC 5011 de l'ICANN avec des roulements accélérés et dans les délais ; autres essais

Description	Impact	Probabilité	Atténuation
Impossibilité d'effectuer des essais principalement pendant les opérations	Faible	Probable	Élaboration de méthodes d'essai distribuées ; élaboration de la liste de contacts
Absence de critères déterministes pour décider d'avancer ou pas	Faible	Probable	Nécessité de préparer les communications et les épreuves ; études de faisabilité des mécanismes utilisés sur le terrain ; effort à long terme pour développer les mesures d'acceptation de l'ancre de confiance mise à jour

12.2 Le mécanisme de l'ancre de confiance automatisé ne fonctionne pas ou est insuffisant

Description	Impact	Probabilité	Atténuation
RFC 5011 pas activé partout	Modérée	Probable	Approches alternatives à la gestion de l'ancre de confiance
RFC 5011 mis en œuvre partiellement	Modérée	Peu probable	Contacter les développeurs de logiciels ; vérifier la compréhension du RFC 5011
Processus de bootstrap validateur mis en œuvre partiellement	Modérée	Peu probable	Contacter les intégrateurs de système et les gestionnaires de l'ancre de confiance
L'ancre de confiance n'est pas disponible sur le site ~~web~~ Web IANA de l'ICANN	Faible	Peu probable	Suivi de la disponibilité

Équipement avec ancre de confiance désuette par manque d'entretien	Faible	Probable	Plan de communication

12.3 L'élimination de la KSK en place provoque des échecs de validation

Description	Impact	Probabilité	Atténuation
Protocole d'ancre de confiance automatisé insuffisamment suivi (par tout participant au processus)	Faible	Probable	Essais, communication ; fournir des ressources pour les opérateurs afin d'accélérer la rémédiation
Trafic élevé en raison de nouvelles tentatives en cas d'échec	Faible	Peu probable	Examen des effets « roulement et fin [28]» ; recommandations de mise en caché négatives

12.4 L'addition de KSK entrantes génère une taille des messages DNS qui dépasse les limites

Description	Impact	Probabilité	Atténuation
La transition de keysets provoque des datagrammes surdimensionnés	Modérée	Peu probable	Planification minutieuse d~~la e~~e la transition en examinant la taille des messages

[28] http://iepg.org/2010-03-ietf77/dnssec-goes-wrong.pdf, http://www.potaroo.net/ispcol/2010-02/rollover.html

Confusion au sujet de la fragmentation d'IPv6 dans le logiciel DNS	Faible	Peu probable	Contrôle et essai du logiciel DNS

12.5 Possibilité d'erreurs opérationnelles

Description	Impact	Probabilité	Atténuation
Le roulement erroné de la KSK éliminera l'élan de l'adoption des DNSSEC	Élevé	Peu probable	Conception / révision minutieuse
Remettre indéfiniment un roulement de clé augmente l'impact, s'il s'avère urgent	Élevé	Peu probable	Engagement de roulement d'une KSK de la zone racine
Une fois commencé, ne peut jamais retourner à l'état acceptable actuel	Élevé	Peu probable	Définition d'un plan de secours
La KSK en place (composante privée) n'est pas suffisamment détruite	Faible	Peu probable	Engagement d'achever le plan

13 Membres de l'équipe de conception

13.1 Bénévoles de la communauté

- Joe Abley, Dyn, Inc., CA
- Jaap Akkerhuis, NLNetLabs, NL
- John Dickinson, Sinodun Internet Technologies, UK

- Geoff Huston, APNIC, AU
- Ondrej Sury, CZ.NIC, CZ
- Paul Wouters, No Hats/Red Hat, NL
- Yoshiro Yoneya, JPRS, JP

13.2 Partenaires de gestion de la zone racine

- David Conrad, ICANN
- Edward Lewis, ICANN
- Richard Lamb, ICANN
- Alain Durand, ICANN
- Hayley Laframboise, ICANN
- Elise Gerich, ICANN
- Kim Davies, ICANN
- Roy Arends, ICANN
- Jakob Schlyter, ICANN
- Fredrik Ljunggren, ICANN
- Brad Verd, Verisign
- Duane Wessels, Verisign
- David Blacka, Verisign
- Al Bolivar, Verisign
- Tim Polk, US DoC NIST
- Scott Rose, US DoC NIST
- Doug Montgomery, US NIST
- Ashley Heineman, US DoC NTIA
- Vernita Harris, US DoC NTIA

14 Références

- RFC 5011 : Mises à jour ~~automatiques~~ automatisées des ancres de confiance de la sécurité du DNS (DNSSEC)
  https://tools.ietf.org/html/rfc5011
- SAC063 : Avis du SSAC sur le roulement des clés des DNSSEC dans la zone racine
  https://www.icann.org/en/system/files/files/sac-063-en.pdf
- Déclaration de pratique des DNSSEC pour l'opérateur de la KSK de la zone racine
  https://www.iana.org/dnssec/icann-dps.txt
- Déclaration de pratique des DNSSEC pour l'opérateur de la ZSK de la zone racine
- https://www.verisigninc.com/assets/dps-zsk-operator-1527.pdf

- Publication de l'ancre de confiance des DNSSEC pour la zone racine https://tools.ietf.org/html/draft-jabley-dnssec-trust-anchor
- Établissement d'une ancre de confiance des DNSSEC appropriée pour la zone racine au départ https://tools.ietf.org/html/draft-jabley-dnsop-validator-bootstrap

15 Annexe : Partenaires de distribution

Le terme « partenaires de distribution » se réfère à des organisations externes qui indépendamment ~~soit~~ activent ou transmettent la valeur de la gestion de la KSK de la zone racine. Ces organisations n'ont aucune relation officielle avec les partenaires de la RZM et cependant la coordination avec eux est en quelque sorte essentielle. Pour chaque organisation, les contacts appropriés doivent être conservés afin d'échanger les statuts et d'autres informations liées à la modification de la KSK de la zone racine.

Les partenaires de distribution ne sont répertoriés dans aucun ordre particulier.

15.1 Producteurs de logiciels

La communication avec ces partenaires se rapporte à la mise en œuvre (ou non) de la gestion de l'ancre de confiance du RFC 5011 dans le logiciel. L'ensemble des partenaires sont ceux qui valident des serveurs de caché récursifs. L'information de contact avec ces organisations ne figure pas dans le présent document.

- BIND de l'ISC (http://www.isc.org)
- Unbound de NLNetLab (https://nlnetlabs.nl)
- Serveur de Microsoft Windows (https://www.microsoft.com/)
- Vantio de Nominum (http://nominum.com/caching-dns/)
- DNSMASQ (http://www.thekelleys.org.uk/dnsmasq/doc.html)
- IRONSIDES (http://ironsides.martincarlisle.com)
- Infoblox (http://www.infoblox.com/
- Secure64 DNS Cache (http://www.secure64.com/)

15.1.1 En cours

L'ensemble des partenaires suivants ont discuté mais n'ont pas publié des serveurs de caché récursifs qui valident les DNSSEC. Ils figurent sur une liste pour être tenus au courant si le code est distribué. (Les autres serveurs de caché DNS récursifs qui ne soutiennent pas les DNSSEC ne dépendent pas de la KSK de la zone racine)

- Serveur récursif à définir de CZ.NIC (outre Knot)
- PowerDNS à définir

15.2 Intégrateurs de systèmes

Ces partenaires transmettent la KSK de la zone racine parmi les données de configuration impliquant, dans certains cas, le logiciel DNS mentionné

précédemment. L'espoir est que ces organisations examineront la KSK entrante de la zone racine et l'incluront dans leurs mises à jour de logiciel.

15.2.1 Linux

- RPM Red Hat Enterprise Linux (RHEL)
- Micro Focus International's SUSE (RPM)
- Borsalino
- CentOS
- Debian and Canonical (Ubuntu) APT
- Montavista Linux

15.2.2 BSD

- Ports de FreeBSD
- NetBSD pkgsrc
- Ports OpenBSD

15.2.3 Autres

- iOS, OS X de Apple
- Android, ChromeOS de Google
- Microsoft
- Cisco
- Juniper
- Belkin
- Cisco / Linksys
- Wind River (RTOS)
- QNX (RTOS)
- OpenVMS
- OpenWRT

15.3 Opérateurs de résolveurs publics

Ces partenaires sont censés exécuter des serveurs DNS récursifs, validant les DNSSEC dans certains cas. L'attente est que ceux-ci incluent la KSK de la zone racine comme données de configuration, donc il pourrait y avoir des révisions internes qui auraient besoin de connaître la KSK entrante de la zone racine.

- Public DNS de Google
- OpenDNS
- DNSAdvantage de Neustar
- ConnectSafe de Symantec
- Level 3

- Censurfridns
- Comodo
- Dyn Internet Guide
- Liquid Telecom

Outre la liste d'opérateurs avec des résolveurs publiques ci-dessus, choisis en fonction de l'acceptation de trafic à partir de n'importe où dans l'Internet (pour autant que l'on puisse voir), il y a des partenaires qui exploitent des résolveurs publics avec des restrictions sur leur base de référence. Vu que ces partenaires sont identifiés, ils seront aussi notifiés des événement de la KSK de la zone racine.