Équipe d'ingénierie de l'Internet (IETF)
Request For Comments : 9615
RFC mises à jour : 7344, 8078
Catégorie : Sur la voie de la normalisation
ISSN : 2070-1721

P. Thomassen, deSEC, Secure Systems Engineering (SSE)
N. Wisiol, deSEC, Technische Universität Berlin
juillet 2024

Traduction Claude Brière de L'Isle

Amorçage automatique DNSSEC à l'aide de signaux authentifiés provenant de l'opérateur de zone

Résumé
Le présent document présente une méthode dans la bande permettant aux opérateurs DNS de publier des informations arbitraires sur les zones pour lesquelles ils sont d'autorité, de manière authentifiée et sur la base de la zone. Le mécanisme permet aux opérateurs DNS gérés d'annoncer en toute sécurité les paramètres clés de DNSSEC pour les zones sous leur gestion, y compris pour les zones qui ne sont pas actuellement déléguées de manière sécurisée.

Lorsque les enregistrements DS sont absents pour la délégation d'une zone, ce signal permet au registre ou au registraire du parent de valider de manière cryptographique les enregistrements CDS/CDNSKEY trouvés au sommet de l'enfant. Le parent peut alors provisionner des enregistrements DS pour la délégation sans recourir à une validation hors bande ou à des types de vérifications croisées plus faibles tels que "Accepter après délai".

Le présent document établit la méthode d'inscription DS décrite dans la section 4 de ce document comme la méthode préférée par rapport à celles de la section 3 de la RFC 8078. Il met également à jour la RFC 7344.

Statut de ce mémoire
Ceci est un document de l'Internet sur la voie de la normalisation.

Le présent document a été produit par l'équipe d'ingénierie de l'Internet (IETF). Il représente le consensus de la communauté de l'IETF. Il a subi une révision publique et sa publication a été approuvée par le groupe de pilotage de l'ingénierie de l'Internet (IESG). Tous les documents approuvés par l'IESG ne sont pas candidats à devenir une norme de l'Internet ; voir la Section 2 de la RFC5741.

Les informations sur le statut actuel du présent document, tout errata, et comment fournir des réactions sur lui peuvent être obtenues à http://www.rfc-editor.org/info/rfc9615.

Table des matières

1. Introduction

Sécuriser pour la première fois une délégation DNS exige que les paramètres DNSSEC de l'enfant soient transmis au parent par un canal de confiance. Bien que la communication doive théoriquement se produire entre le registre parent et le détenteur de la clé DNSSEC, ce que cela signifie exactement et la manière dont la communication est coordonnée dépend traditionnellement de la relation que l'enfant entretient avec le parent.

Une situation typique est celle où la clé est détenue par l'opérateur DNS fils ; donc, la communication implique souvent cette entité. De plus, selon les circonstances, le registraire peut également être impliqué, éventuellement par l'intermédiaire de l'enregistrant (pour plus de détails, voir l'annexe A de la RFC7344).

Comme on l'observé dans la [RFC7344], ces dépendances aboutissent souvent à un processus manuel susceptible de fautes et/ou d'erreurs. De plus, en raison du caractère ennuyeux du processus, les parties concernées peuvent éviter le processus de publication d'un ensemble d'enregistrements de ressources DS (RRset) en premier lieu.

Pour atténuer ces problèmes, le provisionnement automatisé des enregistrements DS a été spécifié dans la [RFC8078]. Il repose sur l'agent parent (registre ou registraire) qui récupère les paramètres clé de DNSSEC à partir des enregistrements CDS et CDNSKEY ([RFC7344]) situés au sommet de la zone fille, et les valide d'une manière ou d'une autre. Cette validation peut être effectuée à l'aide de la chaîne de confiance DNSSEC existante de la zone fille si l'objectif est de mettre à jour un RRset DS existant (comme lors d'un retour à zéro de la clé). Cependant, lors de l'amorçage d'une délégation DNSSEC, la zone fille ne dispose pas d'un chemin de validation DNSSEC existant, il faut donc trouver d'autres moyens de garantir la légitimité des enregistrements CDS/CDNSKEY.

En raison de l'absence d'une solution DNS intégrée complète, soit des méthodes hors bande ont été utilisées jusqu'à présent pour compléter la chaîne de confiance, soit la validation cryptographique a été entièrement supprimée, au prix de types de vérifications croisées plus faibles tels que "Accepter après délai" (paragraphe 3.3 de la [RFC8078]). La [RFC8078] ne définit pas de méthode de validation dans la bande pour activer DNSSEC.

Le présent document vise à combler cette lacune en introduisant une méthode dans la bande permettant aux opérateurs DNS de publier des informations arbitraires sur les zones pour lesquelles ils sont d'autorité, de manière authentifiée et sur la base de la zone. Le mécanisme permet aux opérateurs DNS gérés d'annoncer en toute sécurité les paramètres clé de DNSSEC pour les zones qu'ils gèrent. Le parent peut ensuite utiliser ce signal pour valider de manière cryptographique les RRsets CDS/CDNSKEY trouvés au sommet d'une zone fille non sécurisée et, en cas de succès, de sécuriser la délégation.

Bien qu'applicable à la grande majorité des domaines, le protocole ne prend pas en charge certains cas limites, tels que les noms de zone fille excessivement longs ou l'amorçage DNSSEC pour les domaines avec des serveurs de noms dans le domaine uniquement (voir le paragraphe 4.4).

L'amorçage DNSSEC n'est qu'une application du mécanisme de signalisation générique spécifié dans ce document. D'autres applications pourraient apparaître à l'avenir, telles que la publication de métadonnées opérationnelles ou d'informations auxiliaires que l'opérateur DNS souhaite faire connaître (par exemple, les points d'extrémité d'API pour les interactions avec des tiers).

Les lecteurs doivent être familiarisés avec DNSSEC [BCP237].

1.1 Terminologie

Cette section définit la terminologie utilisée dans ce document.

CDS/CDNSKEY : cette notation fait référence à CDS et/ou CDNSKEY, c'est-à-dire à l'un ou aux deux.

Enfant : voir la section 7 de la [RFC9499].

Opérateur DNS fils : l'entité qui conserve et publie les informations de zone pour le DNS fils.

Parent : voir la section 7 de la [RFC9499].

Agent parental : l'entité qui a l'autorité pour insérer des enregistrements DS dans la zone parente au nom de l'enfant. (Il peut s'agir du registre, du registraire, d'un revendeur ou d'une autre entité autorisée.)

Domaine de signalisation : nom de domaine construit en ajoutant l'étiquette _signal à un nom d'hôte extrait du RRset NS d'une délégation. Il existe autant de domaines de signalisation que de cibles NS distinctes.

Nom de signalisation : les étiquettes qui sont préfixées à un domaine de signalisation afin d'identifier un type de signalisation et le nom d'une zone fille (voir le paragraphe 3.2).

Enregistrement de signalisation : un enregistrement DNS situé à un nom de signalisation sous un domaine de signalisation. Les enregistrements de signalisation sont utilisés par l'opérateur DNS fils pour publier des informations sur l'enfant.

Type de signalisation : un identifiant de type de signal, tel que _dsboot pour l'amorçage DNSSEC.

Zone de signalisation : la zone qui est d'autorité pour un enregistrement de signalisation donné.

1.2 Notation des exigences

Les mots clés "DOIT", "NE DOIT PAS", "EXIGÉ", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDÉ", "NON RECOMMANDÉ", "PEUT" et "FACULTATIF" dans ce document doivent être interprétés comme décrit dans le BCP 14 [RFC2119] [RFC8174] lorsque, et seulement lorsqu'ils apparaissent en majuscules, comme indiqué ici.

2. Mises à jour des RFC

Les méthodes d'inscription DS décrites dans la Section 3 de la [RFC8078] sont moins sûres que la méthode décrite dans la Section 4 du présent document. Par conséquent, les opérateurs DNS fils et les agents parentaux qui souhaitent utiliser les enregistrements CDS/CDNSKEY pour l'inscription DS initiale DEVRAIENT prendre en charge le protocole d'authentification décrit ici.

Afin de faciliter la publication des enregistrements de signalisation à des fins d'amorçage DNSSEC (voir le paragraphe 4.1) le premier alinéa ("Localisation") du paragraphe 4.1 de la [RFC7344] est supprimé.

3. Signalisation

Cette section décrit le mécanisme général par lequel un opérateur DNS fils peut publier un signal authentifié sur une zone fille. Les agents parentaux (ou toute autre partie) peuvent alors découvrir et traiter le signal. L'authenticité est assurée par la validation DNSSEC standard.

3.1 Chaîne de confiance

Si un opérateur DNS fils met en œuvre la présente spécification, chaque zone de signalisation DOIT être signée et validable par l'agent parental (c'est-à-dire avoir une chaîne de confiance DNSSEC valide et résolvable publiquement). Cela est généralement réalisé en déléguant de manière sécurisée chaque zone de signalisation.

Par exemple, lorsqu'il publie un signal relatif à une zone fille avec les enregistrements NS ns1.example.net et ns2.example.org, l'opérateur DNS fils doit s'assurer que l'agent parental dispose d'une chaîne de confiance DNSSEC valide

pour la ou les zones qui sont d'autorité pour les domaines de signalisation _signal.ns1.example.net et _signal.ns2.example.org.

3.2 Noms de signalisation

Pour publier des informations sur la zone fille de manière authentifiée, l'opérateur DNS fils DOIT publier un ou plusieurs enregistrements de signalisation sous un nom de signalisation dans chaque domaine de signalisation.

Les enregistrements de signalisation DOIVENT être accompagnés d'enregistrements RRSIG créés avec la ou les clés de la zone de signalisation correspondante. Le type et le contenu de ces enregistrements de signalisation dépendent du type de signal.

Le nom de signalisation identifie l'enfant et le type de signalisation. Il est identique au nom de l'enfant (avec l'étiquette racine finale supprimée) préfixé par une étiquette contenant le type de signalisation.

4. Amorçage d'une délégation DNSSEC

Lorsque les RRsets CDS/CDNSKEY de la zone fille sont utilisés pour établir la confiance initiale, ils doivent être authentifiés. Cela est réalisé en copubliant les RRsets CDS/CDNSKEY de la zone fille en tant que signal authentifié tel que décrit dans la Section 3. Le parent peut le découvrir et le valider, transférant ainsi la confiance de la chaîne de confiance des serveurs de noms de l'opérateur DNS fils à la zone fille.

Ce protocole n'est pas destiné à mettre à jour un RRset DS existant. Pour cela, l'agent parental peut valider directement les RRsets CDS/CDNSKEY de l'enfant, en utilisant la chaîne de confiance établie par le RRset DS existant (Section 4 de la [RFC7344]).

4.1 Consentement de signalisation pour agir en tant que signataire de l'enfant

Pour confirmer sa volonté d'agir en tant que signataire délégué de l'enfant et d'authentifier les RRsets CDS/CDNSKEY de l'enfant, l'opérateur DNS fils DOIT les copublier sous le nom de signalisation correspondant sous chaque domaine de signalisation, à l'exclusion de ceux qui relèveraient du domaine fils (paragraphe 3.2). Pour simplifier, l'opérateur DNS fils PEUT également copublier les RRsets CDS/CDNSKEY du fils sous des domaines de signalisation au sein du domaine fils, bien que ces domaines de signalisation ne soient pas utilisés pour la validation (paragraphe 4.2).

Contrairement aux RRsets CDS/CDNSKEY au sommet de l'enfant, un RRset de signalisation DOIT être signé avec la ou les clés de la zone de signalisation correspondante. Son contenu DOIT être identique au RRset correspondant publié au sommet de l'enfant.

L'utilisation existante des enregistrements CDS/CDNSKEY a été spécifiée au seul sommet de l'enfant (paragraphe 4.1 de la [RFC7344]). Le présent protocole étend l'utilisation de ces types d'enregistrements aux noms de propriétaires non sommets pour les besoins de l'amorçage DNSSEC. Pour exclure la possibilité d'une collision sémantique, il NE DOIT PAS y avoir de coupure de zone au niveau d'un nom de signalisation.

4.1.1 Exemple

Afin d'amorcer la zone fille example.co.uk avec les enregistrements NS ns1.example.net, ns2.example.org et ns3.example.co.uk, les domaines de signalisation requis sont _signal.ns1.example.net et _signal.ns2.example.org.

Dans les zones contenant ces domaines, l'opérateur DNS fils authentifie les RRsets CDS/CDNSKEY trouvés à l'apex de la zone fille en les copubliant sous forme de RRsets CDS/CDNSKEY aux noms :

_dsboot.example.co.uk._signal.ns1.example.net
_dsboot.example.co.uk._signal.ns2.example.org

Ces RRsets sont signés avec DNSSEC comme toutes les autres données de zone.

La publication des enregistrements de signalisation sous le nom _signal.ns3.example.co.uk dans le domaine n'est pas requise.

4.2 Validation des enregistrements CDS/CDNSKEY pour l'amorçage DNSSEC

Pour valider le RRset CDS/CDNSKEY d'un enfant pour l'amorçage DNSSEC, l'agent parental, connaissant à la fois le nom de la zone fille et ses noms d'hôtes NS, DOIT exécuter les étapes suivantes :

Étape 1 : vérifier que l'enfant n'a pas d'enregistrement DS publié sur le parent et qu'au moins un de ses serveurs de noms est en dehors du domaine fils ;

Étape 2 : interroger le RRset CDS/CDNSKEY au sommet de la zone fille directement à partir de chacun des serveurs d'autorité comme déterminé par le RRset NS de la délégation (côté parent), sans mise en antémémoire ;

Étape 3 : interroger le RRset CDS/CDNSKEY situé au nom de signalisation sous chaque domaine de signalisation (à l'exception de ceux qui relèvent du domaine fils) à l'aide d'un résolveur DNS de confiance et appliquer la validation DNSSEC ;

Étape 4 : vérifier (séparément par type d'enregistrement) que tous les RRsets récupérés aux étapes 2 et 3 ont des contenus égaux ;

Si les étapes ci-dessus réussissent sans erreur, les RRsets CDS/CDNSKEY sont vérifiés avec succès et l'agent parental peut procéder à la publication du RRset DS sous les précautions décrites à la section 5 de la [RFC8078].

L'agent parental DOIT interrompre la procédure si une condition d'erreur se produit, en particulier :

* à l'étape 1 : l'enfant est déjà délégué de manière sécurisée ou n'a des serveurs de noms que dans le domaine ;

* à l'étape 2 : tout échec lors de la récupération du RRset CDS/CDNSKEY situé au sommet de l'enfant à partir de l'un des serveurs de noms d'autorité ;

* à l'étape 3 : tout échec de récupération des RRsets CDS/CDNSKEY situés au nom de signalisation sous n'importe quel domaine de signalisation, y compris l'échec de la validation DNSSEC ou des données non authentifiées (bit AD non établi) ;

4.2.1 Exemple

Pour vérifier les RRsets CDS/CDNSKEY pour l'enfant example.co.uk, l'agent parental (en supposant que les enregistrements NS de la délégation fille sont ns1.example.net, ns2.example.org et ns3.example.co.uk)

1. vérifie que le domaine fils n'est pas encore délégué de manière sécurisée ;

2. interroge les RRsets CDS/CDNSKEY pour example.co.uk directement depuis ns1.example.net, ns2.example.org et ns3.example.co.uk (sans mise en antémémoire) ;

3. interroge et valide les RRsets CDS/CDNSKEY situés à (voir au paragraphe 3.2 ; ns3.example.co.uk est ignoré car il est dans le domaine)
   _dsboot.example.co.uk._signal.ns1.example.net
   _dsboot.example.co.uk._signal.ns2.example.org

4. vérifie que les RRsets CDS/CDNSKEY récupérés aux étapes 2 et 3 correspondent dans les réponses.

Si toutes ces étapes réussissent, l'agent parental peut procéder à la publication d'un RRset DS comme indiqué par le RRset CDS/CDNSKEY validé.

Comme les noms de signalisation dans le domaine n'ont pas de chaîne de confiance au moment de l'amorçage, l'agent parental ne les prend pas en compte pendant la validation. Par conséquent, si tous les noms d'hôtes NS sont dans le domaine, la validation ne peut pas être terminée et les enregistrements DS ne sont pas publiés.

4.3 Déclencheurs

Les agents parentaux DEVRAIENT déclencher la procédure décrite au paragraphe 4.2 une fois que l'une des conditions suivantes est remplie :

* L'agent parent reçoit un RRset NS nouveau ou mis à jour pour un enfant ;

* L'agent parent reçoit une notification indiquant que l'enfant souhaite que son RRset CDS/CDNSKEY soit traité ;

* L'agent parental rencontre un enregistrement de signalisation lors d'un exanen proactif et opportuniste (par exemple, des requêtes quotidiennes d'enregistrements de signalisation pour certaines ou toutes ses délégations) ;

* L'agent parent rencontre un enregistrement de signalisation lors d'un processus NSEC ou lors de l'analyse d'une zone de signalisation (par exemple, lorsqu'il est mis à disposition via AXFR par l'opérateur DNS fils) ;

* Toute autre condition jugée appropriée par la politique locale.

Les mécanismes de déclenchement fondés sur un temporisateur (comme les analyses) présentent des propriétés indésirables en ce qui concerne le délai de traitement et l'adaptation ; les déclencheurs à la demande (comme les notifications) sont préférables. Chaque fois que possible, les opérateurs DNS fils et les agents parentaux sont donc encouragés à les utiliser, réduisant ainsi les délais et le volume de trafic d'analyse.

La plupart des types de découverte (comme les analyses quotidiennes des délégations) sont directement fondés sur le RRset NS de la délégation. Dans ce cas, ces noms NS peuvent être utilisés tels quels par l'algorithme d'amorçage (paragraphe 4.2) pour interroger les enregistrements de signalisation.

Certaines méthodes de découverte n'impliquent cependant pas une connaissance fiable du RRset NS de la délégation. Par exemple, lors de la découverte de noms de signalisation en effectuant un processus NSEC ou un transfert de zone d'une zone de signalisation, l'agent parent NE DOIT PAS supposer qu'un serveur de noms sous le domaine de signalisation duquel un enregistrement de signalisation apparaît est réellement d'autorité pour l'enfant correspondant.

Au lieu de cela, chaque fois qu'une liste de "domaines amorçables" est obtenue par d'autres moyens que directement auprès du parent, l'agent parental DOIT vérifier que la délégation contient réellement le nom d'hôte du serveur de noms vu pendant la découverte et s'assurer que les demandes d'enregistrement de signalisation ne sont effectuées que sur l'ensemble approprié de serveurs de noms tel que répertorié dans la délégation du parent de l'enfant.

4.4 Limitations

En conséquence de l'étape 3 du paragraphe 4.2, l'amorçage DS ne fonctionne pas pour les délégations entièrement dans le domaine, car aucune chaîne de confiance préexistante au domaine fils n'est disponible pendant l'amorçage. (Comme solution de contournement, on peut ajouter un serveur de noms hors domaine au RRset NS initial et le supprimer une fois l'amorçage terminé. L'automatisation pour cela est disponible via les enregistrements CSYNC, voir la [RFC7477].)

Les noms de signalisation pleinement qualifiés doivent être des noms DNS valides. Les exigences de compte d'étiquettes et de longueur pour les noms DNS (paragraphe 3.1 de la [RFC1035]) impliquent que le protocole ne fonctionne pas pour les noms de domaine fils ou les noms d'hôtes NS inhabituellement longs.

5. Recommandations opérationnelles

5.1 Opérateur DNS fils

Il est possible d'ajouter des enregistrements CDS/CDNSKEY et des enregistrements de signalisation correspondants à une zone sans que le propriétaire du domaine en soit explicitement informé. Pour éviter que les propriétaires de domaine ne soient pris au dépourvu par les changements DS qui s'ensuivent, il est conseillé aux opérateurs DNS fils qui suivent cette pratique de rendre cela transparent, par exemple en informant le propriétaire du domaine lors de la création de la zone (par exemple, dans une interface graphique) ou en le notifiant par message électronique.

Lors du transfert d'une zone vers un autre opérateur DNS, l'ancien et le nouvel opérateur DNS fils doivent coopérer pour réaliser une transition en douceur, par exemple, en utilisant les protocoles multi-signataires décrits dans la [RFC8901]. Si tout le reste échoue, le propriétaire du domaine devra peut-être demander la suppression de tous les enregistrements DS et

effectuer le transfert de manière non sécurisée (voir [INSEC]).

Les domaines de signalisation DEVRAIENT être délégués en tant que zones autonomes, de sorte que le sommet de la zone de signalisation coïncide avec le domaine de signalisation (tel que _signal.ns1.example.net). Bien qu'il soit permis que le domaine de signalisation soit contenu dans une zone de signalisation comportant moins d'étiquettes (telle que example.net), une coupure de zone garantit que les activités d'amorçage ne nécessitent pas de modification de la zone contenant le nom d'hôte du serveur de noms.

Une fois qu'un opérateur DNS fils détermine que les ensembles d'enregistrements de signalisation spécifiques ont été traités (par exemple, en voyant le résultat dans la zone parente) il lui est conseillé de les supprimer. Cela réduira la taille de la zone de signalisation et facilitera un traitement en masse plus efficace (par exemple via des transferts de zone).

5.2 Agent parental

Afin de garantir un amorçage DNSSEC en temps utile des domaines non sécurisés, les situations d'impasse dues à une non-concordance des enregistrements en antémémoire obsolètes (étape 4 du paragraphe 4.2) doivent être évitées. Il est donc RECOMMANDÉ que les interrogations dans les domaines de signalisation soient effectuées avec une antémémoire de résolveur (initialement) vide, ou qu'une autre méthode de récupération de données fraîches à partir de serveurs faisant autorité soit utilisée.

Il est également RECOMMANDÉ que la minimisation de QNAME [RFC9156] soit utilisée lors de la résolution des interrogations pour les enregistrements de signalisation afin de se protéger contre certaines attaques (voir la Section 6).

6. Considérations relatives à la sécurité

La méthode d'amorçage DNSSEC présentée dans ce document est fondée sur les approches décrites dans la Section 3 de la [RFC8078], mais ajoute l'authentification au concept de CDS/CDNSKEY. Son niveau de sécurité est donc strictement supérieur à celui des approches existantes décrites dans ce document (par exemple, "Accepter après délai"). À part cette amélioration générale, les mêmes considérations de sécurité s'appliquent que dans [RFC8078].

Le niveau de rigueur du paragraphe 4.2 est nécessaire pour empêcher la publication d'un RRset DS mal conçu (autorisé uniquement sous un sous-ensemble de noms d'hôtes NS). Cela garantit, par exemple, qu'un opérateur dans une configuration multi rattachements ne peut pas activer DNSSEC à moins que tous les autres opérateurs soient d'accord.

Dans tous les cas, comme l'opérateur DNS fils a une connaissance fiable des enregistrements CDS/CDNSKEY de l'enfant, il peut facilement détecter un provisionnement frauduleux d'enregistrements DS.

Afin d'éviter que les parents des noms d'hôtes de serveur de noms ne deviennent un point de défaillance unique pour une délégation (à la fois en termes de disponibilité de résolution et de modèle de confiance de ce protocole) il est conseillé de diversifier le chemin de la racine aux noms d'hôtes de serveur de noms de l'enfant. Par exemple, des TLD différents et exploités indépendamment peuvent être utilisés pour chacun.

Si la minimisation de QNAME [RFC9156] n'est pas utilisée lors de la recherche d'enregistrements de signalisation, un parent en amont d'un domaine de signalisation verra ces interrogations CDS/CDNSKEY et pourra répondre avec une réponse d'autorité signée avec sa propre clé, au lieu d'envoyer la référence. L'activation de la minimisation de QNAME réduit la surface d'attaque pour une telle falsification.

7. Considérations relatives à l'IANA

L'IANA a ajouté les entrées suivantes au registre "Enregistrements de ressource du DNS par des attributs de dénomination d'extrémité avec un caractère"souligné"" [RFC8552] :

Type RR	_NODE NAME	Référence
CDS	_signal	RFC 9615 |
CDNSKEY	_signal	RFC 9615 |

Tableau 1

8. Références

8.1 Références normatives

[RFC1035] P. Mockapetris, "Noms de domaines – Mise en œuvre et spécification", STD 13, novembre 1987. (*MàJ par* RFC1101, 1183, 1348, 1876, 1982, 1995, 1996, 2065, 2136, 2181, 2137, 2308, 2535, 2673, 2845, 3425, 3658, 4033, 4034, 4035, 4343, 5936, 5966, 6604, 7766, 8482, 8767)

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. *(MàJ par* RFC8174). DOI 10.17487/RFC2119.

[RFC7344] W. Kumari, O. Gudmundsson, G. Barwood, "Automatisation de la maintenance de la délégation de confiance DNSSEC", septembre 2014. *(Information ; MàJ par* RFC8078). DOI 10.17487/RFC7344.

[RFC7477] W. Hardaker, "Synchronisation enfant-parent dans le DNS", mars 2015. *(P.S.)*. DOI 10.17487/RFC7477.

[RFC8078] O. Gudmundsson, P. Wouters, "Gestion des enregistrements du DNS provenant du parent via CDS/CDNSKEY", mars 2017. *(P.S. ; MàJ* RFC7344). DOI 10.17487/RFC8078.

[RFC8174] B. Leiba, "Ambiguïté des mots clés en majuscules ou minuscules dans la RFC2119", mai 2017. BCP14. *(MàJ* 2119). DOI 10.17487/RFC8174.

[RFC8552] D. Crocker, "Interprétation limitée des enregistrements de ressource du DNS par des attributs de dénomination d'extrémité avec un caractère "souligné"", mars 2019. BCP 222. DOI 10.17487/RFC8552.

[RFC9156] S. Bortzmeyer, R. Dolmans, P. Hoffman, "Minimisation du nom d'interrogation du DNS pour améliorer la confidentialité", novembre 2021. (DOI : 10.17487/RFC9156) *(P.S. ; remplace* RFC 7816 *).*

[RFC9499] P. Hoffman, K. Fujiwara, "Terminologie du DNS", mars 2024. BCP 219. (DOI : 10.17487/RFC9499) *(Remplace* RFC8499, *MàJ* RFC2308)

8.2 Références pour information

[BCP237] Best Current Practice 237, <https://www.rfc-editor.org/info/bcp237>. Au moment de la rédaction du présent document, ce BCP comprend :

[RFC9364] P. Hoffman, "Extensions à la sécurité du DNS (DNSSEC)", février 2023. BCP 237. (DOI : 10.17487/RFC9364)

[INSEC] Hardaker, W., "Intentionally Temporarily Degraded or Insecure", Travail en cours, octobre 2021, <https://datatracker.ietf.org/doc/html/draft-hardaker-dnsop-intentionally-temporary-insec-01>.

[RFC8901] S. Huque, P. Aras, J. Dickinson, J. Vcelak, D. Blacka, "Modèles DNSSEC multi signataires", septembre 2020. *(Information)* (DOI : 10.17487/RFC8901)

Remerciements

Merci à Brian Dickson, Ondatëj Caletka, John R. Levine, Christian Elmerot, Oli Schacher, Donald Eastlake, Libor Peltan, Warren Kumari, Scott Rose, Linda Dunbar, Tim Wicinski, Paul Wouters, Paul Hoffman, Peter Yee, Benson Muite, Roman Danyliw, Ã‰ric Vyncke, et Joe Abley pour leur relecture des projets et leurs commentaires et suggestions.

Merci aussi à Steve Crocker, Hugo Salgado, et Ulrich Wisser pour les discussions préparatoires.

Adresse des auteurs

Peter Thomassen
deSEC, Secure Systems Engineering (SSE)
Berlin
Germany
mél : peter@desec.io

Nils Wisiol
deSEC, Technische Universität Berlin
Berlin
Germany
mél : nils@desec.io