Groupe de travail Réseau
Request for Comments : 5155
Catégorie : Sur la voie de la normalisation

Traduction Claude Brière de L'Isle

B. Laurie
G. Sisson
R. Arends, Nominet
D. Blacka, VeriSign, Inc.
mars 2008

Déni d'existence authentifié à hachage de la sécurité du DNS (DNSSEC)

Statut du présent mémoire

Le présent document spécifie un protocole sur la voie de la normalisation de l'Internet pour la communauté Internet, et appelle à la discussion et à des suggestions en vue de son amélioration. Prière de se rapporter à l'édition en cours des "Internet Official Protocol Standards" (normes officielles du protocole Internet) (STD 1) pour connaître l'état de la normalisation et le statut du présent protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

Résumé

Les extensions à la sécurité du système des noms de domaine (DNSSEC, *Domain Name System Security*) introduisaient l'enregistrement de ressource (RR, *resource record*) NSEC pour le déni d'existence authentifié. Le présent document introduit un enregistrement de ressource de remplacement, NSEC3, qui fournit de façon similaire un déni d'existence authentifié. Cependant, il fournit aussi des mesures contre l'énumération de zone et permet une expansion graduelle de zones centées sur la délégation.

Table des Matières

1. Introduction

1.1 Motifs

Les extensions de sécurité du DNS incluaient le RR NSEC pour la fourniture du déni d'existence authentifié. Bien que le RR NSEC satisfasse aux exigences du déni d'existence authentifié, il introduit un effet colatéral qui permet l'énumération du contenu d'une zone. Cette propriété introduit des problèmes de politique indésirables.

L'énumération est activée par l'ensemble des enregistrements NSEC qui existent à l'intérieur d'une zone signée. Un enregistrement NSEC fait la liste des deux noms qui sont ordonnés de façon canonique, afin de montrer que rien n'existe entre les deux noms. L'ensemble complet des enregistrements NSEC fait la liste de tous les noms dans une zone. Il est trivial d'énumérer le contenu d'une zone en l'interrogeant pour des noms qui n'existent pas.

Une énumération de zone peut être utilisée, par exemple, comme source d'adresses de messagerie électronique probables pour des pourriels, ou comme clé d'interrogations WHOIS multiples pour révéler des données d'enregistrement que de nombreux registraires peuvent avoir l'obligation légale de protéger. De nombreux registres interdisent donc la copie de leurs données de zone ; cependant, l'utilisation des RR NSEC rend ces politiques impossibles à mettre en application.

Un second problème est que le coût de délégations cryptographiquement sûres à des zones non signées est élevé, par rapport au bénéfice de sécurité perçu, dans deux cas : de grandes zones centrées sur la délégation, et des zones où des délégations non sûres seront mises à jour rapidement. Dans ces cas, les coûts de maintenance d'une chaîne de RR NSEC peuvent être extrêmement élevés et l'utilisation de la convention "Opt-Out" *(option d'exclusion)* peut être plus approprié (pour ces zones non sûres).

Le présent document présente l'enregistrement de ressourcve NSEC3 qui peut être utilisé comme solution de remplacement à NSEC pour atténuer ces problèmes.

Les travaux antérieurs qui traitent de ces questions sont [DNSEXT-NO], [RFC4956], et [DNSEXT-NSEC2v2].

1.2 Exigences

Les mots clés "DOIT", "NE DOIT PAS", "EXIGRE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT" et "FACULTATIF" dans le présent document sont à interpréter comme décrit dans la [RFC2119].

1.3 Terminologie

Le lecteur est supposé familier des concepts de base du DNS et de DNSSEC décrits dans les [RFC1034], [RFC1035], [RFC4033], [RFC4034], [RFC4035], et les RFC ultérieures qui les mettent à jour : [RFC2136], [RFC2181] et [RFC2308].

La terminologie suivante est utilisée tout au long du présent document :

Énumération de zone : pratique de la découverte du contenu complet d'une zone via des interrogations successives. L'énumération de zone n'était pas triviale avant l'introduction de DNSSEC.

Nom de propriétaire original : nom de propriétaire correspondant à un hachage de nom de propriétaire.

Hachage de nom de propriétaire : nom de propriétaire créé après l'application de la fonction de hachage à un nom de propriétaire.

Ordre de hachage : ordre dans lequel les hachages de noms de propriétaires sont arrangés en accord avec leur valeur numérique, en traitant l'octet le plus à gauche (de plus faible numéro) comme l'octet de plus fort poids. Noter que cet ordre est le même que l'ordre canonique des noms du DNS spécifié dans la [RFC4034], quand le hachage des noms de propriétaires est en base32, codé avec un alphabet hexadécimal étendu [RFC4648].

Non terminal vide : nom de domaine qui ne possède pas d'enregistrement de ressource, mais a un ou plusieurs sous domaines qui en ont.

Délégation : un RRSet NS avec un nom différent du sommet de zone actuel (non sommet de zone) signifiant une délégation à une zone fille.

Délégation sûre : nom contenant une délégation (RRSet NS) et un RRSet DS signé, signifiant une délégation à une zone fille signée.

Délégation non sûre : nom contenant une délégation (RRSet NS) mais n'ayant pas de RRSet DS, ce qui signifie une délégation à une zone fille non signée.

Enregistrement de ressource NSEC3 Opt-Out : enregistrement de ressource NSEC3 qui a le fanion Opt-Out réglé à 1.

Zone Opt-Out : zone avec au moins un RR NSEC3 Opt-Out.

Plus proche incluant : plus long ancêtre existant d'un nom. Voir aussi le paragraphe 3.3.1 de la [RFC4592].

Plus proche incluant prouvable : plus long ancêtre d'un nom dont l'existence peut être prouvée. Noter ceci n'est différent du plus proche incluant que dans une zone Opt-Out.

Prochain plus proche nom : nom plus long d'une étiquette que le plus proche incluant prouvable d'un nom.

Base32 : le codage en "Base 32 avec alphabet hexadécimal étendu" est spécifié dans la [RFC4648]. Noter que les caractères ("=") de bourrage en queue ne sont pas utilisés dans la spécification de NSEC3.

Couvrir : un RR NSEC3 est dit "couvrir" un nom si le hachage du nom ou le "prochain plus proche nom" tombe entre le nom de propriétaire et le prochain hachage de nom de propriétaire du NSEC3. En d'autre termes, si il prouve la non existence du nom, soit directement soit en prouvant la non existence d'un ancêtre du nom.

Correspondre : un RR NSEC3 est dit "correspondre" à un nom si le nom de propriétaire du RR NSEC3 est le même que le hachage de nom de propriétaire de ce nom.

2. Rétro compatibilité

La présente spécification décrit un changement de protocole qui n'est pas généralement rétro compatible avec les [RFC4033], [RFC4034], et [RFC4035]. En particulier, les résolveurs à capacité de sécurité qui ignorent la présente spécification (résolveurs sans capacité NSEC3) peuvent échouer à valider les réponses introduites par le présent document.

Afin d'aider au déploiement, la présente spécification utilise une technique de signalisation pour empêcher les résolveurs sans capacité NSEC3 de tenter de valider des réponses provenant de zones signées NSEC3.

La présente spécification alloue les deux nouveaux identifiants d'algorithme DNSKEY pour cela. L'algorithme 6, DSA-NSEC3-SHA1 est un alias pour l'algorithme 3, DSA. L'algorithme 7, RSASHA1-NSEC3-SHA1 est un alias pour l'algorithme 5, RSASHA1. Ce ne sont pas de nouveaux algorithmes, ce sont des identifiants supplémentaires pour les algorithmes existants.

Les zones signées en accord avec la présente spécification DOIVENT seulement utiliser ces identifiants d'algorithme pour leurs RR DNSKEY. Parce que ces nouveaux identifiants vont être des algorithmes inconnus des résolveurs existants, ignorants de NSEC3, ces résolveurs vont alors traiter les réponses provenant de zones signées NSEC3 comme non sûres, comme précisé au paragraphe 5.2 de la [RFC4035].

Ces identifiants d'algorithme sont utilisés avec l'algorithme de hachage SHA1 NSEC3. Utiliser d'autres algorithmes de hachage NSEC3 exige l'allocation d'un nouvel alias (voir le paragraphe 12.1.3).

Les résolveurs à capacité de sécurité qui appliquent la présente spécification DOIVENT reconnaître les nouveaux identifiants d'algorithme et les traiter comme équivalents aux algorithmes dont ils sont des alias.

Une méthodologie pour passer d'un zone signée DNSSEC à une zone signée en utilisant NSEC3 est discutée au paragraphe 10.4.

3. Enregistrement de ressource NSEC3

L'enregistrement de ressource (RR, *Resource Record*) NSEC3 assure le déni d'existence authentifié des ensembles d'enregistrement de ressource du DNS.

Le RR NSEC3 fait la liste des types présents au nom de propriétaire original du RR NSEC3. Il inclut le prochain hachage de nom de propriétaire dans l'ordre des hachages de la zone. L'ensemble complet des RR NSEC3 dans une zone indique quels RRSets existent pour le nom de propriétaire original du RR et forme une chaîne de noms de propriétaires hachés dans la zone. Cette information est utilisée pour fournir un déni d'existence authentifié pour les données du DNS. Pour fournir la protection contre une énumération de zone, les noms de propriétaires utilisés dans le RR NSEC3 sont des hachages cryptographiques du nom de propriétaire original positionné comme une seule étiquette devant le nom de la zone. Le RR NSEC3 indique quelle fonction de hachage est utilisée pour construire le hachage, quel sel est utilisé, et combien d'itérations de la fonction de hachage sont effectuées sur le nom de propriétaire original. La technique de hachage est décrite à la Section 5.

Les noms hachés de propriétaires de délégations non signées peuvent être exclus de la chaîne. Un RR NSEC3 dont la portée couvre le hachage d'un nom de propriétaire ou le "prochain plus proche" nom d'une délégation non signée est appelé un RR NSEC3 Opt-Out et est indiqué par la présence d'un fanion.

Le nom de propriétaire pour le RR NSEC3 est le codage en base32 du hachage de nom de propriétaire précédant comme une seule étiquette le nom de la zone.

La valeur du type pour le RR NSEC3 est 50.

Le format RDATA de RR NSEC3 est indépendant de la classe et est décrit ci-dessous.

La classe DOIT être la même que celle du nom de propriétaire original.

Le RR NSEC3 DEVRAIT avoir la même valeur de TTL que le champ TTL minimum de SOA. C'est dans l'esprit de la mise en antémémoire négative [RFC2308].

3.1 Champs RDATA

3.1.1 Algorithme de hachage

Le champ Algorithme de hachage identifie l'algorithme de hachage cryptographique utilisé pour construire la valeur du hachage.

Les valeurs pour ce champ sont définies dans le registre des algorithmes de hachage NSEC3 défini à la Section 11.

3.1.2 Fanions

Le champ Fanions contient huit fanions d'un bit qui peuvent être utilisés pour indiquer différents traitements. Tous les fanions non définis doivent être à zéro. Le seul fanion défini par la présente spécification est le fanion Opt-Out.

3.1.2.1 Fanion Opt-Out

Si le fanion Opt-Out est établi, l'enregistrement NSEC3 couvre zéro, une ou plusieurs délégations non signées.

Si le fanion Opt-Out est à zéro, l'enregistrement NSEC3 couvre zéro délégation non signée.

Le fanion Opt-Out indique si ce RR NSEC3 peut couvrir des délégations non signées. Il est le bit de moindre poids dans le champ Fanions. Voir à la Section 6 les détails sur l'utilisation de ce fanion.

3.1.3 Itérations

Le champ Itérations définit le nombre de fois que la fonction de hachage doit être effectuée. Plus d'itérations résultent en une plus grande résilience de la valeur de hachage contre les attaques de dictionnaire, mais avec un coût de calcul plus élevé pour le serveur et le résolveur. Voir à la Section 5 les détails de l'utilisation de ce champ, et au paragraphe 10.3 les limitations sur la valeur.

3.1.4 Longueur de sel

Le champ Longueur de sel définit la longueur du champ Sel en octets, dans la gamme de 0 à 255.

3.1.5 Sel

Le champ Sel est ajouté au nom de propriétaire original avant le hachage afin de défendre contre les attaques de dictionnaire pré-calculées. Voir à la Section 5 les détails de la façon dont le sel est utilisé.

3.1.6 Longueur de hachage

Le champ Longueur de hachage définit la longueur du champ Prochain nom de propriétaire haché, dans la gamme de 1 à 255 octets.

3.1.7 Prochain nom de propriétaire haché

Le champ Prochain nom de propriétaire haché contient le prochain hachage de nom de propriétaire dans l'ordre des hachages. Cette valeur est en format binaire. Étant donné l'ordre de tous les noms de propriétaires hachés, le champ Prochain nom de propriétaire haché contient le hachage d'un nom de propriétaire qui suit immédiatement le nom de propriétaire du RR NSEC3 donné. La valeur du champ Prochain nom de propriétaire haché dans le dernier RR NSEC3 dans la zone est le même que le hachage de nom de propriétaire du premier RR NSEC3 dans l'ordre de hachage de la zone.

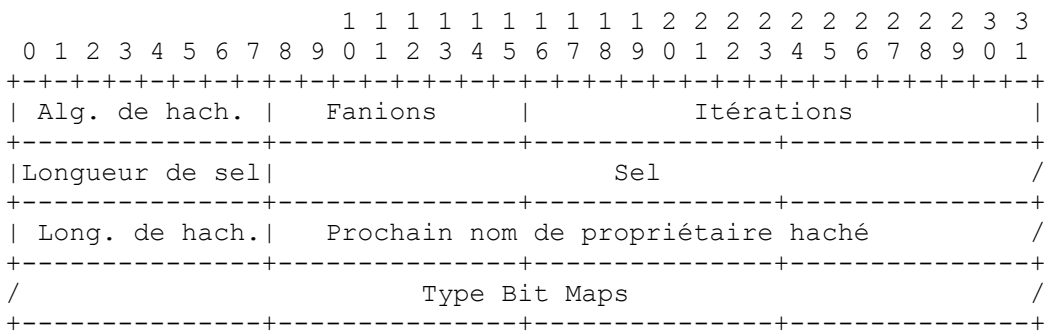
Noter que, à la différence du nom de propriétaire du RR NSEC3, la valeur de ce champ ne contient pas le nom de zone ajouté.

3.1.8 Type Bit Maps

Le champ Type Bit Maps *(concordance de bits)* identifie les types de RRSet qui existent au nom de propriétaire original du RR NSEC3.

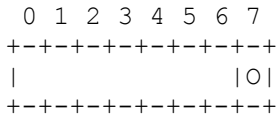
3.2 Format de RDATA NSEC3 sur le réseau

Les RDATA du RR NSEC3 sont comme montré ci-dessous :



Algorithme de hachage est d'un seul octet.

Le champ Fanions est d'un seul octet, le fanion Opt-Out est le bit de moindre poids, comme montré ci-dessous :



Itérations est représenté par un entier non signé de 16 bits, avec le bit de poids fort en premier.

Longueur de sel est représenté par un octet non signé. Longueur de sel représente la longueur du champ Sel en octets. Si la valeur est zéro, le champ Sel suivant est omis.

Sel, si il est présent, est codé comme une séquence d'octets binaires. La longueur de ce champ est déterminée par le champ Longueur de sel précédant.

Longueur de hachage est représenté par un octet non signé. Longeur de hachage représente la longueur du champ Prochain nom de propriétaire haché en octets.

Le prochain hachage de nom de propriétaire n'est pas codé en base32, à la différence du nom de propriétaire du RR NSEC3. Il est la valeur de hachage binaire non modifiée. Il n'inclut pas le nom de la zone contenante. La longueur de ce champ est déterminée par le champ Longueur de hachage précédant.

3.2.1 Codage de type Bit Maps

Le codage du champ Type Bit Maps *(matrice de bits)* est le même que celui utilisé par le RR NSEC, décrit dans la [RFC4034]. Il est expliqué et précisé ici pour être clair.

L'espace de type de RR est partagé en 256 blocs de fenêtres, chacune représentant les 8 bits de moindre poids de l'espace de type de RR de 16 bits. Chaque bloc qui a au moins un type de RR actif est codé en utilisant un numéro de fenêtre d'un seul octet (de 0 à 255), une longueur de matrice de bits d'un seul octet (de 1 à 32) indiquant le nombre d'octets utilisés pour la matrice de bits du bloc de fenêtre, et jusqu'à 32 octets (256 bits) de matrice de bits.

Les blocs sont présents dans les RDATA de RR NSEC3 en ordre numérique croissant.

Champ Type de Bit Maps = (n° de bloc de fenêtre | Longueur de Bitmap | Bitmap)+

où "|" note l'enchaînement.

Chaque matrice de bits code les 8 bits de moindre poids des types de RR au sein du bloc de fenêtre, dans l'ordre des bits du réseau. Le premier bit est le bit 0. Pour le bloc de fenêtre 0, le bit 1 correspond au type de RR 1 (A), le bit 2 correspond au type de RR 2 (NS), et ainsi de suite. Pour le bloc de fenêtre 1, le bit 1 correspond au type de RR 257, le bit 2 au type de RR 258. Si un bit est réglé à 1, il indique qu'un RRSet de ce type est présent pour le nom de propriétaire original du RR NSEC3. Si un bit est réglé à 0, il indique qu'aucun RRSet de ce type n'est présent pour le nom de propriétaire original du RR NSEC3.

Comme le bit 0 dans le bloc de fenêtre 0 se réfère au type de RR non existant 0, il DOIT être réglé à 0. Après vérification, le valideur DOIT ignorer la valeur du bit 0 dans le bloc de fenêtre 0.

Les bits qui représentent des Meta-TYPE ou des QTYPE comme spécifié au paragraphe 3.1 de la [RFC2929] ou dans la gamme réservée seulement aux allocations de QTYPE et Meta-TYPE DOIVENT être réglés à 0, car il n'apparaissent pas dans les données de zone. Si il en est rencontré, ils doivent être ignorés à la lecture.

Les blocs sans type présent NE DOIVENT PAS être inclus. Les octets de zéros en queue dans la matrice de bits DOIVENT être omis. La longueur de la matrice de bits de chaque bloc est déterminée par le code de type avec la plus grande valeur numérique, au sein de ce bloc, parmi l'ensemble des types de RR présents au nom de propriétaire original du RR NSEC3. Les octets de queue non spécifiés DOIVENT être interprétés comme des octets à zéro.

3.3 Format de présentation

Le format de présentation de la portion RDATA est le suivant :

- Le champ Algorithme de hachage est représenté par un entier décimal non signé. La valeur maximum est 255.
- Le champ Fanions est représenté par un entier décimal non signé. Sa valeur maximum est 255.
- Le champ Itérations est représenté par un entier décimal non signé. Sa valeur est entre 0 et 65535, inclus.
- Le champ Longueur de sel n'est pas représenté.
- Le champ Sel est représenté par une séquence de chiffres hexadécimaux insensibles à la casse. Les espaces ne sont pas permis dans la séquence. Le champ Sel est représentée comme "-" (sans les guillemets) quand le champ Longueur de sel a une valeur de 0.
- Le champ Longueur de hachage n'est pas représenté.
- Le champ Prochain nom de propriétaire haché est représenté par une séquence non bourrée de chiffres base32 insensibles à la casse, sans espace.
- Le champ Type Bit Maps est représenté par une séquence de mnémoniques de types de RR. Quand le mnémonique n'est pas connu, la représentation TYPE décrite à la Section 5 de la [RFC3597] DOIT être utilisée.

4. Enregistrement de ressource NSEC3PARAM

Le RR NSEC3PARAM contient les paramètres de NSEC3 (algorithme de hachage, fanions, itérations, et sel) nécessaires aux serveurs d'autorité pour calculer les noms de propriétaires hachés. La présence d'un RR NSEC3PARAM à un sommet de zone indique que les paramètres spécifiés peuvent être utilisés par les serveurs d'autorité pour choisir un ensemble approprié des RR NSEC3 pour des réponses négatives. Le RR NSEC3PARAM n'est pas utilisé par les valideurs ou résolveurs.

Si un RR NSEC3PARAM est présent au sommet d'une zone avec une valeur de champ Fanions de zéro, alors il DOIT être un RR NSEC3 utilisant les mêmes paramètres algorithme de hachage, itérations, et sel présents à chaque hachage de nom de propriétaire dans la zone. C'est-à-dire, la zone DOIT contenir un ensemble complet de RR NSEC3 avec les mêmes paramètres algorithme de hachage, itérations, et sel.

Le nom de propriétaire pour le RR NSEC3PARAM est le nom du sommet de la zone.

La valeur de type pour le RR NSEC3PARAM est 51.

Le format de RDATA du RR NSEC3PARAM est indépendant de la classe et est décrit ci-dessous.

La classe DOIT être la même que celle des RR NSEC3 auxquels ce RR se réfère.

4.1 Champs RDATA

Les RDATA pour ce RR reflètent les quatre premiers champs du RR NSEC3.

4.1.1 Algorithme de hachage

Le champ Algorithme de hachage identifie l'algorithme de hachage cryptographique utilisé pour construire la valeur du hachage.

Les valeurs acceptables sont les mêmes que celle du champ correspondant dans le RR NSEC3.

4.1.2 Champ Fanions

Le fanion Opt-Out n'est pas utilisé et est réglé à zero.
Tous les autres fanions sont réservés pour une utilisation future, et doivent être à zéro.
Les RR NSEC3PARAM avec une valeur du champ Fanions autre que zéro DOIVENT être ignorés.

4.1.3 Itérations

Le champ Itérations définit le nombre de fois supplémentaires que le hachage est effectué.
Ses valeurs acceptables sont les mêmes que celles du champ correspondant dans le RR NSEC3.

4.1.4 Longueur de sel

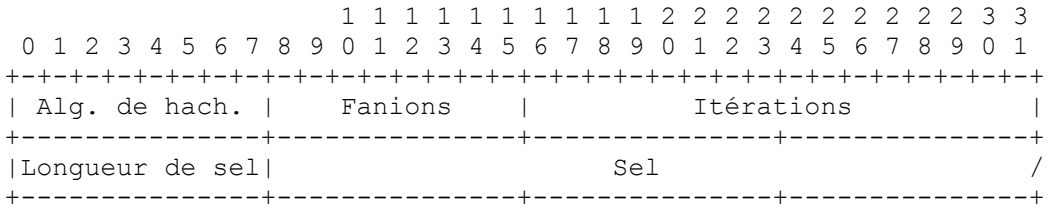
Le champ Longueur de sel définit la longueur du sel en octets, de 0 à 255.

4.1.5 Sel

Le champ Sel est ajouté au nom de propriétaire original avant le hachage.

4.2 Format de RDATA NSEC3PARAM sur le réseau

Les RDATA du RR NSEC3PARAM sont comme montré ci-dessous :



Algorithme de hachage est d'un seul octet.

Le champ Fanions est d'un seul octet.

Itérations est représenté par un entier non signé de 16 bits, le bit de poids fort en premier.

Longueur de sel est représenté par un octet non signé. La longueur de sel représente la longueur du champ Sel qui suit en octets. Si la valeur est zéro, le champ Sel est omis.

Sel, si il est présent, est codé comme une séquence d'octets binaires. La longueur de ce champ est déterminée par le champ Longueur de sel précédent.

4.3 Format de présentation

Le format de présentation de la portion RDATA est le suivant :

- Le champ Algorithme de hachage est représenté par un entier décimal non signé. Sa valeur a un maximum de 255.
- Le champ Fanion est représenté par un entier décimal non signé. Sa valeur a un maximum de 255.
- Le champ Itérations est représenté par un entier décimal non signé. Sa valeur est entre 0 et 65535, inclus.
- Le champ Longueur de sel n'est pas représenté.
- Le champ Sel est représenté par une séquence de chiffres hexadécimaux insensibles à la casse. Les espaces ne sont pas permises dans la séquence. Ce champ est représenté par "-" (sans les guillemens) quand le champ Longueur de sel est zéro.

5. Calcul du hachage

Le calcul du hachage utilise trois champs de RDATA NSEC3 : Algorithme de hachage, Sel, et Itérations.

Définir H(x) comme étant le hachage de x en utilisant l'algorithme de hachage choisi par le RR NSEC3, k comme étant le nombre d'itérations, et || pour indiquer l'enchaînement. Puis définir :

IH(sel, x, 0) = H(x || sel), et IH(sel, x, k) = H(IH(sel, x, k-1) || sel), si k > 0

Alors le hachage calculé d'un nom de propriétaire est :

IH(sel, nom de propriétaire, itérations),

où le nom de propriétaire est dans la forme canonique, définie comme :
Le format du réseau du nom de propriétaire où:
1. Le nom de propriétaire est pleinement expansé (pas de compression de nom DNS) et pleinement qualifié ;
2. toutes les lettres US-ASCII majuscules sont remplacées par les lettres US-ASCII minuscules correspondantes ;
3. si le nom de propriétaire est un nom avec un caractère générique, le nom de propriétaire est dans sa forme originale non expansée, incluant l'étiquette "*" (pas de substitution de caractère générique).

Cette forme est définie au paragraphe 6.2 de la [RFC4034].
La méthode pour calculer le hachage se fonde sur la [RFC2898].

6. Opt-Out

Dans la présente spécification, comme dans les [RFC4033], [RFC4034] et [RFC4035], les RRSet NS aux points de délégation ne sont pas signés et peuvent être accompagnés d'un RRSet DS. Avec le bit Opt-Out à zéro, l'état de sécurité de la zone fille est déterminé par la présence ou l'absence de ce RRSet DS, prouvé cryptographiquement par le RR NSEC3 signé au hachage de nom de propriétaire de la délégation. Établir le fanion Opt-Out modifie cela en permettant que des délégations non sûres existent dans la zone signée sans un RR NSEC3 correspondant au hachage de nom de propriétaire de la délégation.

Un RR NSEC3 Opt-Out est dit couvrir une délégation si le hachage du nom de propriétaire ou si le "prochain plus proche" nom de la délégation est entre le nom de propriétaire du RR NSEC3 et le prochain hachage de nom de propriétaire.

Un RR NSEC3 Opt-Out n'affirme pas l'existence ou la non existence des délégations non sûres qu'il peut couvrir. Cela permet l'ajout ou la suppression de ces délégations sans avoir à recalculer ou re-signer les RR dans la chaîne de RR NSEC3. Cependant, les RR NSEC3 Opt-Out affirment bien l'existence (non existence) d'autres RRSet d'autorité.

Un RR NSEC3 Opt-Out PEUT avoir le même nom de propriétaire original qu'une délégation non sûre. Dans ce cas, la délégation est prouvée non sûre par l'absence d'un bit DS dans le type map et le RR NSEC3 signé n'affirme pas l'existence de la délégation.

Des zones qui utilisent Opt-Out PEUVENT contenir un mélange de RR NSEC3 Opt-Out et non Opt-Out. Si un RR NSEC3 est non Opt-Out, il NE DOIT PAS y avoir de noms de propriétaires hachés de délégations non sûres (ni aucun autre RR) entre lui et le nom indiqué par le prochain hachage de nom de propriétaire dans les RDATA NSEC3. Si il est Opt-Out, il DOIT seulement couvrir des noms de propriétaires hachés ou des noms hachés de "prochain plus proche" de délégations non sûres.

Les effets du fanion Opt-Out sur la signature, le service, et les réponses de validation sont traités dans les paragraphes suivants.

7. Considérations de serveur d'autorité

7.1 Signature de zone

Les zones qui utilisent NSEC3 doivent satisfaire les propriétés suivantes :

- Chaque nom de propriétaire dans la zone qui possède des RRSet d'autorité DOIT avoir un RR NSEC3 correspondant. Les noms de propriétaire qui correspondent aux délégations non signées PEUVENT avoir un RR NSEC3 correspondant. Cependant, si il n'y a pas de RR NSEC3 correspondant, il DOIT y avoir un RR NSEC3 Opt-Out qui couvre le "prochain plus proche" nom pour la délégation. Les autres RR non d'autorité ne sont pas représentés par les RR NSEC3.

- Chaque non terminal vide DOIT avoir un RR NSEC3 correspondant, sauf si le non terminal vide est seulement déduit d'une délégation non sûre couverte par un RR NSEC3 Opt-Out.

- La valeur de TTL pour tout RR NSEC3 DEVRAIT être la même que celle du champ Valeur minimum de TTL dans le RR SOA de la zone.

- Le champ Type Bit Maps de tout RR NSEC3 dans une zone signée DOIT indiquer la présence de tous les types présents au nom de propriétaire original, sauf pour les types seulement contribués par un RR NSEC3 lui-même. Noter que cela signifie que le type NSEC3 lui-même ne va jamais être présent dans le type Bit Maps.

Les étapes suivantes décrivent une méthode de construction appropriée des RR NSEC3. Ce n'est pas la seule méthode possible.

1. Choisir l'algorithme de hachage et les valeurs de sel et d'itérations.

2. Pour chaque nom de propriétaire original unique dans la zone, ajouter un RR NSEC3.
   * Si Opt-Out est utilisé, les noms de propriétaires de délégations non signées PEUVENT être exclus.
   * Le nom de propriétaire du RR NSEC3 est le hachage du nom de propriétaire original, précédant d'une seule étiquette le nom de zone.
   * Le champ Prochain nom de propriétaire haché est laissé en blanc pour le moment.
   * Si Opt-Out est utilisé, régler le bit Opt-Out à un.
   * Pour les besoins de la détection de collision, on garde facultativement trace du nom de propriétaire original avec le RR NSEC3.
   * De plus, pour les besoins de la détection de collision, on crée facultativement un RR NSEC3 supplémentaire correspondant au nom de propriétaire original avec l'étiquette astérisque devant (c'est-à-dire, comme si un caractère générique existait comme fils de ce nom de propriétaire) et garder trace de ce nom de propriétaire original. Marquer ce RR NSEC3 comme temporaire.

3. Pour chaque RRSet au nom de propriétaire original, établir le bit correspondant dans le champ Type Bit Maps.

4. Si la différence en nombre d'étiquettes entre le sommet et le nom de propriétaire original est supérieur à 1, des RR NSEC3 doivent être ajoutés pour chaque non terminal vide entre le sommet et le nom de propriétaire original. Ce processus peut générer des RR NSEC3 avec des noms de propriétaires hachés dupliqués. Facultativement, pour la détection de collision, garder trace des noms de propriétaires originaux de ces RR NSEC3 et créer des RR NSEC3 temporaires pour les collisions de caractères génériques de la même façon qu'à l'étape 1.

5. Trier l'ensemble des RR NSEC3 dans l'ordre du hachage.

6. Combiner les RR NSEC3 avec des noms de propriétaires hachés identiques en les remplaçant par un seul RR NSEC3 avec le champ Type Bit Maps consistant en l'union des types représentés par l'ensemble des RR NSEC3. Si le nom de propriétaire original a été suivi, alors les collisions peuvent être détectées sans les combiner, car tous les RR NSEC3 correspondants devraient avoir le même nom de propriétaire original. Éliminer autant que possible des RR NSEC3 temporaires.

7. Dans chaque RR NSEC3, insérer le prochain hachage de nom de propriétaire en utilisant la valeur du prochain RR NSEC3 dans l'ordre du hachage. Le prochain hachage de nom de propriétaire du dernier RR NSEC3 dans la zone contient la valeur du hachage de nom de propriétaire du premier RR NSEC3 dans l'ordre de hachage.

8. Finalement, ajouter un RR NSEC3PARAM avec les mêmes champs Algorithme de hachage, Itérations, et Sel au sommet de zone.

Si une collision de hachage est détectée, alors un nouveau sel doit être choisi, et le processus de signature est redémarré.

7.2 Desserte de zone

La présente spécification modifie les réponses DNS à capacité DNSSEC générées par les serveurs d'autorité. En particulier, elle remplace l'utilisation des RR NSEC dans ces réponses par les RR NSEC3.

Dans les cas de réponse suivants, les RR NSEC imposés par DNSSEC [RFC4035] sont remplacés par les RR NSEC3 qui prouvent les mêmes faits. Les réponses qui ne vont pas contenir de RR NSEC sont inchangées par cette spécification.

Quand ils retournent des réponses contenant plusieurs RR NSEC3, tous les RR NSEC3 DOIVENT utiliser les mêmes valeurs d'algorithme de hachage, d'itération, et de sel. La valeur du champ Fanions DOIT être zéro ou un.

7.2.1 Preuve de plus proche incluant

Pour de nombreuses réponses NSEC3 une preuve du plus proche incluant est requise. C'est une preuve qu'un ancêtre du QNAME est le plus proche incluant du QNAME.

Cette preuve consiste en jusqu'à deux RR NSEC3 différents :
- un RR NSEC3 qui correspond au plus proche incluant (démontrable) ;
- un RR NSEC3 qui couvre le "prochain plus proche" nom pour le plus proche incluant.

Le premier RR NSEC3 propose essentiellement un plus proche incluant possible, et prouve que l'incluant particulier existe bien. Le second RR NSEC3 prouve que le plus proche incluant possible est le plus proche, et prouve que le QNAME (et tous les ancêtres entre le QNAME et le plus proche incluant) n'existe pas.

Ces RR NSEC3 sont collectivement appelés la "preuve de plus proche incluant" dans les descriptions suivantes.

Par exemple, la preuve du plus proche incluant pour le nom de propriétaire non existant "alpha.beta.gamma.exemple." pourrait prouver que "gamma.exemple." est le plus proche incluant. Cette réponse contiendrait le RR NSEC3 qui correspond à "gamma.exemple.", et contiendrait aussi le RR NSEC3 qui couvre "beta.gamma.exemple." (qui est le nom "prochain plus proche").

Il est possible, quand on utilise Opt-Out (Section 6) de n'être pas capable de prouver le réel plus proche incluant parce qu'il est, ou fait partie d'une délégation non sûre couverte par une portée Opt-Out. Dans ce cas, au lieu de prouver le plus proche incluant réel, le plus proche incluant prouvable est utilisé. C'est-à-dire, le nom d'autorité le plus proche incluant est utilisé à la place. Dans ce cas, l'ensemble des RR NSEC3 utilisé pour cette preuve est appelé la "preuve du plus proche incluant prouvable".

7.2.2 Réponses d'erreur de nom

Pour prouver la non existence de QNAME, une preuve de plus proche incluant et un RR NSEC3 couvrant le (non existant) RR à caractère générique au plus proche incluant DOIT être inclus dans la réponse. Cette collection de jusqu'à trois RR NSEC3 prouve à la fois que ce QNAME n'existe pas et qu'un caractère générique qui pourrait avoir correspondu au QNAME n'existe pas non plus.

Par exemple, si "gamma.exemple." est le plus proche incluant prouvable du QNAME, alors un RR NSEC3 couvrant "*.gamma.exemple." est inclus dans la section d'autorité de la réponse.

7.2.3 Réponses No Data, où le QTYPE n'est pas DS

Le serveur DOIT inclure le RR NSEC3 qui correpond au QNAME. Ce RR NSEC3 NE DOIT PAS avoir les bits correspondant au QTYPE ou CNAME établis dans son champ Type Bit Maps.

7.2.4 Réponses No Data avec DS pour QTYPE

Si il y a un RR NSEC3 qui correspond au QNAME, le serveur DOIT le retourner dans la réponse. Les bits correspondants au DS et CNAME NE DOIVENT PAS être établis dans le champ Type Bit Maps de ce RR NSEC3.

Si aucun RR NSEC3 ne correspond au QNAME, le serveur DOIT retourner une preuve de plus proche incluant prouvable pour le QNAME. Le RR NSEC3 qui couvre le "prochain plus proche" nom DOIT avoir le bit Opt-Out établi (noter que c'est vrai par définition -- si le bit Opt-Out n'est pas établi, quelque chose va de travers).

Si un serveur est d'autorité pour les deux côtés d'une coupure de zone au QNAME, le serveur DOIT retourner la preuve à partir du côté parent de la coupure de zone.

7.2.5 Réponses No Data avec caractères génériques

Si il y a une correspondance de caractère générique pour le QNAME, mais qu'un QTYPE n'est pas présent à ce nom, la réponse DOIT inclure une preuve de plus proche incluant pour le QNAME et DOIT inclure le RR NSEC3 qui correspond au caractère générique. Cette combinaison prouve à la fois que le QNAME lui-même n'existe pas et qu'un caractère générique qui correspond au QNAME existe bien. Noter que le plus proche incluant du QNAME DOIT être l'ancêtre immédiat du RR à caractère générique (si ce n'est pas le cas, alors quelque chose va de travers).

7.2.6 Réponses avec caractères génériques

Si il y a une correspondance de caractère générique pour le QNAME et QTYPE, alors, en plus du RRSet à expansion de caractère générique retourné dans la section réponse de la réponse, la preuve que la correspondance de caractère générique était valide doit être retournée.

Cette preuve est réalisée en prouvant à la fois que le QNAME n'existe pas et que le plus proche incluant du QNAME et l'ancêtre immédiat du caractère générique sont le même (c'est-à-dire, que le caractère générique correct correspond).

À cette fin, le RR NSEC3 qui couvre le "prochain plus proche" nom de l'ancêtre immédiat du caractère générique DOIT être retourné. Il n'est pas nécessaire de retourner un RR NSEC3 qui correspond au plus proche incluant, car l'existence de ce plus proche incluant est prouvée par la présence du caractère générique expansé dans la réponse.

7.2.7 Références à des sous zones non signées

Si il y a un RR NSEC3 qui correspond au nom de délégation, alors ce RR NSEC3 DOIT être inclus dans la réponse. Le bit DS dans le type bit maps du RR NSEC3 NE DOIT PAS être établi.

Si la zone est Opt-Out, alors il ne peut pas y avoir de RR NSEC3 correspondant à la délégation. Dans ce cas, la preuve de plus proche incluant prouvable DOIT être incluse dans la réponse. Le RR NSEC3 inclus qui couvre le "prochain plus proche" nom pour la délégation DOIT avoir le fanion Opt-Out réglé à un. (Noter que cela va être le cas sauf si quelque chose va de travers).

7.2.8 Réponse aux interrogations sur des noms de propriétaire de NSEC3

Les noms de propriétaires des RR NSEC3 ne sont pas représentés dans la chaîne de RR NSEC3 comme les autres noms de propriétaires. Par suite, chaque nom de propriétaire NSEC3 est couvert par un autre RR NSEC3, niant effectivement l'existence du RR NSEC3. C'est un paradoxe, car l'existence d'un RR NSEC3 peut être prouvée par son RRSet RRSIG.

Si les conditions suivantes sont toutes vraies :
- o le QNAME est égal au nom de propriétaire d'un RR NSEC3 existant, et
- o aucun type de RR n'existe au QNAME, ni à un descendant du QNAME,

alors la réponse DOIT être construite comme une réponse Erreur de nom (paragraphe 7.2.2). Ou en d'autres termes, le serveur de noms d'autorité va agir comme si le nom de propriétaire du RR NSEC3 n'existait pas.

Noter que les RR NSEC3 sont retournés par suite d'une interrogation AXFR ou IXFR.

7.2.9 Réponse de serveur à une collision au moment du démarrage

Si le hachage d'un QNAME non existant entre en collision avec le nom de propriétaire d'un RR NSEC3 existant, alors le serveur ne va pas être capable de retourner une réponse qui prouve que le QNAME n'existe pas. Dans ce cas, le serveur DOIT retourner une réponse avec un RCODE de 2 (défaillance du serveur).

Noter qu'avec l'algorithme de hachage spécifié dans ce document, SHA-1, de telles collisions sont très improbables.

7.3 Serveurs secondaires

Les serveurs secondaires (et peut-être d'autres entités) ont besoin de déterminer de façon fiable quels paramètres NSEC3 (c'est-à-dire, hachage, sel, et itérations) sont présents à chaque hachage de nom de propriétaire, afin d'être capables de choisir un ensemble approprié de RR NSEC3 pour des réponses négatives. Ceci est indiqué par la présence d'un RR NSEC3PARAM au sommet de la zone.

Si il y a plusieurs RR NSEC3PARAM présents, il y a plusieurs chaînes NSEC3 valides présentes. Le serveur doit en choisir une, mais peut utiliser tout critère de son choix.

7.4 Zones utilisant des algorithmes de hachage inconnus

Les zones qui sont signées en accord avec la présente spécification, mais utilisent une valeur d'algorithme de hachage NSEC3 non reconnue, ne peuvent pas être servies efficacement. Ces zones DEVRAIENT être rejetées au chargement. Les serveurs DEVRAIENT répondre avec un RCODE=2 (défaillance de serveur) quand ils traitent des interrogations qui tomberaient dans de telles zones.

7.5 Mise à jour dynamique

Une zone signée en utilisant NSEC3 peut accepter des mises à jour dynamiques [RFC2136]. Cependant, NSEC3 introduit des considérations particulières pour les mises à jour dynamiques.

L'ajout et la suppression de noms dans une zone DOIT compter pour la création ou suppression de non terminaux vides.

- Quand on supprime un nom avec un RR NSEC3 correspondant, tous les RR NSEC3 correspondant à des non terminaux vides créés par ce nom DOIVENT être supprimés. Noter que plus d'un nom peut affirmer l'existence d'un non terminal vide particulier.

- Quand on ajoute un nom qui exige l'ajout d'un RR NSEC3, les RR NSEC3 DOIVENT aussi être ajoutés pour tout non terminal vide qui est créé. C'est-à-dire, si il n'y a pas de RR NSEC3 existant qui corresponde à un non terminal vide, il doit être créé et ajouté.

La présence de Opt-Out dans une zone signifie que des ajouts ou des délégations de noms n'exigeront pas de changement aux RR NSEC3 dans une zone.

- Quand on supprime un RRSet de délégation, si cette délégation n'a pas un RR NSEC3 correspondant, alors il a été exclu. Dans ce cas, rien de plus n'a besoin d'être fait.

- Quand on ajoute un RRSet de délégation, si le "prochain plus proche" nom de la délégation est couvert par un RR NSEC3 Opt-Out existant, alors la délégation PEUT être ajoutée sans modifier les RR NSEC3 dans la zone.

La présence de Opt-Out dans une zone signifie que quand on ajoute ou supprime des RR NSEC3, la valeur du fanion Opt-Out qui devrait être établie dans les RR NSEC3 nouveaux ou modifiés est ambiguë. Les serveurs DEVRAIENT suivre cet ensemble de règles de base pour résoudre l'ambiguité.

Le concept central de ces règles est que l'état du fanion Opt-Out du RR NSEC3 couvrant est préservé.

- Quand on supprime un RR NSEC3, la valeur du fanion Opt-Out pour le RR NSEC3 précédent (celui dont le prochain hachage de nom de propriétaire est modifié) ne devrait pas être changée.

- Quand on ajoute un RR NSEC3, la valeur du fanion Opt-Out est réglée à la valeur du fanion Opt-Out du RR NSEC3 qui couvrait précédemment le nom de propriétaire du RR NSEC3. C'est-à-dire, le RR NSEC3 qui est maintenant devenu le précédent.

Si la zone en question est cohérente avec son utilisation du fanion Opt-Out (c'est-à-dire, si tous les RR NSEC3 dans la zone ont la même valeur pour le fanion) alors ces règles vont conserver cette cohérence. Si la zone n'est pas cohérente dans l'utilisation du fanion (c'est-à-dire, une zone partiellement Opt-Out) alors ces règles ne vont pas conserver le même schéma d'utilisation du fanion Opt-Out.

Pour les zones qui utilisent partiellement le fanion Opt-Out, si il y a un schéma logique pour cet usage, le schéma pourrait être conservé en utilisant une politique locale au serveur.

8. Considérations de valideur

8.1 Réponses avec des types de hachage inconnu

Un valideur DOIT ignorer les RR NSEC3 avec des types de hachage inconnus. Le résultat pratique en est que les réponses contenant seulement de tels RR NSEC3 vont généralement être considérées comme boguées.

8.2 Vérification des RR NSEC3

Un valideur DOIT ignorer les RR NSEC3 avec une valeur de champ Fanions autre que zéro ou un.

Un valideur PEUT traiter une réponse comme boguée si la réponse contient des RR NSEC3 avec des valeurs pour l'algorithme de hachage, les itérations, ou le sel, différentes les unes des autres pour cette zone.

8.3 Preuve de plus proche incluant

Afin de vérifier une preuve de plus proche incluant, le valideur DOIT trouver le plus long nom, X, tel que :

- o X soit un ancêtre du QNAME auquel correspond un RR NSEC3 présent dans la réponse. C'est un candidat pour le plus proche incluant, et
- o le nom plus long d'une étiquette que X (mais toujours un ancêtre de -- ou égal à -- QNAME) est couvert par un RR NSEC3 présent dans la réponse.

Un algorithme possible pour vérifier cette preuve est :

1. Régler SNAME=QNAME. Mettre le fanion à zéro.

2. Vérifier si SNAME existe :
   * Si il n'y a pas de RR NSEC3 dans la réponse qui corresponde à SNAME (c'est-à-dire, un RR NSEC3 dont le nom de propriétaire soit le même que dans le hachage de SNAME, ajouté comme une seule étiquette devant le nom de zone) mettre le fanion à zéro.
   * Si il y a un RR NSEC3 dans la réponse qui couvre le SNAME, établir le fanion.
   * Si il y a un RR NSEC3 qui correspond dans la réponse et si le fanion était établi, alors la preuve est complète, et le SNAME est le plus proche incluant.
   * Si il y a un RR NSEC3 correspondant dans la réponse, mais si le fanion n'est pas établi, alors la réponse est boguée.

3. Raccourcir le SNAME d'une étiquette sur la gauche, et repasser à l'étape 2.

Une fois que le plus proche incluant a été découvert, le valideur DOIT vérifier que le RR NSEC3 qui a le plus proche incluant comme nom de propriétaire original provient de la zone appropriée. Le bit Type de DNAME ne doit pas être établi et le bit de type NS peut seulement être établi si le bit Type de SOA est établi. Si ce n'est pas le cas, cela va être l'indication qu'un attaquant les utilise pour dénier faussement l'existence des RR pour lesquels le serveur n'est pas d'autorité.

Dans les descriptions qui suivent, la phrase "une preuve de plus proche incluant (prouvable) pour X" signifie que l'algorithme ci-dessus (ou un algorithme équivalent) prouve que X n'existe pas en prouvant qu'un ancêtre de X est son plus proche incluant.

8.4 Validation de réponses d'erreur de nom

Un valideur DOIT vérifier qu'il y a une preuve de plus proche incluant pour le QNAME présent dans la réponse et que il y a un RR NSEC3 qui couvre le caractère générique au plus proche incluant (c'est-à-dire, le nom formé en ajoutant l'étiquette astérisque au plus proche incluant).

8.5 Validation de réponses No Data où le QTYPE n'est pas DS

Le valideur DOIT vérifier qu'un RR NSEC3 qui correspond au QNAME est présent et que les deux types QTYPE et CNAME ne sont pas établis dans son champ Type Bit Maps.

Noter que cet essai couvre aussi le cas où le RR NSEC3 existe parcc que il correspond à un non terminal vide, et dans ce cas le RR NSEC3 va avoir un champ Type Bit Maps vide.

8.6 Validation de réponses No Data avec DS pour QTYPE

Si il y a un RR NSEC3 qui correspond au QNAME présent dans la réponse, alors ce RR NSEC3 NE DOIT PAS avoir les bits correspondants à DS et CNAME établis dans son champ Type Bit Maps.

Si il n'y a pas de tel RR NSEC3, alors le valideur DOIT vérifier qu'une preuve de plus proche incluant prouvable pour le QNAME est présente dans la réponse, et que le RR NSEC3 qui couvre le "prochain plus proche" nom a le bit Opt-Out établi.

8.7 Validation de réponses No Data avec des caractères génériques

Le valideur DOIT vérifier une preuve de plus proche incluant pour QNAME et DOIT trouver un RR NSEC3 présent dans la réponse qui corresponde au nom à caractère générique généré par l'ajout de l'étiquette astérisque au plus proche incluant. De plus, les bits correspondants au QTYPE et au CNAME NE DOIVENT PAS être établis dans le RR NSEC3 à caractère générique correspondant.

8.8 Validation de réponses avec des caractères génériques

Le RRSet de réponse à caractère générique vérifié dans la réponse donne au valideur un (candidat) plus proche incluant pour le QNAME. Ce plus proche incluant est l'ancêtre immédiat du caractère générique générateur.

Les valideurs DOIVENT vérifier qu'il y a un RR NSEC3 qui couvre le "prochain plus proche" nom du QNAME présent dans la réponse. Cela prouve que le QNAME lui-même n'existe pas et que le caractère générique correct a été utilisé pour générer la réponse.

8.9 Références de validation à des sous zones non signées

Le nom de délégation dans une référence est le nom de propriétaire du RRSet NS présent dans la section d'autorité de la réponse de référence.

Si il y a un RR NSEC3 présent dans la réponse qui correspond au nom de délégation, alors le valideur DOIT s'assurer que le bit NS est établi et que le bit DS n'est pas établi dans le champ Type Bit Maps du RR NSEC3. Le valideur DOIT aussi s'assurer que le RR NSEC3 provient de la zone correcte (c'est-à-dire, parente). Cela est fait en s'assurant que le bit SOA n'est pas établi dans le champ Type Bit Maps de ce RR NSEC3.

Noter que la présence d'un bit NS implique l'absence d'un bit DNAME, de sorte qu'il n'est pas besoin de vérifier le bit DNAME dans le champ Type Bit Maps du RR NSEC3.

Si il n'y a pas de RR NSEC3 présent qui corresponde au nom de délégation, alors le valideur DOIT vérifier une preuve de plus proche incluant prouvable pour le nom de délégation. Le valideur DOIT vérifier que le bit Opt-Out est établi dans le RR NSEC3 qui couvre le "prochain plus proche" nom au nom de délégation.

9. Considérations de résolveur

9.1 Mise en antémémoire d'enregistrement de ressource NSEC3

Les résolveurs qui mettent en antémémoire DOIVENT être capables de restituer les RR NSEC3 appropriés quand ils retournent des réponses qui les contiennent. Dans DNSSEC [RFC4035], il est possible dans de nombreux cas de trouver le RR NSEC correct à retourner dans une réponse par nom (par exemple, quand il retourne une référence, le RR NSEC va toujours avoir le même nom de propriétaire que la délégation). Avec la présente spécification, cela ne sra pas vrai, et une antémémoire ne sera pas capable de calculer le ou les noms des RR NSEC3 appropriés. Les mises en œuvre peuvent avoir besoin d'utiliser de nouvelles méthodes de mise en antémémoire et de restitution des RR NSEC3.

9.2 Utilisation du bit AD

Le bit AD, défini par la [RFC4035], NE DOIT PAS être établi lors du retour d'une réponse contenant une preuve de plus proche incluant (prouvable) dans laquelle le RR NSEC3 qui couvre le "prochain plus proche" nom a le bit Opt-Out établi. Cette règle se fonde sur ce que cette preuve de plus proche incluant prouve réellement : les noms qui seraient couverts par le RR NSEC3 Opt-Out peuvent ou non exister comme des délégations non sûres. À ce titre, toutes les données dans les réponses contenant de telles preuves de plus proche incluant ne vont pas avoir été vérifiées cryptographiquement, de sorte que le bit AD ne peut pas être établi.

10. Considérations particulières

10.1 Restrictions à la longueur du nom de domaine

Les zones signées en utilisant la présente spécification ont des restrictions supplémentaires de longueur de nom de domaine qui leur sont imposées. En particulier, les zones avec des noms qui, quand ils sont convertis en noms de propriétaires hachés qui excèdent la limite de longueur de 255 octets imposée par la [RFC1035], ne peuvent pas utiliser cette spécification.

La longueur maximum réelle d'un nom de domaine dans une zone particulière dépend à la fois de la longueur du nom de zone (par opposition au nom de domaine complet) et de la fonction de hachage particulière utilisée.

Par exemple, SHA-1 produit un hachage de 160 bits. Le codage en base-32 des 160 bits résulte en 32 caractères. Les 32 caractères sont ajoutés devant le nom de la zone comme une seule étiquette, qui inclut un champ Longueur d'un seul octet. La longueur maximum du nom de zone, quand on utilise SHA-1, est 222 octets (255 - 33).

10.2 DNAME au sommet de zone

La spécification de DNAME à la Section 3 de la [RFC2672] a une limitation "pas de descendants". Si un RR DNAME est présent au nœud N, il DOIT n'y avoir de données chez aucun descendant de N.

Si N est le sommet de la zone, il va y avoir des types NSEC3 et RRSIG présents sur les descendants de N. La présente spécification met à jour la spécification de DNAME pour permettre les types NSEC3 et RRSIG aux descendants du sommet sans considération de l'existence de DNAME au sommet.

10.3 Itérations

Régler le nombre d'itérations utilisées permet au propriétaire de zone de choisir le coût du calcul du hachage, et donc le coût de génération d'un dictionnaire. Noter que ceci est distinct de l'effet du sel, qui empêche l'utilisation d'un seul dictionnaire pré-calculé en tous temps.

Évidemment, le nombre d'itérations affecte aussi les coûts pour le propriétaire de la zone de signer et servir la zone ainsi que les coûts chez le valideur pour vérifier les réponses provenant de la zone. On impose donc une limite supérieure au nombre d'itérations. On fonde cela sur le nombre d'itérations qui approxime le coût de la vérification d'un RRSet.

Les limites sont donc fondées sur la taille de la plus petite clé de signature de zone, arrondie à la plus proche valeur supérieure du tableau (ou la valeur inférieure si la clé est plus grande que la plus grande valeur du tableau).

Un propriétaire de zone NE DOIT PAS utiliser une valeur supérieure à ce qui est montré dans le tableau ci-dessous pour les itérations pour la taille de clé donnée. Un résolveur PEUT traiter comme non sûre une réponse avec une valeur supérieure, après que le valideur a vérifié que la signature sur le RR NSEC3 est correcte.

Taille de clé	Itérations
1024	150
2048	500
4096	2 500

Ce tableau se fonde sur une approximation du ratio entre le coût d'un calcul SHA-1 et le coût d'une vérification RSA des clés de taille 1024 bits (150 à 1), 2048 bits (500 à 1), et 4096 bits (2500 à 1).

Le ratio entre le calcul de SHA-1 et la vérification DSA est supérieur (1500 à 1 pour les clé de 1024 bits). Un compte d'itérations supérieur dégrade les performances, tandis que la vérification DSA est déjà plus coûteuse que RSA pour la même taille de clé. Donc, les valeurs du tableau DOIVENT être utilisées indépendamment de l'algorithme de la clé.

10.4 Transition d'une zone signée de NSEC à NSEC3

Lors de la transition d'une zone déjà signée et de confiance à la présente spécification, il faut faire attention à empêcher des échecs de validation de client durant le traitement.

La procédure de base est la suivante :

1. Transition de toutes les DNSKEY à DNSKEY en utilisant les alias d'algorithme décrits à la Section 2. La méthode réelle pour changer en toute sécurité le RRSet DNSKEY de la zone sort du domaine d'application de cette spécification. Cependant, le résultat final DOIT être que tous les RR DS dans le parent utilisent les alias d'algorithme spécifiés.

   Après l'achèvement de cette transition, tous les clients sans capacité NSEC3 vont traiter la zone comme non sûre. À ce point, le serveur d'autorité retourne encore des réponses négatives et de caractère générique qui contiennent des RR NSEC.

2. Ajout des RR NSEC3 signés à la zone, soit par incrément, soit tous à la fois. Si l'ajout est par incrément, alors le dernier RRSet ajouté DOIT être le RRSet NSEC3PARAM.

3. À l'ajout du RRSet NSEC3PARAM, le serveur passe au service de réponses négatives et de caractère générique avec les RR NSEC3 conformément à la présente spécification.

4. Retirer les RR NSEC par incrément ou tous à la fois.

10.5 Transition d'une zone signée de NSEC3 à NSEC

Pour re-transiter en toute sécurité à une zone signée DNSSEC [RFC4035], simplement inverser la procédure ci-dessus :

1. Ajouter les RR NSEC par incrément, ou tous à la fois.
2. Retirer le RRSet NSEC3PARAM. Cela va signaler au serveur d'utiliser les RR NSEC pour les réponses négatives et de caractère générique.
3. Retirer les RR NSEC3 soit par incrément, soit tous à la fois.
4. Passer tous les identifiants d'algorithme de DNSKEY à DNSSEC. Après la fin de cette transition, tous les clients sans capacité NSEC3 vont traiter la zone comme sûre.

11. Considérations relatives à l'IANA

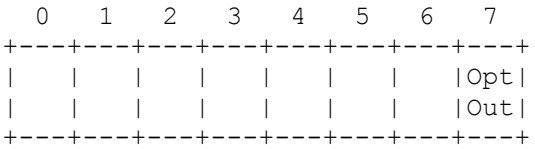
Bien que les formats de RR NSEC3 et NSEC3PARAM incluent un paramètre Algorithme de hachage, le présent document ne définit pas de mécanisme particulier pour passer en toute écurité d'un algorithme de hachage NSEC3 à un autre. Quand on spécifie un nouvel algorithme de hachage à utiliser avec NSEC3, un mécanisme de transition DOIT aussi être défini.

Le présent document met à jour le registre IANA "DOMAIN NAME SYSTEM PARAMETERS" (http://www.iana.org/assignments/dns-parameters) dans le sous registre "TYPES", en définissant deux nouveaux types. La Section 3 définit le type RR NSEC3 50. La Section 4 définit le type de RR NSEC3PARAM 51.

Le présent document met à jour le registre IANA "DNS SECURITY ALGORITHM NUMBERS -- selon la [RFC4035]" (http://www.iana.org/assignments/dns-sec-alg-numbers). La Section 2 définit les alias DSA-NSEC3-SHA1 (6) et RSASHA1-NSEC3-SHA1 (7) pour les enregistrements respectivement existants DSA et RSASHA1 en combinaison avec l'algorithme de hachage NSEC3 SHA1.

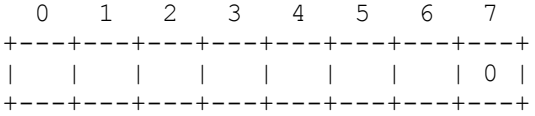
Comme ces numéros d'algorithme sont des alias pour les numéros d'algorithme DNSKEY existants, les fanions qui existent pour l'algorithme original sont valides pour les alias d'algorithme.

Le présent document crée un nouveau registre IANA pour les fanions NSEC3. Ce registre est appelé "DNSSEC NSEC3 Flags". Le contenu initial de ce registre est :



Le bit 7 est le fanion Opt-Out.
Les bits 0 à 6 sont disponible pour des allocations.
L'allocation de fanions NSEC3 supplémentaires dans ce registre exige une action de normalisation de l'IETF [RFC2434].

Le présent document crée un nouveau registre IANA pour les fanions NSEC3PARAM. Ce registre est appelé "DNSSEC NSEC3PARAM Flags". Le contenu initial de ce registre est :



Le bit 7 est réservé et doit être 0.
Les bits 0 à 6 sont disponibles pour allocation.
L'allocation de fanions NSEC3PARAM supplémentaires dans ce registre exige une action de normalisation de l'IETF [RFC2434].

Finalement, ce document crée un nouveau registre IANA pour les algorithmes de hachage NSEC3. Ce registre est appelé "DNSSEC NSEC3 Hash Algorithms". le contenu initial de ce registre est :

0 est Réservé.

1 est SHA-1.
2-255 disponible pour allocation.

L'allocation d'algorithmes de hachage NSEC3 supplémentaires dans ce registre exige une action de normalisation de l'IETF [RFC2434].

12. Considérations sur la sécurité

12.1 Considérations de hachage

12.1.1 Attaques de dictionnaire

Les RR NSEC3 sont encore susceptibles d'attaques de dictionnaire (c'est-à-dire, l'attaquant restitue tous les RR NSEC3, puis calcule les hachages de tous les noms de domaine probables, les compare aux hachages trouvés dans les RR NSEC3, et donc énumère la zone). Ceci est substantiellement plus coûteux que d'énumérer les RR NSEC originaux, et dans tous les cas, une telle attaque pourrait aussi être utilisée directement contre le serveur de noms lui-même en effectuant des interrogations pour tous les noms probables, bien que ce serait évidemment beaucoup plus détectable. Le coût de cette attaque hors ligne peut être choisi en réglant le nombre d'itérations dans le RR NSEC3.

Les zones sont aussi susceptibles d'une attaque de dictionnaire pré-calculé -- c'est-à-dire, une liste de hachages pour tous les noms probables est calculée une fois, puis le RR NSEC3 est examiné périodiquement et comparé aux hachages pré calculés. Cette attaque est prévenue en changeant le sel de façon régulière.

Le sel DEVRAIT être d'au moins 64 bits et imprévisible, afin qu'un attaquant ne puisse pas anticiper la valeur du sel et calculer le prochain ensemble de dictionnaires avant la publication de la zone.

12.1.2 Collisions

Des collisions de hachages entre le QNAME et le nom de propriétaire d'un RR NSEC3 peuvent se produire. Quand cela arrive, il va être impossible de prouver la non existence des QNAME en collision. Cependant, avec SHA-1, ceci est très improbable (de l'ordre de 1 sur 2^160). Noter que DNSSEC s'appuie déjà sur l'hypothèse qu'une fonction de hachage cryptographique est résistante à une seconde pré-image, car ces fonctions de hachage sont utilisées pour générer et valider les signatures et les RR DS.

12.1.3 Transition à un nouvel algorithme de hachage

Bien que les formats de RR NSEC3 et NSEC3PARAM incluent un paramètre d'algorithme de hachage, le présent document ne définit pas de mécanisme particulier pour passer en toute sécurité d'un algorithme de hachage NSEC3 à un autre. Quand on spécifie un nouvel algorithme de hachage à utiliser avec NSEC3, un mécanisme de transition DOIT aussi être défini. Il est possible que les seuls mécanismes de transition pratiques et acceptables puissent exiger une transition intermédiaire à un état non sûr, ou à un état qui utilise des enregistrements NSEC au lieu de NSEC3.

12.1.4 Utilisation de valeurs d'itération élevées

Comme les valideurs devraient traiter les réponses contenant des RR NSEC3 avec de fortes valeurs d'itération comme non sûres, la présence de juste un RR NSEC3 signé avec une valeur d'itérations élevée dans une zone donne aux attaquants une possibilité d'attaque en dégradation.

L'attaque retire simplement tous les RR NSEC3 existants d'une réponse, et remplace ou ajoute un seul (ou plusieurs) RR NSEC3 qui utilisent une forte valeur d'itérations à la réponse. Les valideurs vont alors être forcés de traiter la réponse comme non sûre. Cette attaque ne va être efficace que quand toutes les conditions suivantes sont satisfaites :

- il y a au moins présent dans la zone un RR NSEC3 signé qui utilise une forte valeur d'itérations ;
- l'attaquant a accès à un ou plusieurs de ces RR NSEC3. Ceci est trivialement vrai quand les RR NSEC3 avec de fortes valeurs d'itération sont retournés dans des réponses normales, mais peut aussi être vrai si l'attaquant peut accéder à la zone via des interrogations AXFR ou IXFR, ou toute autre méthodologie.

Utiliser un nombre élevé d'itérations introduit aussi une opportunité supplémentaire de déni de service contre les serveurs, car les serveurs doivent calculer plusieurs hachages par réponse négative ou à caractère générique.

12.2 Considérations sur Opt-Out

Le fanion Opt-Out (O) permet que des noms non signés, sous la forme de délégations à des zones non signées, existent au sein d'une zone par ailleurs signée. Tous les noms non signés sont, par définition, non sûrs, et leur validité ou existence ne peut pas être prouvée cryptographiquement.

En général :

- Les enregistrements de ressource avec des noms non signés (qu'ils existent ou non) souffrent des mêmes vulnérabilités que les RR dans une zone non signée. Ces vulnérabilités sont décrites plus en détails dans la [RFC3833] (en particulier au paragraphe 2.3, "Chaînage de noms" et au paragraphe 2.6, "Négation de nom de domaine authentifiée").
- Les enregistrements de ressource avec des noms signés ont la même sécurité, que Opt-Out soit utilisé ou non.

Noter qu'avec ou sans Opt-Out, une délégation non sûre peut être altérée de façon indétectable par un attaquant. À cause de cela, la principale différence de sécurité quand on utilise Opt-Out est la perte de la capacité de prouver l'existence ou la non existence d'une délégation non sûre dans la portée d'un RR NSEC3 Opt-Out.

En particulier, cela sigifie qu'une entité malveillante peut être capable d'insérer ou supprimer des RR avec des noms non signés. Ces RR sont normalement des RR NS, mais cela inclut aussi des expansions signées de caractère générique (bien que le RR à caractère générique lui-même soit signé, son nom expansé est un nom non signé).

Noter qu'être capable d'ajouter une délégation est fonctionnellement équivalent à être capable d'ajouter tout type de RR : un attaquant a simplement à forger une délégation au serveur de noms sous son contrôle et à placer les RR nécessaires au sommet de la sous zone.

Bien que dans des cas particuliers, cette question puisse ne pas poser de problème de sécurité significatif, en général elle ne devrait pas être prise à la légère. Donc, il est fortement RECOMMANDÉ que Opt-Out soit rarement utilisé. En particulier, les outils de signature de zone NE DEVRAIENT PAS utiliser Opt-Out par défaut, et PEUVENT choisir de ne pas prendre du tout en charge Opt-Out.

12.3 Autres considérations

Parcourir les RR NSEC3 va révéler le nombre total de RR dans la zone (plus les non terminaux vides) et aussi de quels types ils sont. Cela pourrait être atténué en ajoutant des entrées factices, mais une limite supérieure peut certainement toujours être trouvée.

13. Références

13.1 Références normatives

[RFC1034] P. Mockapetris, "Noms de domaines - Concepts et facilités", STD 13, novembre 1987. (*MàJ par* RFC1101, 1183, 1348, 1876, 1982, 2065, 2181, 2308, 2535, 4033, 4034, 4035, 4343, 4035, 4592, 5936, 8020, 8482, 8767)

[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)

[RFC2136] P. Vixie, S. Thomson, Y. Rekhter et J. Bound, "Mises à jour dynamiques dans le système de noms de domaine (DNS UPDATE)", avril 1997.

[RFC2181] R. Elz et R. Bush, "Clarifications pour la spécification du DNS", juillet 1997. *(P.S., MàJ par* RFC4035, RFC2535, RFC4343, RFC4033, RFC4034, RFC5452, RFC8767)

[RFC2308] M. Andrews, "Mise en antémémoire négative des interrogations du DNS (DNS NCACHE)", mars 1998. (*MàJ par les RFC* 4033, 4034, 4035, 6604, 8020) *(P.S.)*

[RFC2434] T. Narten et H. Alvestrand, "Lignes directrices pour la rédaction d'une section Considérations relatives à l'IANA dans les RFC", BCP 26, octobre, 1998. *(Rendue obsolète par la RFC* 5226*)*

[RFC2929] D. Eastlake 3rd, E. Brunner-Williams et B. Manning, "Considérations relatives à l'IANA pour le système des noms de domaine (DNS)", BCP 42, septembre 2000. *(Obsolète, voir la* RFC5395)

[RFC3597] A. Gustafsson, "Traitement des types inconnus d'enregistrement de ressource du DNS ", septembre 2003. *(P.S.)*

[RFC4033] R. Arends, et autres, "Introduction et exigences pour la sécurité du DNS", mars 2005.

[RFC4034] R. Arends et autres, "Enregistrements de ressources pour les extensions de sécurité au DNS", mars 2005. (*MàJ par* RFC9077)

[RFC4035] R. Arends et autres, "Modifications du protocole pour les extensions de sécurité du DNS", mars 2005. *(P.S. ; MàJ par* RFC8198, 9077

[RFC4648] S. Josefsson, "Codages de données Base16, Base32 et Base64", octobre 2006. (*Remplace* RFC3548) *(P.S.)*

13.2 Références pour information

[DNSEXT-NO] S. Josefsson, "Authenticating Denial of Existence in DNS with Minimum Disclosure", *travail en cours*, juillet 2000.

[DNSEXT-NSEC2v2] B. Laurie, "DNSSEC NSEC2 Owner et RDATA Format", *travail en cours*, décembre 2004.

[RFC2672] M. Crawford, "Renumérotage d'un sous-ensemble non terminal du DNS", août 1999. (*MàJ par* RFC4592, RFC6604)) (*Remplacée par la* RFC6672) *(P.S.)*

[RFC2898] B. Kaliski, "PKCS n° 5 : Spécification de la cryptographie fondée sur un mot de passe, version 2.0", septembre 2000. *(Info. ; remplacée par* RFC8018)

[RFC3833] D. Atkins, R. Austein, "Analyse des menaces contre le système des noms de domaines (DNS)", août 2004. *(Info.)*

[RFC4592] E. Lewis, "Le rôle des caractères génériques dans le système des noms de domaines", juillet 2006. *(P.S.)*

[RFC4956] R. Arends et autres, "Modèle Opt-in pour la sécurité du DNS (DNSSEC)", juillet 2007. *(Expérimentale)*

Appendice A Exemple de zone

Voici une zone montrant ses RR NSEC3. Cela peut aussi être utilisé comme des vecteurs d'essai pour l'algorithme de hachage. Le TTL global et la classe sont spécifiés dans le RR SOA, et sont ensuite omis pour que ce soit plus clair.
La zone est précédée d'une liste qui contient les hachages des noms de propriétaire originaux.

```
; H(exemple) = 0p9mhaveqvm6t7vbl5lop2u3t2rp3tom
; H(a.exemple) = 35mthgpgcu1qg68fab165klnsnk3dpvl
; H(ai.exemple) = gjeqe526plbf1g8mklp59enfd789njgi
; H(ns1.exemple) = 2t7b4g4vsa5smi47k61mv5bv1a22bojr
; H(ns2.exemple) = q04jkcevqvmu85r014c7dkba38o0ji5r
; H(w.exemple) = k8udemvp1j2f7eg6jebps17vp3n8i58h
; H(*.w.exemple)  = r53bq7cc2uvmubfu5ocmm6pers9tk9en
; H(x.w.exemple) = b4um86eghhds6nea196smvmlo4ors995
; H(y.w.exemple) = ji6neoaepv8b5o6k4ev33abha8ht9fgc
; H(x.y.w.exemple) = 2vptu5timamqttgl4luu9kg21e0aor3s
; H(xx.exemple) = t644ebqk9bibcna874givr6joj62mlhv
; H(2t7b4g4vsa5smi47k61mv5bv1a22bojr.exemple) = kohar7mbb8dc2ce8a9qvl8hon4k53uhi
  exemple. 3600  IN SOA  ns1.exemple. bugs.x.w.exemple. 1 3600 300 ( 3600000 3600 )
```

```
            RRSIG   SOA 7 1 3600 20150420235959 20051021000000 (
                40430 exemple.
                Hu25UIyNPmvPIVBrldN+9Mlp9Zql39qaUd8i
                q4ZLlYWfUUbbAS41pG+68z81q1xhkYAcEyHd
                VI2LmKusbZsT0Q== )
            NS      ns1.exemple.
            NS      ns2.exemple.
            RRSIG   NS 7 1 3600 20150420235959 20051021000000 (
                40430 exemple.
                PVOgtMK1HHeSTau+HwDWC8Ts+6C8qtqd4pQJ
                qOtdEVgg+MA+ai4fWDEhu3qHJyLcQ9tbD2vv
                CnMXjtz6SyObxA== )
            MX      1 xx.exemple.
            RRSIG   MX 7 1 3600 20150420235959 20051021000000 (
                40430 exemple.
                GgQ1A9xs47k42VPvpL/a1BWUz/6XsnHkjotw
                9So8MQtZtl2wJBsnOQsaoHrRCrRbyriEl/GZ
                n9Mto/Kx+wBo+w== )
            DNSKEY  256 3 7 AwEAAaetidLzsKWUt4swWR8yu0wPHPiUi8LU (
                sAD0QPWU+wzt89epO6tHzkMBVDkC7qphQO2h
                TY4hHn9npWFRw5BYubE= )
            DNSKEY  257 3 7 AwEAAcUlFV1vhmqx6NSOUOq2R/dsR7Xm3upJ (
                j7IommWSpJABVfW8Q0rOvXdM6kzt+TAu92L9
                AbsUdblMFin8CVF3n4s= )
            RRSIG   DNSKEY 7 1 3600 20150420235959 (
                20051021000000 12708 exemple.
                AuU4juU9RaxescSmStrQks3Gh9FblGBlVU31
                uzMZ/U/FpsUb8aC6QZS+sTsJXnLnz7flGOsm
                MGQZf3bH+QsCtg== )
            NSEC3PARAM 1 0 12 aabbccdd
            RRSIG   NSEC3PARAM 7 1 3600 20150420235959 (
                20051021000000 40430 exemple.
                C1Gl8tPZNtnjlrYWDeeUV/sGLCyy/IHie2re
                rN05XSA3Pq0U3+4VvGWYWdUMfflOdxqnXHwJ
                TLQsjlkynhG6Cg== )
0p9mhaveqvm6t7vbl5lop2u3t2rp3tom.exemple. NSEC3 1 1 12 aabbccdd (
                2t7b4g4vsa5smi47k61mv5bv1a22bojr MX DNSKEY NS
                SOA NSEC3PARAM RRSIG )
            RRSIG   NSEC3 7 2 3600 20150420235959 20051021000000 (
                40430 exemple.
                OSgWSm26B+cS+dDL8b5QrWr/dEWhtCsKlwKL
                IBHYH6blRxK9rC0bMJPwQ4mLIuw85H2EY762
                BOCXJZMnpuwhpA== )
2t7b4g4vsa5smi47k61mv5bv1a22bojr.exemple. A 192.0.2.127
            RRSIG   A 7 2 3600 20150420235959 20051021000000 (
                40430 exemple.
                h6c++bzhRuWWt2bykN6mjaTNBcXNq5UuL5Ed
                K+iDP4eY8I0kSiKaCjg3tC1SQkeloMeub2GW
                k8p6xHMPZumXlw== )
            NSEC3   1 1 12 aabbccdd (
                2vptu5timamqttgl4luu9kg21e0aor3s A RRSIG )
            RRSIG   NSEC3 7 2 3600 20150420235959 20051021000000 (
                40430 exemple.
                OmBvJ1Vgg1hCKMXHFiNeIYHK9XVW0iLDLwJN
                4TFoNxZuP03gAXEI634YwOc4YBNITrj413iq
                NI6mRk/r1dOSUw== )
2vptu5timamqttgl4luu9kg21e0aor3s.exemple. NSEC3 1 1 12 aabbccdd (
                35mthgpgcu1qg68fab165klnsnk3dpvl MX RRSIG )
            RRSIG   NSEC3 7 2 3600 20150420235959 20051021000000 (
                40430 exemple.
```

```
                KL1V2oFYghNV0Hm7Tf2vpJjM6l+0g1JCcVYG
                VfI0lKrhPmTsOA96cLEACgo1x8I7kApJX+ob
                TuktZ+sdsZPY1w== )
35mthgpgcu1qg68fab165klnsnk3dpvl.exemple. NSEC3 1 1 12 aabbccdd (
                b4um86eghhds6nea196smvmlo4ors995 NS DS RRSIG )
            RRSIG   NSEC3 7 2 3600 20150420235959 20051021000000 (
                40430 exemple.
                g6jPUUpduAJKRljUsN8gB4UagAX0NxY9shwQ
                Aynzo8EUWH+z6hEIBlUTPGj15eZll6VhQqgZ
                XtAIR3chwgW+SA== )
a.exemple.  NS      ns1.a.exemple.
            NS      ns2.a.exemple.
            DS      58470 5 1 (
                3079F1593EBAD6DC121E202A8B766A6A4837206C )
            RRSIG   DS 7 2 3600 20150420235959 20051021000000 (
                40430 exemple.
                XacFcQVHLVzdoc45EJhN616zQ4mEXtE8FzUh
                M2KWjfy1VfRKD9r1MeVGwwoukOKgJxBPFsWo
                o722vZ4UZ2dIdA== )
ns1.a.exemple. A        192.0.2.5
ns2.a.exemple. A        192.0.2.6
ai.exemple.  A      192.0.2.9
            RRSIG   A 7 2 3600 20150420235959 20051021000000 (
                40430 exemple.
                hVe+wKYMlObTRPhX0NL67GxeZfdxqr/QeR6F
                tfdAj5+FgYxyzPEjIzvKWy00hWIl6wD3Vws+
                rznEn8sQ64UdqA== )
            HINFO   "KLH-10" "ITS"
            RRSIG   HINFO 7 2 3600 20150420235959 20051021000000 (
                40430 exemple.
                Yi42uOq43eyO6qXHNvwwfFnIustWgV5urFcx
                enkLvs6pKRh00VBjODmf3Z4nMO7IOl6nHSQ1
                v0wLHpEZG7Xj2w== )
            AAAA    2001:db8:0:0:0:0:f00:baa9
            RRSIG   AAAA 7 2 3600 20150420235959 20051021000000 (
                40430 exemple.
                LcdxKaCB5bGZwPDg+3JJ4O02zoMBrjxqlf6W
                uaHQZZfTUpb9Nf2nxFGe2XRPfR5tpJT6GdRG
                cHueLuXkMjBArQ== )
b4um86eghhds6nea196smvmlo4ors995.exemple. NSEC3 1 1 12 aabbccdd (
                gjeqe526plbf1g8mklp59enfd789njgi MX RRSIG )
            RRSIG   NSEC3 7 2 3600 20150420235959 20051021000000 (
                40430 exemple.
                ZkPG3M32lmoHM6pa3D6gZFGB/rhL//Bs3Omh
                5u4m/CUiwtblEVOaAKKZd7S959OeiX43aLX3
                pOv0TSTyiTxIZg== )
c.exemple.  NS      ns1.c.exemple.
            NS      ns2.c.exemple.
ns1.c.exemple. A        192.0.2.7
ns2.c.exemple. A        192.0.2.8
gjeqe526plbf1g8mklp59enfd789njgi.exemple. NSEC3 1 1 12 aabbccdd (
                ji6neoaepv8b5o6k4ev33abha8ht9fgc HINFO A AAAA RRSIG )
            RRSIG   NSEC3 7 2 3600 20150420235959 20051021000000 (
                40430 exemple.
                IVnezTJ9iqblFF97vPSmfXZ5Zozngx3KX3by
                LTZC4QBH2dFWhf6scrGFZB980AfCxoD9qbbK
                Dy+rdGIeRSVNyw== )
ji6neoaepv8b5o6k4ev33abha8ht9fgc.exemple. NSEC3 1 1 12 aabbccdd (
                k8udemvp1j2f7eg6jebps17vp3n8i58h )
            RRSIG   NSEC3 7 2 3600 20150420235959 20051021000000 (
```

```
                40430 exemple.
                gPkFp1s2QDQ6wQzcg1uSebZ61W33rUBDcTj7
                2F3kQ490fEdp7k1BUIfbcZtPbX3YCpE+sIt0
                MpzVSKfTwx4uYA== )
k8udemvp1j2f7eg6jebps17vp3n8i58h.exemple. NSEC3 1 1 12 aabbccdd (
                kohar7mbb8dc2ce8a9qvl8hon4k53uhi )
            RRSIG   NSEC3 7 2 3600 20150420235959 20051021000000 (
                40430 exemple.
                FtXGbvF0+wf8iWkyo73enAuVx03klN+pILBK
                S6qCcftVtfH4yVzsEZquJ27NHR7ruxJWDNMt
                Otx7w9WfcIg62A== )
kohar7mbb8dc2ce8a9qvl8hon4k53uhi.exemple. NSEC3 1 1 12 aabbccdd (
                q04jkcevqvmu85r014c7dkba38o0ji5r A RRSIG )
            RRSIG   NSEC3 7 2 3600 20150420235959 20051021000000 (
                40430 exemple.
                VrDXs2uVW21N08SyQIz88zml+y4ZCInTwgDr
                6zz43yAg+LFERjOrj3Ojct51ac7Dp4eZbf9F
                QJazmASFKGxGXg== )
  ns1.exemple.  A       192.0.2.1
            RRSIG   A 7 2 3600 20150420235959 20051021000000 (
                40430 exemple.
                bu6kx73n6XEunoVGuRfAgY7EF/AJqHy7hj0j
                kiqJjB0dOrx3wuz9SaBeGfqWIdn/uta3SavN
                4FRvZR9SCFHF5Q== )
  ns2.exemple.  A       192.0.2.2
            RRSIG   A 7 2 3600 20150420235959 20051021000000 (
                40430 exemple.
                ktQ3TqE0CfRfki0Rb/Ip5BM0VnxelbuejCC4
                zpLbFKA/7eD7UNAwxMgxJPtbdST+syjYSJaj
                4IHfeX6n8vfoGA== )
q04jkcevqvmu85r014c7dkba38o0ji5r.exemple. NSEC3 1 1 12 aabbccdd (
                r53bq7cc2uvmubfu5ocmm6pers9tk9en A RRSIG )
            RRSIG   NSEC3 7 2 3600 20150420235959 20051021000000 (
                40430 exemple.
                hV5I89b+4FHJDATp09g4bbN0R1F845CaXpL3
                ZxlMKimoPAyqletMlEWwLfFia7sdpSzn+ZlN
                NlkxWcLsIlMmUg== )
r53bq7cc2uvmubfu5ocmm6pers9tk9en.exemple. NSEC3 1 1 12 aabbccdd (
                t644ebqk9bibcna874givr6joj62mlhv MX RRSIG )
            RRSIG   NSEC3 7 2 3600 20150420235959 20051021000000 (
                40430 exemple.
                aupviViruXs4bDg9rCbezzBMf9h1ZlDvbW/C
                ZFKulIGXXLj8B/fsDJarXVDA9bnUoRhEbKp+
                HF1FWKW7RIJdtQ== )
t644ebqk9bibcna874givr6joj62mlhv.exemple. NSEC3 1 1 12 aabbccdd (
                0p9mhaveqvm6t7vbl5lop2u3t2rp3tom HINFO A AAAA
                RRSIG )
            RRSIG   NSEC3 7 2 3600 20150420235959 20051021000000 (
                40430 exemple.
                RAjGECB8P7O+F4Pa4Dx3tC0M+Z3KmlLKImca
                fb9XWwx+NWUNz7NBEDBQHivIyKPVDkChcePI
                X1xPl1ATNa+8Dw== )
*.w.exemple.  MX      1 ai.exemple.
            RRSIG   MX 7 2 3600 20150420235959 20051021000000 (
                40430 exemple.
                CikebjQwGQPwijVcxgcZcSJKtfynugtlBiKb
                9FcBTrmOoyQ4InoWVudhCWsh/URX3lc4WRUM
                ivEBP6+4KS3ldA== )
x.w.exemple.  MX      1 xx.exemple.
            RRSIG   MX 7 3 3600 20150420235959 20051021000000 (
```

```
                40430 exemple.
                IrK3tq/tHFIBF0scHiE/1IwMAvckS/55hAVv
                QyxTFbkAdDloP3NbZzu+yoSsr3b3OX6qbBpY
                7WCtwwekLKRAwQ== )
x.y.w.exemple. MX      1 xx.exemple.
          RRSIG   MX 7 4 3600 20150420235959 20051021000000 (
                40430 exemple.
                MqSt5HqJIN8+SLlzTOImrh5h9Xa6gDvAW/Gn
                nbdPc6Z7nXvCpLPJj/5lCwx3VuzVOjkbvXze
                8/8Ccl2Zn2hbug== )
xx.exemple.    A       192.0.2.10
          RRSIG   A 7 2 3600 20150420235959 20051021000000 (
                40430 exemple.
                T35hBWEZ017VC5u2c4OriKyVn/pu+fVK4AlX
                YOxJ6iQylfV2HQIKjv6b7DzINB3aF/wjJqgX
                pQvhq+Ac6+ZiFg== )
          HINFO   "KLH-10" "TOPS-20"
          RRSIG   HINFO 7 2 3600 20150420235959 20051021000000 (
                40430 exemple.
                KimG+rDd+7VA1zRsu0ITNAQUTRlpnsmqWrih
                FRnU+bRa93v2e5oFNFYCs3Rqgv62K93N7AhW
                6Jfqj/8NzWjvKg== )
          AAAA    2001:db8:0:0:0:0:f00:baaa

          RRSIG   AAAA 7 2 3600 20150420235959 20051021000000 (
                40430 exemple.
                IXBcXORITNwd8h3gNwyxtYFvAupS/CYWufVe
                uBUX0O25ivBCULjZjpDxFSxfohb/KA7YRdxE
                NzYfMItpILl/Xw== )
```

Appendice B Exemple de réponses

Les exemples de cette section montrent les messages de réponse en utilisant l'exemple de zone signée de l'Appendice A.

B.1 Erreur de nom

Une erreur de nom d'autorité. Les RR NSEC3 prouvent que le nom n'existe pas et qu'il n'y a pas de RR à caractère générique qui devrait avoir été expansé.

```
;; En-tête : QR AA DO RCODE=3
;;
;; Question
a.c.x.w.exemple.        IN A

;; Réponse
;; (vide)

;; Autorité

exemple.       SOA     ns1.exemple. bugs.x.w.exemple. 1 3600 300 (
                3600000 3600 )
exemple.       RRSIG   SOA 7 1 3600 20150420235959 20051021000000 (
                40430 exemple.
                Hu25UIyNPmvPIVBrldN+9Mlp9Zql39qaUd8i
                q4ZLlYWfUUbbAS41pG+68z81q1xhkYAcEyHd
                VI2LmKusbZsT0Q== )

;; RR NSEC3 qui couvre le "prochain plus proche" nom (c.x.w.exemple)
;; H(c.x.w.exemple) = 0va5bpr2ou0vk0lbqeeljri88laipsfh
```

```
0p9mhaveqvm6t7vbl5lop2u3t2rp3tom.exemple. NSEC3 1 1 12 aabbccdd (
                2t7b4g4vsa5smi47k61mv5bv1a22bojr MX DNSKEY NS
                SOA NSEC3PARAM RRSIG )
0p9mhaveqvm6t7vbl5lop2u3t2rp3tom.exemple. RRSIG NSEC3 7 2 3600 (
                20150420235959 20051021000000 40430 exemple.
                OSgWSm26B+cS+dDL8b5QrWr/dEWhtCsKlwKL
                IBHYH6blRxK9rC0bMJPwQ4mLIuw85H2EY762
                BOCXJZMnpuwhpA== )

;; RR NSEC3 qui correspond au plus proche incluant (x.w.exemple)
;; H(x.w.exemple) = b4um86eghhds6nea196smvmlo4ors995

b4um86eghhds6nea196smvmlo4ors995.exemple. NSEC3 1 1 12 aabbccdd (
                gjeqe526plbf1g8mklp59enfd789njgi MX RRSIG )
b4um86eghhds6nea196smvmlo4ors995.exemple. RRSIG NSEC3 7 2 3600 (
                20150420235959 20051021000000 40430 exemple.
                ZkPG3M32lmoHM6pa3D6gZFGB/rhL//Bs3Omh
                5u4m/CUiwtblEVOaAKKZd7S959OeiX43aLX3
                pOv0TSTyiTxIZg== )

;; RR NSEC3 qui couvre le caractère générique au plus proche incluant (*.x.w.exemple)
;; H(*.x.w.exemple) = 92pqneegtaue7pjatc3l3qnk738c6v5m

35mthgpgcu1qg68fab165klnsnk3dpvl.exemple. NSEC3 1 1 12 aabbccdd (
                b4um86eghhds6nea196smvmlo4ors995 NS DS RRSIG )
35mthgpgcu1qg68fab165klnsnk3dpvl.exemple. RRSIG NSEC3 7 2 3600 (
                20150420235959 20051021000000 40430 exemple.
                g6jPUUpduAJKRljUsN8gB4UagAX0NxY9shwQ
                Aynzo8EUWH+z6hEIBlUTPGj15eZll6VhQqgZ
                XtAIR3chwgW+SA== )

;; Additionnel
;; (vide)
```

L'interrogation a retourné trois RR NSEC3 qui prouvent que les données demandées n'existent pas et qu'aucune expansion de caractère générique ne s'applique. La réponse négative est authentifiée par la vérification des RR NSEC3. Les RRSIG correspondants indiquent que les RR NSEC3 sont signés par un DNSKEY "exemple" d'algorithme 7 et avec l'étiquette de clé 40430. Le résolveur a besoin du RR DNSKEY correspondant afin d'authentifier cette réponse.

Un des noms de propriétaires des RR NSEC3 correspond au plus proche incluant. Un des RR NSEC3 prouve qu'il n'existe pas de nom plus long. Un des RR NSEC3 prouve qu'il n'existe pas de RRSet à caractère générique qui devrait avoir été expansé. Le plus proche incluant peut être trouvé en appliquant l'algorithme du paragraphe 8.3.

Dans l'exemple ci-dessus, le nom 'x.w.exemple' est haché en 'b4um86eghhds6nea196smvmlo4ors995'. Cela indique que ce pourrait être le plus proche incluant. Pour prouver que 'c.x.w.exemple' et '*.x.w.exemple' n'exisent pas, ces noms sont hachés, respectivement, en '0va5bpr2ou0vk0lbqeeljri88laipsfh' et '92pqneegtaue7pjatc3l3qnk738c6v5m'. Le premier et le dernier des RR NSEC3 prouvent que des noms de propriétaires hachés n'existent pas.

B.2 Erreur No Data

Une réponse "no data". Le RR NSEC3 prouve que le nom existe et que le type de RR demandé n'existe pas.

```
;; En-tête : QR AA DO RCODE=0
;;
;; Question
ns1.exemple.       IN MX

;; Réponse
;; (vide)
```

```
;; Autorité
exemple.      SOA     ns1.exemple. bugs.x.w.exemple. 1 3600 300 ( 3600000 3600 )
exemple.      RRSIG   SOA 7 1 3600 20150420235959 20051021000000 (
                      40430 exemple.
                      Hu25UIyNPmvPIVBrldN+9Mlp9Zql39qaUd8i
                      q4ZLlYWfUUbbAS41pG+68z81q1xhkYAcEyHd
                      VI2LmKusbZsT0Q== )

;; Le RR NSEC3 correspond au QNAME et montre que le bit de type MX n'est pas établi.

2t7b4g4vsa5smi47k61mv5bv1a22bojr.exemple. NSEC3 1 1 12 aabbccdd (
                      2vptu5timamqttgl4luu9kg21e0aor3s A RRSIG )
2t7b4g4vsa5smi47k61mv5bv1a22bojr.exemple. RRSIG NSEC3 7 2 3600 (
                      20150420235959 20051021000000 40430 exemple.
                      OmBvJ1Vgg1hCKMXHFiNeIYHK9XVW0iLDLwJN
                      4TFoNxZuP03gAXEI634YwOc4YBNITrj413iq
                      NI6mRk/r1dOSUw== )
;; Additionnel
;; (vide)
```

L'interrogation a retourné un RR NSEC3 qui prouve que le nom demandé existe ("ns1.exemple." et son hachage est "2t7b4g4vsa5smi47k61mv5bv1a22bojr") mais le type de RR demandé n'existe pas (le type MX est absent dans la liste de codes de type du RR NSEC3) et n'est pas un CNAME (le type CNAME est aussi absent dans la liste des codes de type du RR NSEC3).

B.2.1 Erreur No Data, non terminal vide

Une réponse "no data" à cause d'un non terminal vide. Le RR NSEC3 prouve que le nom existe et que le type de RR demandé n'existe pas.

```
;; En-tête : QR AA DO RCODE=0
;;
;; Question
y.w.exemple.      IN A

;; Réponse
;; (vide)

;; Autorité
exemple.      SOA     ns1.exemple. bugs.x.w.exemple. 1 3600 300 ( 3600000 3600 )
exemple.      RRSIG   SOA 7 1 3600 20150420235959 20051021000000 (
                      40430 exemple.
                      Hu25UIyNPmvPIVBrldN+9Mlp9Zql39qaUd8i
                      q4ZLlYWfUUbbAS41pG+68z81q1xhkYAcEyHd
                      VI2LmKusbZsT0Q== )

;; Le RR NSEC3 correspond au QNAME et montre que le bit de type A n'est pas établi.

ji6neoaepv8b5o6k4ev33abha8ht9fgc.exemple. NSEC3 1 1 12 aabbccdd (
                      k8udemvp1j2f7eg6jebps17vp3n8i58h )
ji6neoaepv8b5o6k4ev33abha8ht9fgc.exemple. RRSIG NSEC3 7 2 3600 (
                      20150420235959 20051021000000 40430 exemple.
                      gPkFp1s2QDQ6wQzcg1uSebZ61W33rUBDcTj7
                      2F3kQ490fEdp7k1BUIfbcZtPbX3YCpE+sIt0
                      MpzVSKfTwx4uYA== )

;; Additionnel
;; (vide)
```

L'interrogation a retourné un RR NSEC3 qui prouve que le nom demandé existe ("y.w.exemple." est haché en "ji6neoaepv8b5o6k4ev33abha8ht9fgc") mais le type de RR demandé n'existe pas (le type A est absent dans le champ Type Bit Maps du RR NSEC3). Noter que à la différence d'une preuve de non terminal vide en utilisant des NSEC, ceci est identique à l'erreur No Data. Cet exemple n'est mentionné que pour être complet.

B.3 Référence à une zone non signée Opt-Out

Les RR NSEC3 prouvent que rien n'a été signé pour cette délégation. Il n'y a pas de preuve que la délégation non signée existe.

```
;; En-tête : QR DO RCODE=0
;;
;; Question
mc.c.exemple.       IN MX

;; Réponse
;; (vide)

;; Autorité
c.exemple.     NS      ns1.c.exemple.
               NS      ns2.c.exemple.

;; RR NSEC3 qui couvre le "prochain plus proche" nom (c.exemple)
;; H(c.exemple) = 4g6p9u5gvfshp30pqecj98b3maqbn1ck

35mthgpgcu1qg68fab165klnsnk3dpvl.exemple. NSEC3 1 1 12 aabbccdd (
                b4um86eghhds6nea196smvmlo4ors995 NS DS RRSIG )
 35mthgpgcu1qg68fab165klnsnk3dpvl.exemple. RRSIG NSEC3 7 2 3600 (
                20150420235959 20051021000000 40430 exemple.
                g6jPUUpduAJKRljUsN8gB4UagAX0NxY9shwQ
                Aynzo8EUWH+z6hEIBlUTPGj15eZll6VhQqgZ
                XtAIR3chwgW+SA== )

;; RR NSEC3 qui correspond au plus proche incluant (exemple)
;; H(exemple) = 0p9mhaveqvm6t7vbl5lop2u3t2rp3tom

0p9mhaveqvm6t7vbl5lop2u3t2rp3tom.exemple. NSEC3 1 1 12 aabbccdd (
                2t7b4g4vsa5smi47k61mv5bv1a22bojr MX DNSKEY NS
                SOA NSEC3PARAM RRSIG )
0p9mhaveqvm6t7vbl5lop2u3t2rp3tom.exemple. RRSIG NSEC3 7 2 3600 (
                20150420235959 20051021000000 40430 exemple.
                OSgWSm26B+cS+dDL8b5QrWr/dEWhtCsKlwKL
                IBHYH6blRxK9rC0bMJPwQ4mLIuw85H2EY762
                BOCXJZMnpuwhpA== )

;; Additionnel
ns1.c.exemple. A       192.0.2.7
ns2.c.exemple. A       192.0.2.8
```

L'interrogation a retourné une référence à la zone non signée "c.exemple.". La réponse contient le plus proche incluant prouvable de "c.exemple" comme étant "exemple", car le hachage ("4g6p9u5gvfshp30pqecj98b3maqbn1ck") de "c.exemple" est couvert par le premier RR NSEC3 et son bit Opt-Out est établi.

B.4 Expansion de caractère générique

Une interrogation à laquelle il a été répondu avec une réponse contenant une expansion de caractère générique. Le compte d'étiquettes dans le RRSet RRSIG dans la section réponse indique qu'un RRSet à caractère générique a été expansé pour produire cette réponse, et le RR NSEC3 prouve qu'aucun "prochain plus proche" nom n'existe dans la zone.

```
;; En-tête : QR AA DO RCODE=0
;;
```

```
;; Question
a.z.w.exemple. IN MX

;; Réponse
a.z.w.exemple. MX      1 ai.exemple.
a.z.w.exemple. RRSIG   MX 7 2 3600 20150420235959 20051021000000 (
                       40430 exemple.
                       CikebjQwGQPwijVcxgcZcSJKtfynugtlBiKb
                       9FcBTrmOoyQ4InoWVudhCWsh/URX3lc4WRUM
                       ivEBP6+4KS3ldA== )

;; Autorité
exemple.       NS      ns1.exemple.
exemple.       NS      ns2.exemple.
exemple.       RRSIG   NS 7 1 3600 20150420235959 20051021000000 (
                       40430 exemple.
                       PVOgtMK1HHeSTau+HwDWC8Ts+6C8qtqd4pQJ
                       qOtdEVgg+MA+ai4fWDEhu3qHJyLcQ9tbD2vv
                       CnMXjtz6SyObxA== )

;; RR NSEC3 qui couvre le "prochain plus proche" nom (z.w.exemple)
;; H(z.w.exemple) = qlu7gtfaeh0ek0c05ksfhdpbcgglbe03

q04jkcevqvmu85r014c7dkba38o0ji5r.exemple. NSEC3 1 1 12 aabbccdd (
                       r53bq7cc2uvmubfu5ocmm6pers9tk9en A RRSIG )
q04jkcevqvmu85r014c7dkba38o0ji5r.exemple. RRSIG NSEC3 7 2 3600 (
                       20150420235959 20051021000000 40430 exemple.
                       hV5I89b+4FHJDATp09g4bbN0R1F845CaXpL3
                       ZxlMKimoPAyqletMlEWwLfFia7sdpSzn+ZlN
                       NlkxWcLsIlMmUg== )

;; Additionnel
ai.exemple.    A       192.0.2.9
ai.exemple.    RRSIG   A 7 2 3600 20150420235959 20051021000000 (
                       40430 exemple.
                       hVe+wKYMlObTRPhX0NL67GxeZfdxqr/QeR6F
                       tfdAj5+FgYxyzPEjIzvKWy00hWIl6wD3Vws+
                       rznEn8sQ64UdqA== )
ai.exemple.    AAAA    2001:db8:0:0:0:0:f00:baa9
ai.exemple.    RRSIG   AAAA 7 2 3600 20150420235959 20051021000000 (
                       40430 exemple.
                       LcdxKaCB5bGZwPDg+3JJ4O02zoMBrjxqlf6W
                       uaHQZZfTUpb9Nf2nxFGe2XRPfR5tpJT6GdRG
                       cHueLuXkMjBArQ== )
```

L'interrogation a retourné une réponse qui a été produite par suite de l'expansion de caractère générique. La section réponse contient un RRSet à caractère générique expansé comme il le serait dans une réponse DNS traditionnelle. La valeur du champ Étiquettes RRSIG de 2 indique que la réponse est le résultat d'une expansion de caractère générique, car le nom "a.z.w.exemple" contient 4 étiquettes. Cela montre aussi que "w.exemple" existe, de sorte qu'il n'est pas besoin d'un RR NSEC3 qui corresponde au plus proche incluant.

Le RR NSEC3 prouve qu'aucune correspondance plus proche n'aurait pu être utilisée pour répondre à cette interrogation.

B.5 Erreur No Data avec caractère générique

Une réponse "no data" pour un nom couvert par un caractère générique. Les RR NSEC3 prouvent que le nom à caractère générique correspondant n'a aucun RR du type demandé et qu'aucune correspondance plus proche n'existe dans la zone.

```
;; En-tête : QR AA DO RCODE=0
;;
;; Question
```

```
a.z.w.exemple.      IN AAAA

;; Réponse
;; (vide)

;; Autorité
exemple.        SOA     ns1.exemple. bugs.x.w.exemple. 1 3600 300 (
                        3600000 3600 )
exemple.        RRSIG   SOA 7 1 3600 20150420235959 20051021000000 (
                        40430 exemple.
                        Hu25UIyNPmvPIVBrldN+9Mlp9Zql39qaUd8i
                        q4ZLlYWfUUbbAS41pG+68z81q1xhkYAcEyHd
                        VI2LmKusbZsT0Q== )

;; RR NSEC3 qui correspond au plus proche incluant (w.exemple)
;; H(w.exemple) = k8udemvp1j2f7eg6jebps17vp3n8i58h

k8udemvp1j2f7eg6jebps17vp3n8i58h.exemple. NSEC3 1 1 12 aabbccdd (
                        kohar7mbb8dc2ce8a9qvl8hon4k53uhi )
k8udemvp1j2f7eg6jebps17vp3n8i58h.exemple. RRSIG NSEC3 7 2 3600 (
                        20150420235959 20051021000000 40430 exemple.
                        FtXGbvF0+wf8iWkyo73enAuVx03klN+pILBK
                        S6qCcftVtfH4yVzsEZquJ27NHR7ruxJWDNMt
                        Otx7w9WfcIg62A== )

;; RR NSEC3 qui couvre le "prochain plus proche" nom (z.w.exemple)
;; H(z.w.exemple) = qlu7gtfaeh0ek0c05ksfhdpbcgglbe03

q04jkcevqvmu85r014c7dkba38o0ji5r.exemple. NSEC3 1 1 12 aabbccdd (
                        r53bq7cc2uvmubfu5ocmm6pers9tk9en A RRSIG )
q04jkcevqvmu85r014c7dkba38o0ji5r.exemple. RRSIG NSEC3 7 2 3600 (
                        20150420235959 20051021000000 40430 exemple.
                        hV5I89b+4FHJDATp09g4bbN0R1F845CaXpL3
                        ZxlMKimoPAyqletMlEWwLfFia7sdpSzn+ZlN
                        NlkxWcLsIlMmUg== )

;; RR NSEC3 qui correspond à un caractère générique au plus proche incluant.
;; H(*.w.exemple) = r53bq7cc2uvmubfu5ocmm6pers9tk9en

r53bq7cc2uvmubfu5ocmm6pers9tk9en.exemple. NSEC3 1 1 12 aabbccdd (
                        t644ebqk9bibcna874givr6joj62mlhv MX RRSIG )
r53bq7cc2uvmubfu5ocmm6pers9tk9en.exemple. RRSIG NSEC3 7 2 3600 (
                        20150420235959 20051021000000 40430 exemple.
                        aupviViruXs4bDg9rCbezzBMf9h1ZlDvbW/C
                        ZFKulIGXXLj8B/fsDJarXVDA9bnUoRhEbKp+
                        HF1FWKW7RIJdtQ== )

;; Additionnel
;; (vide)
```

L'interrogation a retourné les RR NSEC3 qui prouvent que les données demandées n'existent pas et qu'aucun RR à caractère générique ne s'applique.

B.6 Erreur No Data de zone fille DS

Une réponse "no data" pour une interrogation QTYPE=DS qui a été envoyée par erreur à un serveur de noms pour la zone fille.

```
;; En-tête : QR AA DO RCODE=0
;;
;; Question
```

```
exemple.          IN DS

;; Réponse
;; (vide)

;; Autorité
exemple.       SOA     ns1.exemple. bugs.x.w.exemple. 1 3600 300 (
                       3600000 3600 )
exemple.       RRSIG   SOA 7 1 3600 20150420235959 20051021000000 (
                       40430 exemple.
                       Hu25UIyNPmvPIVBrldN+9Mlp9Zql39qaUd8i
                       q4ZLlYWfUUbbAS41pG+68z81q1xhkYAcEyHd
                       VI2LmKusbZsT0Q== )

;; Le RR NSEC3 correspond au QNAME et montre que le bit de type DS n'est pas établi.

0p9mhaveqvm6t7vbl5lop2u3t2rp3tom.exemple. NSEC3 1 1 12 aabbccdd (
                       2t7b4g4vsa5smi47k61mv5bv1a22bojr MX DNSKEY NS
                       SOA NSEC3PARAM RRSIG )
0p9mhaveqvm6t7vbl5lop2u3t2rp3tom.exemple. RRSIG NSEC3 7 2 3600
                       20150420235959 20051021000000 40430 exemple.
                       OSgWSm26B+cS+dDL8b5QrWr/dEWhtCsKlwKL
                       IBHYH6blRxK9rC0bMJPwQ4mLIuw85H2EY762
                       BOCXJZMnpuwhpA== )

;; Additionnel
;; (vide)
```

L'interrogation a retourné un RR NSEC3 montrant que la demande a reçu une réponse par le serveur d'autorité pour la zone "exemple". Le RR NSEC3 indique la présence d'un RR SOA, montrant que ce RR NSEC3 est du sommet de la fille, et non de la portion de zone du parent. Les interrogations pour le RRSet DS "exemple" devraient être envoyées aux serveurs parents (qui dans ce cas sont les serveurs racines).

Appendice C. Considérations spéciales

Les paragraphes qui suivent précisent le comportement spécifique et expliquent les considérations spéciales pour les mises en œuvre.

C.1 Salage

Augmenter les noms de propriétaires originaux avec un sel avant le hachage augmente le coût d'un dictionnaire de valeurs de hachage généré à l'avance. Pour chaque bit de sel, le coût d'un dictionnaire pré-calculé double (parce qu'il doit y avoir une entrée pour chaque mot combiné avec chaque valeur de sel possible). Le RR NSEC3 peut utiliser un maximum de 2040 bits (255 octets) de sel, multipliant le coût par 2^2040. Cela signifie qu'un attaquant doit, en pratique, recalculer le dictionnaire chaque fois que le sel est changé.

Inclure un sel, sans considération de sa taille, n'affecte pas le coût de la construction des RR NSEC3. Cela augmente la taille du RR NSEC3.

Il DOIT y avoir au moins un ensemble complet de RR NSEC3 pour la zone qui utilise la même valeur de sel.

Le sel DEVRAIT être changé périodiquement pour empêcher le pré-calcul en utilisant un seul sel. Il est RECOMMANDÉ que le sel soit changé pour chaque re-signature.

Noter que cela pourrait être cause qu'un résolveur voit les RR avec des valeurs de sel différentes pour la même zone. Ceci est sans danger car chaque RR est autonome (c'est-à-dire, il dénie l'ensemble de noms de propriétaires dont les hachages, en utilisant le sel dans le RR NSEC3, tombe entre les deux hachages dans le RR NSEC3) -- c'est seulement le serveur qui a besoin d'un ensemble complet des RR NSEC3 avec le même sel afin d'être capable de répondre à chaque interrogation possible.

Il n'est pas interdit d'avoir des RR NSEC3 avec des sels différents au sein de la même zone. Cependant, afin que les serveurs d'autorité soient capables de couvrir de façon cohérente les RR NSEC3, le serveur d'autorité DOIT choisir un seul ensemble de paramètres (algorithme, sel, et itérations) à utiliser lors du choix des RR NSEC3.

C.2 Collision de hachage

Des collisions de hachage se produisent quand différents messages ont la même valeur de hachage. Le nombre attendu de noms de domaine nécessaire pour donner une chance sur deux d'une seule collision est d'environ 2^(n/2) pour un hachage de longueur n bits (c'est-à-dire, 2^80 pour SHA-1). Bien que cette probabilité soit extrêmement faible, les paragraphes qui suivent traitent de l'évitement de collisions et de la constatation des dommages possibles dans le cas d'une attaque utilisant les collisions de hachage.

C.2.1 Évitement de collisions de hachage durant la génération

Durant la génération des RR NSEC3, les valeurs de hachage sont supposée être uniques. Dans le cas (académique) de la survenance d'une collision, un sel de remplacement DOIT être choisi et toutes les valeurs de hachage DOIVENT être regénérées.

C.2.2 Analyse de l'exigence de seconde pré-image

Une fonction de hachage cryptographique a une propriété de résistance de seconde pré-image. La propriété de résistance de seconde pré-image signifie qu'il est infaisable par le calcul de trouver un autre message avec la même valeur de hachage qu'un message donné, c'est-à-dire, étant donnée la pré-image X, de trouver une seconde pré-image X' != X telles que hachage(X) = hachage(X'). Le facteur de travail pour trouver une seconde pré-image est de l'ordre de 2^160 pour SHA-1. Pour monter une attaque en utilisant un RR NSEC3 existant, un adversaire doit trouver une seconde pré-image.

En supposant qu'un adversaire soit capable de monter une attaque aussi extrême, le dommage réel est qu'un message de réponse peut être généré qui prétend qu'un certain QNAME (c'est-à-dire, la seconde pré-image) existe bien, alors qu'en réalité ce QNAME n'existe pas (un faux positif) qui va causer la réinterrogation par un résolveur à capacité de sécurité du nom non existant, ou l'échec de l'interrogation initiale. Noter que l'adversaire ne peut pas monter cette attaque sur un nom existant, mais seulement sur un nom que l'adversaire ne peut pas choisir et qui n'existe pas encore.

Adresse des auteurs

Ben Laurie
Nominet
17 Perryn Road
London W3 7LR
UK
téléphone : +44 20 8735 0686
mél : ben@links.org

David Blacka
VeriSign, Inc.
21355 Ridgetop Circle
Dulles, VA 20166
US
téléphone : +1 703 948 3200
mél : davidb@verisign.com

Geoffrey Sisson
Nominet
Minerva House
Edmund Halley Road
Oxford Science Park
Oxford OX4 4DQ
UK
téléphone : +44 1865 332211
mél : geoff-s@panix.com

Roy Arends
Nominet
Minerva House
Edmund Halley Road
Oxford Science Park
Oxford OX4 4DQ
UK
téléphone : +44 1865 332211
mél : roy@nominet.org.uk

Déclaration complète de droits de reproduction