Groupe de travail Réseau
Request for Comments : 4035
RFC rendues obsolètes : 2535, 3008, 3090, 3445, 3655, 3658, 3755, 3757, 3845
RFC mises à jour : 1034, 1035, 2136, 2181, 2308, 3225, 3007, 3597, 3226
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

R. Arends, Telematica Instituut
R. Austein, ISC
M. Larson, VeriSign
D. Massey, Colorado State University
S. Rose, NIST
mars 2005

Modifications de protocole pour les extensions de sécurité du DNS

Statut de ce mémoire

Le présent document spécifie un protocole Internet sur la voie de la normalisation pour la communauté de l'Internet, et appelle à des discussions et suggestions pour son amélioration. Prière de se reporter à l'édition actuelle du STD 1 "Normes des protocoles officiels de l'Internet" pour connaître l'état de normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

Résumé

Le présent document fait partie d'une famille de documents qui décrivent les extensions de sécurité du DNS (DNSSEC). Les extensions de sécurité du DNS sont une collection de nouveaux enregistrements de ressource et de modifications de protocole qui ajoutent l'authentification d'origine des données et l'intégrité des données au DNS. Le présent document décrit les modifications du protocole DNSSEC. Le présent document définit le concept de zone signée, avec les exigences de service et de résolution en utilisant DNSSEC. Ces techniques permettent à un résolveur à capacité de sécurité d'authentifier aussi bien les enregistrements de ressource du DNS que les indications d'erreur du DNS d'autorité.

Le présent document rend obsolète la RFC 2535 et incorpore les changements survenus dans toutes les mises à jour à la RFC 2535.

Table des Matières

1. Introduction

Les extensions de sécurité du DNS sont une collection de nouveaux enregistrements de ressource et de modifications de protocole qui ajoutent l'authentification d'origine des données et l'intégrité des données au DNS. Le présent document décrit les modifications du protocole DNSSEC. La Section 2 du document définit le concept de zone signée et fait la liste des exigences pour la signature de zone. La Section 3 décrit les modifications du comportement du serveur de noms d'autorité qui sont nécessaires pour le traitement des zones signées. La Section 4 décrit le comportement des entités qui comportent des fonctions de résolveur à capacité de sécurité. Finalement, la Section 5 définit comment utiliser les RR DNSSEC pour authentifier une réponse.

1.1 Fondements et documents en rapport

Le présent document fait partie d'une famille de documents qui définissent DNSSEC et devraient être lus comme un ensemble.

La [RFC4033] contient une introduction au DNSSEC et les définitions des termes communs ; le lecteur est supposé familier avec ce document. La [RFC4033] contient aussi une liste des autres documents mis à jour et rendus obsolètes par cet ensemble de documents.

La [RFC4034] définit les enregistrements de ressource DNSSEC.

Le lecteur est aussi supposé familiarisé avec les concepts de base du DNS décrits dans les [RFC1034], [RFC1035], et dans les documents ultérieurs qui les mettent à jour, en particulier les [RFC2181] et [RFC2308].

Le présent document définit les opérations de protocole de DNSSEC.

1.2 Mots réservés

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

2. Signature de zone

DNSSEC introduit le concept de zone signée. Une zone signée comporte un enregistrement de clé publique DNS (DNSKEY, *DNS Public Key*), une signature d'enregistrement de ressource (RRSIG, *Resource Record Signature*), le prochain enregistrement sécurisé (NSEC, *Next Secure*), et (facultativement) des enregistrements de signataire de délégation (DS, *Delegation Signer*) conformément aux règles spécifiées aux paragraphes 2.1 à 2.4. Une zone qui ne comporte pas ces enregistrements conformément aux règles de cette section est une zone non signée.

DNSSEC exige un changement de la définition de l'enregistrement de ressource CNAME ([RFC1035]). Le paragraphe 2.5 change le RR CNAME pour permettre aux RR RRSIG et NSEC d'apparaître sous le même nom de propriétaire, comme le fait un RR CNAME.

DNSSEC spécifie le placement de deux nouveaux types de RR, NSEC et DS, qui peuvent être placés du côté parent d'une coupure de zone (c'est-à-dire, à un point de délégation). Ceci est une exception à l'interdiction générale de mettre des données dans la zone parente à une coupure de zone. Le paragraphe 2.6 décrit ce changement.

2.1 Inclusion des RR DNSKEY dans une zone

Pour signer une zone, l'administrateur de la zone génère une ou plusieurs paires de clés publiques/privées et utilise la ou les clés privées pour signer les RRset d'autorité dans la zone. Pour chaque clé privée utilisée pour créer des RR RRSIG dans une zone, la zone DEVRAIT inclure un RR DNSKEY de zone contenant la clé publique correspondante. Un RR DNSKEY de clé de zone DOIT avoir le bit Clé de zone des fanions de champ RDATA établi (voir au paragraphe 2.1.1 de la [RFC4034]). Les clés publiques associées à d'autres opérations du DNS PEUVENT être mémorisées dans les RR DNSKEY qui ne sont pas marqués comme clés de zone mais NE DOIVENT PAS être utilisées pour vérifier les RRSIG.

Si l'administrateur de zone veut qu'une zone signée soit utilisable autrement que comme un îlot de sécurité, le sommet *(apex)* de zone DOIT contenir au moins un RR DNSKEY qui agisse comme point d'entrée sécurisé de la zone. Ce point d'entrée sécurisé pourrait alors être utilisé comme cible d'une délégation sécurisée via un RR DS correspondant dans la zone parente (voir la [RFC4034]).

2.2 Inclusion des RR RRSIG dans une zone

Pour chaque RRset d'autorité dans une zone signée, il DOIT y avoir au moins un enregistrement RRSIG qui satisfait aux exigences suivantes :

- Le nom de propriétaire du RRSIG est égal au nom de propriétaire du RRset.
- La classe du RRSIG est égale à la classe du RRset.
- Le champ Type couvert du RRSIG est égal au type du RRset.
- Le champ TTL d'origine du RRSIG est égal au TTL du RRset.
- Le TTL du RR RRSIG est égal au TTL du RRset.
- Le champ Étiquettes du RRSIG est égal au nombre d'étiquettes dans le nom de propriétaire du RRset, sans compter l'étiquette racine nulle et sans compter l'étiquette la plus à gauche si c'est un caractère générique.
- Le champ Nom du signataire du RRSIG est égal au nom de la zone qui contient le RRset.
- Les champs Algorithme, Nom du signataire et Étiquette de clé du RRSIG identifient un enregistrement de ressource DNSKEY de clé de zone au sommet de la zone.

Le processus de construction du RR RRSIG pour un RRset donné est décrit dans la [RFC4034]. Un RRset PEUT avoir plusieurs RR RRSIG qui lui sont associés. Noter que comme les RR RRSIG sont étroitement liés aux RRset dont ils contiennent les signatures, les RR RRSIG, à la différence de tous les autres types de RR du DNS, ne forment pas de RRset. En particulier, les valeurs de TTL parmi les RR RRSIG ayant un nom de propriétaire commun ne suivent pas les règles de RRset décrites dans la [RFC2181].

Un RR RRSIG NE DOIT PAS lui-même être signé, car signer un RR RRSIG n'ajouterait rien et créerait une boucle infinie dans le processus de signature.

Le RRset NS qui apparaît au nom sommet de zone DOIT être signé, mais les RRset NS qui apparaissent aux points de délégation (c'est-à-dire, les RRset NS dans la zone parente qui délègue le nom aux serveurs de nom de la zone fille) NE DOIVENT PAS être signés. Les RRset d'adresse glu associés aux délégations NE DOIVENT PAS être signés.

Il DOIT y avoir un RRSIG pour chaque RRset utilisant au moins une DNSKEY de chaque algorithme dans le RRset DNSKEY du sommet de zone. Le RRset DNSKEY sommet lui même DOIT être signé par chaque algorithme qui apparaît dans le RRset DS localisé chez le parent délégataire (s'il en est).

2.3 Inclusion des RR NSEC dans une zone

Chaque nom de propriétaire qui dans une zone a des données d'autorité ou un RRset NS de point de délégation DOIT avoir un enregistrement de ressource NSEC. Le format des RR NSEC et le processus de construction du RR NSEC pour un nom donné sont décrits dans la [RFC4034].

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

Un enregistrement NSEC (et son RRset RRSIG associé) NE DOIT PAS être le seul RRset chez un nom de propriétaire quelconque. C'est-à-dire que le processus de signature NE DOIT PAS créer de RR NSEC ou RRSIG pour les nœuds de nom de propriétaire qui n'étaient pas le nom du propriétaire d'un RRset avant que la zone ne soit signée. La principale raison en est le désir d'une certaine cohérence de l'espace de noms entre les versions signées et non signées de la même zone ainsi que de réduire le risque d'incohérence des réponses dans les serveurs de noms récurrents oublieux de la sécurité.

La correspondance binaire de type de tout enregistrement de ressource NSEC dans une zone signée DOIT indiquer la présence à la fois de l'enregistrement NSEC lui-même et de son enregistrement RRSIG correspondant.

La différence entre l'ensemble des noms de propriétaires qui exigent des enregistrements RRSIG et l'ensemble des noms de propriétaires qui exigent des enregistrements NSEC est subtile et vaut d'être soulignée. Les enregistrements RRSIG sont présents chez les noms de propriétaire de tous les RRset d'autorité. Les enregistrements NSEC sont présents chez les noms de propriétaire de tous les noms pour lesquels la zone signée est d'autorité et aussi chez les noms de propriétaire de délégations de la zone signée à ses enfants. Les enregistrements ni NSEC ni RRSIG ne sont présents (dans la zone parente) chez les noms de propriétaire des RRset d'adresse glu. Noter, cependant, que cette distinction n'est pour l'essentiel visible que durant le processus de signature de zone, car les RRset NSEC sont des données d'autorité et sont donc signées. Et donc, tout nom de propriétaire qui a un RRset NSEC aura aussi des RR RRSIG dans la zone signée.

La correspondance binaire pour le RR NSEC à un point de délégation exige une attention particulière. Les bits qui correspondent au RRset NS de délégation et tout RRset pour lequel la zone parente a des données d'autorité DOIVENT être établis ; les bits qui correspondent à un RRset non NS pour lequel le parent n'est pas d'autorité DOIVENT être à zéro.

2.4 Inclusion des RR DS dans une zone

L'enregistrement de ressource DS établit les chaînes d'authentification entre les zones du DNS. Un RRset DS DEVRAIT être présent à un point de délégation lorsque la zone fille est signée. Le RRset DS PEUT contenir plusieurs enregistrements, chacun faisant référence à une clé publique dans la zone fille, utilisée pour vérifier les RRSIG dans cette zone. Tous les RRset DS dans une zone DOIVENT être signés, et les RRset DS NE DOIVENT PAS apparaître au sommet d'une zone.

Un RR DS DEVRAIT pointer sur un RR DNSKEY qui est présent dans le RRset DNSKEY sommet de la fille, et le RRset DNSKEY sommet de la fille DEVRAIT être signé par la clé privée correspondante. Les RR DS qui ne réussissent pas à satisfaire à ces conditions ne sont pas utilisables pour la validation, mais parce que le RR DS et son RR DNSKEY correspondant sont dans des zones différentes, et parce que le DNS n'a qu'une cohérence assez lâche, des discordances temporaires peuvent survenir.

Le TTL d'un RRset DS DEVRAIT correspondre au TTL du RRset NS délégataire (c'est-à-dire, le RRset NS provenant de la même zone que celle qui contient le RRset DS).

La construction d'un RR DS exige la connaissance du RR DNSKEY correspondant dans la zone fille, ce qui implique une communication entre les zones fille et parente. Cette communication est une affaire de fonctionnement non traitée par ce document.

2.5 Changements à l'enregistrement de ressource CNAME

Si un RRset CNAME est présent sur un nom dans une zone signée, les RRset RRSIG et NSEC appropriés sont EXIGÉS sur ce nom. Un RRset KEY à ce nom est aussi permis aux fins de mise à jour dynamique sécurisée ([RFC3007]). D'autres types NE DOIVENT PAS être présents sur ce nom.

C'est une modification de la définition originale de CNAME donnée dans la [RFC1034]. La définition originale du RR CNAME ne permettait à aucun autre type de coexister avec un enregistrement CNAME, mais une zone signée exige des RR NSEC et RRSIG pour chaque nom d'autorité. Pour résoudre ce conflit, la présente spécification modifie la définition de l'enregistrement de ressource CNAME pour lui permettre de coexister avec les RR NSEC et RRSIG.

2.6 Types de RR DNSSEC qui apparaissent aux coupures de zone

DNSSEC a introduit deux nouveaux types de RR qui sont inhabituels en ce qu'ils peuvent apparaître du côté parent d'une coupure de zone. Du côté parent d'une coupure de zone (c'est-à-dire, à un point de délégation) les RR NSEC sont EXIGÉS sur le nom de propriétaire. Un RR DS pourrait aussi être présent si la zone qui va être déléguée est signée et cherche à avoir une chaîne d'authentification de la zone parente. Ceci est une exception à la spécification DNS d'origine ([RFC1034]), qui déclare que seuls les RRset NS peuvent apparaître du côté parent d'une coupure de zone.

La présente spécification met à jour la spécification DNS d'origine pour permettre les types de RR NSEC et DS du côté parent d'une coupure de zone. Ces RRset sont d'autorité pour le parent lorsqu'ils apparaissent du côté parental d'une coupure de zone.

2.7 Exemple d'une zone sécurisée

L'Appendice A donne un exemple complet d'une petite zone signée.

3. Service

La présente section décrit le comportement d'entités qui comportent des fonctions de serveur de noms à capacité de sécurité. Dans de nombreux cas, de telles fonctions feront partie d'un serveur de noms récurrent à capacité de sécurité, mais un serveur de nom d'autorité à capacités de sécurité a certaines des mêmes exigences. Les fonctions spécifiques des serveurs de noms récurrents à capacité de sécurité sont décrites au paragraphe 3.2 ; les fonctions spécifiques des serveurs d'autorité sont décrites au paragraphe 3.1.

Dans l'exposé qui suit, les termes "SNAME", "SCLASS" et "STYPE" sont tels que définis dans la [RFC1034].

Un serveur de noms à capacité de sécurité DOIT prendre en charge l'extension de taille de message EDNS0 ([RFC2671]), il DOIT prendre en charge une taille de message d'au moins 1220 octets, et il DEVRAIT accepter une taille de message de 4000 octets. Comme les paquets IPv6 ne peuvent être fragmentés que par l'hôte de source, un serveur de noms à capacité de sécurité DEVRAIT prendre des mesures pour s'assurer que les datagrammes UDP qu'il transmet sur IPv6 sont fragmentés, si nécessaire, à la MTU IPv6 minimum, sauf si la MTU de chemin est connue. Prière de se reporter aux [RFC1122], [RFC2460] et [RFC3226] pour des précisions sur les questions de taille de paquet et de fragmentation.

Un serveur de noms à capacité de sécurité qui reçoit une interrogation DNS ne comportant pas le pseudo-RR OPT EDNS ou qui a le bit DO à zéro DOIT traiter les RR RRSIG, DNSKEY et NSEC comme il le ferait de tout autre RRset et NE DOIT PAS effectuer un des traitements additionnels décrits ci-dessous. Parce que le type de RR DS a la propriété particulière de n'exister que dans la zone parente aux points de délégation, les RR DS exigent toujours un traitement particulier, comme décrit au paragraphe 3.1.4.1.

Les serveurs de noms à capacité de sécurité qui reçoivent des interrogations explicites pour les types de RR de sécurité qui correspondent au contenu de plus d'une zone qu'ils desservent (par exemple, les RR NSEC et RRSIG au dessus et en dessous d'un point de délégation où le serveur est d'autorité pour les deux zones) devraient se comporter de façon cohérente en interne. Pour autant que la réponse soit toujours cohérente pour chaque interrogation de serveur de noms, le serveur de noms PEUT retourner une des réponses suivantes :

- Les RRset au dessus du point de délégation.
- Les RRset en dessous du point de délégation.
- Les RRset au dessus et au dessous du point de délégation.
- Une section de réponse vide (pas d'enregistrement).
- Une autre réponse.
- Une erreur.

DNSSEC alloue deux nouveaux bits dans l'en-tête de message DNS : le bit CD (Checking Disabled, *vérification désactivée*) et le bit AD (Authentic Data, *données authentiques*). Le bit CD est contrôlé par les résolveurs ; un serveur de noms à capacité de sécurité DOIT copier le bit CD d'une interrogation dans la réponse correspondante. Le bit AD est contrôlé par les serveurs de noms ; un serveur de noms à capacité de sécurité DOIT ignorer le réglage du bit AD dans les interrogations. Voir aux paragraphes 3.1.6, 3.2.2, 3.2.3, 4, et 4.9 les détails du comportement de ces bits.

Un serveur de noms à capacité de sécurité qui fait la synthèse des RR CNAME à partir des RR DNAME comme décrit dans la [RFC2672] NE DEVRAIT PAS générer de signatures pour les RR CNAME synthétisés.

3.1 Serveurs de noms d'autorité

À réception d'une interrogation pertinente qui a le bit DO [RFC3225] de pseudo RR OPT EDNS [RFC2671] établi, un serveur de noms d'autorité à capacité de sécurité pour une zone signée DOIT inclure des RR RRSIG, NSEC, et DS supplémentaires, conformément aux règles suivantes :

- o les RR RRSIG qui peuvent être utilisés pour authentifier une réponse DOIVENT être inclus dans la réponse conformément aux règles du paragraphe 3.1.1.

- o les RR NSEC qui peuvent être utilisés pour fournir un déni d'existence authentifié DOIVENT être inclus dans la réponse automatique conformément aux règles du paragraphe 3.1.3.

- o Un RRset DS ou un RR NSEC prouvant qu'il n'existe aucun RR DS DOIT être inclus dans les références automatiques conformément aux règles du paragraphe 3.1.4.

Ces règles ne s'appliquent qu'aux réponses dont la sémantique porte des informations sur la présence ou l'absence d'enregistrements de ressource. C'est-à-dire, ces règles ne sont pas destinées à exclure des réponses comme RCODE 4 ("Non mis en œuvre") ou RCODE 5 ("Refusé").

DNSSEC ne change pas le protocole de transfert de zone du DNS. Le paragraphe 3.1.5 expose les exigences de transfert de zone.

3.1.1 Inclusion des RR RRSIG dans une réponse

Lorsque il répond à une interrogation qui a le bit DO établi, un serveur de noms d'autorité à capacité de sécurité DEVRAIT tenter d'envoyer les RR RRSIG qu'un résolveur à capacité de sécurité peut utiliser pour authentifier les RRset dans la réponse. Un serveur de noms DEVRAIT tout tenter pour garder ensemble le RRset et ses RRSIG associés dans une réponse. L'inclusion des RR RRSIG dans une réponse est soumise aux règles suivantes :

- o Lorsque il place un RRset signé dans la section Réponse, le serveur de noms DOIT aussi placer ses RR RRSIG dans la section Réponse. Les RR RRSIG ont une plus forte priorité d'inclusion que tous les autres RRset qui peuvent avoir à être inclus. Si l'espace ne permet pas l'inclusion de ces RR RRSIG, le serveur de noms DOIT établir le bit TC.

- o Lorsque il place un RRset signé dans la section Autorité, le serveur de noms DOIT aussi placer ses RR RRSIG dans la section Autorité. Les RR RRSIG ont une plus forte priorité d'inclusion que tous les autres RRset qui peuvent devoir être inclus. Si l'espace ne permet pas l'inclusion de ces RR RRSIG, le serveur de noms DOIT établir le bit TC.

- o Lorsque il place un RRset signé dans la section Additionnelle, le serveur de noms DOIT aussi placer ses RR RRSIG dans la section Additionnelle. Si l'espace ne permet pas l'inclusion du RRset et de ses RR RRSIG associés, le serveur de noms PEUT conserver le RRset tout en abandonnant les RR RRSIG. Si cela arrive, le serveur de noms NE DOIT PAS établir le bit TC seulement parce que les RR RRSIG ne tenaient pas.

3.1.2 Inclusion des RR DNSKEY dans une réponse

Lorsque il répond à une interrogation qui a le bit DO établi et qui demande les RR SOA ou NS au sommet d'une zone signée, un serveur de noms d'autorité à capacités de sécurité pour cette zone PEUT retourner le RRset DNSKEY sommet de zone dans la section Additionnelle. Dans cette situation, le RRset DNSKEY et les RR RRSIG associés ont une plus faible priorité que toutes les autres informations qui seraient placées dans la section Additionnelle. Le serveur de noms NE DEVRAIT PAS inclure le RRset DNSKEY sauf si il y a assez d'espace dans le message de réponse pour le RRset DNSKEY et ses RR RRSIG associés. Si il n'y a pas assez d'espace pour inclure ce DNSKEY et les RR RRSIG, le serveur de noms DOIT les omettre et NE DOIT PAS établir le bit TC seulement parce que ces RR ne tenaient pas (voir au paragraphe 3.1.1).

3.1.3 Inclusion des RR NSEC dans une réponse

Lorsque il répond à une interrogation qui a le bit DO établi, un serveur de noms d'autorité à capacités de sécurité pour une zone signée DOIT inclure les RR NSEC dans chacun des cas suivants :

Pas de données : la zone contient des RRset qui correspondent exactement à <SNAME, SCLASS> mais ne contient aucun RRset qui corresponde exactement à <SNAME, SCLASS, STYPE>.

Erreur de nom : la zone ne contient aucun RRset qui corresponde à <SNAME, SCLASS> soit exactement, soit via une expansion de nom par caractère générique.

Réponse avec caractère générique : la zone ne contient aucun RRset qui corresponde exactement à <SNAME, SCLASS> mais contient un RRset qui correspond à <SNAME, SCLASS, STYPE> via une expansion de nom par caractère générique.

Caractère générique sans données : la zone ne contient aucun RRset qui corresponde exactement à <SNAME, SCLASS> et contient un ou plusieurs RRset qui correspondent à <SNAME, SCLASS> via une expansion de nom par caractère générique, mais ne contient aucun RRset qui corresponde à <SNAME, SCLASS, STYPE> via une expansion de nom par caractère générique.

Dans chacun de ces cas, le serveur de noms inclut les RR NSEC dans la réponse pour prouver qu'il n'y avait pas de correspondance exacte pour <SNAME, SCLASS, STYPE> dans la zone et que la réponse que le serveur de noms retourne est correcte selon les données de la zone.

3.1.3.1 Inclusion des RR NSEC : pas de réponse de données

Si la zone contient des RRset qui correspondent à <SNAME, SCLASS> mais ne contient pas de RRset correspondant à <SNAME, SCLASS, STYPE>, alors le serveur de noms DOIT inclure le RR NSEC pour <SNAME, SCLASS> avec ses RR RRSIG associés dans la section Autorité de la réponse (voir le paragraphe 3.1.1). Si l'espace ne permet pas l'inclusion du RR NSEC ou de ses RR RRSIG associés, le serveur de noms DOIT établir le bit TC (voir le paragraphe 3.1.1).

Comme le nom recherché existe, l'expansion de nom par caractère générique ne s'applique pas à cette interrogation, et un seul RR NSEC signé suffit à prouver que le type de RR demandé n'existe pas.

3.1.3.2 Inclusion des RR NSEC : réponse d'erreur de nom

Si la zone ne contient aucun RRset correspondant à <SNAME, SCLASS> soit exactement soit via l'expansion de nom par caractère générique, alors le serveur de noms DOIT inclure les RR NSEC suivants dans la section Autorité, avec leurs RR RRSIG associés :

- un RR NSEC prouvant qu'il n'y a pas de correspondance exacte pour <SNAME, SCLASS>,
- un RR NSEC prouvant que la zone ne contient pas de RRset qui correspondrait à <SNAME, SCLASS> via l'expansion de nom par caractère générique.

Dans certains cas, un seul RR NSEC peut prouver ces deux points. Si il le fait, le serveur de noms DEVRAIT seulement inclure le RR NSEC et ses RR RRSIG une fois dans la section Autorité.

Si l'espace ne permet pas l'inclusion de ces RR NSEC et RRSIG, le serveur de noms DOIT établir le bit TC (voir le paragraphe 3.1.1).

Les noms de possesseur de ces RR NSEC et RRSIG ne sont pas sujets à l'expansion de nom par caractère générique lorsque ces RR sont inclus dans la section Autorité de la réponse.

Noter que cette forme de réponse inclut des cas dans lesquels le SNAME correspond à un nom vide non terminal au sein de la zone (un nom qui n'est pas le nom du possesseur pour tout RRset mais qui est le nom parent d'un ou plusieurs RRset).

3.1.3.3 Inclusion des RR NSEC : Réponse avec expansion de caractère générique

Si la zone ne contient aucun RRset qui corresponde exactement à <SNAME, SCLASS> mais contient un RRset qui correspond à <SNAME, SCLASS, STYPE> via l'expansion de nom par caractère générique, le serveur de noms DOIT inclure la réponse expansée par le caractère générique et les RR RRSIG correspondants expansés par caractères génériques dans la section Réponse et DOIT inclure dans la section Autorité un RR NSEC et les RR RRSIG associés qui prouvent que la zone ne contient pas une correspondance plus proche pour <SNAME, SCLASS>. Si l'espace ne permet pas l'inclusion dans la réponse des RR NSEC et RRSIG, le serveur de noms DOIT établir le bit TC (voir le paragraphe 3.1.1).

3.1.3.4 Inclusion des RR NSEC : réponse sans données de caractère générique

Ce cas est une combinaison des précédents. La zone ne contient pas une correspondance exacte pour <SNAME, SCLASS>, et bien que la zone contienne des RRset qui correspondent à <SNAME, SCLASS> via l'expansion de caractère générique, aucun de ces RRset ne correspond au STYPE. Le serveur de noms DOIT inclure les RR NSEC suivants dans la section Autorité, avec leurs RR RRSIG associés :

- o un RR NSEC prouvant qu'il n'y a pas de RRset correspondant à STYPE au nom de propriétaire avec caractère générique qui corresponde à <SNAME, SCLASS> via l'expansion du caractère générique,
- o un RR NSEC prouvant qu'il n'y a pas de RRset dans la zone qui aurait été une meilleure correspondance plus proche pour <SNAME, SCLASS>.

Dans certains cas, un seul RR NSEC peut prouver ces deux points. Si il le fait, le serveur de noms DEVRAIT seulement inclure le RR NSEC et ses RR RRSIG une fois dans la section Autorité.

Les noms de propriétaire de ces RR NSEC et RRSIG ne sont pas soumis à l'expansion de nom par caractère générique lorsque ces RR sont inclus dans la section Autorité de la réponse.

Si l'espace ne permet pas l'inclusion de ces RR NSEC et RRSIG, le serveur de noms DOIT établir le bit TC (voir le paragraphe 3.1.1).

3.1.3.5 Trouver les bons RR NSEC

Comme expliqué ci-dessus, il y a plusieurs situations dans lesquelles un serveur de noms d'autorité à capacités de sécurité doit localiser un RR NSEC qui prouve qu'il n'existe aucun RRset correspondant à un SNAME particulier. Localiser un tel RR NSEC au sein d'une zone d'autorité est relativement simple, au moins en théorie. La discussion qui suit suppose que le serveur de noms est d'autorité pour la zone qui aurait contenu les RRset non existants correspondants à SNAME. L'algorithme ci-dessous a été écrit pour la clarté, non pour l'efficacité.

Pour trouver le NSEC qui prouve qu'aucun RRset correspondant au nom N n'existe dans la zone Z qui l'aurait contenu, construire une séquence, S, consistant en les noms de propriétaire de chaque RRset dans Z, triés dans l'ordre canonique ([RFC4034]), sans nom dupliqué. Trouver le nom M qui aurait immédiatement précédé N dans S si un RRset avec le nom de propriétaire N avait existé. M est le nom de propriétaire du RR NSEC qui prouve qu'aucun RRset n'existe avec le nom de propriétaire N.

L'algorithme pour trouver le RR NSEC qui prouve qu'un certain nom n'est pas couvert par un caractère générique applicable est similaire mais requiert une étape supplémentaire. Plus précisément, l'algorithme pour trouver le NSEC prouvant qu'aucun RRset n'existe avec le nom à caractère générique applicable est précisément le même que l'algorithme pour trouver le RR NSEC qui prouve que des RRset avec tout autre nom de propriétaire n'existent pas. La partie qui manque est une méthode pour déterminer le nom du caractère générique non existant applicable. En pratique, c'est facile, parce que le serveur de noms d'autorité a déjà vérifié la présence précisément de ce nom à caractère générique au titre de l'étape (1)(c) de l'algorithme normal de recherche décrit au paragraphe 4.3.2 de la [RFC1034].

3.1.4 Inclusion des RR DS dans une réponse

Lorsque il répond à une interrogation qui a le bit DO établi, un serveur de noms d'autorité à capacités de sécurité qui retourne une référence inclut des données de DNSSEC avec le RRset NS.

Si un RRset DS est présent au point de délégation, le serveur de noms DOIT retourner le RRset DS et les RR RRSIG associés dans la section Autorité avec le RRset NS.

Si aucun RRset DS n'est présent au point de délégation, le serveur de noms DOIT retourner le RR NSEC qui prouve que le RRset DS n'est pas présent et les RR RRSIG associés du RR NSEC avec le RRset NS. Le serveur de noms DOIT placer le RRset NS avant le RRset NSEC et ses RR RRSIG associés.

Inclure ces RR DS, NSEC, et RRSIG augmente la taille des messages de référence et peut être cause que certains RR glu ou tous soient omis. Si l'espace ne permet pas l'inclusion du RR DS ou des RR NSEC et des RR RRSIG associés, le serveur de noms DOIT établir le bit TC (voir le paragraphe 3.1.1).

3.1.4.1 Réponse aux interrogations pour les RR DS

Le type d'enregistrement de ressource DS est inhabituel en ce qu'il apparaît seulement sur le côté de la zone parente d'une coupure de zone. Par exemple, le RRset DS pour la délégation de "foo.exemple" est mémorisé dans la zone "exemple" plutôt que dans la zone "foo.exemple". Cela exige des règles de traitement spéciales aussi bien pour les serveurs de noms

que pour les résolveurs, car le serveur de noms pour la zone fille est d'autorité pour le nom dans la zone coupée selon les règles normales du DNS mais la zone fille ne contient pas le RRset DS.

Un résolveur à capacités de sécurité envoie des interrogations à la zone parente lorsque il cherche un RR DS dont il a besoin à un point de délégation (voir le paragraphe 4.2). Cependant, des règles particulières sont nécessaires pour éviter de perturber les résolveurs sans capacité de sécurité qui pourraient être impliqués dans le traitement d'une telle interrogation (par exemple, dans une configuration de réseau qui force un résolveur à capacités de sécurité à passer ses interrogations à travers un serveur de noms récurrent sans capacité de sécurité). Le reste de ce paragraphe décrit comment un serveur de noms à capacité de sécurité traite les interrogations DS afin d'éviter ce problème.

Le besoin d'un traitement spécial par un serveur de noms à capacité de sécurité ne survient que lorsque toutes les conditions suivantes sont réunies :
- o le serveur de noms a reçu une interrogation pour le RRset DS à une coupure de zone,
- o le serveur de noms est d'autorité pour la zone fille,
- o le serveur de noms n'est pas d'autorité pour la zone parente,
- o le serveur de noms n'offre pas la récurrence.

Dans tous les autres cas, le serveur de noms a des moyens d'obtenir le RRset DS ou ne pourrait pas être supposé avoir le RRset DS même par les règles de traitement pré DNSSEC, de sorte que le serveur de noms peut retourner soit le RRset DS soit une réponse d'erreur selon les règles de traitement normales.

Si toutes les conditions ci-dessus sont réunies, le serveur de noms est d'autorité pour SNAME mais ne peut cependant pas fournir le RRset demandé. Dans ce cas, le serveur de noms DOIT retourner une réponse d'autorité "pas de données" montrant que le RRset DS n'existe pas dans le sommet de la zone fille. Voir à l'Appendice B.8 un exemple d'une telle réponse.

3.1.5 Réponse aux interrogations pour le type AXFR ou IXFR

DNSSEC ne change pas le processus de transfert de zone DNS. Une zone signée va contenir des enregistrements de ressource RRSIG, DNSKEY, NSEC, et DS, mais ces enregistrements n'ont pas de signification particulière à l'égard d'une opération de transfert de zone.

Un serveur de noms d'autorité n'est pas obligé de vérifier qu'une zone est correctement signée avant d'envoyer ou accepter un transfert de zone. Cependant, un serveur de noms d'autorité PEUT choisir de rejeter le transfert de zone entier si la zone ne peut pas satisfaire les exigences de signature décrites à la Section 2. Le principal objectif d'un transfert de zone est de s'assurer que tous les serveurs de noms d'autorité ont des copies identiques de la zone. Un serveur de noms d'autorité qui choisit d'effectuer sa propre validation de zone NE DOIT PAS sélectivement rejeter certains RR et en accepter d'autres.

Le RRset DS apparaît seulement sur le côté parent d'une coupure de zone et ce sont des données d'autorité dans la zone parente. Comme avec tout autre RRset d'autorité, le RRset DS DOIT être inclus dans les transferts de zone de la zone dans laquelle le RRset est d'autorité. Dans le cas du RRset DS, c'est la zone parente.

Les RR NSEC apparaissent dans les deux zones parente et fille à une coupure de zone et sont des données d'autorité dans les deux zones parente et fille. Les RR NSEC parent et fille à une coupure de zone ne sont jamais identiques, car le RR NSEC dans le sommet de la zone fille va toujours indiquer la présence du RR SOA de la zone fille tandis que le RR NSEC parent à la coupure de zone ne va jamais indiquer la présence d'un RR SOA. Comme avec tous les autres RR d'autorité, les RR NSEC DOIVENT être inclus dans les transferts de zone de la zone dans laquelle ils sont des données d'autorité. Le RR NSEC parent à une coupure de zone DOIT être inclus dans les transferts de zone de la zone parente, et le NSEC au sommet de zone de la zone fille DOIT être inclus dans les transferts de zone de la zone fille.

Les RR RRSIG apparaissent dans les deux zones parente et fille à une coupure de zone et sont d'autorité dans celle, quelle qu'elle soit, qui contient le RRset d'autorité pour lequel le RR RRSIG fournit la signature. C'est-à-dire, le RR RRSIG pour un RRset DS ou un RR NSEC parent à une coupure de zone sera d'autorité dans la zone parente, et le RRSIG pour tout RRset dans le sommet de la zone fille sera d'autorité dans la zone fille. Les RR RRSIG parent et fils à une coupure de zone ne seront jamais identiques l'un à l'autre parce que le champ Nom du signataire d'un RR RRSIG dans le sommet de la zone fille va indiquer un RR DNSKEY dans le sommet de la zone fille tandis que le même champ d'un RR RRSIG parent à la coupure de zone va indiquer un RR DNSKEY dans le sommet de la zone parente. Comme avec tous les autres RR d'autorité, les RR RRSIG DOIVENT être inclus dans les transferts de zone de la zone dans laquelle ils sont des données d'autorité.

3.1.6 Bits AD et CD dans une réponse d'autorité

Les bits CD et AD sont conçus pour être utilisés dans la communication entre un résolveur à capacités de sécurité et un serveur de noms récurrent à capacités de sécurité. Ces bits ne sont pour la plupart pas pertinents pour le traitement des interrogations par les serveurs de noms d'autorité à capacités de sécurité.

Un serveur de noms à capacité de sécurité n'effectue pas de validation de signature pour les données d'autorité durant le traitement de l'interrogation, même lorsque le bit CD est à zéro. Un serveur de noms à capacité de sécurité DEVRAIT mettre à zéro le bit CD lorsque il compose une réponse d'autorité.

Un serveur de noms à capacité de sécurité NE DOIT PAS établir le bit AD dans une réponse sauf si le serveur de noms considère tous les RRset dans les sections Réponse et Autorité de la réponse comme authentiques. La politique locale d'un serveur de noms à capacité de sécurité PEUT considérer les données provenant d'une zone d'autorité comme authentiques sans autre validation. Cependant, le serveur de noms NE DOIT le faire que si le serveur de noms a obtenu la zone d'autorité via des moyens sûrs (comme un mécanisme sûr de transfert de zone) et NE DOIT faire ainsi que si ce comportement a été explicitement configuré.

Un serveur de noms à capacité de sécurité qui prend en charge la récurrence DOIT suivre les règles données au paragraphe 3.2 pour les bits CD et AD lors de la génération d'une réponse qui implique des données obtenues via une récurrence.

3.2 Serveurs de noms récurrents

Comme l'explique la [RFC4033], un serveur de noms récurrent à capacités de sécurité est une entité qui agit dans les deux rôles de serveur de noms à capacité de sécurité et de résolveur à capacités de sécurité. Ce paragraphe utilise les termes de "côté serveur de noms" et "côté résolveur" pour se référer respectivement au code au sein d'un serveur de noms récurrent à capacités de sécurité qui met en œuvre le rôle de serveur de noms à capacité de sécurité et au code qui met en œuvre le rôle de résolveur à capacités de sécurité.

Le côté résolveur suit les règles usuelles pour la mise en antémémoire et la mise en antémémoire négative qui s'appliqueraient à tout résolveur à capacités de sécurité.

3.2.1 Bit DO

Le côté résolveur d'un serveur de noms récurrent à capacités de sécurité DOIT établir le bit DO lors de l'envoi des demandes, sans considération de l'état du bit DO dans la demande initiatrice reçue par le côté serveur de noms. Si le bit DO dans une interrogation initiatrice n'est pas établi, le côté serveur de noms DOIT supprimer tout RR DNSSEC authentifiant de la réponse mais NE DOIT PAS supprimer de types RR DNSSEC que l'interrogation initiatrice a explicitement demandé.

3.2.2 Bit CD

Le bit CD existe afin de permettre à un résolveur à capacités de sécurité de désactiver la validation de signature dans le traitement d'un serveur de noms à capacité de sécurité d'une interrogation particulière.

Le côté serveur de noms DOIT copier le réglage du bit CD provenant d'une interrogation dans la réponse correspondante.

Le côté serveur de noms d'un serveur de noms récurrent à capacités de sécurité DOIT passer l'état du bit CD au côté résolveur avec le reste d'une interrogation initiatrice, afin que le côté résolveur sache si il doit vérifier les données de la réponse qu'il retourne au côté serveur de noms. Si le bit CD est établi, cela indique que le résolveur générateur veut effectuer toute authentification qu'exige sa politique locale. Donc, le côté résolveur du serveur de noms récurrent n'a pas besoin d'effectuer d'authentification sur les RRset de la réponse. Lorsque le bit CD est établi, le serveur de noms récurrent DEVRAIT, si possible, retourner les données demandées au résolveur générateur, même si la politique d'authentification locale du serveur de noms récurrent va rejeter les enregistrements en question. C'est-à-dire qu'en établissant le bit CD, le résolveur générateur a indiqué qu'il prend la responsabilité d'effectuer sa propre authentification, et que le serveur de noms récurrent ne devrait pas interférer.

Si le côté résolveur met en œuvre une antémémoire BAD (voir le paragraphe 4.7) et si le côté serveur de noms reçoit une interrogation qui correspond à une entrés dans l'antémémoire BAD du côté résolveur, la réponse du côté serveur de noms va dépendre de l'état du bit CD dans l'interrogation d'origine. Si le bit CD est établi, le côté serveur de noms DEVRAIT retourner les données provenant de l'antémémoire BAD ; si le bit CD n'est pas établi, le côté serveur de noms DOIT retourner le RCODE 2 (défaillance du serveur).

L'intention de la règle ci-dessus est de fournir les données brutes aux clients qui sont capables d'effectuer leurs propres vérifications de signature tout en protégeant les clients qui dépendent du côté résolveur d'un serveur de noms récurrent à capacités de sécurité pour effectuer de telles vérifications. Plusieurs des raisons possibles de l'échec d'une validation de

signature impliquent les conditions qui peuvent ne pas s'appliquer également au serveur de noms récurrent et au client qui l'invoquent. Par exemple, l'horloge du serveur de noms récurrent peut être mal réglée, ou le client peut avoir connaissance qu'un îlot de sécurité pertinent n'est pas partagé par le serveur de noms récurrent. Dans ce cas, "protéger" un client qui est capable d'effectuer sa propre validation de signature contre la vue de "mauvaises" données n'aide pas le client.

3.2.3 Bit AD

Le côté serveur de noms d'un serveur de noms récurrent à capacités de sécurité NE DOIT PAS établir le bit AD dans une réponse à moins que le serveur de noms considère tous les RRset dans les sections Réponse et Autorité de la réponse comme authentiques. Le côté serveur de noms DEVRAIT établir le bit AD si et seulement si le côté résolveur considère tous les RRset dans la section Réponse et tout RR pertinent de réponse négative dans la section Autorité comme authentiques. Le côté résolveur DOIT suivre la procédure décrite à la Section 5 pour déterminer si les RR en question sont authentiques. Cependant, pour la rétro compatibilité, un serveur de noms récurrent PEUT établir le bit AD lorsque une réponse inclut des RR CNAME non signés si ces RR CNAME pourraient de façon démontrable avoir été synthétisés à partir d'un RR DNAME authentique qui est aussi inclus dans la réponse conformément aux règles de synthèse décrites dans la [RFC2672].

3.3 Exemple de réponses du DNSSEC

Voir à l'Appendice B un exemple de paquets de réponse.

4. Résolution

Cette section décrit le comportement des entités qui incluent des fonctions de résolveur à capacités de sécurité. Dans de nombreux cas, de telles fonctions feront partie d'un serveur de noms récurrent à capacités de sécurité, mais un résolveur à capacités de sécurité autonome a beaucoup des mêmes exigences. Les fonctions spécifiques de serveur de noms récurrent à capacités de sécurités sont décrites au paragraphe 3.2.

4.1 Prise en charge de EDNS

Un résolveur à capacités de sécurité DOIT inclure un pseudo-RR OPT EDNS ([RFC2671]) avec le bit DO ([RFC3225]) établi lors de l'envoi des interrogations.

Un résolveur à capacités de sécurité DOIT prendre en charge une taille de message d'au moins 1220 octets, DEVRAIT prendre en charge une taille de message de 4000 octets, et DOIT utiliser le champ "taille de charge utile UDP d'envoyeur" dans le pseudo-RR OPT EDNS pour annoncer la taille de message qu'il veut accepter. La couche IP d'un résolveur à capacités de sécurité DOIT traiter correctement les paquets UDP fragmentés sans considérer si de tels paquets fragmentés ont été reçus via IPv4 ou IPv6. Voir les [RFC1122], [RFC2460], et [RFC3226] pour la discussion de ces exigences.

4.2 Prise en charge de la vérification de signature

Un résolveur à capacités de sécurité DOIT prendre en charge les mécanismes de vérification de signature décrit à la Section 5 et DEVRAIT les appliquer à chaque réponse reçue, sauf quand :

- o le résolveur à capacités de sécurité fait partie d'un serveur de noms récurrent à capacités de sécurité, et que la réponse est le résultat d'une récurrence au nom d'une interrogation reçue avec le bit CD établi ;
- o la réponse est le résultat d'une interrogation générée directement via une forme d'interface d'application qui a ordonné au résolveur à capacités de sécurité de ne pas effectuer de validation pour cette interrogation ; ou
- o la validation pour cette interrogation a été désactivée par la politique locale.

La prise en charge par un résolveur à capacités de sécurité de la vérification de signature DOIT inclure la prise en charge de la vérification des noms de propriétaires avec caractères génériques.

Les résolveurs à capacité de sécurité PEUVENT interroger les RR de sécurité manquants pour tenter d'effectuer la validation ; les mises en œuvre qui choisissent de faire ainsi doivent savoir que les réponses reçues peuvent n'être pas suffisantes pour valider la réponse originale. Par exemple, une mise à jour de zone peut avoir changé (ou supprimé) les informations désirées entre les interrogations d'origine et les suivantes.

Lorsque on tente de restituer les RR NSEC manquants qui résident sur le côté parent d'une coupure de zone, un résolveur à capacité de sécurité en mode itératif DOIT interroger les serveurs de noms sur la zone parente, et non la zone fille.

Lorsque il tente de restituer un DS manquant, un résolveur à capacités de sécurité en mode itératif DOIT interroger les serveurs de noms sur la zone parente, et non la zone fille. Comme expliqué au paragraphe 3.1.4.1, les serveurs de noms à capacités de sécurité doivent appliquer des règles de traitement spéciales pour traiter le RR DS, et dans certaines situations le résolveur peut aussi devoir appliquer des règles spéciales pour localiser les serveurs de noms sur la zone parente si le résolveur n'a pas déjà le RRset NS du parent. Pour localiser le RRset NS parent, le résolveur peut commencer par le nom de délégation, supprimer l'étiquette la plus à gauche, et interroger pour ce nom un RRset NS. Si aucun RRset NS n'est présent à ce nom, le résolveur supprime alors l'étiquette la plus à gauche restante et réessaye l'interrogation pour ce nom, répétant ce processus de parcours de l'arborescence jusqu'à ce qu'il trouve le RRset NS ou n'ait plus d'étiquettes.

4.3 Détermination de l'état de sécurité des données

Un résolveur à capacités de sécurité DOIT être capable de déterminer si il devrait s'attendre à ce qu'un RRset particulier soit signé. Plus précisément, un résolveur à capacités de sécurité doit être capable de distinguer quatre cas :

Sûr : un RRset pour lequel le résolveur est capable de construire une chaîne de RR DNSKEY et DS signés depuis une ancre de confiance de sécurité jusqu'au RRset. Dans ce cas, le RRset devrait être signé et est soumis à validation de signature, comme décrit ci-dessus.

Non sûr : un RRset pour lequel le résolveur sait qu'il n'y a pas de chaîne de RR DNSKEY et DS signés à partir un point de départ de confiance jusqu'au RRset. Cela peut se produire lorsque le RRset cible se trouve dans un zone non signée ou dans un descendant d'une zone non signée. Dans ce cas, le RRset peut ou non être signé, mais le résolveur ne sera pas capable de vérifier la signature.

Bogué : un RRset pour lequel le résolveur estime qu'il devrait être capable d'établir une chaîne de confiance mais pour lequel il est incapable de le faire, soit à cause de signatures qui ont échoué à la validation pour une raison quelconque ou à cause de données manquantes dont les RR DNSSEC pertinents indiquent qu'elles devraient être présentes. Ce cas peut indiquer une attaque mais peut aussi indiquer une erreur de configuration ou une forme de corruption des données.

Indéterminé : un RRset pour lequel le résolveur n'est pas capable de déterminer si le RRset devrait être signé, car le résolveur n'est pas capable d'obtenir les RR DNSSEC nécessaires. Cela peut arriver quand le résolveur à capacités de sécurité n'est pas capable de contacter les serveurs de noms à capacité de sécurité pour les zones pertinentes.

4.4 Ancres de confiance configurées

Un résolveur à capacités de sécurité DOIT être capable d'être configuré avec au moins une clé publique ou RR DS de confiance et DEVRAIT être capable d'être configuré avec plusieurs clés publiques ou DS RR de confiance. Comme un résolveur à capacités de sécurité ne sera pas capable de valider des signatures sans une telle ancre de confiance configurée, le résolveur DEVRAIT avoir des mécanismes raisonnablement robustes pour obtenir de telles clés lors de l'amorçage ; des exemples d'un tel mécanisme seraient une forme de mémorisation non volatile (comme un pilote de disque) ou une forme de mécanisme de configuration de réseau local de confiance.

Noter que les ancres de confiance couvrent aussi le matériel de clé qui est mis à jour d'une manière sûre. Cette manière sûre pourrait être par un support physique, un protocole d'échange de clés, ou quelque autre moyen hors bande.

4.5 Mise en antémémoire des réponses

Un résolveur à capacités de sécurité DEVRAIT mettre en antémémoire chaque réponse comme une seule entrée atomique contenant la réponse entière, incluant le RRset désigné et tous les RR DNSSEC associés. Le résolveur DEVRAIT éliminer l'entrée atomique entière lorsque un des RR contenus arrive à expiration. Dans la plupart des cas, l'indice approprié d'antémémoire pour l'entrée atomique sera le triplet <QNAME, QTYPE, QCLASS>, mais dans le cas de la forme de réponse décrite au paragraphe 3.1.3.2, l'indice approprié d'antémémoire sera le doublet <QNAME,QCLASS>.

La raison de ces recommandations est que, entre l'interrogation initiale et l'expiration des données de l'antémémoire, les données d'autorité peuvent avoir changé (par exemple, via une mise à jour dynamique).

Ceci est pertinent dans deux situations :

1. En utilisant l'enregistrement RRSIG, il est possible de déduire qu'une réponse a été synthétisée à partir d'un caractère générique. Un serveur de noms récurrent à capacités de sécurité pourrait mémoriser ces données de caractère générique et les utiliser pour générer des réponses positives à des interrogations autres que le nom pour lequel la réponse d'origine avait d'abord été reçue.
2. Les RR NSEC reçus pour prouver la non existence d'un nom pourraient être réutilisés par un résolveur à capacités de sécurité pour prouver la non existence de tout nom dans la gamme de noms sur laquelle il s'étend.

En théorie, un résolveur pourrait utiliser des caractères génériques ou les RR NSEC pour générer des réponses positives et négatives (respectivement) jusqu'à ce que le TTL ou les signatures expirent sur les enregistrements en question. Cependant, il semble prudent que les résolveurs évitent de bloquer de nouvelles données d'autorité ou de synthétiser de nouvelles données de leur propre chef. Les résolveurs qui suivent cette recommandation auront une vue plus cohérente de l'espace de noms.

4.6 Traitement des bits CD et AD

Un résolveur à capacités de sécurité PEUT établir le bit CD d'une interrogation afin d'indiquer que le résolveur prend la responsabilité d'effectuer l'authentification que sa politique locale exige sur les RRset dans la réponse. Voir au paragraphe 3.2 les effets qu'a ce bit sur le comportement du serveur de noms récurrent à capacités de sécurité.

Un résolveur à capacités de sécurité DOIT mettre à zéro le bit AD lorsque il compose les messages d'interrogation pour se protéger contre les serveurs de noms fautifs qui copient aveuglément les bits d'en-tête qu'ils ne comprennent pas provenant d'un message d'interrogation dans le message de réponse.

Un résolveur DOIT ne pas prendre en compte la signification des bits CD et AD dans une réponse sauf si la réponse a été obtenue en utilisant un canal sûr ou si le résolveur a été spécifiquement configuré à prendre en compte les bits d'en-tête de message sans utiliser un canal sûr.

4.7 Mise en antémémoire des données BAD

Bien que de nombreuses erreurs de validation soient temporaires, certaines seront vraisemblablement plus persistantes, comme celles causées par des erreurs administratives (oubli de re-signer une zone, biais d'horloge, et ainsi de suite). Comme la répétition de l'interrogation ne sera d'aucun secours dans ces cas, les résolveurs de validation peuvent générer une quantité significative de trafic DNS inutile par suite d'interrogations répétées pour des RRset qui ont des échecs persistants de validation.

Pour empêcher ce trafic DNS inutile, les résolveurs à capacités de sécurité PEUVENT mettre en antémémoire les données avec des signatures invalides, avec quelques restrictions.

Théoriquement, la mise en antémémoire de telles données est similaire à la mise en antémémoire négative de la [RFC2308], sauf qu'au lieu de mettre en antémémoire une réponse négative valide, le résolveur met en antémémoire le fait qu'une réponse particulière a échoué à la validation. Le présent document se réfère à une antémémoire de données avec des signatures invalides comme une "antémémoire BAD".

Les résolveurs qui mettent en œuvre une antémémoire BAD DOIVENT prendre des mesures pour empêcher l'antémémoire d'être utilisée comme amplificateur d'attaque de déni de service, en particulier :

- Comme les RRset qui ont échoué à la validation n'ont pas un TTL digne de confiance, la mise en œuvre DOIT allouer un TTL. Ce TTL DEVRAIT être bref, afin d'atténuer les effets de la mise en antémémoire du résultat d'une attaque.
- Afin d'empêcher la mise en antémémoire d'un échec de validation temporaire (qui peut être le résultat d'une attaque) les résolveurs DEVRAIENT faire le suivi des interrogations qui résultent en un échec de validation et DEVRAIENT ne répondre qu'à partir de l'antémémoire BAD après que le nombre de fois que les réponses aux interrogations pour des <QNAME, QTYPE, QCLASS> particuliers ont échoué à la validation excède un certain seuil.

Les résolveurs NE DOIVENT PAS retourner des RRset à partir d'une antémémoire BAD sauf si le résolveur n'est pas obligé de valider les signatures des RRset en question selon les règles du paragraphe 4.2 ci-dessus. Voir au paragraphe 3.2.2 la discussion sur la façon dont les réponses retournées par un serveur de noms récurrent à capacités de sécurité interagissent avec une antémémoire BAD.

4.8 CNAME synthétisés

Un résolveur valideur à capacités de sécurité DOIT traiter la signature d'un RR DNAME valide signé comme couvrant aussi les RR CNAME non signés qui pourraient avoir été synthétisés à partir du RR DNAME, comme décrit dans la [RFC2672], au moins dans la mesure où il ne rejette pas un message de réponse seulement parce qu'il contient de tels RR CNAME. Le résolveur PEUT conserver de tels RR CNAME dans son antémémoire ou dans les réponses qu'il renvoie, mais il n'est pas obligé de le faire.

4.9 Résolveurs de bout

Un résolveur de bout à capacités de sécurité DOIT prendre en charge les types de RR DNSSEC, au moins en n'appliquant pas un mauvais traitement aux réponses pour la seule raison qu'elles contiennent des RR DNSSEC.

4.9.1 Traitement du bit DO

Un résolveur de bout à capacités de sécurité non valideur PEUT inclure les RR DNSSEC retournés par un serveur de noms récurrent à capacités de sécurité au titre des données que le résolveur de bout renvoie à l'application qui l'a invoqué, mais il n'est pas obligé de le faire. Un résolveur de bout non valideur qui cherche à faire cela devra établir le bit DO afin de recevoir les RR DNSSEC provenant du serveur de noms récurrent.

Un résolveur valideur à capacités de sécurité DOIT établir le bit DO, parce que autrement, il ne va pas recevoir les RR DNSSEC dont il a besoin pour effectuer la validation de signature.

4.9.2 Traitement du bit CD

Un résolveur de bout à capacités de sécurité non valideur NE DEVRAIT PAS établir le bit CD lors de l'envoi d'interrogations sauf si cela lui est demandé par la couche application, car par définition, un résolveur de bout non valideur dépend du serveur de noms récurrent à capacités de sécurité pour effectuer la validation en son nom.

Un résolveur valideur à capacités de sécurité DEVRAIT établir le bit CD, parce que autrement le serveur de noms récurrent à capacités de sécurité va répondre à l'interrogation en utilisant la politique locale du serveur de noms, ce qui peut empêcher le résolveur de bout de recevoir des données qui seraient acceptable pour la politique locale du résolveur de bout.

4.9.3 Traitement du bit AD

Un résolveur de bout à capacités de sécurité non valideur PEUT choisir d'examiner le réglage du bit AD dans les messages de réponse qu'il reçoit afin de déterminer si le serveur de noms récurrent à capacités de sécurité qui a envoyé la réponse prétend avoir vérifié cryptographiquement les données dans les sections Réponse et Autorité du message de réponse. Noter cependant que les réponses reçues par un résolveur de bout à capacités de sécurité dépendent fortement de la politique locale du serveur de noms récurrent à capacités de sécurité. Donc, il n'y a pas beaucoup d'intérêt pratique à vérifier l'état du bit AD, sauf peut-être comme aide au débogage. En tous cas, un résolveur de bout à capacités de sécurité NE DOIT PAS faire confiance à des allégations de validation de signature effectuées en son nom, sauf lorsque le résolveur de bout à capacités de sécurité a obtenu les données en question d'un serveur de noms récurrent à capacités de sécurité de confiance via un canal sûr.

Un résolveur valideur à capacités de sécurité NE DEVRAIT PAS examiner le réglage du bit AD dans les messages de réponse, car, par définition, le résolveur de bout effectue sa propre validation de signature sans considération du réglage du bit AD.

5. Authentification des réponses du DNS

Afin d'utiliser les RR DNSSEC pour l'authentification, un résolveur à capacités de sécurité exige la configuration de la connaissance d'au moins un RR DNSKEY ou DS authentifié. Le processus d'obtention et d'authentification de cette ancre de confiance initiale est réalisé via un mécanisme externe. Par exemple, un résolveur pourrait utiliser un échange authentifié hors ligne pour obtenir le RR DNSKEY d'une zone pour obtenir un RR DS qui identifie et authentifie le RR DNSKEY d'une zone. Le reste de cette section suppose que le résolveur a obtenu d'une façon quelconque un ensemble initial d'ancres de confiance.

Un RR DNSKEY initial peut être utilisé pour authentifier le RRset DNSKEY sommet d'une zone. Pour authentifier un RRset DNSKEY sommet en utilisant une clé initiale, le résolveur DOIT :

1. vérifier que le RR DNSKEY initial apparaît dans le RRset DNSKEY sommet, et que le RR DNSKEY a le fanion Clé de zone (bit 7 des RDATA DNSKEY) établi ; et
2. vérifier qu'il y a un RR RRSIG qui couvre le RRset DNSKEY sommet, et que la combinaison du RR RRSIG et du RR DNSKEY initial authentifie le RRset DNSKEY. Le processus d'utilisation d'un RR RRSIG pour authentifier un RRset est décrit au paragraphe 5.3.

Une fois que le résolveur a authentifié le RRset DNSKEY sommet en utilisant un RR DNSKEY initial, les délégations à partir de cette zone peuvent être authentifiées en utilisant le RR DS. Cela permet à un résolveur de commencer à partir d'une clé initiale et d'utiliser les RRset DS pour procéder de façon récurrente le long de l'arborescence du DNS, et d'obtenir les autres RRset DNSKEY. Si le résolveur était configuré avec un RR DNSKEY racine, et si chaque délégation avait un

RR DS associé, alors le résolveur pourrait obtenir et valider tout RRset DNSKEY sommet. Le processus d'utilisation des RR DS pour authentifier les références est décrit au paragraphe 5.2.

Le paragraphe 5.3 montre comment le résolveur peut utiliser les RR DNSKEY dans le RRset DNSKEY sommet et les RR RRSIG de la zone pour authentifier tous les autres RRset de la zone une fois que le résolveur a authentifié un RRset DNSKEY sommet d'une zone. Le paragraphe 5.4 montre comment le résolveur peut utiliser les RRset NSEC authentifiés de la zone pour prouver qu'un RRset n'est pas présent dans la zone.

Lorsque un résolveur indique la prise en charge de DNSSEC (en établissant le bit DO) un serveur de noms à capacité de sécurité devrait tenter de fournir les RRset DNSKEY, RRSIG, NSEC, et DS nécessaires dans une réponse (voir la Section 3). Cependant, un résolveur à capacités de sécurité peut encore recevoir une réponse qui manque des RR DNSSEC appropriés, que ce soit dû à des problèmes de configuration comme un serveur de noms récurrent en amont sans capacité de sécurité qui interfère accidentellement avec les RR DNSSEC ou dû à une attaque délibérée dans laquelle un adversaire falsifie une réponse, supprime des RR DNSSEC d'une réponse, ou modifie une interrogation de sorte que les RR DNSSEC paraissent n'être pas demandés. L'absence de données DNSSEC dans une réponse NE DOIT PAS être prise par elle-même comme une indication qu'il n'existe pas d'informations d'authentification.

Un résolveur DEVRAIT attendre des informations d'authentification provenant des zones signées. Un résolveur DEVRAIT penser qu'une zone est signée si le résolveur a été configuré avec des informations de clé publique pour la zone, ou si le parent de la zone est signé et si la délégation du parent contient un RRset DS.

5.1 Considérations particulières pour les îlots de sécurité

Les îlots de sécurité (voir la [RFC4033]) sont des zones signées pour lesquelles il n'est pas possible de construire une chaîne d'authentification allant de la zone à sa parente. Valider les signatures au sein d'un îlot de sécurité exige que le valideur ait d'autres moyens d'obtenir une clé initiale de zone authentifiée pour l'îlot. Si un valideur ne peut pas obtenir une telle clé, il DEVRAIT sauter l'opération comme si les zones dans l'îlot de sécurité n'étaient pas signées.

Tous les processus normaux de validation des réponses s'appliquent aux îlots de sécurité. La seule différence entre la validation normale et la validation au sein d'un îlot de sécurité est dans la façon dont le valideur obtient une ancre de confiance pour la chaîne d'authentification.

5.2 Authentification des références

Une fois que le RRset DNSKEY sommet pour une zone parente signée a été authentifiée, le RRset DS peut être utilisé pour authentifier la délégation d'une zone fille signée. Un RR DS identifie un RR DNSKEY dans le RRset DNSKEY sommet de zone fille et contient un résumé cryptographique du RR DNSKEY de la zone fille. Utiliser un algorithme fort de résumé cryptographique assure qu'il est infaisable pour un adversaire de générer par le calcul un RR DNSKEY qui corresponde au résumé. Donc, l'authentification du résumé permet à un résolveur d'authentifier le RR DNSKEY correspondant. Le résolveur peut alors utiliser ce RR DNSKEY fils pour authentifier le RRset DNSKEY sommet fils entier.

Étant donné un RR DS pour une délégation, le RRset DNSKEY sommet de la zone fille peut être authentifié si tout ce qui suit tient :

- Le RR DS a été authentifié en utilisant un RR DNSKEY dans le RRset DNSKEY sommet de la zone parente (voir le paragraphe 5.3).
- L'algorithme et l'étiquette de clé dans le RR DS correspondent au champ Algorithme et à l'étiquette de clé d'un RR DNSKEY dans le RRset DNSKEY sommet de la zone fille, et, lorsque le nom du propriétaire et les RDATA des RR DNSKEY sont hachés en utilisant l'algorithme de résumé spécifié dans le champ Type de résumé du RR DS, la valeur de résumé résultante correspond au champ Résumé du RR DS.
- Le RR DNSKEY correspondant dans la zone fille a le bit Fanion de zone établi, la clé privée correspondante a signé la RRset DNSKEY sommet de la zone fille, et le RRSIG RR résultant authentifie le RRset DNSKEY sommet de la zone fille.

Si le référant de la zone parente ne contenait pas un RRset DS, la réponse devrait avoir inclus un RRset NSEC prouvant qu'aucun RRset DS n'existe pour le nom délégué (voir le paragraphe 3.1.4). Un résolveur à capacités de sécurité DOIT interroger le serveur de noms pour la zone parente sur le RRset DS si le référant n'inclut ni un RRset DS ni des RRset NSEC prouvant que le RRset DS n'existe pas (voir la Section 4).

Si le valideur authentifie les RRset NSEC qui prouvent qu'aucun RRset DS n'est présent pour cette zone, alors il n'y a pas de chemin d'authentification conduisant de la parente à la fille. Si le résolveur a un RR DNSKEY ou DS initial qui appartient à la zone fille ou à toute délégation en dessous de la zone fille, ce RR DNSKEY ou DS initial PEUT être utilisé

pour rétablir un chemin d'authentification. Si aucun RR DNSKEY ou DS initial n'existe, le valideur ne peut pas authentifier les RRset dans ou en dessous de la zone fille.

Si le valideur ne prend en charge aucun des algorithmes mentionnés dans un RRset DS authentifié, alors le résolveur n'a pas de chemin d'authentification pris en charge qui conduise de la zone parente à la fille. Le résolveur devrait traiter ce cas comme il le ferait du cas d'un RRset NSEC authentifié prouvant qu'aucun RRset DS n'existe, comme décrit ci-dessus.

Noter que, pour une délégation signée, il y a deux RR NSEC associés au nom délégué. Un RR NSEC réside dans la zone parente et peut être utilisé pour prouver si un RRset DS existe pour le nom délégué. Le second RR NSEC réside dans la zone fille et identifie quels RRset sont présents au sommet de la zone fille. Le RR NSEC parent et le RR NSEC fils peuvent toujours être distingués parce que le bit SOA sera établi dans le RR NSEC fils et à zéro dans le RR NSEC parent. Un résolveur à capacités de sécurité DOIT utiliser le RR NSEC parent lorsque il tente de prouver qu'un RRset DS n'existe pas.

Si le résolveur ne prend en charge aucun des algorithmes mentionnés dans un RRset DS authentifié, alors le résolveur ne sera pas capable de vérifier le chemin d'authentification vers la zone fille. Dans ce cas, le résolveur DEVRAIT traiter la zone fille comme si elle n'était pas signée.

5.3 Authentification d'un RRset avec un RR RRSIG

Un valideur peut utiliser un RRSIG RR et son RR DNSKEY correspondant pour tenter d'authentifier les RRset. Le valideur vérifie d'abord le RR RRSIG pour s'assurer qu'il couvre le RRset, a un intervalle de temps valide, et identifie un RR DNSKEY valide. Le valideur construit alors la forme canonique des données signées en ajoutant le RDATA RRSIG (excluant le champ Signature) avec la forme canonique du RRset couvert. Finalement, le valideur utilise la clé publique et la signature pour authentifier les données signées. Les paragraphes 5.3.1, 5.3.2, et 5.3.3 décrivent chaque étape en détail.

5.3.1 Vérification de la validité du RR RRSIG

Un résolveur à capacités de sécurité peut utiliser un RR RRSIG pour authentifier un RRset si toutes les conditions suivantes tiennent :

- Le RR RRSIG et le RRset DOIVENT avoir le même nom de propriétaire et la même classe.
- Le champ Nom du signataire du RR RRSIG DOIT être le nom de la zone qui contient le RRset.
- Le champ Type couvert du RR RRSIG DOIT être égal au type du RRset.
- Le nombre d'étiquettes dans le nom du propriétaire du RRset DOIT être supérieur ou égal à la valeur dans le champ Étiquettes du RR RRSIG.
- La notion qu'a le valideur de l'heure actuelle DOIT être inférieure ou égale à l'heure mentionnée dans le champ Expiration du RR RRSIG.
- La notion qu'a le valideur de l'heure actuelle DOIT être supérieure ou égale à l'heure mentionnées dans le champ Début du RR RRSIG.
- Les champs Nom, Algorithme, et Étiquette de clé de signature du RR RRSIG DOIVENT correspondre au nom du propriétaire, de l'algorithme, et de l'étiquette de clé pour un RR DNSKEY dans le RRset DNSKEY sommet de la zone.
- Le RR DNSKEY correspondant DOIT être présent dans le RRset DNSKEY sommet de la zone, et DOIT avoir le bit Fanion de zone (bit 7 du fanion RDATA DNSKEY) établi.

Il est possible que plus d'un RR DNSKEY corresponde aux conditions ci-dessus. Dans ce cas, le valideur ne peut pas prédéterminer quel RR DNSKEY utiliser pour authentifier la signature, et il DOIT essayer chaque RR DNSKEY correspondant jusqu'à ce que soit la signature soit validée, soit que le valideur arrive au bout des clés publiques correspondantes à essayer.

Noter que ce processus d'authentification n'a de sens que si le valideur authentifie le RR DNSKEY avant de l'utiliser pour valider les signatures. Le RR DNSKEY correspondant est considéré comme authentique si :

- le RRset DNSKEY sommet contenant le RR DNSKEY est considéré comme authentique ; ou
- le RRset couvert par le RR RRSIG est le RRset DNSKEY sommet lui-même, et le RR DNSKEY soit correspond à un RR DS authentifié provenant de la zone parente, soit correspond à une ancre de confiance.

5.3.2 Reconstruction des données signées

Une fois que le RR RRSIG a satisfait aux exigences de validité décrites au paragraphe 5.3.1, le valideur doit reconstruire les données signées originales. Les données signées originales incluent les RDATA RRSIG (à l'exclusion du champ Signature) et la forme canonique du RRset. En plus d'être ordonnée, la forme canonique du RRset peut aussi différer du RRset reçu à cause de la compression de noms du DNS, des TTL décrémentés, ou de l'expansion de caractères génériques. Le valideur devrait utiliser ce qui suit pour reconstruire les données signées originales :

signed_data = RRSIG_RDATA | RR(1) | RR(2)...

où"|" note l'enchaînement, RRSIG_RDATA est le format réseau des champs RDATA RRSIG avec le champ Signature exclu et le nom du signataire en forme canonique.

RR(i) = nom | type | classe | OrigTTL | longueur RDATA | RDATA

nom est calculé conformément à la fonction ci-dessous ; classe est la classe du RRset ; type est le type du RRset et de tous les RR dans la classe ; OrigTTL est la valeur provenant du champ TTL du RRSIG d'origine. Tous les noms dans le champ RDATA sont en forme canonique. L'ensemble de tous les RR(i) est trié dans l'ordre canonique.

Pour calculer le nom :
Soit rrsig_labels = valeur du champ Étiquettes du RRSIG
Soit fqdn = le nom de domaine pleinement qualifié du RRset en forme canonique
Soit fqdn_labels = compte d'étiquettes du fqdn ci-dessus.

Si rrsig_labels = fqdn_labels, nom = fqdn

Si rrsig_labels < fqdn_labels, nom = "*." | les étiquettes rrsig_label les plus à droite du fqdn.

Si rrsig_labels > fqdn_labels, le RR RRSIG ne réussit pas aux vérifications de validité nécessaires et NE DOIT PAS être utilisé pour authentifier ce RRset.

Les formes canoniques pour les noms et les RRset sont définies dans la [RFC4034].

Les RRset NSEC aux limites de délégation exigent un traitement spécial. Deux RRset NSEC distincts sont associés à un nom délégué signé. Un des RRset NSEC réside dans la zone parente, et spécifie quels RRset sont présents chez la zone parente. Le second RRset NSEC réside dans la zone fille et identifie quels RRset sont présents au sommet dans la zone fille. Les RRset NSEC parent et fils peuvent toujours être distingués car seul un RR NSEC fils indique qu'un RRset SOA existe au nom. Lors de la reconstruction du RRset NSEC original pour la délégation de la zone parente, les RR NSEC NE DOIVENT PAS être combinés avec les RR NSEC provenant de la zone fille. Lors de la reconstruction du RRset NSEC original pour le sommet de la zone fille, les RR NSEC NE DOIVENT PAS être combinés avec les RR NSEC provenant de la zone parente.

Noter que chacun des deux RRset NSEC à un point de délégation a un RR RRSIG correspondant, avec un nom de propriétaire correspondant au nom délégué, et chacun de ces RR RRSIG est de données d'autorité associées à la même zone qui contient le RRset NSEC correspondant. Si nécessaire, un résolveur peut donner ces RR RRSIG sans vérifier le champ Nom du signataire.

5.3.3 Vérification de la signature

Une fois que le résolveur a validé le RR RRSIG comme décrit au paragraphe 5.3.1 et reconstruit les données signées originales comme décrit au paragraphe 5.3.2, le valideur peut tenter d'utiliser la signature cryptographique pour authentifier les données signées, et donc (enfin !) authentifier le RRset.

Le champ Algorithme dans le RR RRSIG identifie l'algorithme cryptographique utilisé pour générer la signature. La signature elle-même est contenue dans le champ Signature du RDATA RRSIG, et la clé publique utilisée pour vérifier la signature est contenue dans le champ Clé publique de la ou des RR DNSKEY correspondants (qu'on trouve au paragraphe 5.3.1). La [RFC4034] donne une liste des types d'algorithmes et donne des pointeurs sur les documents qui définissent chaque utilisation d'algorithme.

Noter qu'il est possible que plus d'un RR DNSKEY corresponde aux conditions du paragraphe 5.3.1. Dans ce cas, le valideur peut seulement déterminer quel RR DNSKEY est correct en essayant chaque clé publique correspondante jusqu'à ce que le valideur réussisse à valider la signature ou n'ait plus de clé à essayer.

Si le champ Étiquettes *(Labels)* du RR RRSIG n'est pas égal au nombre d'étiquettes dans le nom de propriétaire pleinement qualifié du RRset, alors le RRset est soit invalide, soit est le résultat de l'expansion de caractère générique. Le résolveur DOIT vérifier que l'expansion de caractère générique a été appliquée correctement avant de considérer le RRset comme authentique. Le paragraphe 5.3.4 décrit comment déterminer si un caractère générique a été appliqué correctement.

Si d'autres RR RRSIG couvrent aussi ce RRset, la politique de sécurité du résolveur local détermine si le résolveur doit aussi vérifier ces RR RRSIG et comment résoudre les conflits si ces RR RRSIG conduisent à des résultats différents.

Si le résolveur accepte le RRset comme authentique, le valideur DOIT régler le TTL du RR RRSIG et de chaque RR dans le RRset authentifié à une valeur non supérieure au minimum :

- o du TTL du RRset tel que reçu dans la réponse,
- o du TTL du RR RRSIG tel que reçu dans la réponse,
- o de la valeur du champ TTL original dans le RR RRSIG, et
- o de la différence de l'heure d'expiration de signature du RR RRSIG et l'heure actuelle.

5.3.4 Authentification d'une réponse positive de RRset par expansion de caractère générique

Si le nombre d'étiquettes dans le nom de propriétaire d'un RRset est supérieur à celui du champ Étiquettes du RR RRSIG qui le couvre, alors le RRset et son RR RRSIG couvrant ont été créés par suite d'une expansion de caractère générique. Une fois que le valideur a vérifié la signature, comme décrit au paragraphe 5.3, il doit prendre des mesures supplémentaires pour vérifier la non existence d'une correspondance exacte ou plus proche correspondance de caractère générique pour l'interrogation. Ces étapes sont exposées au paragraphe 5.4.

Noter que la réponse reçue par le résolveur devrait inclure tous les RR NSEC nécessaires pour authentifier la réponse (voir le paragraphe 3.1.3).

5.4 Déni d'existence authentifié

Un résolveur peut utiliser des RR NSEC authentifiés pour prouver qu'un RRset n'est pas présent dans une zone signée. Les serveurs de noms à capacité de sécurité devraient automatiquement inclure tous les RR NSEC nécessaires pour les zones signées dans leurs réponses aux résolveurs à capacités de sécurité.

Le déni d'existence est déterminé par les règles suivantes :

- o Si le nom du RR demandé correspond au nom du propriétaire d'un RR NSEC authentifié, alors le champ Type de correspondance binaire du RR NSEC fait la liste de tous les types de RR présents chez ce nom de propriétaire, et un résolveur peut prouver que le type de RR demandé n'existe pas en cherchant le type RR dans la correspondance binaire. Si le nombre d'étiquettes dans le nom de propriétaire d'un RR NSEC authentifié est égal au champ Étiquettes du RR RRSIG couvrant, alors l'existence du RR NSEC prouve que l'expansion de caractère générique n'a pas pu être utilisée pour la confrontation avec la demande.
- o Si le nom de RR demandé devait apparaître après le nom de propriétaire d'un RR NSEC authentifié et avant le nom mentionné dans la liste du champ Prochain nom de domaine de RR NSEC conformément à l'ordre canonique des noms du DNS défini dans la [RFC4034], alors aucun RRset avec le nom demandé n'existe dans la zone. Cependant, il est possible qu'un caractère générique ait pu être utilisé pour correspondre au nom de propriétaire et type du RR demandé, et donc prouver que le RRset demandé n'existe pas exige aussi de prouver qu'il n'existe aucun RRset à caractère générique possible qui aurait pu être utilisé pour générer une réponse positive.

De plus, les résolveurs à capacités de sécurité DOIVENT authentifier les RRset NSEC qui comprennent la preuve de la non existence, comme décrit au paragraphe 5.3.

Pour prouver la non existence d'un RRset, le résolveur doit être capable de vérifier que le RRset demandé n'existe pas et qu'aucun RRset à caractère générique pertinent n'existe. Prouver cela peut exiger plus d'un RRset NSEC provenant de la zone. Si le jeu complet de RRset NSEC nécessaire n'est pas présent dans une réponse (peut-être à cause d'un message tronqué) un résolveur à capacités de sécurité DOIT alors envoyer à nouveau l'interrogation afin de tenter d'obtenir la collection complète des RR NSEC nécessaire pour vérifier la non existence du RRset demandé. Comme avec toutes les opérations du DNS, le résolveur DOIT cependant limiter le travail consacré à la réponse à toute interrogation particulière.

Comme un RR NSEC validé prouve l'existence à la fois de lui-même et de son RR RRSIG correspondant, un valideur DOIT ignorer les réglages des bits NSEC et RRSIG dans un RR NSEC.

5.5 Comportement du résolveur quand les signatures ne se valident pas

Si pour quelque raison que ce soit aucun des RRSIG ne peut être validé, la réponse DEVRAIT être considérée comme mauvaise. Si la validation a été faite pour servir une interrogation récurrente, le serveur de noms DOIT retourner le RCODE 2 au client qui l'a générée. Cependant, il ne DOIT retourner une réponse complète que si et seulement si l'interrogation originale avait le bit CD établi. Voir aussi le paragraphe 4.7 sur la mise en antémémoire des réponses qui ne sont pas validées.

5.6 Exemple d'authentification

L'Appendice C donne un exemple du processus d'authentification.

6. Considérations relatives à l'IANA

La [RFC4034] contient une revue des considérations relatives à l'IANA introduites par DNSSEC. Les considérations relatives à l'IANA supplémentaires suivantes sont discutées dans ce document :

La [RFC2535] réservait les bits CD et AD dans l'en-tête de message. La signification du bit AD a été redéfinie dans la [RFC3655], et la signification des deux bits CD et AD est réaffirmée dans le présent document. Aucun nouveau bit de l'en-tête de message DNS n'est défini dans le présent document.

La [RFC2671] introduisait EDNS, et la [RFC3225] réservait le bit OK DNSSEC et définissait son usage. Cet usage est réaffirmé sans changement dans le présent document.

7. Considérations pour la sécurité

Le présent document décrit comment les extensions de sécurité du DNS utilisent la cryptographie à clé publique pour signer et authentifier les ensembles de ressources du DNS. Prière de se reporter à la [RFC4033] pour la terminologie et les considérations générales de sécurité relatives à DNSSEC ; voir dans la [RFC4034] les considérations spécifiques des types d'enregistrement de ressource DNSSEC.

Un attaquant actif qui peut établir le bit CD dans un message d'interrogation du DNS ou le bit AD dans un message de réponse du DNS peut utiliser ces bits pour vaincre la protection que DNSSEC tente de fournir aux résolveurs en mode récurrent oublieux de la sécurité. Pour cette raison, l'utilisation de ces bits de contrôle par un résolveur en mode récurrent capable de sécurité exige un canal sûr. Voir l'exposé des paragraphes 3.2.2 et 4.9.

Le protocole décrit dans le présent document essaye d'étendre les bénéfices de DNSSEC aux résolveurs de bout oublieux de la sécurité. Cependant, comme la récupération des échecs de validation va probablement être spécifique des applications particulières, les facilités que fournit DNSSEC aux résolveurs d'extrémité peuvent se révéler inadéquates. Les opérateurs de serveurs de noms en mode récurrent à capacité de sécurité devront porter une attention soutenue au comportement des applications qui utilisent leurs services lors du choix d'une politique locale de validation ; ne pas le faire pourrait facilement résulter en le refus accidentel de service du serveur de noms récurrent aux clients qu'il est destiné à prendre en charge.

8. Remerciements

Le présent document a été créé à partir des apports et idées de la liste de diffusion des membres du groupe de travail Extensions DNS. Les éditeurs tiennent à exprimer leurs remerciements pour leurs commentaires et suggestions reçus durant la révision de ces spécifications d'extensions de sécurité. Bien, que la liste explicite de tous ceux qui ont contribué durant la décade du développement de DNSSEC soit impossible à établir, la [RFC4033] comporte une liste de quelques uns des participants qui ont eu la gentillesse de commenter ces documents.

9. Références

9.1 Références normatives

[RFC1034] P. Mockapetris, "Noms de domaines - Concepts et facilités", STD 13, novembre 1987. (*MàJ par* RFC 1101, RFC 1183, RFC 1348, RFC 1876, RFC 1982, RFC 2065, RFC 2181, RFC 2308, RFC 2535, RFC 4033, RFC 4034, RFC 4035, RFC 4343, RFC 4035, RFC 4592, RFC 5936, RFC 8020)

[RFC1035] P. Mockapetris, "Noms de domaines – Mise en œuvre et spécification", STD 13, novembre 1987. (*MàJ par* RFC 1101, RFC 1183, RFC 1348, RFC 1876, RFC 1982, RFC 1995, RFC 1996, RFC 2065, RFC 2136, RFC 2181, RFC 2137, RFC 2308, RFC 2535, RFC 2673, RFC 2845, RFC 3425, RFC 3658, RFC 4033, RFC 4034, RFC 4035, RFC 4343, RFC 5936, RFC 5966, RFC 6604, RFC 7766)

[RFC1122] R. Braden, "Exigences pour les hôtes Internet – couches de communication", STD 3, octobre 1989. *(MàJ par la* RFC6633)

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

[RFC2181] R. Elz et R. Bush, "Clarifications pour la spécification du DNS", juillet 1997. *(P.S., MàJ par* RFC 4035, RFC 2535, RFC 4343, RFC 4033, RFC 4034, RFC 5452*)*

[RFC2460] S. Deering et R. Hinden, "Spécification du protocole Internet, version 6 (IPv6) ", décembre 1998. *(MàJ par RFC5095, D.S)*

[RFC2671] P. Vixie, "Mécanismes d'extension pour le DNS (EDNS0)", août 1999. *(P.S.)*

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

[RFC3225] D. Conrad, "Indication de la prise en charge de DNSSEC par le résolveur", décembre 2001. (*MàJ par* RFC4033, RFC4034, RFC4035) *(P.S.)*

[RFC3226] O. Gudmundsson, "Exigences de taille de message de serveur/résolveur à capacité DNSSEC et IPv6 A6", décembre 2001. (*MàJ par* RFC4033, RFC4034, RFC4035) *(P.S.)*

[RFC4033] R. Arends, R. Austein, M. Larson, D. Massey et S. Rose, "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.

9.2 Références pour information

[RFC2308] M. Andrews, "Mise en antémémoire négative des interrogations du DNS (DNS NCACHE)", mars 1998. (*MàJ par* RFC4035, RFC4033, RFC4034) *(P.S.)*

[RFC2535] D. Eastlake, 3rd, "Extensions de sécurité du système des noms de domaines", mars 1999. (*Obsolète, voir* RFC4033, RFC4034, RFC4035) *(P.S.)*

[RFC3007] B. Wellington, "Mise à jour dynamique sécurisée du système des noms de domaine (DNS)", novembre 2000.

[RFC3655] B. Wellington, O. Gudmundsson, "Redéfinition du bit Données authentifiées (AD) du DNS", novembre 2003. (*Obsolète, voir* RFC4033, RFC4034, RFC4035) (*MàJ* RFC2535) *(P.S.)*

Appendice A Exemple de zone signée

L'exemple suivant montre comment se termine une (petite) zone signée.

```
exemple.      3600 IN SOA ns1.exemple. bugs.x.w.exemple. (
                       1081539377
                       3600
                       300
                       3600000
                       3600
                       )
              3600 RRSIG  SOA 5 1 3600 20040509183619 (
                       20040409183619 38519 exemple.
                       ONx0k36rcjaxYtcNgq6iQnpNV5+drqYAsC9h
                       7TSJaHCqbhE67Sr6aH2xDUGcqQWu/n0UVzrF
                       vkgO9ebarZ0GWDKcuwlM6eNB5SiX2K74l5LW
                       DA7S/Un/IbtDq4Ay8NMNLQI7Dw7n4p8/rjkB
                       jV7j86HyQgM5e7+miRAz8V01b0I= )
              3600 NS     ns1.exemple.
              3600 NS     ns2.exemple.
              3600 RRSIG  NS 5 1 3600 20040509183619 (
                       20040409183619 38519 exemple.
                       gl13F00f2U0R+SWiXXLHwsMY+qStYy5k6zfd
                       EuivWc+wd1fmbNCyql0Tk7lHTX6UOxc8AgNf
                       4ISFve8XqF4q+o9qlnqIzmppU3LiNeKT4FZ8
                       RO5urFOvoMRTbQxW3U0hXWuggE4g3ZpsHv48
                       0HjMeRaZB/FRPGfJPajngcq6Kwg= )
              3600 MX     1 xx.exemple.
```

```
                3600 RRSIG  MX 5 1 3600 20040509183619 (
                        20040409183619 38519 exemple.
                        HyDHYVT5KHSZ7HtO/vypumPmSZQrcOP3tzWB
                        2qaKkHVPfau/DgLgS/IKENkYOGL95G4N+NzE
                        VyNU8dcTOckT+ChPcGeVjguQ7a3Ao9Z/ZkUO
                        6gmmUW4b89rz1PUxW4jzUxj66PTwoVtUU/iM
                        W6OISukd1EQt7a0kygkg+PEDxdI= )
                3600 NSEC   a.exemple. NS SOA MX RRSIG NSEC DNSKEY
                3600 RRSIG  NSEC 5 1 3600 20040509183619 (
                        20040409183619 38519 exemple.
                        O0k558jHhyrC97ISHnislm4kLMW48C7U7cBm
                        FTfhke5iVqNRVTB1STLMpgpbDIC9hcryoO0V
                        Z9ME5xPzUEhbvGnHd5sfzgFVeGxr5Nyyq4tW
                        SDBgIBiLQUv1ivy29vhXy7WgR62dPrZ0PWvm
                        jfFJ5arXf4nPxp/kEowGgBRzY/U= )
                3600 DNSKEY 256 3 5 (
                        AQOy1bZVvpPqhg4j7EJoM9rI3ZmyEx2OzDBV
                        rZy/lvI5CQePxXHZS4i8dANH4DX3tbHol61e
                        k8EFMcsGXxKciJFHyhl94C+NwILQdzsUlSFo
                        vBZsyl/NX6yEbtw/xN9ZNcrbYvgjjZ/UVPZI
                        ySFNsgEYvh0z2542lzMKR4Dh8uZffQ==
                        )
                3600 DNSKEY 257 3 5 (
                        AQOeX7+baTmvpVHb2CcLnL1dMRWbuscRvHXl
                        LnXwDzvqp4tZVKp1sZMepFb8MvxhhW3y/0QZ
                        syCjczGJ1qk8vJe52iOhInKROVLRwxGpMfzP
                        RLMlGybr51bOV/1se0ODacj3DomyB4QB5gKT
                        Yot/K9alk5/j8vfd4jWCWD+E1Sze0Q==
                        )
                3600 RRSIG  DNSKEY 5 1 3600 20040509183619 (
                        20040409183619 9465 exemple.
                        ZxgauAuIj+k1YoVEOSlZfx41fcmKzTFHoweZ
                        xYnz99JVQZJ33wFS0Q0jcP7VXKkaElXk9nYJ
                        XevO/7nAbo88iWsMkSpSR6jWzYYKwfrBI/L9
                        hjYmyVO9m6FjQ7uwM4dCP/bIuV/DKqOAK9NY
                        NC3AHfvCV1Tp4VKDqxqG7R5tTVM= )
                3600 RRSIG  DNSKEY 5 1 3600 20040509183619 (
                        20040409183619 38519 exemple.
                        eGL0s90glUqcOmloo/2y+bSzyEfKVOQViD9Z
                        DNhLz/Yn9CQZlDVRJffACQDAUhXpU/oP34ri
                        bKBpysRXosczFrKqS5Oa0bzMOfXCXup9qHAp
                        eFIku28Vqfr8Nt7cigZLxjK+u0Ws/4lIRjKk
                        7z5OXogYVaFzHKillDt3HRxHIZM= )
a.exemple.      3600 IN NS  ns1.a.exemple.
                3600 IN NS  ns2.a.exemple.
                3600 DS     57855 5 1 (
                        B6DCD485719ADCA18E5F3D48A2331627FDD3
                        636B )
                3600 RRSIG  DS 5 2 3600 20040509183619 (
                        20040409183619 38519 exemple.
                        oXIKit/QtdG64J/CB+Gi8dOvnwRvqrto1AdQ
                        oRkAN15FP3iZ7suB7gvTBmXzCjL7XUgQVcoH
                        kdhyCuzp8W9qJHgRUSwKKkczSyuL64nhgjuD
                        EML8l9wlWVsl7PR2VnZduM9bLyBhaaPmRKX/
                        Fm+v6ccF2EGNLRiY08kdkz+XHHo= )
                3600 NSEC   ai.exemple. NS RR DSSIG NSEC
                3600 RRSIG  NSEC 5 2 3600 20040509183619 (
                        20040409183619 38519 exemple.
                        cOlYgqJLqlRqmBQ3iap2SyIsK4O5aqpKSoba
                        U9fQ5SMApZmHfq3AgLflkrkXRXvgxTQSKkG2
                        039/cRUs6Jk/25+fi7Xr5nOVJsb0lq4zsB3I
                        BBdjyGDAHE0F5ROJj87996vJupdm1fbH481g
                        sdkOW6Zyqtz3Zos8N0BBkEx+2G4= )
```

```
ns1.a.exemple. 3600 IN A   192.0.2.5
ns2.a.exemple. 3600 IN A   192.0.2.6
ai.exemple.    3600 IN A   192.0.2.9
        3600 RRSIG  A 5 2 3600 20040509183619 (
                20040409183619 38519 exemple.
                pAOtzLP2MU0tDJUwHOKE5FPIIHmdYsCgTb5B
                ERGgpnJluA9ixOyf6xxVCgrEJW0WNZSsJicd
                hBHXfDmAGKUajUUlYSAH8tS4ZnrhyymIvk3u
                ArDu2wfT130e9UHnumaHHMpUTosKe22PblOy
                6zrTpg9FkS0XGVmYRvOTNYx2HvQ= )
        3600 HINFO  "KLH-10" "ITS"
        3600 RRSIG  HINFO 5 2 3600 20040509183619 (
                20040409183619 38519 exemple.
                Iq/RGCbBdKzcYzlGE4ovbr5YcB+ezxbZ9W0l
                e/7WqyvhOO9J16HxhhL7VY/IKmTUY0GGdcfh
                ZEOCkf4lEykZF9NPok1/R/fWrtzNp8jobuY7
                AZEcZadp1WdDF3jc2/ndCa5XZhLKD3JzOsBw
                FvL8sqlS5QS6FY/ijFEDnI4RkZA= )
        3600 AAAA   2001:db8::f00:baa9
        3600 RRSIG  AAAA 5 2 3600 20040509183619 (
                20040409183619 38519 exemple.
                nLcpFuXdT35AcE+EoafOUkl69KB+/e56XmFK
                kewXG2IadYLKAOBIoR5+VoQV3XgTcofTJNsh
                1rnF6Eav2zpZB3byI6yo2bwY8MNkr4A7cL9T
                cMmDwV/hWFKsbGBsj8xSCN/caEL2CWY/5XP2
                sZM6QjBBLmukH30+w1z3h8PUP2o= )
        3600 NSEC   b.exemple. A HINFO AAAA RRSIG NSEC
        3600 RRSIG  NSEC 5 2 3600 20040509183619 (
                20040409183619 38519 exemple.
                QoshyPevLcJ/xcRpEtMft1uoIrcrieVcc9pG
                CScIn5Glnib40T6ayVOimXwdSTZ/8ISXGj4p
                P8Sh0PlA6olZQ84L453/BUqB8BpdOGky4hsN
                3AGcLEv1Gr0QMvirQaFcjzOECfnGyBm+wpFL
                AhS+JOVfDI/79QtyTI0SaDWcg8U= )
b.exemple.     3600 IN NS  ns1.b.exemple.
        3600 IN NS  ns2.b.exemple.
        3600 NSEC   ns1.exemple. NS RRSIG NSEC
        3600 RRSIG  NSEC 5 2 3600 20040509183619 (
                20040409183619 38519 exemple.
                GNuxHn844wfmUhPzGWKJCPY5ttEX/RfjDoOx
                9ueK1PtYkOWKOOdiJ/PJKCYB3hYX+858dDWS
                xb2qnV/LSTCNVBnkm6owOpysY97MVj5VQEWs
                0lm9tFoqjcptQkmQKYPrwUnCSNwvvclSF1xZ
                vhRXgWT7OuFXldoCG6TfVFMs9xE= )
ns1.b.exemple. 3600 IN A   192.0.2.7
ns2.b.exemple. 3600 IN A   192.0.2.8
ns1.exemple.   3600 IN A   192.0.2.1
        3600 RRSIG  A 5 2 3600 20040509183619 (
                20040409183619 38519 exemple.
                F1C9HVhIcs10cZU09G5yIVfKJy5yRQQ3qVet
                5pGhp82pzhAOMZ3K22JnmK4c+IjUeFp/to06
                im5FVpHtbFisdjyPq84bhTv8vrXt5AB1wNB+
                +iAqvIfdgW4sFNC6oADb1hK8QNauw9VePJhK
                v/iVXSYC0b7mPSU+EOlknFpVECs= )
        3600 NSEC   ns2.exemple. A RRSIG NSEC
        3600 RRSIG  NSEC 5 2 3600 20040509183619 (
                20040409183619 38519 exemple.
                I4hj+Kt6+8rCcHcUdolks2S+Wzri9h3fHas8
                1rGN/eILdJHN7JpV6lLGPIh/8fIBkfvdyWnB
                jjf1q3O7JgYO1UdI7FvBNWqaaEPJK3UkddBq
                ZIaLi8Qr2XHkjq38BeQsbp8X0+6h4ETWSGT8
                IZaIGBLryQWGLw6Y6X8dqhlnxJM= )
ns2.exemple.   3600 IN A   192.0.2.2
```

```
            3600 RRSIG  A 5 2 3600 20040509183619 (
                    20040409183619 38519 exemple.
                    V7cQRw1TR+knlaL1z/psxlS1PcD37JJDaCMq
                    Qo6/u1qFQu6x+wuDHRH22Ap9ulJPQjFwMKOu
                    yfPGQPC8KzGdE3vt5snFEAoE1Vn3mQqtu7SO
                    6amIjk13Kj/jyJ4nGmdRIc/3cM3ipXFhNTKq
                    rdhx8SZ0yy4ObIRzIzvBFLiSS8o= )
            3600 NSEC   *.w.exemple. A RRSIG NSEC
            3600 RRSIG  NSEC 5 2 3600 20040509183619 (
                    20040409183619 38519 exemple.
                    N0QzHvaJf5NRw1rE9uxS1Ltb2LZ73Qb9bKGE
                    VyaISkqzGpP3jYJXZJPVTq4UVEsgT3CgeHvb
                    3QbeJ5Dfb2V9NGCHj/OvF/LBxFFWwhLwzngH
                    l+bQAgAcMsLu/nL3nDi1y/JSQjAcdZNDl4bw
                    Ymx28EtgIpo9A0qmP08rMBqs1Jw= )
*.w.exemple.   3600 IN MX  1 ai.exemple.
            3600 RRSIG  MX 5 2 3600 20040509183619 (
                    20040409183619 38519 exemple.
                    OMK8rAZlepfzLWW75Dxd63jy2wswESzxDKG2
                    f9AMN1CytCd10cYISAxfAdvXSZ7xujKAtPbc
                    tvOQ2ofO7AZJ+d01EeeQTVBPq4/6KCWhqe2X
                    TjnkVLNvvhnc0u28aoSsG0+4InvkkOHknKxw
                    4kX18MMR34i8lC36SR5xBni8vHI= )
            3600 NSEC   x.w.exemple. MX RRSIG NSEC
            3600 RRSIG  NSEC 5 2 3600 20040509183619 (
                    20040409183619 38519 exemple.
                    r/mZnRC3I/VIcrelgIcteSxDhtsdlTDt8ng9
                    HSBlABOlzLxQtfgTnn8f+aOwJIAFe1Ee5RvU
                    5cVhQJNP5XpXMJHfyps8tVvfxSAXfahpYqtx
                    91gsmcV/1V9/bZAG55CefP9cM4Z9Y9NT9XQ8
                    s1InQ2UoIv6tJEaaKkP701j8OLA= )
x.w.exemple.   3600 IN MX  1 xx.exemple.
            3600 RRSIG  MX 5 3 3600 20040509183619 (
                    20040409183619 38519 exemple.
                    Il2WTZ+Bkv+OytBx4LItNW5mjB4RCwhOO8y1
                    XzPHZmZUTVYL7LaA63f6T9ysVBzJRI3KRjAP
                    H3U1qaYnDoN1DrWqmi9RJe4FoObkbcdm7P3I
                    kx70ePCoFgRz1Yq+bVVXCvGuAU4xALv3W/Y1
                    jNSlwZ2mSWKHfxFQxPtLj8s32+k= )
            3600 NSEC   x.y.w.exemple. MX RRSIG NSEC
            3600 RRSIG  NSEC 5 3 3600 20040509183619 (
                    20040409183619 38519 exemple.
                    aRbpHftxggzgMXdDlym9SsADqMZovZZl2QWK
                    vw8J0tZEUNQByH5Qfnf5N1FqH/pS46UA7A4E
                    mcWBN9PUA1pdPY6RVeaRlZlCr1IkVctvbtaI
                    NJuBba/VHm+pebTbKcAPIvL9tBOoh+to1h6e
                    IjgiM8PXkBQtxPq37wDKALkyn7Q= )
x.y.w.exemple. 3600 IN MX  1 xx.exemple.
            3600 RRSIG  MX 5 4 3600 20040509183619 (
                    20040409183619 38519 exemple.
                    k2bJHbwP5LH5qN4is39UiPzjAWYmJA38Hhia
                    t7i9t7nbX/e0FPnvDSQXzcK7UL+zrVA+3MDj
                    q1ub4q3SZgcbLMgexxIW3Va//LVrxkP6Xupq
                    GtOB9prkK54QTl/qZTXfMQpW480YOvVknhvb
                    +gLcMZBnHJ326nb/TOOmrqNmQQE= )
            3600 NSEC   xx.exemple. MX RRSIG NSEC
            3600 RRSIG  NSEC 5 4 3600 20040509183619 (
                    20040409183619 38519 exemple.
                    OvE6WUzN2ziieJcvKPWbCAyXyP6ef8cr6Csp
                    ArVSTzKSquNwbezZmkU7E34o5lmb6CWSSSpg
                    xw098kNUFnHcQf/LzY2zqRomubrNQhJTiDTX
                    a0ArunJQCzPjOYq5t0SLjm6qp6McJI1AP5Vr
                    QoKqJDCLnoAlcPOPKAm/jJkn3jk= )
```

```
xx.exemple.  3600 IN A  192.0.2.10
             3600 RRSIG  A 5 2 3600 20040509183619 (
                    20040409183619 38519 exemple.
                    kBF4YxMGWF0D8r0cztL+2fWWOvN1U/GYSpYP
                    7SoKoNQ4fZKyk+weWGlKLIUM+uE1zjVTPXoa
                    0Z6WG0oZp46rkl1EzMcdMgoaeUzzAJ2BMq+Y
                    VdxG9IK1yZkYGY9AgbTOGPoAgbJyO9EPULsx
                    kbIDV6GPPSZVusnZU6OMgdgzHV4= )
             3600 HINFO  "KLH-10" "TOPS-20"
             3600 RRSIG  HINFO 5 2 3600 20040509183619 (
                    20040409183619 38519 exemple.
                    GY2PLSXmMHkWHfLdggiox8+chWpeMNJLkML0
                    t+U/SXSUsoUdR91KNdNUkTDWamwcF8oFRjhq
                    BcPZ6EqrF+vl5v5oGuvSF7U52epfVTC+wWF8
                    3yCUeUw8YklhLWlvk8gQ15YKth0ITQy8/wI+
                    RgNvuwbioFSEuv2pNlkq0goYxNY= )
             3600 AAAA   2001:db8::f00:baaa
             3600 RRSIG  AAAA 5 2 3600 20040509183619 (
                    20040409183619 38519 exemple.
                    Zzj0yodDxcBLnnOIwDsuKo5WqiaK24DlKg9C
                    aGaxDFiKgKobUj2jilYQHpGFn2poFRetZd4z
                    ulyQkssz2QHrVrPuTMS22knudCiwP4LWpVTr
                    U4zfeA+rDz9stmSBP/4PekH/x2IoAYnwctd/
                    xS9cL2QgW7FChw16mzlkH6/vsfs= )
             3600 NSEC   exemple. A HINFO AAAA RRSIG NSEC
             3600 RRSIG  NSEC 5 2 3600 20040509183619 (
                    20040409183619 38519 exemple.
                    ZFWUln6Avc8bmGl5GFjD3BwT530DUZKHNuoY
                    9A8lgXYyrxu+pqgFiRVbyZRQvVB5pccEOT3k
                    mvHgEa/HzbDB4PIYY79W+VHrgOxzdQGGCZzi
                    asXrpSGOWwSOElghPnMIi8xdF7qtCntr382W
                    GghLahumFIpg4MO3LS/prgzVVWo= )
```

L'ensemble DNSKEY sommet inclut deux RR DNSKEY, et les fanions RDATA DNSKEY indiquent que chacun de ces RR DNSKEY est une clé de zone. Un de ces RR DNSKEY a aussi le fanion SEP établi et a été utilisé pour signer le RRset DNSKEY sommet ; c'est la clé qui devrait être hachée pour générer un enregistrement DS à insérer dans la zone parente. L'autre DNSKEY est utilisé pour signer tous les autres RRset de la zone.

La zone comporte une entrée de caractère générique, "*.w.exemple". Noter que le nom "*.w.exemple" est utilisé dans la construction des chaînes NSEC, et que le RRSIG qui couvre le RRset MX "*.w.exemple" a un compte d'étiquettes de 2.

La zone comporte aussi deux délégations. La délégation à "b.exemple" inclut un RRset NS, des enregistrements d'adresse glu, et un RR NSEC ; noter que seul le RRset NSEC est signé. La délégation à "a.exemple" fournit un RR DS ; noter que seuls les RRset NSEC et DS sont signés.

Appendice B Exemples de réponses

Les exemples de cette section montrent des messages de réponse qui utilisent l'exemple de zone signée de l'Appendice A.

B.1 Réponse

Une interrogation réussie à un serveur d'autorité.

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

;; Réponse
x.w.exemple.   3600 IN MX  1 xx.exemple.
x.w.exemple.   3600 RRSIG  MX 5 3 3600 20040509183619 (
```

```
                20040409183619 38519 exemple.
                Il2WTZ+Bkv+OytBx4LItNW5mjB4RCwhOO8y1
                XzPHZmZUTVYL7LaA63f6T9ysVBzJRI3KRjAP
                H3U1qaYnDoN1DrWqmi9RJe4FoObkbcdm7P3I
                kx70ePCoFgRz1Yq+bVVXCvGuAU4xALv3W/Y1
                jNSlwZ2mSWKHfxFQxPtLj8s32+k= )

;; Autorité
exemple.    3600 NS     ns1.exemple.
exemple.    3600 NS     ns2.exemple.
exemple.    3600 RRSIG  NS 5 1 3600 20040509183619 (
                20040409183619 38519 exemple.
                gl13F00f2U0R+SWiXXLHwsMY+qStYy5k6zfd
                EuivWc+wd1fmbNCyql0Tk7lHTX6UOxc8AgNf
                4ISFve8XqF4q+o9qlnqIzmppU3LiNeKT4FZ8
                RO5urFOvoMRTbQxW3U0hXWuggE4g3ZpsHv48
                0HjMeRaZB/FRPGfJPajngcq6Kwg= )

;; Additionnelle
xx.exemple.   3600 IN A   192.0.2.10
xx.exemple.   3600 RRSIG  A 5 2 3600 20040509183619 (
                20040409183619 38519 exemple.
                kBF4YxMGWF0D8r0cztL+2fWWOvN1U/GYSpYP
                7SoKoNQ4fZKyk+weWGlKLIUM+uE1zjVTPXoa
                0Z6WG0oZp46rkl1EzMcdMgoaeUzzAJ2BMq+Y
                VdxG9IK1yZkYGY9AgbTOGPoAgbJyO9EPULsx
                kbIDV6GPPSZVusnZU6OMgdgzHV4= )
xx.exemple.   3600 AAAA   2001:db8::f00:baaa
xx.exemple.   3600 RRSIG  AAAA 5 2 3600 20040509183619 (
                20040409183619 38519 exemple.
                Zzj0yodDxcBLnnOIwDsuKo5WqiaK24DlKg9C
                aGaxDFiKgKobUj2jilYQHpGFn2poFRetZd4z
                ulyQkssz2QHrVrPuTMS22knudCiwP4LWpVTr
                U4zfeA+rDz9stmSBP/4PekH/x2IoAYnwctd/
                xS9cL2QgW7FChw16mzlkH6/vsfs= )
ns1.exemple.  3600 IN A   192.0.2.1
ns1.exemple.  3600 RRSIG  A 5 2 3600 20040509183619 (
                20040409183619 38519 exemple.
                F1C9HVhIcs10cZU09G5yIVfKJy5yRQQ3qVet
                5pGhp82pzhAOMZ3K22JnmK4c+IjUeFp/to06
                im5FVpHtbFisdjyPq84bhTv8vrXt5AB1wNB+
                +iAqvIfdgW4sFNC6oADb1hK8QNauw9VePJhK
                v/iVXSYC0b7mPSU+EOlknFpVECs= )
ns2.exemple.  3600 IN A   192.0.2.2
ns2.exemple.  3600 RRSIG  A 5 2 3600 20040509183619 (
                20040409183619 38519 exemple.
                V7cQRw1TR+knlaL1z/psxlS1PcD37JJDaCMq
                Qo6/u1qFQu6x+wuDHRH22Ap9ulJPQjFwMKOu
                yfPGQPC8KzGdE3vt5snFEAoE1Vn3mQqtu7SO
                6amIjk13Kj/jyJ4nGmdRIc/3cM3ipXFhNTKq
                rdhx8SZ0yy4ObIRzIzvBFLiSS8o= )
```

B.2 Erreur de nom

Une erreur de nom d'autorité. Les RR NSEC prouvent que le nom n'existe pas et qu'aucun caractère générique couvrant n'existe.

```
;; En-tête : QR AA DO RCODE=3
;;
;; Question
ml.exemple.       IN A

;; Réponse
```

```
;; (vide)

;; Autorité
exemple.      3600 IN SOA ns1.exemple. bugs.x.w.exemple. (
                   1081539377
                   3600
                   300
                   3600000
                   3600
                   )
exemple.      3600 RRSIG  SOA 5 1 3600 20040509183619 (
                   20040409183619 38519 exemple.
                   ONx0k36rcjaxYtcNgq6iQnpNV5+drqYAsC9h
                   7TSJaHCqbhE67Sr6aH2xDUGcqQWu/n0UVzrF
                   vkgO9ebarZ0GWDKcuwlM6eNB5SiX2K74l5LW
                   DA7S/Un/IbtDq4Ay8NMNLQI7Dw7n4p8/rjkB
                   jV7j86HyQgM5e7+miRAz8V01b0I= )
b.exemple.    3600 NSEC   ns1.exemple. NS RRSIG NSEC
b.exemple.    3600 RRSIG  NSEC 5 2 3600 20040509183619 (
                   20040409183619 38519 exemple.
                   GNuxHn844wfmUhPzGWKJCPY5ttEX/RfjDoOx
                   9ueK1PtYkOWKOOdiJ/PJKCYB3hYX+858dDWS
                   xb2qnV/LSTCNVBnkm6owOpysY97MVj5VQEWs
                   0lm9tFoqjcptQkmQKYPrwUnCSNwvvclSF1xZ
                   vhRXgWT7OuFXldoCG6TfVFMs9xE= )
exemple.      3600 NSEC   a.exemple. NS SOA MX RRSIG NSEC DNSKEY
exemple.      3600 RRSIG  NSEC 5 1 3600 20040509183619 (
                   20040409183619 38519 exemple.
                   O0k558jHhyrC97ISHnislm4kLMW48C7U7cBm
                   FTfhke5iVqNRVTB1STLMpgpbDIC9hcryoO0V
                   Z9ME5xPzUEhbvGnHd5sfzgFVeGxr5Nyyq4tW
                   SDBgIBiLQUv1ivy29vhXy7WgR62dPrZ0PWvm
                   jfFJ5arXf4nPxp/kEowGgBRzY/U= )

;; Additionnelle
;; (vide)
```

B.3 Erreur Pas de données

Une réponse "Pas de données". Le RR NSEC 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.      3600 IN SOA ns1.exemple. bugs.x.w.exemple. (
                   1081539377
                   3600
                   300
                   3600000
                   3600
                   )
exemple.      3600 RRSIG  SOA 5 1 3600 20040509183619 (
                   20040409183619 38519 exemple.
                   ONx0k36rcjaxYtcNgq6iQnpNV5+drqYAsC9h
                   7TSJaHCqbhE67Sr6aH2xDUGcqQWu/n0UVzrF
                   vkgO9ebarZ0GWDKcuwlM6eNB5SiX2K74l5LW
                   DA7S/Un/IbtDq4Ay8NMNLQI7Dw7n4p8/rjkB
```

```
                jV7j86HyQgM5e7+miRAz8V01b0I= )
ns1.exemple.  3600 NSEC   ns2.exemple. A RRSIG NSEC
ns1.exemple.  3600 RRSIG  NSEC 5 2 3600 20040509183619 (
                20040409183619 38519 exemple.
                I4hj+Kt6+8rCcHcUdolks2S+Wzri9h3fHas8
                1rGN/eILdJHN7JpV6lLGPIh/8fIBkfvdyWnB
                jjf1q3O7JgYO1UdI7FvBNWqaaEPJK3UkddBq
                ZIaLi8Qr2XHkjq38BeQsbp8X0+6h4ETWSGT8
                IZaIGBLryQWGLw6Y6X8dqhlnxJM= )

;; Additionnelle
;; (vide)
```

B.4 Référence à une zone signée

Référence à une zone signée. Le RR DS contient les données dont le résolveur va devoir valider le RR DNSKEY correspondant dans le sommet de la zone fille.

```
;; En-tête : QR DO RCODE=0
;;

;; Question
mc.a.exemple.      IN MX

;; Réponse
;; (vide)

;; Autorité
a.exemple.    3600 IN NS  ns1.a.exemple.
a.exemple.    3600 IN NS  ns2.a.exemple.
a.exemple.    3600 DS     57855 5 1 ( B6DCD485719ADCA18E5F3D48A2331627FDD3636B )
a.exemple.    3600 RRSIG  DS 5 2 3600 20040509183619 (
                20040409183619 38519 exemple.
                oXIKit/QtdG64J/CB+Gi8dOvnwRvqrto1AdQ
                oRkAN15FP3iZ7suB7gvTBmXzCjL7XUgQVcoH
                kdhyCuzp8W9qJHgRUSwKKkczSyuL64nhgjuD
                EML8l9wlWVsl7PR2VnZduM9bLyBhaaPmRKX/
                Fm+v6ccF2EGNLRiY08kdkz+XHHo= )

;; Additionnelle
ns1.a.exemple. 3600 IN A   192.0.2.5
ns2.a.exemple. 3600 IN A   192.0.2.6
```

B.5 Référence à une zone non signée

Référence à une zone non signée. Le RR NSEC prouve qu'aucun RR DS n'existe pour cette délégation dans la zone parente.

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

;; Réponse
;; (empty)

;; Autorité
b.exemple.    3600 IN NS  ns1.b.exemple.
b.exemple.    3600 IN NS  ns2.b.exemple.
b.exemple.    3600 NSEC   ns1.exemple. NS RRSIG NSEC
b.exemple.    3600 RRSIG  NSEC 5 2 3600 20040509183619 (
                20040409183619 38519 exemple.
                GNuxHn844wfmUhPzGWKJCPY5ttEX/RfjDoOx
```

```
                9ueK1PtYkOWKOOdiJ/PJKCYB3hYX+858dDWS
                xb2qnV/LSTCNVBnkm6owOpysY97MVj5VQEWs
                0lm9tFoqjcptQkmQKYPrwUnCSNwvvclSF1xZ
                vhRXgWT7OuFXldoCG6TfVFMs9xE= )

;; Additionnelle
ns1.b.exemple. 3600 IN A   192.0.2.7
ns2.b.exemple. 3600 IN A   192.0.2.8
```

B.6 Expansion de caractère générique

Interrogation réussie via l'expansion de caractère générique. Le compte d'étiquettes dans le RR RRSIG de la réponse indique qu'un RRset à caractère générique a été expansé pour produire cette réponse, et le RR NSEC prouve qu'il n'existe pas de correspondance plus proche dans la zone.

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

;; Réponse
a.z.w.exemple. 3600 IN MX  1 ai.exemple.
a.z.w.exemple. 3600 RRSIG  MX 5 2 3600 20040509183619 (
                20040409183619 38519 exemple.
                OMK8rAZlepfzLWW75Dxd63jy2wswESzxDKG2
                f9AMN1CytCd10cYISAxfAdvXSZ7xujKAtPbc
                tvOQ2ofO7AZJ+d01EeeQTVBPq4/6KCWhqe2X
                TjnkVLNvvhnc0u28aoSsG0+4InvkkOHknKxw
                4kX18MMR34i8lC36SR5xBni8vHI= )

;; Autorité
exemple.      3600 NS     ns1.exemple.
exemple.      3600 NS     ns2.exemple.
exemple.      3600 RRSIG  NS 5 1 3600 20040509183619 (
                20040409183619 38519 exemple.
                gl13F00f2U0R+SWiXXLHwsMY+qStYy5k6zfd
                EuivWc+wd1fmbNCyql0Tk7lHTX6UOxc8AgNf
                4ISFve8XqF4q+o9qlnqIzmppU3LiNeKT4FZ8
                RO5urFOvoMRTbQxW3U0hXWuggE4g3ZpsHv48
                0HjMeRaZB/FRPGfJPajngcq6Kwg= )
x.y.w.exemple. 3600 NSEC   xx.exemple. MX RRSIG NSEC
x.y.w.exemple. 3600 RRSIG  NSEC 5 4 3600 20040509183619 (
                20040409183619 38519 exemple.
                OvE6WUzN2ziieJcvKPWbCAyXyP6ef8cr6Csp
                ArVSTzKSquNwbezZmkU7E34o5lmb6CWSSSpg
                xw098kNUFnHcQf/LzY2zqRomubrNQhJTiDTX
                a0ArunJQCzPjOYq5t0SLjm6qp6McJI1AP5Vr
                QoKqJDCLnoAlcPOPKAm/jJkn3jk= )

;; Additionnelle
ai.exemple.   3600 IN A   192.0.2.9
ai.exemple.   3600 RRSIG  A 5 2 3600 20040509183619 (
                20040409183619 38519 exemple.
                pAOtzLP2MU0tDJUwHOKE5FPIIHmdYsCgTb5B
                ERGgpnJluA9ixOyf6xxVCgrEJW0WNZSsJicd
                hBHXfDmAGKUajUUlYSAH8tS4ZnrhyymIvk3u
                ArDu2wfT130e9UHnumaHHMpUTosKe22PblOy
                6zrTpg9FkS0XGVmYRvOTNYx2HvQ= )
ai.exemple.   3600 AAAA   2001:db8::f00:baa9
ai.exemple.   3600 RRSIG  AAAA 5 2 3600 20040509183619 (
                20040409183619 38519 exemple.
                nLcpFuXdT35AcE+EoafOUkl69KB+/e56XmFK
                kewXG2IadYLKAOBIoR5+VoQV3XgTcofTJNsh
```

```
                1rnF6Eav2zpZB3byI6yo2bwY8MNkr4A7cL9T
                cMmDwV/hWFKsbGBsj8xSCN/caEL2CWY/5XP2
                sZM6QjBBLmukH30+w1z3h8PUP2o= )
```

B.7 Erreur Pas de données pour un caractère générique

Une réponse "Pas de données" pour un nom couvert par un caractère générique. Le RR NSEC prouve que la correspondance d'un nom à caractère générique 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
;; (empty)

;; Autorité
exemple.       3600 IN SOA ns1.exemple. bugs.x.w.exemple. (
                    1081539377
                    3600
                    300
                    3600000
                    3600
                    )
exemple.       3600 RRSIG  SOA 5 1 3600 20040509183619 (
                    20040409183619 38519 exemple.
                    ONx0k36rcjaxYtcNgq6iQnpNV5+drqYAsC9h
                    7TSJaHCqbhE67Sr6aH2xDUGcqQWu/n0UVzrF
                    vkgO9ebarZ0GWDKcuwlM6eNB5SiX2K74l5LW
                    DA7S/Un/IbtDq4Ay8NMNLQI7Dw7n4p8/rjkB
                    jV7j86HyQgM5e7+miRAz8V01b0I= )
x.y.w.exemple. 3600 NSEC   xx.exemple. MX RRSIG NSEC
x.y.w.exemple. 3600 RRSIG  NSEC 5 4 3600 20040509183619 (
                    20040409183619 38519 exemple.
                    OvE6WUzN2ziieJcvKPWbCAyXyP6ef8cr6Csp
                    ArVSTzKSquNwbezZmkU7E34o5lmb6CWSSSpg
                    xw098kNUFnHcQf/LzY2zqRomubrNQhJTiDTX
                    a0ArunJQCzPjOYq5t0SLjm6qp6McJI1AP5Vr
                    QoKqJDCLnoAlcPOPKAm/jJkn3jk= )
*.w.exemple.   3600 NSEC   x.w.exemple. MX RRSIG NSEC
*.w.exemple.   3600 RRSIG  NSEC 5 2 3600 20040509183619 (
                    20040409183619 38519 exemple.
                    r/mZnRC3I/VIcrelgIcteSxDhtsdlTDt8ng9
                    HSBlABOlzLxQtfgTnn8f+aOwJIAFe1Ee5RvU
                    5cVhQJNP5XpXMJHfyps8tVvfxSAXfahpYqtx
                    91gsmcV/1V9/bZAG55CefP9cM4Z9Y9NT9XQ8
                    s1InQ2UoIv6tJEaaKkP701j8OLA= )

;; Additionnelle
;; (vide)
```

B.8 Erreur Pas de données pour la zone fille DS

Une réponse "pas de données" 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.      3600 IN SOA ns1.exemple. bugs.x.w.exemple. (
                   1081539377
                   3600
                   300
                   3600000
                   3600
                   )
exemple.      3600 RRSIG  SOA 5 1 3600 20040509183619 (
                   20040409183619 38519 exemple.
                   ONx0k36rcjaxYtcNgq6iQnpNV5+drqYAsC9h
                   7TSJaHCqbhE67Sr6aH2xDUGcqQWu/n0UVzrF
                   vkgO9ebarZ0GWDKcuwlM6eNB5SiX2K74l5LW
                   DA7S/Un/IbtDq4Ay8NMNLQI7Dw7n4p8/rjkB
                   jV7j86HyQgM5e7+miRAz8V01b0I= )
exemple.      3600 NSEC   a.exemple. NS SOA MX RRSIG NSEC DNSKEY
exemple.      3600 RRSIG  NSEC 5 1 3600 20040509183619 (
                   20040409183619 38519 exemple.
                   O0k558jHhyrC97ISHnislm4kLMW48C7U7cBm
                   FTfhke5iVqNRVTB1STLMpgpbDIC9hcryoO0V
                   Z9ME5xPzUEhbvGnHd5sfzgFVeGxr5Nyyq4tW
                   SDBgIBiLQUv1ivy29vhXy7WgR62dPrZ0PWvm
                   jfFJ5arXf4nPxp/kEowGgBRzY/U= )

;; Additionnelle
;; (vide)
```

Appendice C Exemples d'authentification

Les exemples de cette section montrent comment les messages de réponse de l'Appendice B sont authentifiés.

C.1 Authentification d'une réponse

L'interrogation de l'Appendice B.1 a retourné un RRset MX pour "x.w.exemple.com". Le RRSIG correspondant indique que le RRset MX était signé par un "exemple" DNSKEY avec l'algorithme 5 et l'étiquette de clé 38519. Le résolveur a besoin du RR DNSKEY correspondant afin d'authentifier cette réponse. La discussion ci-dessous décrit comment un résolveur peut obtenir ce RR DNSKEY.

Le RRSIG indique que le TTL d'origine du RRset MX était 3600, et, pour les besoins de l'authentification, le TTL courant est remplacé par 3600. La valeur du champ Étiquettes du RRSIG de 3 indique que la réponse n'était pas le résultat d'une expansion de caractère générique. Le RRset MX "x.w.exemple.com" est mis en forme canonique, et, en supposant que l'heure actuelle tombe entre les dates de début et d'expiration de la signature, la signature est authentifiée.

C.1.1 Exemple d'authentification du RR DNSKEY

Cet exemple montre le processus logique d'authentification qui commence à une DNSKEY (ou RR DS) racine configurée et descend l'arborescence pour authentifier le RR DNSKEY "exemple" désiré. Noter que l'ordre logique est présenté pour la clarté de l'exposé. Une mise en œuvre peut choisir de construire l'authentification comme les références sont reçues ou de construire la chaîne d'authentification seulement après que tous les RRset ont été obtenus, ou dans toute autre combinaison qu'elle estime convenir. L'exemple donné ici montre seulement le processus logique et ne dicte aucune règle de mise en œuvre.

On suppose que le résolveur commence par un RR DNSKEY configuré pour la zone racine (ou un RR DS configuré pour la zone racine). Le résolveur vérifie si ce RR DNSKEY configuré est présent dans le RRset DNSKEY (ou si le RR DS correspond à une DNSKEY dans le RRset DNSKEY racine) si ce RR DNSKEY a signé le RRset DNSKEY racine, et si la durée de vie de la signature est valide. Si toutes ces conditions sont satisfaites, toutes les clés dans le RRset DNSKEY sont considérées comme authentifiées. Le résolveur utilise alors un (ou plusieurs) des RR DNSKEY racine pour authentifier le

RRset DS "exemple". Noter que le résolveur peut devoir interroger la zone racine pour obtenir le RRset DNSKEY racine ou le RRset DS "exemple".

Une fois que le RRset DS a été authentifié en utilisant le DNSKEY racine, le résolveur vérifie le RRset DNSKEY "exemple" à la recherche d'un RR DNSKEY "exemple" qui corresponde à un des RR DS "exemple" authentifié. Si un tel DNSKEY "exemple" correspondant est trouvé, le résolveur cherche si ce RR DNSKEY a signé le RRset DNSKEY "exemple" et si la durée de vie de la signature est valide. Si ces conditions sont satisfaites, toutes les clés dans le RRset DNSKEY "exemple" sont considérées comme authentifiées.

Finalement, le résolveur vérifie qu'un RR DNSKEY dans le RRset DNSKEY "exemple" utilise l'algorithme 5 et a une étiquette de clé de 38519. Ce DNSKEY est utilisé pour authentifier le RRSIG inclus dans la réponse. Si plusieurs RR DNSKEY "exemple" correspondent à cet algorithme et étiquette de clé, alors chaque RR DNSKEY est essayé, et la réponse est authentifiée si un des RR DNSKEY correspondants valide la signature comme décrit ci-dessus.

C.2 Erreur de nom

L'interrogation de l'Appendice B.2 a retourné les RR NSEC qui prouvent que les données demandées n'existent pas et qu'aucun caractère générique ne s'applique. La réponse négative est authentifiée en vérifiant les deux RR NSEC. Les RR NSEC sont authentifiés de manière identique à celle du RRset MX discuté ci-dessus.

C.3 Pas d'erreur de données

L'interrogation de l'Appendice B.3 a retourné un RR NSEC qui prouve que le nom demandé existe, mais le type de RR demandé n'existe pas. La réponse négative est authentifiée en vérifiant le RR NSEC. Le RR NSEC est authentifié d'une manière identique à celle du RRset MX discuté plus haut.

C.4 Référence à une zone signée

L'interrogation de l'Appendice B.4 a retourné une référence à la zone signée "a.exemple.". Le RR DS est authentifié d'une manière identique à celle du RRset MX discuté plus haut. Ce RR DS est utilisé pour authentifier le RRset DNSKEY "a.exemple".

Une fois que le RRset DS "a.exemple" a été authentifié en utilisant le DNSKEY "exemple", le résolveur cherche dans le RRset DNSKEY "a.exemple" un RR DNSKEY "a.exemple" qui corresponde au RR DS. Si un tel DNSKEY "a.exemple" correspondant est trouvé, le résolveur cherche si ce RR DNSKEY a signé le RRset DNSKEY "a.exemple" et si la durée de vie de la signature est valide. Si toutes ces conditions sont satisfaites, toutes les clés dans le RRset DNSKEY "a.exemple" sont considérées comme authentifiées.

C.5 Référence à zone non signée

L'interrogation de l'Appendice B.5 a retourné une référence à une zone "b.exemple." non signée. Le NSEC prouve qu'aucune authentification ne conduit de "exemple" à "b.exemple", et le RR NSEC est authentifié d'une manière identique à celle du RRset MX discuté plus haut

C.6 Expansion de caractère générique

L'interrogation de l'Appendice B.6 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 ce serait le cas dans une réponse DNS traditionnelle, et le RRSIG correspondant indique que le RRset MX à caractère générique expansé a été signé par une DNSKEY "exemple" avec l'algorithme 5 et l'étiquette de clé 38519. Le RRSIG indique que le TTL original du RRset MX était 3600, et, pour les besoins de l'authentification, le TTL courant est remplacé par 3600. La valeur du champ Étiquettes du 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. Le nom "a.z.w.w.exemple" est remplacé par "*.w.exemple", le RRset MX est mis en forme canonique, et, en supposant que l'heure actuelle tombe entre les dates de début et d'expiration de la signature, celle-ci est authentifiée.

Le NSEC prouve qu'aucune correspondance plus proche (exacte ou caractère générique plus proche) ne pouvait être utilisée pour répondre à cette interrogation, et le RR NSEC doit aussi être authentifié avant que la réponse soit considérée valide.

C.7 Pas d'erreur de données avec caractère générique

L'interrogation de l'Appendice B.7 a retourné les RR NSEC qui prouvent que les données demandées n'existent pas et qu'aucun caractère générique ne s'applique. La réponse négative est authentifiée en vérifiant les deux RR NSEC.

C.8 Pas d'erreur de données avec zone DS fille

L'interrogation de l'Appendice B.8 a retourné des RR NSEC qui montrent que c'est un serveur fils (le serveur "exemple") qui a répondu. Le RR NSEC indique la présence d'un RR SOA, montrant que la réponse est du fils. Les interrogations pour le RRset DS "exemple" devraient être envoyées aux serveurs parents (serveurs "racines").

Adresse des auteurs

Roy Arends
Telematica Instituut
Brouwerijstraat 1
7523 XC Enschede
NL
mél : roy.arends@telin.nl

Rob Austein
Internet Systems Consortium
950 Charter Street
Redwood City, CA 94063
USA
mél : sra@isc.org

Matt Larson
VeriSign, Inc.
21345 Ridgetop Circle
Dulles, VA 20166-6503
USA
mél : mlarson@verisign.com

Dan Massey
Colorado State University
Department of Computer Science
Fort Collins, CO 80523-1873
USA
mél : massey@cs.colostate.edu

Scott Rose
National Institute for Standards et Technology
100 Bureau Drive
Gaithersburg, MD 20899-8920
USA
mél : scott.rose@nist.gov

Déclaration complète de droits de reproduction

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