Groupe de travail Réseau
Request for Comments : 4034
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
Tradution 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

Enregistrements de ressource 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, *DNS Security Extensions*). Les extensions de sécurité du DNS sont une collection d'enregistrements de ressource et de modifications du protocole qui fournissent l'authentification de la source pour le DNS. Ce document définit les enregistrements de ressource de clé publique (DNSKEY), de signataire de délégation (DS), de signature numérique d'enregistrement de ressource (RRSIG), et de non existence authentifiée (NSEC). L'objet et le format de chaque enregistrement de ressource est décrit en détail, et un exemple de chaque enregistrement de ressource est fourni.

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

Table des Matières

1. Introduction

Les extensions de sécurité du DNS (DNSSEC) introduisent quatre nouveaux types d'enregistrement de ressource du DNS : Clé publique DNS (DNSKEY), Signature d'enregistrement de ressource (RRSIG), Prochain enregistrement sûr (NSEC), et signataire de délégation (DS). Le présent document définit l'objet de chaque enregistrement de ressource (RR), le format RDATA du RR, et son format de présentation (représentation ASCII).

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

La [RFC4035] définit les opérations du protocole DNSSEC.

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

Le présent document définit les enregistrements de ressource de DNSSEC. Tous les codes numériques de type DNS donnés dans le présent document sont des entiers décimaux.

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. L'enregistrement de ressource DNSKEY

DNSSEC utilise la cryptographie à clé publique pour signer et authentifier les ensembles d'enregistrements de ressource (RRset) du DNS. Les clés publiques sont mémorisées dans les enregistrements de ressource DNSKEY et sont utilisés dans le processus d'authentification DNSSEC décrit dans la [RFC4035] : une zone signe ses RRset d'autorité en utilisant une clé privée et mémorise la clé publique correspondante dans un RR DNSKEY. Un résolveur peut alors utiliser la clé publique pour valider les signatures couvrant les RRset dans la zone, et donc les authentifier.

Le RR DNSKEY n'est pas destiné à être un enregistrement pour mémoriser des clés publiques arbitraires et NE DOIT PAS être utilisé pour mémoriser des certificats ou des clés publiques qui ne se rapportent pas directement à l'infrastructure du DNS.

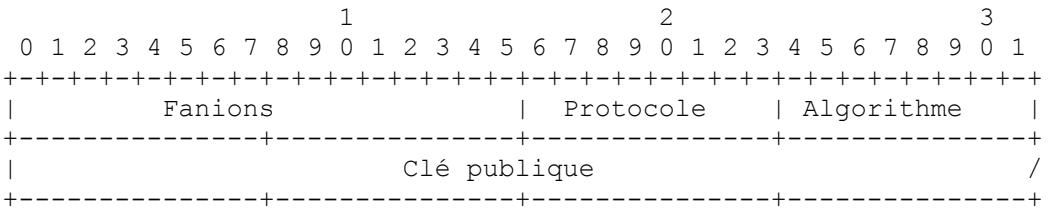
La valeur de Type pour le type de RR DNSKEY est 48.

Le RR DNSKEY RR est indépendant de la classe.

Le RR DNSKEY n'a pas d'exigence de TTL particulière.

2.1 Format réseau de RDATA DNSKEY

Le RDATA pour un RR DNSKEY consiste en un champ Fanions de 2 octets, un champ Protocole de 1 octet, un champ Algorithme de 1 octet, et le champ Clé publique.



2.1.1 Le champ Fanions

Le bit 7 du champ Fanions est le fanion de clé de zone. Si le bit 7 a la valeur 1, l'enregistrement DNSKEY détient alors une clé de zone DNS, et le nom du propriétaire du RR DNSKEY DOIT être le nom d'une zone. Si le bit 7 a la valeur 0, l'enregistrement DNSKEY détient un autre type de clé publique DNS et NE DOIT PAS être utilisé pour vérifier les RRSIG qui couvrent les RRset.

Le bit 15 du champ Fanions est le fanion de point d'entrée sécurisé, décrit dans la [RFC3757]. Si le bit 15 a la valeur 1, l'enregistrement DNSKEY détient une clé destinée à être utilisée comme point d'entrée sécurisé. Ce fanion est seulement destiné à être une indication pour le logiciel de signature de zone ou de débogage de l'usage de destination de cet enregistrement DNSKEY ; les valideurs NE DOIVENT en aucune façon altérer leur comportement durant le processus de validation de signature quant au réglage de ce bit. Cela signifie aussi qu'un RR DNSKEY avec le bit SEP établi aura aussi besoin que le fanion Clé de zone soit établi afin d'être capable de générer les signatures en toute légalité. Un RR DNSKEY avec le bit SEP mis et le fanion Clé de zone non mis NE DOIT PAS être utilisé pour vérifier les RRSIG qui couvrent les RRset.

Les bits 0-6 et 8-14 sont réservés : ces bits DOIVENT avoir une valeur de 0 à la création du RR DNSKEY et DOIVENT être ignorés à réception.

2.1.2 Le champ Protocole

Le champ Protocole DOIT avoir la valeur 3, et le RR DNSKEY DOIT être traité comme invalide durant la vérification de signature si il est trouvé avec une valeur autre que 3.

2.1.3 Le champ Algorithme

Le champ Algorithme identifie l'algorithme cryptographique de la clé publique et détermine le format du champ Clé publique. Une liste des types d'algorithmes DNSSEC se trouve dans l'appendice A.1.

2.1.4 Le champ Clé publique

Le champ Clé publique détient le matériel de clé publique. Le format dépend de l'algorithme de la clé qui est mémorisée et il est décrit dans des documents différents.

2.1.5 Notes sur la conception du RDATA de DNSKEY

Bien que le champ Protocole ait toujours la valeur 3, il est conservé pour la rétro-compatibilité avec les versions antérieures de l'enregistrement CLÉ.

2.2 Format de présentation du RR DNSKEY

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

Le champ Fanion DOIT être représenté comme entier décimal non signé. Étant donnés les fanions actuellement définis, les valeurs possibles sont : 0, 256, et 257.

Le champ Protocole DOIT être représenté comme entier décimal non signé d'une valeur de 3.

Le champ Algorithme DOIT être représenté soit comme un entier décimal non signé soit comme un mnémonique d'algorithme comme spécifié à l'Appendice A.1.

Le champ Clé publique DOIT être comme un codage en Base64 de la clé publique. Les espaces blanches sont admises dans le texte en Base64. Voir la définition du codage Base64 dans la [RFC3548].

2.3 Exemple de RR DNSKEY

Le RR DNSKEY suivant mémorise une clé de zone DNS pour "example.com." :

```
example.com. 86400 IN DNSKEY 256 3 5
( AQPSKmynfzW4kyBv015MUG2DeIQ3Cbl+BBZH4b/0PY1kxkmvHjcZc8nokfzj31GajIQKY+5CptLr3buXA10hWq
TkF7H6RfoRqXQeogmMHfpftf6zMv1LyBUgia7za6ZEzOJBOztyvhjL742iU/TpPSEDhm2SNKLijfUppn1UaNvv4w=
= )
```

Les quatre premiers champs de texte spécifient le nom du propriétaire, le TTL, la classe, et le type de RR (DNSKEY). La valeur 256 indique que le bit de clé de zone (bit 7) dans le champ Fanions a la valeur 1. La valeur 3 est la valeur fixée du protocole. La valeur 5 indique l'algorithme de clé publique. L'appendice A.1 identifie l'algorithme de type 5 comme RSA/SHA1 et indique que le format du champ de clé publique RSA/SHA1 est défini dans la [RFC3110]. Le reste du texte est un codage Base64 de la clé publique.

3. Enregistrement de ressource RRSIG

DNSSEC utilise la cryptographie de clé publique pour signer et authentifier les ensembles d'enregistrements de ressource (RRset, *resource record set*) du DNS. Les signatures numériques sont mémorisées dans les enregistrements de ressource RRSIG et sont utilisées dans le processus d'authentification de DNSSEC décrit dans la [RFC4035]. Un valideur peut utiliser ces RR RRSIG pour authentifier les RRset de la zone. Le RR RRSIG ne DOIT être utilisé que pour porter le matériel de vérification (signatures numériques) utilisé pour sécuriser les opérations du DNS.

Un enregistrement RRSIG contient la signature pour un RRset avec un nom, une classe et un type particuliers. Le RR RRSIG spécifie un intervalle de validité pour la signature et utilise l'algorithme, le nom du signataire et l'étiquette de clé pour identifier le RR DNSKEY qui contient la clé publique que peut utiliser un valideur pour vérifier la signature.

Parce que chaque RRset d'autorité dans une zone doit être protégé par une signature numérique, les RR RRSIG doivent être présents pour les noms qui contiennent un RR CNAME. Ceci est un changement par rapport à la spécification traditionnelle du DNS [RFC1034], qui déclarait que si un CNAME est présent pour un nom, il est le seul type admis à ce nom. Un RRSIG et un NSEC (voir la Section 4) DOIVENT exister pour le même nom qu'un enregistrement de ressource CNAME dans une zone signée.

La valeur de Type pour le type de RR RRSIG est 46.

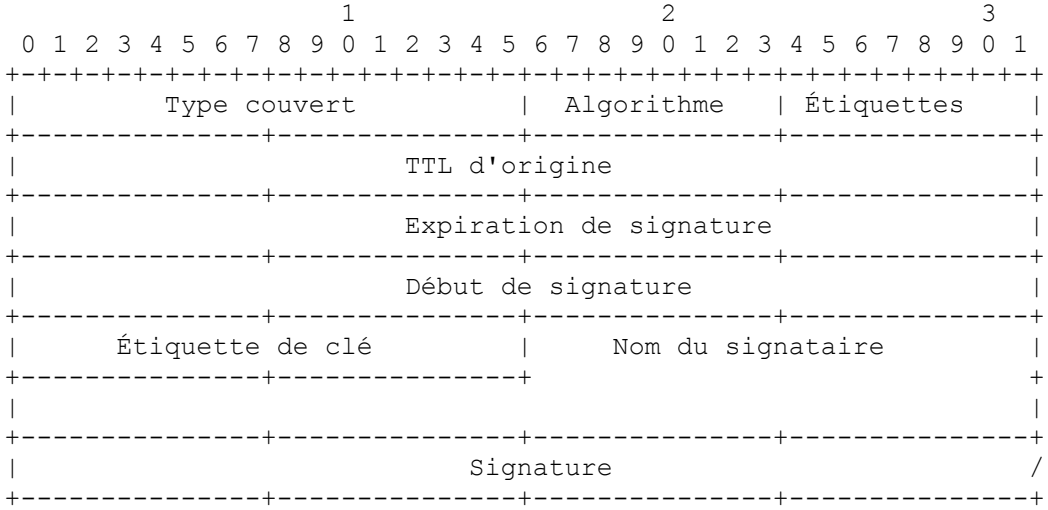
Le RR RRSIG est indépendant de la classe.

Un RR RRSIG DOIT avoir la même classe que le RRset qu'il couvre.

La valeur de TTL d'un RR RRSIG DOIT correspondre à la valeur de TTL du RRset qu'il couvre. C'est une exception aux règles de la [RFC2181] pour les valeurs de TTL des RR individuels au sein d'un RRset : les RR RRSIG individuels avec le même nom de propriétaire auront des valeurs de TTL différentes si les RRset qu'ils couvrent ont des valeurs de TTL différentes.

3.1 Format incorporé de RDATA RRSIG

Le RDATA pour un RRSIG consiste en un champ Type couvert de deux octets, un champ Algorithme de un octet, un champ Étiquette de un octet, un champ TTL d'origine de quatre octets, un champ Expiration de signature de quatre octets, un champ Début de signature de quatre octets, une étiquette de clé de deux octets, le champ Nom du signataire, et le champ Signature.



3.1.1 Champ Type couvert

Le champ Type couvert identifie le type du RRset qui est couvert par cet enregistrement RRSIG.

3.1.2 Champ Numéro d'algorithme

Le champ Numéro d'algorithme identifie l'algorithme cryptographique utilisé pour créer la signature. Une liste des types d'algorithmes DNSSEC se trouve dans l'Appendice A.1

3.1.3 Champ Étiquettes

Le champ Étiquettes spécifie le nombre d'étiquettes dans le RR RRSIG d'origine du nom du propriétaire. La signification de ce champ est qu'un valideur l'utilise pour déterminer si la réponse a été synthétisée à partir d'un caractère générique. Si c'est le cas, il peut être utilisé pour déterminer quel nom de propriétaire a été utilisé pour générer la signature.

Pour valider une signature, le valideur a besoin du nom du propriétaire d'origine qui a été utilisé pour créer la signature. Si le nom du propriétaire d'origine contient une étiquette de caractère générique ("*"), le nom du propriétaire peut avoir été étendu par le serveur durant le processus de réponse, auquel cas le valideur devra reconstruire le nom du propriétaire d'origine afin de valider la signature. La [RFC4035] décrit comment utiliser le champ Étiquettes pour reconstruire le nom de propriétaire d'origine.

La valeur du champ Étiquettes NE DOIT PAS compter l'étiquette nulle (racine) qui termine le nom de propriétaire ou l'étiquette de caractère générique (si elle est présente). La valeur du champ Étiquette DOIT être inférieure ou égale au nombre d'étiquettes contenues dans le nom du propriétaire du RRSIG. Par exemple, "www.example.com." a une valeur de champ Étiquettes de 3, et "*.example.com." a une valeur de champ Étiquettes de 2. Racine (".") a une valeur de champ Étiquettes de 0.

Bien que l'étiquette de caractère générique ne soit pas incluse dans le compte mémorisé dans le champ Étiquettes du RR RRSIG, l'étiquette de caractère générique fait partie du nom de propriétaire du RRset lorsque la signature est générée ou vérifiée.

3.1.4 Champ TTL d'origine

Le champ TTL d'origine spécifie le TTL du RRset couvert tel qu'il apparaît dans la zone d'autorité.

Le champ TTL d'origine est nécessaire parce qu'un résolveur à antémémoire décrémente la valeur du TTL d'un RRset en antémémoire. Afin de valider une signature, un valideur exige le TTL d'origine. La [RFC4035] décrit comment utiliser la valeur du champ TTL d'origine pour reconstruire le TTL d'origine.

3.1.5 Champs Expiration de signature et Début de signature

Les champs Expiration de signature et Début de signature spécifient une période de validité de la signature. L'enregistrement RRSIG NE DOIT PAS être utilisé pour l'authentification avant la date de début et NE DOIT PAS être utilisé pour l'authentification après la date d'expiration.

Les valeurs des champs Expiration de signature et Début de signature spécifient une date et heure sous la forme d'un nombre de 32 bits non signé de secondes écoulées depuis le 1er janvier 1970 à 00:00:00 UTC, en ignorant les secondes d'ajustement, dans l'ordre des octets du réseau. Le plus long intervalle qui peut être exprimé par ce format sans retour à zéro est approximativement de 136 ans. Un RR RRSIG peut avoir une valeur de champ Expiration qui est numériquement plus petite que la valeur du champ Début si la valeur du champ Expiration est proche du point de retour à zéro des 32 bits ou si la signature a une longue durée de vie. À cause de cela, toutes les comparaisons qui impliquent ces champs DOIVENT utiliser "l'arithmétique des numéros de série", définie dans la [RFC1982]. Comme conséquence directe, les valeurs contenues dans ces champs ne peuvent pas se référer à des dates de plus de 68 ans dans le passé ou l'avenir.

3.1.6 Champ Étiquette de clé

Le champ Étiquette de clé contient la valeur de l'étiquette de clé du RR DNSKEY qui valide cette signature, dans l'ordre des octets du réseau. L'Appendice B explique comment calculer les valeurs d'étiquette de clé.

3.1.7 Champ Nom du signataire

La valeur du champ Nom du signataire identifie le nom du propriétaire du RR DNSKEY qu'un valideur est supposé utiliser pour valider cette signature. Le champ Nom du signataire DOIT contenir le nom de la zone du RRset couvert. L'envoyeur NE DOIT PAS utiliser la compression de nom DNS sur le champ Nom du signataire lors de la transmission d'un RR RRSIG.

3.1.8 Champ Signature

Le champ Signature contient la signature cryptographique qui couvre le RDATA RRSIG (à l'exclusion du champ Signature) et le RRset spécifié par le nom du propriétaire du RRSIG, la classe RRSIG, et le champ Type couvert RRSIG. Le format de ce champ dépend de l'algorithme utilisé, et ces formats sont décrits dans des documents distincts.

3.1.8.1 Calcul de la signature

Une signature couvre le RDATA RRSIG (à l'exclusion du champ Signature) et couvre les champs RRset de données spécifiés par le nom du propriétaire du RRSIG, la classe RRSIG, et le Type couvert RRSIG. Le RRset est en forme canonique (voir la Section 6), et l'ensemble RR(1),...RR(n) est signé comme suit :

signature = sign(RRSIG_RDATA | RR(1) | RR(2)...)

où
"|" note l'enchaînement ;
RRSIG_RDATA est le format incorporé des champs RDATA de RRSIG avec le champ Nom du signataire en forme canonique et le champ Signature exclu ;
RR(i) = propriétaire | type | classe | TTL | longueur de RDATA | RDATA
"propriétaire" est le nom pleinement qualifié du propriétaire du RRset en forme canonique (pour les RR avec des noms de propriétaire qui ont des caractères génériques, l'étiquette de caractère générique est incluse dans le nom du propriétaire) ;
chaque RR DOIT avoir le même nom de propriétaire que le RR RRSIG ;
chaque RR DOIT avoir la même classe que le RR RRSIG ;

chaque RR dans le RRset DOIT avoir le type RR dont la liste figure dans le champ Type couvert du RR RRSIG ;
chaque RR dans le RRset DOIT avoir le TTL figurant dans le champ TTL d'origine du RRSIG ;
tous les noms DNS dans le champ RDATA de chaque RR DOIVENT être en forme canonique ; et
le RRset DOIT être trié en ordre canonique.

Voir aux paragraphes 6.2 et 6.3 les détails sur la forme canonique et l'ordre des RRsets.

3.2 Format de présentation de RR RRSIG

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

Le champ Type couvert est représenté comme un mnémonique de type de RR. Lorsque le mnémonique n'est pas connu, la représentation TYPE, telle que décrite dans la [RFC3597], Section 5, DOIT être utilisée.

La valeur du champ Algorithme DOIT être représentée soit comme un entier décimal non signé, soit comme un mnémonique d'algorithme, comme spécifié dans l'Appendice A.1.

La valeur du champ Étiquette DOIT être représentée comme un entier décimal non signé.

La valeur du champ TTL d'origine DOIT être représentée par un entier décimal non signé.

Les valeurs des champs Heure d'expiration et Heure de début DOIVENT être représentées soit par un entier décimal non signé indiquant les secondes depuis le 1er janvier 1970 à 00:00:00 UTC, soit sous la forme AAAAMMJJHHmmSS en UTC, où :
AAAA est l'année (0001-9999, mais voir au paragraphe 3.1.5) ;
MM est le numéro du mois (01-12) ;
JJ est le jour du mois (01-31) ;
HH est l'heure, en notation sur 24 heures (00-23) ;
mm sont les minutes (00-59) ; et
SS sont les secondes (00-59).

Noter qu'il est toujours possible de distinguer entre ces deux formats parce que le format AAAMMJJHHmmSS fera toujours exactement 14 chiffres, alors que la représentation décimale d'un entier non signé de 32 bits ne peut jamais dépasser 10 chiffres.

Le champ Étiquette de clé DOIT être représenté par un entier décimal non signé.

La valeur du champ Nom du signataire DOIT être représentée comme un nom de domaine.

Le champ Signature est représenté comme un codage en Base64 de la signature. Les espaces sont admises dans le texte en Base64. Voir au paragraphe 2.2.

3.3 Exemple de RR RRSIG

Le RR RRSIG suivant mémorise la signature pour le RRset A de host.example.com :

```
host.example.com. 86400 IN RRSIG A 5 3 86400 20030322173103 ( 20030220173103 2642
example.com.oJB1W6WNGv+ldvQ3WDG0MQkg5IEhjRip8WTrPYGv07h108dUKGMeDPKijVCHX3DDKdfb+v
6oB9wfuh3DTJXUAfI/M0zmO/zz8bW0Rznl8O3tGNazPwQKkRN20XPXV6nwwfoXmJQbsLNrLfkGJ5D6fwFm8
nN+6pBzeDQfsS3Ap3o= )
```

Les quatre premiers champs spécifient le nom du propriétaire, le TTL, la classe, et le type de RR (RRSIG). Le "A" représente le champ Type couvert. La valeur 5 identifie l'algorithme utilisé (RSA/SHA1) pour créer la signature. La valeur 3 est le nombre d'étiquettes dans le nom du propriétaire d'origine. La valeur 86400 dans le RDATA RRSIG est le TTL d'origine pour le RRset A couvert. 20030322173103 et 20030220173103 sont, respectivement, les dates d'expiration et de début. 2642 est l'étiquette de clé, et example.com. est le nom du signataire. Le texte restant est un codage en Base64 de la signature.

Noter que la combinaison du nom du propriétaire, de la classe et du type couvert du RR RRSIG indique que ce RRSIG couvre le RRset A de "host.example.com". La valeur d'étiquette de 3 indique qu'aucune expansion de caractère générique n'a été utilisée. L'algorithme, le nom du signataire, et l'étiquette de clé indiquent que cette signature peut être authentifiée en utilisant un RR DNSKEY de zone example.com dont l'algorithme est 5 et dont l'étiquette de clé est 2642.

4. Enregistrement de ressource NSEC

L'enregistrement de ressource NSEC fait la liste de deux choses distinctes : le prochain nom de propriétaire (dans l'ordre canonique de la zone) qui contient des données d'autorité ou un RRset NS de point de délégation, et l'ensemble des types de RR présents au nom de propriétaire du RR NSEC [RFC3845]. L'ensemble complet des RR NSEC dans une zone indique quels RRset d'autorité existent dans une zone et forme aussi une chaîne de noms de propriétaires d'autorité dans la zone. Ces informations sont utilisées pour fournir un déni d'existence authentifié pour les données du DNS, comme décrit dans la [RFC4035].

Comme chaque nom d'autorité dans une zone doit faire partie de la chaîne NSEC, les RR NSEC doivent être présents pour les noms qui contiennent un RR CNAME. Ceci est un changement par rapport à la spécification traditionnelle de la [RFC1034], qui déclarait que si un CNAME est présent pour un nom, il est le seul type permis à ce nom. Un RRSIG (voir la Section 3) et un NSEC DOIVENT exister pour le même nom comme le fait un enregistrement de ressource CNAME dans une zone signée.

Voir dans la [RFC4035] l'exposé de la façon dont un signataire de zone détermine précisément quels RR NSEC il doit inclure dans une zone.

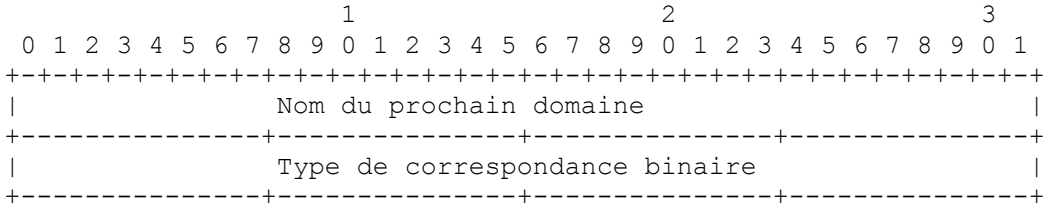
La valeur de type pour le RR NSEC est 47.

Le RR NSEC est indépendant de la classe.

Le RR NSEC DEVRAIT avoir la même valeur de TTL que le champ TTL SOA minimum. Ceci est dans l'esprit d'une mise en antémémoire négative ([RFC2308]).

4.1 Format incorporé de RDATA NSEC

Le RDATA du RR NSEC est comme indiqué ci-dessous.



4.1.1 Champ Nom du prochain domaine

Le champ Prochain domaine contient le nom du prochain propriétaire (dans l'ordre canonique de la zone) qui a des données d'autorité ou contient un RRset NS de point de délégation ; voir au paragraphe 6.1 une explication de l'ordre canonique. La valeur du champ Nom du prochain domaine dans le dernier enregistrement NSEC dans la zone est le nom du sommet de la zone (le nom de propriétaire du RR SOA de la zone). Cela indique que le nom du propriétaire du RR NSEC est le dernier nom dans l'ordre canonique de la zone.

Un envoyeur NE DOIT PAS utiliser la compression de nom du DNS sur le champ Nom du prochain domaine lors de la transmission d'un RR NSEC.

Les noms de propriétaire des RRset pour lesquels la zone en question n'est pas d'autorité (comme les enregistrements glus) NE DOIVENT PAS figurer dans la liste de nom de prochain domaine sauf si au moins un RRset d'autorité existe à ce même nom de propriétaire.

4.1.2 Champ Type de correspondance binaire

Le champ Type de correspondance binaire identifie les types de RRset qui existent au nom de propriétaire du RR NSEC.

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

Les blocs sont présents dans le RDATA RR NSEC en ordre numérique croissant.

Champ Type de correspondance binaire = (n° de bloc de fenêtre | Longueur de correspondance binaire | correspondance binaire)+

où "|" note l'enchaînement.

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

Les bits qui représentent des pseudo-types DOIVENT être mis à 0, car ils n'apparaissent pas dans les données de zone. Si on en rencontre, ils DOIVENT être ignorés à la lecture.

Les blocs où aucun type n'est présent NE DOIVENT PAS être inclus. Les octets à zéro en queue dans la correspondance binaire DOIVENT être omis. La longueur de la correspondance binaire de chaque bloc est déterminée par le code de type ayant la plus grande valeur numérique, au sein de ce bloc, parmi l'ensemble des types de RR présents dans le nom de propriétaire du RR NSEC. Les octets à zéro en queue non spécifiés DOIVENT être interprétés comme des octets à zéro.

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 les types de RR pour lesquels 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 mis à zéro.

Une zone NE DOIT PAS inclure de RR NSEC pour un nom de domaine qui ne contient que des enregistrements glus.

4.1.3 Inclusion de nom à caractère générique dans un RDATA NSEC

Si un nom de propriétaire à caractère générique apparaît dans une zone, l'étiquette caractère générique ("*") est traitée comme un symbole littéral et est traitée de la même façon que tout autre nom de propriétaire pour les besoins de la génération des RR NSEC. Les noms de propriétaire à caractère générique apparaissent dans le champ Prochain nom de domaine sans aucune expansion de caractère générique. La [RFC4035] décrit l'impact des caractères génériques sur le déni d'existence authentifié.

4.2 Format de présentation de RR NSEC

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

Le champ Prochain nom de domaine est représenté comme un nom de domaine.

Le champ Type de correspondance binaire est représenté comme une séquence de mnémoniques de type de RR. Lorsque le mnémonique n'est pas connu, la représentation TYPE décrite dans la [RFC3597], Section 5, DOIT être utilisée.

4.3 Exemple de RR NSEC

Le RR NSEC suivant identifie les RRset associés à alfa.example.com. et identifie le prochain nom d'autorité après alfa.example.com.

```
alfa.example.com. 86400 IN NSEC host.example.com. ( A MX RRSIG NSEC TYPE1234 )
```

Les quatre premiers champs de texte spécifient le nom, le TTL, la classe, et le type de RR (NSEC). L'entrée host.example.com. est le prochain nom d'autorité après alfa.example.com. en ordre canonique. Les mnémoniques A, MX, RRSIG, NSEC, et TYPE1234 indiquent qu'il y a les RRset A, MX, RRSIG, NSEC, et TYPE1234 associés au nom alfa.example.com.

La section RDATA du RR NSEC ci-dessus devrait être codée par :

```
0x04 'h'  'o'  's'  't'
0x07 'e'  'x'  'a'  'm'  'p'  'l'  'e'
0x03 'c'  'o'  'm'  0x00
0x00 0x06 0x40 0x01 0x00 0x00 0x00 0x03
```

0x04 0x1b 0x00 0x00 0x00 0x00 0x00 0x00
0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x00 0x00 0x00 0x00 0x20

En supposant que le valideur peut authentifier cet enregistrement NSEC, il pourraît être utilisé pour prouver que beta.example.com n'existe pas, ou pour prouver qu'il n'y a pas d'enregistrement AAAA associé à alfa.example.com. Le déni d'existence authentifié est exposé dans la [RFC4035].

5. Enregistrement de ressource DS

L'enregistrement de ressource DS se réfère à un RR DNSKEY et est utilisé dans le processus d'authentification de DNSKEY du DNS. Un RR DS se réfère à un RR DNSKEY en mémorisant l'étiquette de clé, le numéro d'algorithme, et un résumé du RR DNSKEY. Noter qu'alors que le résumé devrait être suffisant pour identifier la clé publique, la mémorisation de l'étiquette de clé et de l'algorithme de clé aide à rendre le processus d'identification plus efficace. En authentifiant l'enregistrement DS, un résolveur peut authentifier le RR DNSKEY sur lequel pointe l'enregistrement DS. Le processus d'authentification de clé est décrit dans la [RFC4035].

Le RR DS et son RR DNSKEY correspondant ont le même nom de propriétaire, mais ils sont mémorisés dans des localisations différentes. Le RR DS n'apparaît que sur le côté supérieur (parental) d'une délégation, et ses données d'autorité dans la zone parente. Par exemple, le RR DS pour "example.com" est mémorisé dans la zone "com" (la zone parente) plutôt que dans la zone "example.com" (la zone fille). Le RR DNSKEY correspondant est mémorisé dans la zone "example.com" (la zone fille). Cela simplifie la gestion de zone du DNS et la signature de zone mais introduit des exigences particulières de traitement des réponses pour le RR DS ; celles-ci sont décrites dans la [RFC4035].

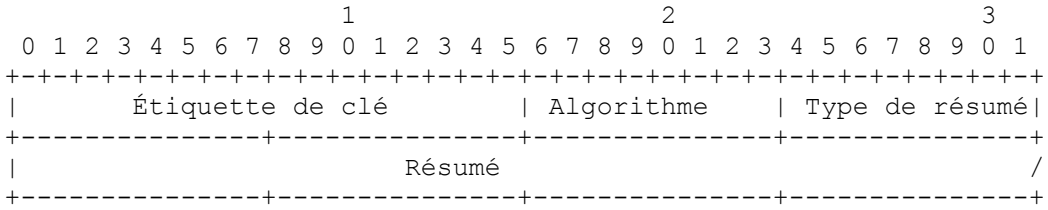
Le numéro de type pour l'enregistrement DS est 43.

L'enregistrement de ressource DS est indépendant de la classe.

Le RR DS n'a pas d'exigence particulière de TTL.

5.1 Format incorporé de RDATA DS

Le RDATA pour un RR DS consiste en un champ Étiquette de clé de 2 octets, un champ Algorithme de 1 octet, un champ Type de résumé de 1 octet, et un champ Résumé.



5.1.1 Champ Étiquette de clé

Le champ Étiquette de clé fait la liste des étiquettes de clés du RR DNSKEY visé par l'enregistrement DS, dans l'ordre des octets du réseau.

L'étiquette de clé utilisée par le RR DS est identique à l'étiquette de clé utilisée par les RR RRSIG. L'Appendice B décrit comment calculer une étiquette de clé.

5.1.2 Champ Algorithme

Le champ Algorithme fait la liste des numéros d'algorithme du RR DNSKEY visé par l'enregistrement DS.

Le numéro d'algorithme utilisé par le RR DS est identique au numéro d'algorithme utilisé par les RR RRSIG et DNSKEY. L'Appendice A.1 fait la liste des types de numéro d'algorithme.

5.1.3 Champ Type de résumé

Le RR DS se réfère à un RR DNSKEY en incluant un résumé de ce RR DNSKEY. Le champ Type de résumé identifie l'algorithme utilisé pour construire le résumé. L'Appendice A.2 fait la liste des types d'algorithme de résumé possibles.

5.1.4 Champ Résumé

L'enregistrement DS se réfère à un RR DNSKEY en incluant un résumé de ce RR DNSKEY.

Le résumé est calculé en enchaînant la forme canonique du nom de propriétaire pleinement qualifié du RR DNSKEY avec le RDATA DNSKEY, et en appliquant ensuite l'algorithme de résumé.

résumé = algorithme_de_résumé(nom de propriétaire DNSKEY | RDATA DNSKEY);

"|" note l'enchaînement

RDATA DNSKEY = Fanions | Protocole | Algorithme | Clé publique.

La taille du résumé peut varier selon l'algorithme de résumé et la taille du RR DNSKEY. Au moment de la rédaction du présent document, le seul algorithme de résumé défini est SHA-1, qui produit un résumé de 20 octets.

5.2 Traitement des RR DS lors de la validation des réponses

Le RR DS relie la chaîne d'authentification à travers les frontières de zone, de sorte que le RR DS exige des soins particuliers lors de son traitement. Le RR DNSKEY visé dans le RR DS DOIT être une clé de zone DNSSEC. Les fanions de RR DNSKEY DOIVENT avoir le bit 7 des fanions établi. Si les fanions DNSKEY n'indiquent pas une clé de zone DNSSEC, le RR DS (et le RR DNSKEY auquel il fait référence) NE DOIT PAS être utilisé dans le processus de validation.

5.3 Format de présentation du RR DS

Le format de présentation de la portion RDATA est le suivant :
Le champ Étiquette de clé DOIT être représenté par un entier décimal non signé.
Le champ Algorithme DOIT être représenté soit par un entier décimal non signé, soit par un mnémonique d'algorithme spécifié à l'Appendice A.1.
Le champ Type de résumé DOIT être représenté par un entier décimal non signé.
Le résumé DOIT être représenté comme une séquence de chiffres hexadécimaux insensibles à la casse. Les espaces sont permises dans le texte hexadécimal.

5.4 Exemple de RR DS

L'exemple suivant montre un RR DNSKEY et son RR DS correspondant.

```
dskey.example.com. 86400 IN DNSKEY 256 3 5
( AQOeiiR0GOMYkDshWoSKz9XzfwJr1AYtsmx3TGkJaNXVbfi/2pHm822aJ5iI9BMzNXxeYCmZDRD99WYwYqUSdj
MmmAphXdvxegXd/M5+X7OrzKBaMbCVdFLUUh6DhweJBjEVv5f2wwjM9XzcnOf+EPbtG9DMBmADjFDc2w/rljwv
Fw== ) ;  key id = 60485

dskey.example.com. 86400 IN DS 60485 5 1 ( 2BB183AF5F22588179A53B0A 98631FAD1A292118 )
```

Les quatre premiers champs de texte spécifient le nom, le TTL, la classe, et le type de RR (DS). La valeur 60485 est l'étiquette de clé pour le RR DNSKEY correspondant "dskey.example.com.", et la valeur 5 note l'algorithme utilisé par ce RR DNSKEY "dskey.example.com.". La valeur 1 est l'algorithme utilisé pour construire le résumé, et le reste du texte de RDATA est le résumé en hexadécimal.

6. Formes canoniques et ordre des enregistrements de ressource

Cette section définit une forme canonique pour les enregistrements de ressource, un ordre canonique des noms du DNS, et un ordre canonique des enregistrements de ressource au sein d'un RRset. Un ordre de nom canonique est exigé pour construire la

chaîne des noms NSEC. Une forme et un ordre canonique des RR au sein d'un RRset sont exigés afin de construire et vérifier les RR RRSIG.

6.1 Ordre canonique de nom du DNS

Pour les besoins de la sécurité du DNS, les noms de propriétaires sont ordonnés en traitant les étiquettes individuelles comme des chaînes d'octets non signés justifiés à gauche. L'absence d'un octet sort du tri avant un octet de valeur zéro, et les lettres majuscules US-ASCII sont traitées comme si elles étaient des lettres US-ASCII minuscules.

Pour calculer l'ordre canonique d'un ensemble de noms DNS, commencer par trier les noms selon les étiquettes de plus fort poids (les plus à droite). Pour les noms dans lesquels l'étiquette de plus fort poids est identique, continuer le tri selon l'étiquette de plus fort poids suivante, et ainsi de suite.

Par exemple, les noms suivants sont triés dans l'ordre canonique de nom DNS. L'étiquette de plus fort poids est "example". À ce niveau, "example" sort du tri en premier, suivi par les noms qui se terminent par "a.example", puis par les noms qui se terminent par "z.example". Les noms au sein de chaque niveau sont triés de la même façon.

example
a.example
yljkjljk.a.example
Z.a.example
zABC.a.EXAMPLE
z.example
\001.z.example
*.z.example
\200.z.example

6.2 Forme canonique de RR

Pour les besoins de la sécurité du DNS, la forme canonique d'un RR est le format incorporé du RR où :

1. chaque nom de domaine dans le RR est pleinement développé (pas de compression du nom DNS) et pleinement qualifié ;
2. toutes les lettres majuscules US-ASCII dans le nom de propriétaire du RR sont remplacées par les lettres US-ASCII minuscules correspondantes ;
3. si le type du RR est NS, MD, MF, CNAME, SOA, MB, MG, MR, PTR, HINFO, MINFO, MX, HINFO, RP, AFSDB, RT, SIG, PX, NXT, NAPTR, KX, SRV, DNAME, A6, RRSIG, ou NSEC, toutes les lettres majuscules US-ASCII dans les noms DNS contenus au sein du RDATA sont remplacées par les lettres US-ASCII minuscules correspondantes ;
4. si le nom de propriétaire du RR est un nom générique, le nom de propriétaire est dans sa forme originale non expansée, y compris l'étiquette "*" (pas de substitution de caractère générique) ; et
5. le TTL du RR est réglé à sa valeur d'origine telle qu'elle apparaît dans la zone d'autorité d'origine ou dans le champ TTL d'origine du RR RRSIG qui le couvre.

6.3 Ordre canonique des RR au sein d'un RRset

Pour les besoins de la sécurité du DNS, les RR avec le même nom de propriétaire, la même classe, et le même type sont triés en traitant la portion RDATA de la forme canonique de chaque RR comme une séquence d'octets non signés justifiés à gauche dans laquelle l'absence d'un octet sort du tri avant un octet à zéro.

La [RFC2181] spécifie qu'un RRset n'a pas le droit de contenir des enregistrements dupliqués (plusieurs RR avec le même nom de propriétaire, même classe, même type, et même RDATA). Donc, si une mise en œuvre détecte des RR dupliqués lorsqu'elle met le RRset en forme canonique, elle DOIT traiter cela comme une erreur de protocole. Si la mise en œuvre choisit de traiter cette erreur de protocole dans l'esprit du principe de robustesse (être libérale dans ce qu'elle accepte) elle DOIT retirer tous les RR dupliqués sauf un pour les besoins du calcul de la forme canonique du RRset.

7. Considérations relatives à l'IANA

Le présent document n'introduit pas de nouvelles considérations pour l'IANA, car tous les paramètres de protocole utilisés dans le présent document ont déjà été alloués par des spécifications antérieures. Cependant, comme l'évolution de DNSSEC a été longue et quelque peu tourmentée, la présente section s'efforce de décrire l'état actuel des registres de l'IANA et les autres paramètres de protocole qui se rapportent (ou se sont rapportés) au DNSSEC.

Prière de se reporter à la [RFC4035] pour des considérations relatives à l'IANA supplémentaires.

Types d'enregistrement de ressource du DNS :
La [RFC2535] a alloué les types 24, 25 et 30 respectivement aux RR SIG, KEY et NXT.
La [RFC3658] a alloué le type d'enregistrement de ressource DNS 43 à DS.
La [RFC3755] a alloué les types 46, 47 et 48 respectivement aux RR RRSIG, NSEC et DNSKEY.
La [RFC3755] a aussi marqué le type 30 (NXT) comme obsolète et restreint l'utilisation des types 24 (SIG) et 25 (KEY) au protocole de sécurité de transaction "SIG(0)" décrit dans la [RFC2931] et aux transactions d'enregistrement de ressource KEY décrites dans la [RFC2930].

Numéros d'algorithme de sécurité du DNS :
La [RFC2535] a créé un registre IANA pour les numéros de champ Algorithme d'enregistrement de ressource DNSSEC et alloué les valeurs 1 à 4 et 252 à 255.
La [RFC3110] a alloué la valeur 5.
La [RFC3755] a modifié ce registre pour y inclure des fanions pour chaque entrée concernant son utilisation avec les extensions de sécurité du DNS. Chaque entrée d'algorithme peut se référer à un algorithme qui peut être utilisé pour la signature de zone, la sécurité de la transaction (voir la [RFC2931]) ou les deux. Les valeurs 6 à 251 sont disponibles pour être allouées par action de normalisation de l'IETF ([RFC3755]). Voir à l'Appendice A une liste complète des entrées de numéros d'algorithme de sécurité du DNS au moment de la rédaction du présent mémoire, et leur statut pour l'utilisation dans le DNSSEC.

La [RFC3658] a créé un registre IANA pour les types de résumé DS de DNSSEC et mis en réserve la valeur 0 et alloué la valeur 1 à SHA-1.

Valeurs de protocole KEY :
La [RFC2535] a créé un registre IANA pour les valeurs de protocole KEY, mais la [RFC3445] a réalloué toutes les valeurs autres que 3 en réserve et fermé ce registre IANA. Le registre reste clos, et tous les enregistrements KEY et DNSKEY sont obligés d'avoir une valeur d'octet de protocole de 3.

Bits fanions dans les RR KEY et DNSKEY :
La [RFC3755] a créé un registre IANA pour les bits fanion de KEY DNSSEC et RR DNSKEY. Au départ, ce registre ne contenait d'allocation que pour les bit 7 (le bit ZONE) et 15 (le bit fanion de point d'entrée sécurisée (SEP, *Secure Entry Point*) ; voir la [RFC3757]). Comme mentionné dans la [RFC3755], les bits 0 à 6 et 8 à 14 sont disponibles pour être alloués par action de normalisation de l'IETF.

8. Considérations pour la sécurité

Le présent document décrit le format de quatre enregistrements de ressource du DNS utilisés par les extensions de sécurité du DNS et présente un algorithme pour calculer une étiquette de clé pour une clé publique. À part les éléments décrits ci-dessous, les enregistrements de ressource eux-mêmes n'introduisent aucun problème de sécurité à considérer. Prière de se reporter à la [RFC4033] et à la [RFC4035] pour des considérations relatives à la sécurité supplémentaires se rapportant à l'utilisation de ces enregistrements.

L'enregistrement DS pointe sur un RR DNSKEY en utilisant un résumé cryptographique, le type d'algorithme de clé, et une étiquette de clé. L'enregistrement DS est destiné à identifier un RR DNSKEY existant, mais il est théoriquement possible à un attaquant de générer une DNSKEY qui satisfasse tous les champs DS. La probabilité de construire une DNSKEY qui corresponde dépend du type d'algorithme de résumé utilisé. Le seul actuellement défini est SHA-1, et le groupe de travail estime que la construction d'une clé publique qui correspondrait à l'algorithme, à l'étiquette de clé, et au résumé SHA-1 d'un enregistrement DS donné serait un problème suffisamment difficile pour qu'une telle attaque ne soit pas une menace sérieuse pour le moment.

L'étiquette de clé est utilisée pour aider à choisir efficacement les enregistrements de ressource DNSKEY, mais elle n'identifie pas de façon univoque un seul enregistrement de ressource DNSKEY. Il est possible que deux RR DNSKEY distincts aient le même nom de propriétaire, le même type d'algorithme, et la même étiquette de clé. Une mise en œuvre qui n'utilise que l'étiquette de clé pour choisir un RR DNSKEY pourrait dans certaines circonstances choisir la mauvaise clé publique. Prière de se reporter à l'Appendice B pour des détails complémentaires

Le tableau des algorithmes de l'Appendice A et les algorithmes de calcul des étiquettes de clé de l'Appendice B incluent l'algorithme RSA/MD5 par souci d'exhaustivité, mais l'algorithme RSA/MD5 N'EST PAS RECOMMANDÉ, comme expliqué dans la [RFC3110].

9. Remerciements

Le présent document a été créé à partir des apports et des idées des membres du groupe de travail Extensions du DNS et de la liste de diffusion du groupe de travail. Les éditeurs tiennent à exprimer leurs remerciements pour les commentaires et suggestions reçus durant la révision de ces spécifications d'extensions de sécurité. Bien qu'il soit impossible de faire une liste exhaustive de tous ceux qui ont contribué à ces travaux pendant les dix années durant lesquelles a été développé DNSSEC, la [RFC4033] comporte une liste de quelques uns des participants qui ont eu la gentillesse de faire des commentaires sur ces documents.

10. Références

10.1 Références normatives

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

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

[RFC1982] R. Elz, R. Bush, "Arithmétique des numéros de série", août 1996. (*MàJ* RFC1034, RFC1035) *(P.S.)*

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

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

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

[RFC2536] D. Eastlake 3rd , "Clés DSA et SIG dans le système des noms de domaines (DNS)", mars 1999. *(P.S.)*

[RFC2931] D. Eastlake 3rd, "Signatures de demandes et de transactions du DNS (SIG(0))", septembre 2000. *(P.S.)*

[RFC3110] D. Eastlake 3rd, "SIG RSA/SHA-1 et clés RSA dans le système des noms de domaine (DNS)", mai 2001. *(MàJ par* RFC6944) *(PS)*

[RFC3445] D. Massey, S. Rose, "Limitation de la portée de l'enregistrement de ressource (RR) KEY", décembre 2002. (*Obsolète, voir* RFC4033, RFC4034, RFC4035) (MàJ RFC2535) *(P.S.)*

[RFC3548] S. Josefsson, "Codages de données Base16, Base32, et Base64", juillet 2003. *(Obsolète, voir RFC 4648) (Info)*

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

[RFC3658] O. Gudmundsson, "Enregistrement de ressource (RR) signataire par délégation (DS)", décembre 2003. (*Obsolète, voir* RFC4033, RFC4034, RFC4035) *(P.S.)*

[RFC3755] S. Weiler, "Compatibilité de résolveur traditionnel pour la délégation de signature", mai 2004. (*Obsolète, voir* RFC4033, RFC4034, RFC4035) *(P.S.)*

[RFC3757] O. Kolkman, J. Schlyter, E. Lewis, "Fanion de pont d'entrée sécurisée (SED) d'enregistrement de ressource (RR) KEY du système de noms de domaines (DNSKEY)", avril 2004. (*Obsolète, voir* RFC4033, RFC4034, RFC4035)

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

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

10.2 Références pour information

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

[RFC2537] D. Eastlake 3rd, "Clés RSA/MD5 et SIG dans le système des noms de domaines (DNS)", mars 1999. (*Obsolète, voir* RFC3110) *(P.S.)*

[RFC2539] D. Eastlake 3rd, "Mémorisation des clés Diffie-Hellman dans le système des noms de domaines (DNS)", mars 1999. *(P.S.)*

[RFC2930] D. Eastlake 3rd, "Établissement de clés secrètes pour le DNS (TKEY RR)", septembre 2000. *(P.S.)*

[RFC3845] J. Schlyter, éd., "Format RDATA NextSECure (NSEC) pour la sécurité du DNS (DNSSEC)", août 2004. (*Obsolète, voir* RFC4033, RFC4034, RFC4035) (MàJ RFC3755, RFC2535) *(P.S.)*

Appendice A. Types d'algorithme et de résumé DNSSEC

Les extensions de sécurité du DNS sont conçues pour être indépendantes des algorithmes cryptographiques sous-jacents. Les enregistrements de ressource DNSKEY, RRSIG et DS utilisent tous un numéro d'algorithme DNSSEC pour identifier l'algorithme cryptographique utilisé par l'enregistrement de ressource. L'enregistrement de ressource DS spécifie aussi un numéro d'algorithme de résumé pour identifier l'algorithme de résumé utilisé pour construire l'enregistrement DS. L'algorithme et les types de résumé actuellement définis sont énumérés ci-dessous. Des algorithmes ou types de résumé pourraient être ajoutés lorsque les progrès de la cryptographie pourront les garantir.

Un résolveur ou serveur de nom à capacité DNSSEC DOIT mettre en œuvre tous les algorithmes OBLIGATOIRES.

A.1 Types d'algorithme DNSSEC

Les RR DNSKEY, RRSIG et DS utilisent un numéro à 8 bits pour identifier l'algorithme de sécurité utilisé. Ces valeurs sont mémorisées dans le champ "Numéro d'algorithme" dans le RDATA de l'enregistrement de ressource.

Certains algorithmes ne sont utilisables que pour la signature de zone (DNSSEC), certains seulement pour des mécanismes de transaction de sécurité (SIG(0) et TSIG), et certains pour les deux. Ceux qui sont utilisables pour la signature de zone peuvent apparaître dans les RR DNSKEY, RRSIG et DS. Ceux qui sont utilisables pour la sécurité des transactions seront présents dans les RR SIG(0) et KEY, comme décrit dans la [RFC2931].

Valeur	Algorithme [Mnémonique]	Signature de zone	Références	Statut
0	réservé			
1	RSA/MD5 [RSAMD5]	non	[RFC2537]	NON RECOMMANDÉ
2	Diffie-Hellman [DH]	non	[RFC2539]	-
3	DSA/SHA-1 [DSA]	oui	[RFC2536]	FACULTATIF
4	Courbe elliptique [ECC]		TBA	-
5	RSA/SHA-1 [RSASHA1]	oui	[RFC3110]	OBLIGATOIRE
252	Indirect [INDIRECT]	non	-	
253	Privé [PRIVATEDNS]	oui	voir ci-dessous	FACULTATIF
254	Privé [PRIVATEOID]	oui	voir ci-dessous	FACULTATIF
255	réservé			
6 – 251	Disponible pour allocation par action de normalisation de l'IETF.			

A.1.1 Types d'algorithme privés

Le numéro d'algorithme 253 est réservé pour utilisation privée et ne sera jamais alloué à un algorithme spécifique. Le domaine des clés publiques dans le RR DNSKEY et le domaine de signature dans le RR RRSIG commencent par un nom de domaine à

codage incorporé, qui NE DOIT PAS être compressé. Le nom de domaine indique l'algorithme privé à utiliser, et le reste du domaine de la clé publique est déterminé par cet algorithme. Les entités devraient n'utiliser que les noms de domaine qu'elles contrôlent pour désigner leurs algorithmes privés.

Le numéro d'algorithme 254 est réservé pour utilisation privée et ne sera jamais alloué à un algorithme spécifique. Le domaine de clé publique dans le RR DNSKEY et le domaine de signature dans le RR RRSIG commencent par un octet de longueur non signé suivi par un identifiant d'objet codé en BER (ISO OID) de cette longueur. L'OID indique l'algorithme privé utilisé, et le reste de la zone est ce qui est demandé par cet algorithme. Les entités devraient n'utiliser que les OID qu'elles contrôlent pour désigner leurs algorithmes privés.

A.2 Types de résumé DNSSEC

Un champ "Type de résumé" dans le type d'enregistrement de ressource DS identifie l'algorithme cryptographique de résumé utilisé par l'enregistrement de ressource. Le tableau suivant fait la liste des types d'algorithme de résumé actuellement définis.

Valeur	Algorithme	STATUT
0	Réservé	-
1	SHA-1	OBLIGATOIRE
2-255	Non alloués	-

Appendice B. Calcul d'étiquette de clé

Le champ Étiquette de clé dans les types d'enregistrement de ressource RRSIG et DS fournit un mécanisme pour choisir efficacement une clé publique. Dans la plupart des cas, une combinaison du nom du propriétaire, de l'algorithme et de l'étiquette de clé peut identifier efficacement un enregistrement DNSKEY. Les enregistrements de ressource RRSIG et DS ont tous deux leurs enregistrements DNSKEY correspondants. Le champ Étiquette de clé dans les enregistrements RRSIG et DS peut être utilisé pour aider à choisir efficacement le RR DNSKEY correspondant lorsque plus d'un candidat RR DNSKEY est disponible.

Cependant, il est essentiel de noter que l'étiquette de clé n'est pas un identifiant univoque. Il est théoriquement possible que deux RR DNSKEY distincts aient le même nom de propriétaire, le même algorithme et la même étiquette de clé. L'étiquette de clé est utilisée pour limiter les clés candidates possibles, mais elle n'identifie pas de façon univoque un enregistrement DNSKEY. Les mises en œuvre NE DOIVENT PAS supposer que l'étiquette de clé identifie de façon univoque un RR DNSKEY.

L'étiquette de clé est la même pour tous les types d'algorithme DNSKEY excepté l'algorithme 1 (prière de se reporter à l'Appendice B.1 pour la définition de l'étiquette de clé pour l'algorithme 1). L'algorithme d'étiquette de clé est la somme du format incorporé du RDATA DNSKEY coupé en groupes de deux octets. D'abord, le RDATA (en format incorporé) est traité comme une série de groupes de 2 octets. Ces groupes sont ensuite ajoutés les uns aux autres, en ignorant tout bit de report.

Une mise en œuvre de référence de l'algorithme d'étiquette de clé comme fonction C ANSI est donnée ci-dessous, avec la portion RDATA du RR DNSKEY utilisée en entrée. Il n'est pas nécessaire d'utiliser mot à mot le code de référence suivant, mais la valeur numérique de l'Étiquette de clé DOIT être identique à ce que la mise en œuvre de référence génèrerait pour la même entrée.

Prière de noter que l'algorithme pour le calcul de l'étiquette de clé est presque, mais pas tout à fait, identique à la somme de contrôle familière de complément à un utilisée dans de nombreux autres protocoles Internet. Les étiquettes de clé DOIVENT être calculées en utilisant l'algorithme décrit ici plutôt que celui de la somme de contrôle de complément à un.

La mise en œuvre de référence ANSI C suivante calcule la valeur d'une étiquette de clé. Cette mise en œuvre de référence s'applique à tous les types d'algorithme excepté l'algorithme 1 (voir l'Appendice B.1). L'entrée est le format incorporé de la portion RDATA du RR DNSKEY. Le code est écrit pour être clair, pas pour l'efficacité.

```
/*
 * On suppose que int fait au moins 16 bits.
 * Le premier octet de l'étiquette de clé sont les 8 bits de plus fort poids de la valeur retournée ;
 * Le second octet de l'étiquette de clé sont les 8 bits de moindre poids de la valeur retournée.
 */
```

```
unsigned int
keytag (
        unsigned char key[],            /* la partie RDATA du RR DNSKEY */
        unsigned int keysize            /* le RDLENGTH */
       )
{
        unsigned long ac;               /* supposé faire 32 bits ou plus */
        int i;                          /* indice de boucle */

        for ( ac = 0, i = 0; i < keysize; ++i )
                ac += (i & 1) ? key[i] : key[i] << 8;
        ac += (ac >> 16) & 0xFFFF;
        return ac & 0xFFFF;
}
```

B.1 Étiquette de clé pour l'algorithme 1 (RSA/MD5)

L'étiquette de clé pour l'algorithme 1 (RSA/MD5) est définie différemment de l'étiquette de clé pour tous les autres algorithmes, pour des raisons historiques. Pour un RR DNSKEY avec l'algorithme 1, l'étiquette de clé est définie comme étant les 16 bits de plus fort poids des 24 bits de plus fort poids du module de clé publique (en d'autres termes, du 4ème au dernier et du 3ème au dernier octet du module de clé publique).

Prière de noter que l'algorithme 1 est NON RECOMMANDÉ.

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 and Technology
100 Bureau Drive
Gaithersburg, MD 20899-8920
USA
mél : scott.rose@nist.gov

Déclaration complète de droits de reproduction

accompli aucun effort pour identifier de tels droits. Les informations sur les procédures de l'ISOC au sujet des droits dans les documents de l'ISOC figurent dans les BCP 78 et BCP 79.

Des copies des dépôts d'IPR faites au secrétariat de l'IETF et toutes assurances de disponibilité de licences, ou le résultat de tentatives faites pour obtenir une licence ou permission générale d'utilisation de tels droits de propriété par ceux qui mettent en œuvre ou utilisent la présente spécification peuvent être obtenues sur le répertoire en ligne des IPR de l'IETF à http://www.ietf.org/ipr.

L'IETF invite toute partie intéressée à porter son attention sur tous copyrights, licences ou applications de licence, ou autres droits de propriété qui pourraient couvrir les technologies qui peuvent être nécessaires pour mettre en œuvre la présente norme. Prière d'adresser les informations à l'IETF à ietf- ipr@ietf.org.

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