Groupe de travail Réseau
Request for Comments : 4509
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

W. Hardaker, Sparta

mai 2006

Utilisation de SHA-256 dans les enregistrements de ressource de signataire de délégation (DS) DNSSEC

Statut du présent mémoire
Le présent document spécifie un protocole de l'Internet en cours de normalisation pour la communauté de l'Internet, et appelle à des discussions et suggestions pour son amélioration. Prière de se référer à l'édition en cours des "Protocoles officiels de l'Internet" (STD 1) pour voir 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 spécifie comment utiliser le type de résumé SHA-256 dans les enregistrements de ressources (RR, *Resource Record*) de signataire de délégation (DS, *Delegation Signer*) du DNS. Les enregistrements DS, lorsque ils sont mémorisés dans une zone parente, pointent sur les DNSKEY dans une zone fille.

Table des matières

1. Introduction

L'enregistrement de ressource DS du DNSSEC [RFC4033], [RFC4034], [RFC4035] est publié dans les zones parentes pour distribuer un résumé chiffré d'une clé dans un ensemble d'enregistrements de ressources *(RRset)* DNSKEY fils. Le RRset DS est signé par au moins une des clés de signature de données de zone privée de la zone parente pour chaque algorithme utilisé par le parent. Chaque signature est publiée dans un enregistrement de ressource RRSIG, possédé par le même domaine que le RRset DS, avec un type couvert du DS.

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119].

2. Mise en œuvre de l'algorithme SHA-256 pour la prise en charge d'enregistrement DS

Le présent document spécifie que le code 2 de type de résumé a été alloué à SHA-256 [SHA256] [RFC4634] pour être utilisé dans les enregistrements DS. Le résultat de l'algorithme de résumé NE DOIT PAS être tronqué, et le résultat entier de 32 octets du résumé est à publier dans l'enregistrement DS.

2.1 Valeurs du champ d'enregistrement DS

L'utilisation de l'algorithme de résumé SHA-256 dans un enregistrement DS va utiliser les champs d'enregistrement DS suivants :

Type de résumé : 2

Résumé : valeur de résumé SHA de 256 bits calculée en utilisant la formule suivante ("|" note l'enchaînement). La valeur résultante n'est pas tronquée, le résultat entier de 32 octets est utilisé dans l'enregistrement DS résultant et les calculs en rapport.

digest = SHA_256(nom du possesseur de DNSKEY | DNSKEY RDATA)

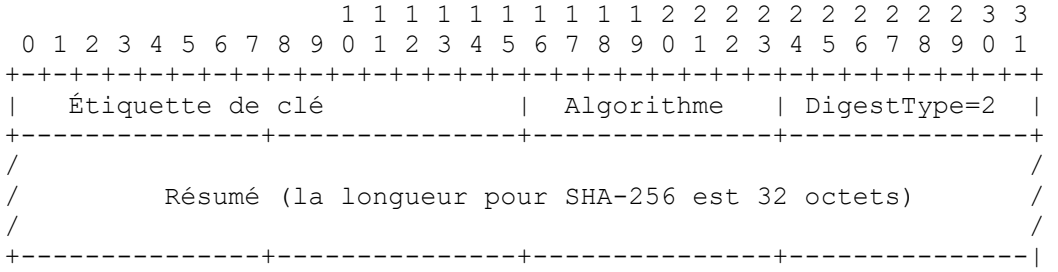
où DNSKEY RDATA est défini dans la [RFC4034] comme :

DNSKEY RDATA = Fanions | Protocole | Algorithme | Clé publique

Les champs "Étiquette de clé" et "Algorithme" restent inchangés par le présent document et sont spécifiés dans la [RFC4034].

2.2 Enregistrement DS avec le format SHA-256 de réseau

Le format du réseau pour l'enregistrement DS résultant sera comme suit :



2.3 Exemple d'enregistrement DS avec SHA-256

Voici un exemple de DNSKEY et de l'enregistrement DS correspondant. Cet enregistrement DNSKEY vient de l'exemple d'enregistrements DNSKEY/DS du paragraphe 5.4 de la [RFC4034].

Enregistrement DNSKEY :

```
dskey.exemple.com. 86400 IN DNSKEY 256 3 5 ( AQOeiiR0GOMYkDshWoSKz9XzfwJr1AYtsmx3TGkJaNXVbfi/
                                2pHm822aJ5iI9BMzNXxeYCmZDRD99WYwYqUSdjMmmAphXdvx
                                egXd/M5+X7OrzKBaMbCVdFLUUh6DhweJBjEVv5f2wwjM9Xzc
                                nOf+EPbtG9DMBmADjFDc2w/rljwvFw==
                                ) ;  key id = 60485
```

Enregistrement DS résultant qui couvre l'enregistrement DNSKEY ci-dessus avec un résumé SHA-256 :

```
dskey.exemple.com. 86400 IN DS 60485 5 2
( D4B7D520E7BB5F0F67674A0CCEB1E3E0614B93C4F9E99B8383F6A1E4469DA50A )
```

3. Exigences de mise en œuvre

Les mises en œuvre DOIVENT prendre en charge l'utilisation de l'algorithme SHA-256 dans les RR DS. Les mises en œuvre de valideurs DEVRAIENT ignorer les RR DS contenant des résumés SHA-1 si les RR DS avec des résumés SHA-256 sont présents dans le RRset DS.

4. Considérations de déploiements

Si un valideur ne prend pas en charge le type de résumé SHA-256 et si aucun autre RR DS n'existe dans le RRset DS d'une zone avec un type de résumé accepté, le valideur n'a alors pas de chemin d'authentification pris en charge conduisant du parent à l'enfant. Le résolveur devrait traiter ce cas comme celui d'un RRset NSEC authentifié prouvant qu'il n'existe aucun RRset DS, comme décrit au paragraphe 5.2 de la [RFC4035].

Parce que les administrateurs de zone ne peuvent pas contrôler la vitesse de déploiement de la prise en charge de SHA-256 dans les valideurs qui pourraient référencer une de leurs zones, les opérateurs de zone devraient considérer de déployer des enregistrements DS fondés sur SHA-1 et sur SHA-256. Ceci devrait être fait pour chaque DNSKEY pour lequel des enregistrements DS sont générés. La durée pendant laquelle utiliser les deux types de résumé et si on doit le faire est une décision de politique qui sort du domaine d'application du présent document.

5. Considérations relatives à l'IANA

Une seule action de l'IANA est requise par le présent document :

Le type de résumé à utiliser pour la prise en charge de SHA-256 au sein des enregistrements DS a été alloué par l'IANA.

Au moment de cette rédaction, les types de résumés actuels alloués pour l'usage des enregistrements DS sont les suivants :

Valeur	Type de résumé	Statut
0	Réservé	-
1	SHA-1	Obligatoire
2	SHA-256	Obligatoire
3-255	non alloué	-

6. Considérations sur la sécurité

6.1 Potentielles attaques en dégradation du type de résumé

Une attaque en dégradation d'un type de résumé plus fort à un plus faible est possible si tout ce qui suit est vrai :
- o une zone inclut plusieurs enregistrements DS pour une certaine DNSKEY de fils, dont chacun utilise un type de résumé différent ;
- o un valideur accepte un résumé plus faible même si un plus fort est présent mais invalide.

Par exemple, si les conditions suivantes sont toutes vraies :
- o les résumés fondés sur SHA-1 et SHA-256 sont tous deux publiés dans des enregistrements DS au sein d'une zone parente pour la DNSKEY d'une zone fille donnée ;
- o l'enregistrement DS avec le résumé SHA-1 correspond au résumé calculé en utilisant la DNSKEY de la zone fille ;
- o l'enregistrement DS avec le résumé SHA-256 échoue à correspondre au résumé calculé en utilisant la DNSKEY de la zone fille.

Alors, si le valideur accepte la situation ci-dessus comme sûre, cela peut être utilisé pour une attaque en dégradation car le plus fort résumé SHA-256 est ignoré.

6.2 SHA-1 ou SHA-256 pour les enregistrements DS

Les utilisateurs de DNSSEC sont encouragés à déployer SHA-256 aussitôt que les mises en œuvre de logiciel le permettent. SHA-256 est largement estimé être plus résilient à l'attaque que SHA-1, et la confiance en la force de SHA-1 est atteinte par les attaques récemment annoncées. Sans considérer si les attaques sur SHA-1 affecteront DNSSEC, il est estimé (au moment de la rédaction du présent document) que SHA-256 est le meilleur choix pour l'utilisation des enregistrements DS.

Au moment de cette publication, l'algorithme de résumé SHA-256 est considéré comme suffisamment fort pour le futur immédiat. Il est aussi considéré comme suffisant pour l'usage des RR DS DNSSEC pour le futur immédiat. Cependant, de futures attaques publiées peuvent affaiblir l'utilisabilité de cet algorithme au sein des RR DS. Il sort du domaine d'application de ce document de spéculer extensivement sur la force cryptographique de l'algorithme de résumé SHA-256.

De même, il sort du domaine d'application de ce document de spécifier si et pour combien de temps les enregistrement DS fondés sur SHA-1 devraient être simultanément publiés à côté des enregistrements DS fondés sur SHA-256.

7. Remerciements

Le présent document est une extension mineure aux documents DNSSEC existants et dont les auteurs sont chaleureusement remerciés pour le travail apprécié qu'ils ont accompli pour des documents de base.

Les personnes suivantes ont contribué à des portions de ce document d'une façon ou d'une autre : Mark Andrews, Roy Arends, Olafur Gudmundsson, Paul Hoffman, Olaf M. Kolkman, Edward Lewis, Scott Rose, Stuart E. Schechter, Sam Weiler.

8. Références

8.1 Références normatives

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

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

[RFC4034] R. Arends et autres, "Enregistrements de ressources pour les extensions de sécurité au DNS", mars 2005.

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

[SHA256] National Institute of Standards and Technology, "Secure Hash Algorithm. NIST FIPS 180-2", août 2002.

8.2 Références pour information

[RFC4634] D. Eastlake 3rd, T. Hansen, "Algorithmes de hachage sécurisé aux USA (SHA et HMAC-SHA)", juillet 2006. *(Info.)*

Adresse de l'auteur

Wes Hardaker
Sparta
P.O. Box 382
Davis, CA 95617
USA

mél : hardaker@tislabs.com

Déclaration complète de droits de reproduction

Remerciement
Le financement de la fonction d'édition des RFC est fourni par l'activité de soutien administatif (IASA) de l'IETF.