Groupe de travail Réseau
Request for Comments : 5011
Catégorie : En cours de normalisation

M. StJohns,
septembre 2007
Traduction Claude Brière de L'Isle

Mise à jour automatisée des ancres de confiance de la sécurité du DNS (DNSSEC)

Statut du présent mémoire

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

Résumé

Le présent document décrit un moyen de mise à jour automatisée, authentifiée, et autorisée des "ancres de confiance" DNSSEC. La méthode fournit la protection contre la compromission de N-1 clés parmi N clés dans l'ensemble des clés de point de confiance. Sur la base de la confiance établie par la présence d'une ancre actuelle, d'autres ancres peuvent être ajoutées au même endroit dans la hiérarchie, et finalement, supplanter la ou les ancres existantes.

Ce mécanisme exigera des changements du comportement de gestion des résolveurs (mais pas du comportement de résolution des résolveurs) et l'ajout d'un seul bit de fanion à l'enregistrement DNSKEY.

Table des Matières

1. Introduction

Au titre de la réalité des champs de DNSSEC (Extensions de sécurité du système des noms de domaine) [RFC4033] [RFC4034] [RFC4035], la communauté de l'Internet en est venue à réaliser qu'il n'y aura pas qu'un seul espace de nom signé, mais plutôt des îlots d'espaces de noms signés provenant chacun de points spécifiques (c'est-à-dire, des 'points de confiance') dans l'arborescence du DNS. Chacun de ces îlots sera identifié par le nom du point de confiance, et validé par au moins une clé publique associée. Pour les besoins du présent document, nous appellerons l'association de ce nom et d'une clé particulière une 'ancre de confiance'. Un point de confiance particulier peut avoir plus d'une clé désignée comme ancre de confiance.

Pour qu'un résolveur à capacité DNSSEC valide les informations dans une branche de la hiérarchie protégée par DNSSEC, il doit avoir connaissance d'une ancre de confiance applicable à cette branche. Il peut aussi avoir plus d'une ancre de confiance pour tout point de confiance donné. Selon les règles actuelles, une chaîne de confiance pour des données protégées par DNSSEC qui enchaîne son chemin de retour à TOUTE ancre de confiance connue est considérée comme 'sûre'.

À cause de la probable balkanisation de l'arborescence de DNSSEC due aux vides de signatures aux localisations de clés, un résolveur peut avoir besoin de connaître littéralement des milliers d'ancres de confiance pour effectuer ses tâches (par exemple, envisageons un ".COM" non signé). Exiger du propriétaire du résolveur qu'il gère manuellement ces nombreuses relations serait problématique. Ce le serait encore plus si on considère l'exigence éventuelle de remplacement/mise à jour de clé pour une ancre de confiance donnée. Le mécanisme décrit ici n'aidera pas à la configuration initiale des ancres de confiance dans les résolveurs, mais devrait rendre plus viable le remplacement/retournement de clé de point de confiance.

Comme mentionné ci-dessus, le présent document décrit un mécanisme par lequel un résolveur peut mettre à jour les ancres de confiance pour un point de confiance donné, principalement sans intervention humaine sur le résolveur. Quelques cas particuliers sont exposés (par exemple, la compromission de plusieurs clés) qui peuvent exiger une intervention manuelle, mais il devrait y en avoir peu et rarement. Le présent document NE DISCUTE PAS du problème général de la configuration initiale des ancres de confiance pour le résolveur.

1.1 Nomenclature de conformité

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

2. Théorie du fonctionnement

Le concept général de ce mécanisme est que les ancres de confiance existantes peuvent être utilisées pour authentifier de nouvelles ancres de confiance au même point dans la hiérarchie du DNS. Lorsque un opérateur de zone ajoute une nouvelle clé SEP (c'est-à-dire, une DNSKEY avec le bit de point d'entrée sécurisée établi) (voir au paragraphe 2.1.1 de la [RFC4034]) à un point de confiance RRSet de DNSKEY, et lorsque ce RRSet est validé par une ancre de confiance existante, le résolveur peut alors ajouter la nouvelle clé à son ensemble d'ancres de confiance valides pour ce point de confiance.

Certains aspects de cette approche doivent être atténués. Par exemple, la compromission de l'une des clés existantes pourrait permettre à un agresseur d'ajouter ses propres données 'valides'. Cela implique qu'on a besoin d'une méthode pour révoquer une clé existante sans considération du fait que cette clé est ou non compromise. Pour un autre exemple, supposons qu'une seule clé soit compromise ; nous avons besoin d'empêcher un agresseur d'ajouter une nouvelle clé et de l'empêcher de révoquer toutes les autres anciennes clés.

2.1 Révocation

Supposons deux clés A et B d'ancre de confiance. Supposons que B a été compromise. Sans un bit de révocation spécifique, B pourrait invalider A simplement en envoyant un ensemble de clés de point de confiance signé qui ne contient pas A. Pour régler ce problème, nous ajoutons un mécanisme qui exige la connaissance de la clé privé d'une DNSKEY pour révoquer cette DNSKEY.

Une clé est considérée comme révoquée lorsque le résolveur voit la clé dans un RRSet auto-signé et que la clé a le bit REVOKE (voir la Section 7 ci-dessous) mis à '1'. Une fois que le résolveur voit le bit REVOKE, il NE DOIT PLUS utiliser cette clé comme ancre de confiance pour quelque objet que ce soit excepté pour valider le RRSIG qu'il a signé sur le RRSet DNSKEY spécifiquement dans le but de valider la révocation. À la différence de l'opération 'Add' ci-dessous, la révocation est immédiate et permanente à réception d'une révocation valide au résolveur.

Un RRSet auto-signé est un RRSet DNSKEY qui contient la DNSKEY spécifique et pour lequel il y a un enregistrement RRSIG validé correspondant. Ce n'est pas un RRSet DNSKEY particulier, simplement une façon de décrire les exigences devalidation pour ce RRSet.

Note : Une DNSKEY avec le bit REVOKE établi a une empreinte différente de celle qui n'a pas le bit établi. Cela affecte la correspondance d'une DNSKEY avec les enregistrements DS dans la [RFC3755] parente, ou bien l'empreinte mémorisée chez un résolveur qui est utilisée pour configurer un point de confiance.

Dans l'exemple donné, l'agresseur pourrait révoquer B parce qu'il a connaissance de la clé privée de B, mais il ne pourrait pas révoquer A.

2.2 Ajout de la mise en garde

Supposons deux clés A et B de point de confiance. Supposons que B a été compromise. Un agresseur pourrait générer et ajouter une nouvelle clé C d'ancre de confiance (en ajoutant C au RRSet de DNSKEY et en la signant avec B), puis invalider la clé compromise. Il en résulterait que l'agresseur et le propriétaire seraient tous deux capables de signer des données dans la zone et les voir acceptées comme valides par les résolveurs.

Pour atténuer mais non résoudre complètement ce problème, nous ajoutons un temporisateur de mise en garde à l'ajout de l'ancre de confiance. Lorsque le résolveur voit une nouvelle clé SEP dans un RRSet de DNSKEY de point de confiance validé, le résolveur lance un temporisateur d'acceptation, et se souvient de toutes les clés qui ont validé le RRSet. Si le résolveur voit le RRSet de DNSKEY sans la nouvelle clé mais avec une signature valide, il arrête le processus d'acceptation pour cette clé et remet à zéro le temporisateur d'acceptation. Si toutes les clés qui étaient utilisées à l'origine pour valider cette clé ont été révoquées avant l'arrivée à expiration du temporisateur, le résolveur arrête le processus d'acceptation et remet le temporisateur à zéro.

Une fois le temporisateur arrivé à expiration, la nouvelle clé sera ajoutée comme ancre de confiance la prochaine fois que le RRSet validé avec la nouvelle clé sera vu au résolveur. Le résolveur NE DOIT PAS traiter la nouvelle clé comme une ancre de confiance avant l'arrivée à expiration du temporisateur de mise en garde ET avant d'avoir restitué et validé un RRSet DNSKEY après la temporisation de mise en garde qui contient la nouvelle clé.

Note : Une fois que le résolveur a accepté une clé comme ancre de confiance, la clé DOIT être considérée comme une ancre de confiance valide par ce résolveur jusqu'à ce qu'elle soit explicitement révoquée comme décrit ci-dessus.

Dans l'exemple donné, le propriétaire de la zone peut récupérer d'une compromission en révoquant B et en ajoutant une nouvelle clé D et en signant le RRSet DNSKEY avec les deux clés A et B.

La raison pour laquelle ceci ne résout pas complètement le problème a à voir avec la nature répartie du DNS. Le résolveur ne sait que ce qu'il voit. Un agresseur déterminé qui détient une clé compromise pourrait empêcher un seul résolveur de réaliser que la clé a été compromise en interceptant les données 'réelles' provenant de la zone d'origine et en y substituant les siennes (par exemple, en utilisant l'exemple, signé seulement avec B). Ceci n'est pas pire que la situation actuelle en supposant une clé compromise.

2.3 Rafraîchissement actif

Un résolveur qui a été configuré pour une mise à jour automatique des clés à partir d'un point de confiance particulier DOIT interroger ce point de confiance (par exemple, faire une recherche de RRSet DNSKEY et des enregistrements RRSIG qui s'y rapportent) pas moins souvent que ce qui est le plus court de 15 jours, de la moitié de la TTL d'origine pour le RRSset DNSKEY, ou de la moitié de l'intervalle d'expiration de la RRSIG , et pas plus souvent que une fois par heure. L'intervalle d'expiration est la quantité de temps à partir du moment où la RRSIG a été restituée pour la dernière fois jusqu'au moment de l'expiration dans la RRSIG. C'est à dire que queryInterval = MAX(1 heure, MIN (15 jours, 1/2*OrigTTL, 1/2*RRSigExpirationInterval))

Si l'interrogation échoue, le résolveur DOIT répéter l'interrogation jusqu'à la satisfaire pas plus souvent qu'une fois par heure et pas moins souvent que ce qui est le plus petit de 1 jour, 10 % de la TTL d'origine, ou 10 % de l'intervalle d'expiration original. C'est-à-dire que retryTime = MAX (1 heure, MIN (1 jour, .1 * origTTL, .1 * expireInterval)).

2.4 Paramètres de résolveur

2.4.1 Ajout du temporisateur de mise en garde

La durée de la temporisation de mise en garde ajoutée est de 30 jours ou l'arrivée à expiration de la durée de vie originale du premier RRSet DNSKEY de point de confiance à contenir la nouvelle clé, selon ce qui est le plus grand. Cela assure

qu'au moins deux RRSet DNSKEY validés qui contiennent la nouvelle clé DOIVENT être vus par le résolveur avant l'acceptation de la clé.

2.4.2 Retrait du temporisateur de mise en garde

La durée de la temporisation du retrait de mise en garde est de 30 jours. Ce paramètre est seulement un paramètre pour tenir à jour une base de données de gestion de clés. Si on ne réussit pas à retirer les informations sur l'état des défuntes clés de la base de données, la sécurité de ce protocole n'en sera pas contrariée pour autant, mais cela peut se terminer par une base de données complètement encombrée d'informations de clés obsolètes.

2.4.3 Ancre de confiance minimum par point de confiance

Un résolveur conforme DOIT être capable de gérer au moins cinq clés SEP par point de confiance.

3. Changements au format RDATA de DNSKEY

Le bit 8 du champ des fanions de DNSKEY est conçu comme étant le fanion 'REVOKE'. Si ce bit est mis à '1', ET si le résolveur voit un RRSIG(DNSKEY) signé par la clé associée, le résolveur DOIT alors considérer cette clé comme définitivement invalide pour tout usage excepté pour valider la révocation.

4. Tableau d'état

La chose la plus importante à comprendre est la façon dont le résolveur voit une clé à un point de confiance. Le tableau d'état suivant décrit cette vue à divers points de la vie de la clé. Le tableau est une partie normative de la présente spécification. L'état initial de la clé est 'Start'. La vue du résolveur sur l'état de la clé change alors que surviennent divers événements.

C'est l'état d'une clé de point de confiance tel que vu du résolveur. La colonne de gauche indique l'état actuel. La ligne du haut montre l'état suivant. L'intersection des deux montre l'événement qui va causer la transition d'état de l'état en cours à l'état suivant.

	État suivant					
À partir de	Start	AddPend	Valid	Missing	Revoked	Removed
Start		NewKey				
AddPend	KeyRem		AddTime			
Valid				KeyRem	Revbit	
Missing			KeyPres		Revbit	
Revoked						RemTime
Removed						

Tableau des états

4.1 Événements

NewKey Le résolveur voit un RRSet DNSKEY valide avec une nouvelle clé SEP. Cette clé va devenir une nouvelle ancre de confiance pour le point de confiance désigné après qu'elle a été présente dans le RRSet pendant au moins le 'add time'.

KeyPres La clé est retournée au RRSet DNSKEY valide.

KeyRem Le résolveur voit un RRSet DNSKEY valide qui ne contient pas cette clé.

AddTime La clé a été vue dans tous les RRSet DNSKEY valides vus pendant au moins le 'add time'.

RemTime Une clé révoquée a été manquante dans le RRSet DNSKEY de point de confiance pendant une durée suffisante pour être retirée de l'ensemble de confiance.

RevBit La clé est apparue dans le RRSet DNSKEY d'ancre de confiance avec son bit "REVOKE" mis, et il y a une

RRSig sur la RRSet DNSKEY signée par cette clé.

4.2 États

Start La clé n'existe pas encore comme ancre de confiance chez le résolveur. Elle peut exister ou non au serveur de zone, mais soit n'a pas encore été vue du résolveur, soit a été vue mais était absente du dernier RRSet DNSKEY (par exemple, KeyRem event).

AddPend La clé a été vue au résolveur, a son bit 'SEP' mis, et a été incluse dans un RRSet DNSKEY validé. Il y a une temporisation de mise en garde avant que la clé puisse être utilisée comme ancre de confiance.

Valid La clé a été vue du résolveur et a été incluse dans tous les RRSet DNSKEY validés depuis le moment où elle a été vue pour la première fois jusqu'à la fin de la temporisation de mise en garde. Elle est maintenant valide pour vérifier les RRSet qui arrivent après la fin de la temporisation de mise en garde. Précision : Le RRSet DNSKEY n'a pas besoin d'être continuellement présent au résolveur (par exemple, sa TTL peut arriver à expiration). Si le RRSet est vu et est validé (c'est-à-dire, vérifié par rapport à une ancre de confiance existante), cette clé DOIT être dans le RRSet, autrement un événement 'KeyRem' est déclenché.

Missing C'est un cas anormal. La clé reste une clé de point de confiance valide, mais n'a pas été vue du résolveur dans le dernier RRSet DNSKEY validé. C'est un état anormal parce que l'opérateur de zone devrait utiliser le bit REVOKE avant le retrait de la clé.

Revoked C'est l'état dans lequel passe une clé une fois que le résolveur voit un RRSIG(DNSKEY) signé par cette clé dans lequel le RRSet DNSKEY contient cette clé avec son bit REVOKE mis à '1'. Une fois dans cet état, cette clé DOIT définitivement être considérée comme invalide comme ancre de confiance.

Removed Après un délai assez long de mise en garde, les informations relatives à cette clé peuvent être purgées du résolveur. Une clé dans l'état Removed NE DOIT PAS être considérée comme une ancre de confiance valide. (Noter que cet état est plus ou moins équivalent à l'état "Start", sauf que c'est une mauvaise pratique de réintroduire des clés précédemment utilisées – il faut voir cet état comme l'état de conservation de toutes les vieilles clés dont le résolveur n'a plus besoin de garder trace de l'état.)

5. Suppression de point de confiance

Un point de confiance qui a toutes ses ancres de confiance révoquées est considéré comme supprimé et est traité comme si le point de confiance n'avait jamais été configuré. Si il n'y a pas de point de confiance supérieur configuré, les données à ce point et au delà du point de confiance supprimé sont considérées comme non sûres par le résolveur. Si il y a des points de confiance supérieurs configurés, les données au point de confiance supprimé et au delà sont évaluées par rapport au ou aux points de confiance supérieurs.

Autrement, un point de confiance qui est subordonné à un autre point de confiance configuré PEUT être supprimé par un résolveur après 180 jours, lorsque un tel point de confiance subordonné s'enchaîne de façon valide à un point de confiance supérieur. La décision de supprimer l'ancre de confiance subordonnée est une décision de configuration locale. Une fois le point de confiance subordonné supprimé, la validation de la zone subordonnée dépend de la validation de la chaîne de confiance envers le point de confiance supérieur.

6. **Scénarios** (informatif)

Le modèle suggéré pour le fonctionnement est d'avoir une clé active et une clé en attente à chaque point de confiance. La clé active sera utilisée pour signer le RRSet DNSKEY. La clé en attente ne signera normalement pas ce RRSet, mais le résolveur l'acceptera comme ancre de confiance si/lorsque il voit la signature sur le RRSet DNSKEY de point de confiance.

Comme la clé en attente n'est pas utilisée pour la signature active, la clé privée associée peut (et devrait) être fournie avec des protections supplémentaires normalement non disponibles pour une clé qui doit être utilisée fréquemment (par exemple, verrouillée dans un coffre, partagée entre de nombreuses parties, etc). En principe, la clé en attente devrait être moins sujette à compromission qu'une clé active, mais cela va dépendre de préoccupations fonctionnelles qui ne sont pas traitées ici.

6.1 Ajout d'une ancre de confiance

Supposons une clé 'A' d'ancre de confiance existante.

1. Générer une nouvelle paire de clés.

2. Créer un enregistrement DNSKEY à partir de la paire de clés et établir les bits SEP et Clé de zone.

3. Ajouter la DNSKEY au RRSet.

4. Signer le RRSet DNSKEY SEULEMENT avec la clé 'A' d'ancre de confiance existante.

5. Attendre l'arrivée à expiration des divers temporisateurs de résolveur pour restituer le nouveau RRSet DNSKEY et les signatures.

6. La nouvelle ancre de confiance sera fournie aux résolveurs selon le programme décrit par le tableau d'état et l'algorithme de mise à jour – voir les Sections 2 et 4 ci-dessus.

6.2. Suppression d'une ancre de confiance

Supposons qu'existent les ancres de confiance 'A' et 'B' et qu'on veuille révoquer et supprimer 'A'.

1. Régler le bit de révocation sur la clé 'A'.

2. Signer le RRSet DNSKEY avec les deux clés 'A' et 'B'. 'A' est maintenant révoquée. L'opérateur devrait inclure la clé révoquée 'A' dans le RRSet pendant au moins le délai de mise en garde de révocation, mais peut ensuite la retirer du RRSet DNSKEY.

6.3 Renouvellement des clés

Supposons les clés existantes A et B. 'A' est activement utilisée (c'est-à-dire a signé le RRSet DNSKEY). 'B' était la clé en attente (c'est-à-dire a été dans le RRSet DNSKEY et est une ancre de confiance valide, mais n'a pas été utilisée pour signer le RRSet).

1. Générer une nouvelle paire de clés 'C'.
2. Ajouter 'C' au RRSet DNSKEY.
3. Établir le bit de révocation sur la clé 'A'.
4. Signer le RRSet avec 'A' et 'B'.

'A' est maintenant révoqué, 'B' est maintenant la clé active, et 'C' sera la clé en attente une fois le délai de mise en garde expiré. L'opérateur devrait inclure la clé révoquée 'A' dans le RRSet pendant au moins le délai de temporisation de mise en garde de retrait, mais peut alors la retirer du RRSet DNSKEY.

6.4 Clé active compromise

C'est la même chose qu'avec le mécanisme de renouvellement de clé (paragraphe 6.3) ci-dessus, en supposant que 'A' est la clé active.

6.5 Clé en attente compromise

En utilisant les mêmes hypothèses et conventions de dénomination que pour le renouvellement de clé (paragraphe 6.3) ci-dessus.

1. Générer une nouvelle paire de clés 'C'.
2. Ajouter 'C' au RRSet DNSKEY.
3. Régler le bit de révocation sur la clé 'B'.
4. Signer le RRSet avec 'A' et 'B'.

'B' est maintenant révoquée, 'A' reste la clé active, et 'C' sera la clé en attente une fois l'arrivée à expiration de la temporisation de mise en garde. 'B' devrait continuer à être incluse dans le RRSet pendant la durée de la temporisation de mise en garde de retrait.

6.6 Suppression de point de confiance

Pour supprimer un point de confiance qui est subordonné à un autre point de confiance configuré (par exemple, example.com à .com) exige un peu de jonglerie avec les données. Le processus spécifique est :

1. Générer une nouvelle DNSKEY et un nouvel enregistrement DS et fournir l'enregistrement DS au parent avec les enregistrements DS pour les vieilles clés.

2. Une fois que le parent a publié les DS, ajouter la nouvelle DNSKEY au RRSet et révoquer TOUTES les vieilles clés en même temps, tout en signant le RRSet DNSKEY avec toutes les anciennes et les nouvelles clés.

3. Après 30 jours, arrêter la publication des vieilles clés révoquées et retirer tout enregistrement DS correspondant dans le parent.

Révoquer les vieilles clés de point de confiance en même temps qu'on ajoute les nouvelles clés qui relient à un point de confiance supérieur empêche le résolveur d'ajouter les nouvelles clés comme ancres de confiance. L'ajout des enregistrements DS pour les vieilles clés évite une condition de compétition où la zone subordonnée devient soit non sûre (à cause de la suppression du point de confiance) soit devient fautive (parce qu'elle ne s'est pas bien reliée à la zone supérieure).

7. Considérations relatives à l'IANA

L'IANA a alloué un bit dans le champ des fanions DNSKEY (voir la Section 7 de la [RFC4034]) pour le bit REVOKE (8).

8. Considérations pour la sécurité

En plus des paragraphes suivants, voir aussi la Théorie du fonctionnement ci-dessus (Section 2) et particulièrement le paragraphe 2.2 pour l'exposé qui s'y rapporte.

Les considérations pour la sécurité du renouvellement des ancres de confiance non spécifique de ce protocole sont exposées dans la [RFC4986].

8.1 Propriété des clés contre politique d'acceptation

Le lecteur devrait noter que, alors que le propriétaire de la zone est responsable de la création de la distribution des clés, il est entièrement de la décision du propriétaire du résolveur de savoir s'il accepte de telles clés pour l'authentification des informations de zone. Cela implique que la décision de mettre à jour les clés d'ancre de confiance sur la base de la confiance envers une clé actuelle d'ancre de confiance est aussi la décision du propriétaire du résolveur.

Le propriétaire du résolveur (et celui qui met en œuvre le résolveur) PEUT choisir de permettre ou d'empêcher la mise à jour de l'état des clés sur la base de ce mécanisme pour des points de confiance spécifiques. Si ils choisissent d'empêcher la mise à jour automatisée, ils auront besoin d'établir un mécanisme de mise à jour manuelle ou autrement hors bande, ce qui sort du domaine d'application du présent document.

8.2 Plusieurs clés compromises

Ce schéma permet la récupération pour autant qu'au moins une clé valide d'ancre de confiance reste non compromise, par exemple, si il y a trois clés, on peut récupérer si deux d'entre elles sont compromises. Le propriétaire de la zone devrait déterminer son propre niveau de confort par rapport au nombre d'ancres de confiance actives, valides dans une zone et devrait être prêt à mettre en œuvre des procédures de récupération dès qu'il détecte une compromission. Une mise à jour manuelle ou autre hors bande de tous les résolveurs sera nécessaire si toutes les clés d'ancre de confiance sont compromises sur un point de confiance.

8.3 Mise à jour dynamique

Permettre à un résolveur de mettre à jour son ensemble d'ancres de confiance sur la base d'informations de clés dans la bande est potentiellement moins sûr qu'un processus manuel. Cependant, étant donné la nature du DNS, le nombre de résolveurs qui nécessiteraient une mise à jour si une clé d'ancre de confiance était compromise, et l'absence d'un cadre de gestion standard pour le DNS, cette approche n'est pas pire que la situation existante.

9. Références normatives

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997.
[RFC3755] S. Weiler, "Compatibilité de résolveur traditionnel pour la délégation de signature", mai 2004. (*Obsolète, voir* 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.
[RFC4035] R. Arends et autres, "Modifications du protocole pour les extensions de sécurité du DNS", mars 2005.

10. Références informatives

[RFC4986] H. Eland, R. Mundy, S. Crocker et S. Krishnaswamy, "Exigences relatives au changement d'ancre de confiance de la sécurité du DNS (DNSSEC)", août 2007. *(Information)*

Adresse de l'auteur

Michael StJohns
Indépendant
mél : mstjohns@comcast.net

Déclaration de copyright
Copyright (C) The IETF Trust (2007).

Le présent document est soumis aux droits, licences et restrictions contenus dans le BCP 78, et à www.rfc-editor.org, et sauf pour ce qui est mentionné ci-après, les auteurs conservent tous leurs droits.

Le présent document et les informations contenues sont fournies sur une base "EN L'ÉTAT" et LE CONTRIBUTEUR, L'ORGANISATION QU'IL OU ELLE REPRÉSENTE OU QUI LE/LA FINANCE (S'IL EN EST), LA INTERNET SOCIETY ET LA INTERNET ENGINEERING TASK FORCE DÉCLINENT TOUTES GARANTIES, EXPRIMÉES OU IMPLICITES, Y COMPRIS MAIS NON LIMITÉES À TOUTE GARANTIE QUE L'UTILISATION DES INFORMATIONS CI ENCLOSES NE VIOLENT AUCUN DROIT OU AUCUNE GARANTIE IMPLICITE DE COMMERCIALISATION OU D'APTITUDE À UN OBJET PARTICULIER.

Propriété intellectuelle
L'IETF ne prend pas position sur la validité et la portée de tout droit de propriété intellectuelle ou autres droits qui pourraient être revendiqués au titre de la mise en œuvre ou l'utilisation de la technologie décrite dans le présent document ou sur la mesure dans laquelle toute licence sur de tels droits pourrait être ou n'être pas disponible ; pas plus qu'elle ne prétend avoir 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 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.