Groupe de travail Réseau
Request for Comments : 5011
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

M. StJohns, Indépendant

septembre 2007

Mises à jour automatiques des ancres de confiance de la sécurité du DNS (DNSSEC)

Statut du présent mémoire

Le présent document spécifie un protocole de l'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 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 décrit un moyen pour mettre à jour automatiquement des "ancres de confiance" authentifiées, et autorisées de DNSSEC. La méthode assure la protection contre la compromission de N-1 clé parmi N clés dans l'ensemble de clés du 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 point de la hiérarchie, et, finalement, supplanter la ou les ancres existantes.

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

Table des Matières

1. Introduction

Au titre de la réalité des champs des extensions de sécurité du système des noms de domaines (DNSSEC, *Domain Name System Security Extensions*) [RFC4033], [RFC4034], [RFC4035], la communauté en est venue à réaliser qu'il n'y a pas un espace de noms signés, mais plutôt des îlots d'espaces de noms signés dont chacun a pour origine un point spécifique (c'est-à-dire, un "point de confiance") dans l'arborescence du DNS. Chacun de ces îlots va être identifié par le nom du point de confiance, et validé par au moins une clé publique associée. Pour les besoins du présent document, on appellera l'association de ce nom et d'une clé particulière une "ancre de confiance"'. Un point de confianc 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 protégée par DNSSEC de la hiérarchie, il doit avoir connaissance d'une ancre de confiance applicable à cette branche. Il peut aussi avoir plus d'une ancre de confiance pour un point de confiance donné. Selon les règles actuelles, une chaîne de confiance pour les 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 du DNSSEC due aux vides de signature aux localisations de clés, un résolveur peut avoir besoin de connaître littéralement des milliers d'ancres de confiance pour effectuer ses tâches (par exemple, considérer un ".COM" non signé). Exiger du propriétaire du résolveur qu'il gère manuellement ces nombreuses relations est problématique. C'est encore plus problématique quand on considère l'exigence éventuelle d'un remplacement/mise à jour de clé pour une ancre de confiance donnée. Le mécanisme décrit ici ne va pas aider à la configuration initiale des ancres de confiance dans les résolveurs, mais devrait rendre le remplacement/mise à jour de clé de point de confiance plus viable.

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 au résolveur. Il y a quelques cas limites discutés (par exemple, la compromission de plusieurs clés) qui peuvent exiger une intervention manuelle , mais ils devraient être peu nombreux et peu fréquents. 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" en majuscules dans ce 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. Quand un opérateur de zone ajoute une nouvelle clé SEP (c'est-à-dire, une DNSKEY avec le bit Point d'entrée sécurisé (SEP, *Secure Entry Point*) établi) (voir au paragraphe 2.1 de la [RFC4034]) à un RRSet DNSKEY point de confiance, et quand 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.

Cette approche pose quelques problèmes qui doivent être résolus. Par exemple, la compromission d'une des clés existantes pourrait permettre à un attaquant d'ajouter ses propres données "valides". Cela implique le besoin d'une méthode pour révoquer une clé existante sans considération de si cette clé est compromise ou non. Un autre exemple serait de supposer qu'une seule clé est compromise, et on a besoin d'empêcher un attaquant d'ajouter une nouvelle clé et de révoquer toutes les autres anciennes clés.

2.1 Révocation

Supposons deux clés d'ancre de confiance A et B. Supposons que B soit compromise. Sans un bit de révocation spécifique, B pourrait invalider A en envoyant simplement un ensemble de clés de point de confiance signées qui ne contient pas A. Pour corriger cela, on ajoute un mécanisme qui exige la connaissance de la clé privée d'une DNSKEY pour révoquer cette DNSKEY.

Une clé est considérée révoquée quand le résolveur voit la clé dans un RRSet auto-signé et que la clé a le bit REVOKE (voir la Section 7) établi à "1". Une fois que le résolveur voit le bit REVOKE, il NE DOIT PAS utiliser cette clé comme ancre de confiance ou pour tout autre objet sauf valider le RRSIG qu'il a signé sur le RRSet DNSKEY spécifiquement pour les besoins de la validation de 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 le DNSKEY spécifique et pour lequel il y a un enregistrement RRSIG validé correspondant. Ce n'est pas un RRSet DNSKEY spécial, juste un moyen de décrire les exigences de validation pour ce RRSet.

Note : une DNSKEY avec le bit REVOKE établi a une empreinte différente d'une qui ne l'a pas. Cela affecte la confrontation d'une DNSKEY aux enregistrements DS dans le parent [RFC3755], ou à l'empreinte mémorisée dans un résolveur qui est utilisée pour configurer un point de confiance.

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

2.2 Ajout du maintien

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

Pour atténuer mais pas résoudre complètement ce problème, on ajoute un temps de maintien à l'ajout de l'ancre de confiance. Quand le résolveur voit une nouvelle clé SEP validée dans un RRSet DNSKEY de point de confiance, 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 DNSKEY sans la nouvelle clé mais validement signé, il arrête le processus d'acceptation pour cette clé et relance le temporisateur d'acceptation. Si toutes les clés qui ont à l'origine été utilisées pour valider cette clé sont révoquées avant l'expiration du temporisateur, le résolveur arrête le processus d'acceptation et relance le temporisateur.

Une fois le temporisateur arrivé à expiration, la nouvelle clé va être ajoutée comme ancre de confiance la prochaine fois que le RRSet validé avec la nouvelle clé est vu au résolveur. Le résolveur NE DOIT PAS traiter la nouvelle clé comme une ancre de confiance avant l'expiration de délai de maintien ET qu'il ait restitué et validé un RRSet DNSKEY après le délai de maintien 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 zone peut récupérer d'une clé compromise en révoquant B et en ajoutant une nouvelle clé D et en signant le RRSet DNSKEY avec A et B.

La raison pour laquelle ceci ne résout pas complètement le problème est à mettre en rapport avec la nature répartie du DNS. Le résolveur connaît seulement ce qu'il voit. Un attaquant 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 leur substituant les siennes (par exemple, en utilisant l'exemple, celles signées seulement de B). Ceci n'est pas pire que la situation actuelle où on suppose 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 pour le RRSet DNSKEY et les enregistrements RRSIG qui s'y rapportent) pas moins souvent que le moins de 15 jours, la moitié du TTL original pour le RRSet DNSKEY, ou la moitié de l'intervalle d'expiration du RRSIG et pas plus souvent qu'une fois par heure. L'intervalle d'expiration est la durée entre le moment où le RRSIG a été restitué pour la dernière fois et l'heure d'expiration dans le RRSIG. C'est-à-dire, Intervalle d'interrogation = MAX(1 heure, MIN (15 jours, 1/2*OrigTTL, 1/2*RRSigExpirationIntervalle))

Si l'interrogation échoue, le résolveur DOIT répéter l'interrogation jusqu'à satisfaction pas plus souvent qu'une fois par heure et pas moins souvent que le plus petit de 1 jour, 10 % du TTL original, ou 10 % de l'intervalle original d'expiration.

C'est-à-dire, retryTime = MAX (1 heure, MIN (1 jour, 0,1 * origTTL, 0,1 * expirationIntervalle)).

2.4 Paramètres de résolveur

2.4.1 Le temps d'ajout de maintien

Le temps d'ajout de maintien est le plus grand de 30 jours ou du temps d'expiration du TTL original du premier RRSet DNSKEY de point de confiance qui contenait la nouvelle clé. 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 Temps de suppression de maintien

Le temps de suppression de maintien est 30 jours. Ce paramètre est seulement un paramètre de tenue de base de données de gestion de clé. L'échec de suppression des informations sur l'état des clés défuntes de la base de données n'aura pas d'impact négatif sur la sécurité de ce protocole, mais peut finir par une base de données encombrée d'informations de clés obsolètes.

2.4.3 Minimum d'ancres de confiance 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 de RDATA DNSKEY sur le réseau

Le bit 8 du champ des fanions DNSKEY est conçu comme le fanion "REVOKE". Si ce bit est établi à "1", ET si le résolveur voit un RRSIG(DNSKEY) signé par la clé associée, le résolveur DOIT alors considérer cette clé comme invalide en permanence pour tous les besoins excepté la validation de la révocation.

4. Tableau des états

La chose la plus importante à comprendre est la vue du résolveur de toute clé à un point de confiance. Le tableau d'états suivant décrit cette vue à divers points de la vie d'une clé. Le tableau est une partie normative de cette spécification. L'état initial de la clé est "Start". La vue du résolveur de l'état de la clé change lorsque divers événements se produisent.

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

	PROCHAIN ÉTAT					
FROM	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'il a été présent dans le RRSet pour au moins "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 éé dans chaque RRSet DNSKEY valide vu pendant au moins "add time".

RemTime : une clé révoquée a été manquante au RRSet DNSKEY du point de confiance pendant un temps suffisant pour être supprimée de l'ensemble de confiance.

RevBit : la clé est apparue dans le RRSet DNSKEY d'ancre de confiance avec son bit "REVOKED" établi, et il y a un RRSig sur le RRSet DNSKEY signé par cette clé.

4.2 États

Start *(début)* : la clé n'existe pas encore comme ancre de confiance au résolveur. Elle peut ou non exister au serveur de zone, mais soit elle n'a pas encore été vue au résolveur, soit elle a été vue mais était absente du dernier RRSet DNSKEY (par exemple, un événement KeyRem).

AddPend *(ajout en cours)* : la clé a été vue au résolveur, a son bit "SEP" établi, et a été incluse dans un RRSet DNSKEY validé. Il y a un temps de maintien pour la clé avant qu'elle puisse être utilisée comme ancre de confiance .

Valid *(valide)* : la clé a été vue au résolveur et a été incluse dans tous les RRSet DNSKEY validés depuis le temps où elle a été vue pour la première fois jusqu'au temps de maintien. Elle est maintenant valide pour vérifier les RRSet qui arrivent après le temps de maintien. Précision : le RRSet DNSKEY n'a pas besoin d'être continuellement présent au résolveur (par exemple, son TTL pourrait expirer). 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 *(manquante)* : c'est un état anormal. La clé reste une clé valide de point de confiance, mais n'a pas été vue au résolveur dans le dernier RRSet DNSKEY validé. C'est un état anormal parce que l'opérateur de zone devrait utiliser le bit REVOKE avant la suppression.

Revoked *(révoquée)* : c'est l'état où passe une clé une fois que le résolveur a vu un RRSIG(DNSKEY) signé par cette clé quand ce RRSet DNSKEY contient cette clé avec son bit REVOKE établi à "1". Une fois dans cet état, cette clé DOIT être considérée comme invalide en permanence comme ancre de confiance.

Removed *(supprimée)* : après un très long temps de maintien, les informations sur cette clé peuvent être purgées au résolveur. Une clé dans l'état supprimé NE DOIT PAS être considérée comme une ancre de confiance valide. (Note : cet état est plus ou moins équivalent à l'état "Start", sauf que c'est une mauvaise pratique de réintroduire des clés précédemment utilisées -- on voit cela comme l'état de maintien pour toutes les vieilles clés pour lesquelles le résolveur n'a plus besoin de garder trace de l'état.)

5. Suppression de point de confiance

Un point de confiance dont toutes les ancres de confiance sont révoquées est considéré comme supprimé et est traité comme si le point de confiance n'avait jamais été configuré. Si aucun point de confiance supérieur n'est configuré, les données au point de confiance supprimé et en dessous 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 en dessous 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, où un tel point de confiance subordonné s'enchaîne valablement 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 auprès du point de confiance supérieur.

6. Scénarios - pour information

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 va être utilisée pour signer le RRSet DNSKEY. La clé en attente ne va normalement pas signer ce RRSet, mais le résolveur va l'accepter comme ancre de confiance si/quand il voit la signature sur le RRSet DNSKEY du point de confiance.

Comme la clé en attente n'est pas utilisée dans 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, enfermée dans un coffre, partagée entre de nombreuses parties, etc). À noter que la clé en attente devrait être moins sujette à compromission qu'une clé active, mais cela va dépendre de probèmes de fonctionnement non traités ici.

6.1 Ajout d'une ancre de confiance

On suppose une clé d'ancre de confiance existante 'A'.
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 d'ancre de confiance existante - 'A'.
5. Attendre l'expiration des divers temporisateurs de résolveurs et leur restitution du nouveau RRSet DNSKEY et des signatures.
6. La nouvelle ancre de confiance va être remplie aux résolveurs selon le plan décrit par le tableau des états et l'algorithme de mise à jour -- voir les Sections 2 et 4.

6.2 Suppression d'une ancre de confiance

On suppose les ancres de confiance existantes 'A' et 'B' et on veut révoquer et supprimer 'A'.
1. Établir 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 maintien de suppression, mais ensuite il peut la supprimer du RRSet DNSKEY.

6.3 Changement de clé

On suppose les clés existantes A et B. 'A' en utilisation active (c'est-à-dire qu'elles ont signé le RRSet DNSKEY). 'B' a été 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 révoquée, 'B' est maintenant la clé active, et 'C' va être la clé en attente une fois que le temporisateur de maintien arrive à expiration. L'opérateur devrait inclure la clé révoquée 'A' dans le RRSet pour au moins le temps de maintien de suppression, mais peut alors la supprimer du RRSet DNSKEY.

6.4 Compromission d'une clé active

C'est le même mécanisme que pour le changement de clé (au paragraphe 6.3) en supposant que 'A' est la clé active.

6.5 Compromission d'une clé en attente

En utilisant les mêmes hypothèses et conventions de dénomination que pour le changement de clés (paragraphe 6.3) :
1. Générer une nouvelle paire de clés 'C'.
2. Ajouter 'C' au RRSet DNSKEY.

3. Établir 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' va être la clé en attente à l'expiration de la période de maintien. 'B' devrait continuer d'être incluse dans le RRSet pendant la période de maintien de suppression.

6.6 Suppression d'un point de confiance

Pour supprimer un point de confiance qui est subordonné à un autre point de confiance configuré (par exemple, exemple.com à .com) exige de jongler avec les données. Le processus est le suivant :

1. Générer un nouveau DNSKEY et 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 le nouveau DNSKEY au RRSet et révoquer TOUTES les vieilles clés en même temps, tout en signant le RRSet DNSKEY avec toutes les clés, vieilles et nouvelles.

3. Après 30 jours, arrêter de publier les vieilles clés révoquées et supprimer tous les enregistrements DS correspondants dans le parent.

Révoquer les vieilles clés de point de confiance en même temps qu'ajouter les nouvelles clés qui chaînent à un point de confiance supérieur empêche le résolveur d'ajouter les nouvelles clés comme ancres de confiance. Ajouter les enregistrements DS pour les vieilles clés évite une condition de concurrence où la zone subordonnée devient non sûre (parce que le point de confiance a été supprimé) ou devient boguée (parce qu'elle ne s'est pas enchaînée à la zone supérieure).

7. Considérations relatives à l'IANA

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

8. Considérations sur la sécurité

En plus des paragraphes suivants, voir aussi la Section 2 "Théorie de fonctionnement et en particulier le paragraphe 2.2 pour les discussions qui s'y rapportent.

Les considérations sur la sécurité pour le changement d'ancre de confiance non spécifique de ce protocole sont discutées dans la [RFC4986].

8.1 Propriété de clé contre politique d'acceptation

Le lecteur devrait noter que, bien que le propriétaire de zone soit responsable de la création et de la distribution des clés, il relève entièrement de la décision du propriétaire du résolveur d'accepter ou non 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 accordée à une clé d'ancre de confiance courante est aussi la décision du propriétaire du résolveur.

Le propriétaire du résolveur (et les mises en œuvre de résolveur) PEUT choisir de permettre ou empêcher les mises à jour d'état de clé sur la base de ce mécanisme pour des points de confiance spécifiques. Si il choisit d'empêcher les mises à jour automatisées, il va avoir besoin d'établir un mécanisme pour des mises à jour manuelles ou autres, hors bande, qui sortent du domaine d'application du présent document.

8.2 Compromission de plusieurs clés

Ce schéma permet la récupération tant qu'au moins une clé d'ancre de confiance valide reste non compromise, par exemple, si il y a trois clés, on peut récupérer si deux d'entre elles sont compromises. Le propriétaire de 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 quand il détecte une compromission. Une mise à jour manuelle ou autre hors bande de tous les résolveurs va être requise si toutes les clés d'ancre de confiance à un point de confiance sont compromises.

8.3 Mises à jour dynamiques

Permettre à un résolveur de mettre à jour son ensemble d'ancres de confiance sur la base d'informations de clé dans la bande est potentiellement moins sûr qu'un processus manuel. Cependant, étant donnée la nature du DNS, le nombre de résolveurs qui exigeraient une mise à jour si une clé d'ancre de confiance était compromise, et l'absence de cadre standard de gestion 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. *(MàJ par* RFC8174)

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

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

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

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

10. Références pour information

[RFC4986] H. Eland et autres, "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 complète de droits de reproduction

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 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.