Groupe de travail Réseau
Request for Comments : 4033
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 : En cours de normalisation
Traduction Claude Brière de L'Isle

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

Introduction et exigences pour la sécurité du DNS

Résumé
Les extensions de sécurité du système de noms de domaines (DNSSEC, *Domain Name System Security Extensions*) ajoutent l'authentification de l'origine des données et l'intégrité des données au système des noms de domaines. Le présent document introduit ces extensions et décrit leurs capacités et leurs limitations. Le présent document expose aussi les services que les extensions de sécurité du DNS fournissent ou ne fournissent pas. Enfin, le présent document décrit les relations entre les documents qui décrivent collectivement le DNSSEC.

Table des matières

1. Introduction

Le présent document introduit les extensions de sécurité du système des noms de domaine (DNSSEC, *Domain Name System Security Extensions*). Le présent document et les deux documents qui l'accompagnent ([RFC4034] et [RFC4035]) mettent à jour, précisent, et redéfinissent les extensions de sécurité définies dans la [RFC2535] et ses prédécesseurs. Ces extensions de sécurité consistent en un ensemble de nouveaux types d'enregistrements de ressource et en des modifications au protocole DNS existant ([RFC1035]). Les nouveaux enregistrements et les modifications du protocole ne sont pas pleinement décrites dans le présent document, mais sont décrites dans une famille de documents précisés à la Section 10. Les Sections 3 et 4 décrivent les capacités et les limitations des extensions de sécurité en plus grand détail. La Section 5

expose la portée de l'ensemble de documents. Les Sections 6, 7, 8, et 9 exposent les effets qu'auront ces extensions de sécurité sur les résolveurs, les résolveurs de bout, les zones, et les serveurs de noms.

Le présent document et ses deux compagnons rendent obsolètes les [RFC2535], [RFC3008], [RFC3090], [RFC3445], [RFC3655], [RFC3658], [RFC3755], [RFC3757], et [RFC3845]. Le présent ensemble de documents met aussi à jour sans les rendre obsolètes les [RFC1034], [RFC1035], [RFC2136], [RFC2181], [RFC2308], [RFC3225], [RFC3007], [RFC3597], et les portions de la [RFC3226] qui traitent de DNSSEC.

Les extensions de sécurité du DNS fournissent l'authentification de l'origine et la protection de l'intégrité des données du DNS, et sont aussi un moyen de distribution de clés publiques. Ces extensions ne fournissent pas la confidentialité.

2. Définitions des termes importants de DNSSEC

La présente section définit un certain nombre de termes utilisés dans cet ensemble de documents. Comme elles sont destinées à être utilisées comme références lors de la lecture du reste de l'ensemble de documents, les personnes qui les lisent pour la première fois peuvent souhaiter parcourir rapidement cette section, lire le reste de ce document, et revenir ensuite à cette section.

Chaîne d'authentification : Une séquence alternée de clé publiques du DNS (DNSKEY) de RRset et de RRSet de signataires par délégation (DS, *Delegation Signer*) forme une chaîne de données signées, dont chaque lien dans la chaîne se porte garant pour le suivant. Un RR de DNSKEY est utilisé pour vérifier la signature couvrant un RR de DS et permet au RR de DS d'être authentifié. Le RR de DS contient un hachage d'un autre RR de DNSKEY et le nouveau RR de DNSKEY est authentifié par confrontation au hachage dans le RR de DS. Ce nouveau RR de DNSKEY authentifie à son tour un autre RRset de DNSKEY et, à leur tour, certains RR de DNSKEY dans cet ensemble peuvent être utilisés pour authentifier un autre RR de DS, et ainsi de suite jusqu'à ce que la chaîne se termine finalement avec un RR de DNSKEY dont la clé privée correspondante signe les données de DNS désirées. Par exemple, la racine RRset de DNSKEY peut être utilisée pour authentifier le RRset DS pour "exemple." Le RRset de DS "exemple." contient un hachage qui correspond à une certaine DNSKEY "exemple.", et cette clé privé correspondante de DNSKEY signe le RRset de DNSKEY "exemple.". Les contreparties en clé privée du RRset de DNSKEY "exemple." signent les enregistrements de données tels que "www.exemple." et les RR de DS pour des délégations telles que "sous-zone.exemple."

Clé d'authentification : Une clé publique qu'un résolveur à capacité de sécurité a vérifiée et peut donc utiliser pour authentifier des données. Un résolveur à capacité de sécurité peut obtenir des clés d'authentification de trois façons. D'abord, le résolveur est généralement configuré pour connaître au moins une clé publique ; ces données configurées sont généralement soit la clé publique elle-même soit un hachage de la clé publique tel qu'il se trouve dans le RR de DS (voir "ancre de confiance"). Ensuite, le résolveur peut utiliser une clé publique authentifiée pour vérifier un RR de DS et le RR de DNSKEY auquel la RR de DS se réfère. Enfin, le résolveur peut être capable de déterminer qu'une nouvelle clé publique a été signée par la clé privée correspondant à une autre clé publique que le résolveur a vérifiée. Noter que le résolveur doit toujours être guidé par la politique locale lorsqu'il décide d'authentifier une nouvelle clé publique, même si la politique locale est simplement d'authentifier toute nouvelle clé publique pour laquelle le résolveur est capable de vérifier la signature.

RRset d'autorité : Dans le contexte d'une zone particulière, un RRset est "d'autorité" si et seulement si le nom propriétaire du RRset se tient dans le sous-ensemble de l'espace de nom qui est au sommet de la zone ou en dessous et à la coupure qui sépare la zone de ses enfants ou au-dessus, s'il en est. Tous les RRset au sommet de la zone sont d'autorité, sauf pour certains RRset à ce nom de domaine qui, s'il sont présents, appartiennent au parent de cette zone. Ces RRset pourraient inclure un RRset de DS, le RRset NSEC qui fait référence à ce RRset de DS (le "NSEC parental"), et les RR RRSIG associés à ces RRset, qui sont tous d'autorité dans la zone parente. De même, si cette zone contient un ou des points de délégation, seul le RRset NSEC parental, les RRset de DS, et tout RR RRSIG associé à ces RRset sont d'autorité pour cette zone.

Point de délégation : Terme utilisé pour décrire le nom du côté parental d'une coupure de zone. C'est-à-dire que le point de délégation pour "foo.example" serait le nœud foo.example dans la zone "example" (par opposition au sommet de zone de la zone "foo.example"). Voir aussi à sommet de zone.

Îlot de sécurité : Terme utilisé pour décrire une zone déléguée signée, qui n'a pas une chaîne d'authentification de la part de son parent délégataire. C'est-à-dire qu'il n'y a pas de RR du DS contenant un hachage d'un RR de DNSKEY pour l'îlot dans sa zone parente délégataire (voir la [RFC4034]). Un îlot de sécurité est servi par des serveurs de noms à capacité de sécurité et peut fournir des chaînes d'authentification à toute les zones déléguées filles. Les réponses provenant d'un îlot de sécurité ou de ses descendants ne peuvent être authentifiées que si ses clés d'authentification peuvent être authentifiées par des moyens de confiance hors bande appartenant au protocole DNS.

Clé de signature de clé (KSK, *Key Signing Key*) : Clé d'authentification qui correspond à une clé privée utilisée pour signer une ou plusieurs autres clés d'authentification pour une zone donnée. Normalement, la clé privée correspondant à une clé de signature signera une clé de signature de zone, qui à son tour a une clé privée correspondante qui va signer d'autres données de zone. La politique locale peut exiger que la clé de signature de zone soit changée fréquemment, alors que la clé de signature de clé peut avoir une période de validité plus longue afin de fournir un point d'entrée sûr plus stable dans la zone. La conception d'une clé d'authentification comme clé de signature de clé est une pure question de fonctionnement : la validation DNSSEC ne fait pas de distinction entre les clés de signature et les autres clés d'authentification DNSSEC, et il est possible d'utiliser une seule clé à la fois comme clé de signature de clé et clé de signature de zone. Les clés de signature de clé sont exposées plus en détail dans la [RFC3757]. Voir aussi à clé de signature de zone.

Résolveur de bout à capacité de sécurité non validant : résolveur de bout à capacité de sécurité qui fait confiance à un ou plusieurs serveurs de noms récurrents à capacité de sécurité pour effectuer en son nom la plupart des tâches exposées dans le présent ensemble de documents. En particulier, un résolveur de bout à capacité de sécurité non validant est une entité qui envoie des interrogations de DNS, reçoit des réponses de DNS, et est capable d'établir un canal sécurisé approprié à un serveur récurrent à capacité de sécurité qui va fournir ces services au nom du résolveur de bout à capacité de sécurité. Voir aussi à Résolveur de bout à capacité de sécurité, et à Résolveur de bout à capacité de sécurité validant.

Résolveur de bout non validant : terme plus commode pour un Résolveur de bout à capacité de sécurité non validant.

Serveur de noms à capacité de sécurité : entité qui agit comme serveur de nom (défini au paragraphe 2.4 de la [RFC1034]) qui comprend les extensions de sécurité au DNS définies dans cet ensemble de documents. En particulier, un serveur de noms à capacité de sécurité est une entité qui reçoit des interrogations de DNS, envoie des réponses de DNS, prend en charge l'extension de taille de message EDNS0 ([RFC2671]) et le bit DO ([RFC3225]), et prend en charge les bits de types de RR et d'en-tête de message définis dans cet ensemble de documents.

Serveur de noms récurrent à capacité de sécurité : entité qui agit à la fois comme serveur de noms à capacité de sécurité et comme résolveur à capacité de sécurité. Une phrase équivalente mais plus encombrante serait "un serveur de noms à capacité de sécurité qui offre un service récurrent".

Résolveur à capacité de sécurité : entité qui agit comme résolveur (défini au paragraphe 2.4 de la [RFC1034]) qui comprend les extensions de sécurité du DNS définies dans le présent ensemble de documents. En particulier, un résolveur à capacité de sécurité est une entité qui envoie des interrogations du DNS, reçoit des réponses du DNS, prend en charge l'extension de taille de message EDNS0 ([RFC2671]) et le bit DO ([RFC3225]), et est capable d'utiliser les bits de type de RR et d'en-tête de message définis dans le présent ensemble de documents pour fournir les services de DNSSEC.

Résolveur de bout à capacité de sécurité : entité qui agit comme résolveur de bout (défini au paragraphe 5.3.1 de la [RFC1034]) qui a assez de compréhension des extensions de sécurité du DNS définies dans le présent ensemble de documents pour fournir des services supplémentaires non disponibles à partir d'un résolveur de bout ignorant la sécurité. Les résolveurs de bout à capacité de sécurité peuvent être "validants" ou "non validants", selon que le résolveur de bout tente de lui-même de vérifier les signatures DNSSEC ou qu'il fait confiance à un serveur de noms à capacité de sécurité ami pour le faire. Voir aussi à Résolveur de bout validant, et à Résolveur de bout non validant.

<quelque chose> ignorant la sécurité : un <quelque chose> qui n'est pas "à capacité de sécurité".

Zone signée : une zone dont les RRset sont signés et qui contient des enregistrements DNSKEY, des signatures d'enregistrement de ressource (RRSIG, *Resource Record Signature*), des enregistrements suivants sécurisés (NSEC, *Next Secure*), et (facultativement) des enregistrements DS, construits de façon appropriée.

Ancre de confiance : RR configuré de DNSKEY ou hachage de RR de DS d'un RR de DNSKEY. Un résolveur à capacité de sécurité validant utilise cette clé publique ou ce hachage comme point de départ pour construire la chaîne d'authentification pour une réponse signée de DNS. En général, un résolveur validant devra obtenir les valeurs initiales de ses ancres de confiance via des moyens sécurisés ou de confiance en dehors du protocole DNS. La présence d'une ancre de confiance implique aussi que le résolveur devrait s'attendre à ce que la zone sur laquelle pointe l'ancre de confiance soit signée.

Zone non signée : une zone qui n'est pas signée.

Résolveur de bout à capacité de sécurité validant : résolveur à capacité de sécurité qui envoie des interrogations en mode récurrent mais qui effectue de lui-même la validation de signature plutôt que de faire aveuglément confiance à un serveur de noms amont récurrent à capacité de sécurité. Voir aussi à Résolveur de bout à capacité de sécurité, et à Résolveur de bout à capacité de sécurité non validant.

Résolveur de bout validant : terme plus court pour un résolveur de bout à capacité de sécurité validant.

Sommet de zone : terme utilisé pour décrire le nom du côté enfant de la coupure d'une zone. Voir aussi à Point de délégation.

Clé de signature de zone (ZSK, *Zone Signing Key*) : clé d'authentification qui correspond à une clé privée utilisée pour signer une zone. Normalement, une clé de signature de zone fera partie du même RRset de DNSKEY que la clé de signature de clé dont la clé correspondante signe ce RRset de DNSKEY, mais la clé de signature de zone est utilisée pour un objet légèrement différent et peut différer de la clé de signature de clé d'autre façon, telle que de durée de vie de validité. Concevoir une clé d'authentification comme une clé de signature de zone est une pure question de fonctionnement ; la validation DNSSEC ne fait pas la distinction entre les clés de signature de zone et les autres clés d'authentification DNSSEC, et il est possible d'utiliser une seule clé à la fois comme clé de signature de clé et comme clé de signature de zone. Voir aussi à Clé de signature de clé.

3. Services fournis par la sécurité du DNS

Les extensions de sécurité du système des noms de domaines (DNS, *Domain Name System*) fournissent les services d'authentification de l'origine et d'assurance d'intégrité pour les données du DNS, y compris les mécanismes pour l'authentification de la non existence de données dans le DNS. Ces mécanismes sont décrits ci-dessous.

Ces mécanismes exigent des changements au protocole du DNS. DNSSEC ajoute quatre nouveaux types d'enregistrements de ressource : la signature d'enregistrement de ressource (RRSIG, *Resource Record Signature*), la clé publique du DNS (DNSKEY, *DNS Public Key*), le signataire de délégation (DS, *Delegation Signer*), et le prochain enregistrement sécurisé (NSEC, *Next Secure*). Il ajoute aussi deux nouveaux bits d'en-tête de message : vérification désactivée (CD, *Checking Disabled*) et donnés authentifiées (AD, *Authenticated Data*). Afin de prendre en charge les plus grandes tailles de message du DNS qui résultent de l'ajout des RR de DNSSEC, DNSSEC exige aussi la prise en charge de EDNS0 ([RFC2671]). Finalement, DNSSEC exige la prise en charge du bit d'en-tête EDNS DNSSEC OK (DO) ([RFC3225]) de sorte qu'un résolveur à capacité de sécurité puisse indiquer dans ses interrogations qu'il souhaite recevoir des RR DNSSEC dans les messages de réponse.

Ces services protègent contre la plupart des menaces contre le système des noms de domaines décrites dans la [RFC3833]. Prière de se reporter à la Section 12 sur l'exposé des limitations à ces extensions.

3.1 Authentification de l'origine des données et intégrité des données

NSSEC fournit l'authentification en associant les signatures numériques générées par cryptographie avec les RRset du DNS. Ces signatures numériques sont mémorisées dans un nouvel enregistrement de ressource, l'enregistrement RRSIG. Normalement, il y aura une seule clé privée pour signer les données d'une zone, mais des clés multiples sont possibles. Par exemple, il peut y avoir des clés pour chacun des différents algorithmes de signature numérique. Si un résolveur à capacité de sécurité apprend de façon fiable la clé publique d'une zone, il peut authentifier les données signées de cette zone. Un concept important de DNSSEC est que la clé qui signe les données d'une zone est associée à la zone elle-même et non aux serveurs de noms d'autorité de la zone. (Les clés publiques pour les mécanismes d'authentification des transactions du DNS peuvent aussi apparaître dans les zones, comme décrit dans la [RFC2931], mais DNSSEC lui-même est concerné par la sécurité des objets des données du DNS, et non par la sécurité des canaux des transactions du DNS. Les clés associées à la sécurité des transactions peuvent être mémorisées dans des types de RR différents. Voir les détails dans la [RFC3755].)

Un résolveur à capacité de sécurité peut apprendre la clé publique d'une zone soit en ayant une ancre de confiance configurée dans le résolveur soit par la résolution DNS normale. Pour permettre cette dernière, les clés publiques sont mémorisées dans un nouveau type d'enregistrement de ressource, le RR DNSKEY. Noter que les clés privées utilisées pour signer les données de zone doivent être conservées en sécurité et devraient être mémorisées hors ligne lorsque c'est possible. Pour découvrir fiablement une clé publique via la résolution DNS, la clé cible elle –même doit être signée soit par une clé d'authentification configurée soit par une autre clé qui a été authentifiée au préalable. Les résolveurs à capacité de sécurité authentifient les informations de zone en formant une chaîne d'authentification à partir d'une clé publique nouvellement apprise avec une clé publique d'authentification préalablement connue, qui à son tour a soit été configurée dans le résolveur soit doit avoir été apprise et vérifiée préalablement. Donc, le résolveur doit être configuré avec au moins une ancre de confiance.

Si l'ancre de confiance configurée est une clé de signature de zone, elle va alors authentifier la zone associée ; si la clé configurée est une clé de signature de clé, elle va authentifier une clé de signature de zone. Si l'ancre de confiance configurée est le hachage d'une clé plutôt que la clé elle-même, le résolveur peut devoir obtenir la clé via une interrogation du DNS. Pour aider les résolveurs à capacité de sécurité à établir cette chaîne d'authentification, les serveurs de noms à

capacité de sécurité essayent d'envoyer la ou les signatures nécessaires pour authentifier la ou les clés publiques d'une zone dans le message de réponse du DNS avec la clé publique elle-même, pourvu qu'il y ait de l'espace disponible dans le message.

Le type de RR signataire de délégation (DS) simplifie certaines des tâches administratives impliquées dans la signature des délégations à travers les frontières organisationnelles. Le RRset DS réside à un point de délégation dans une zone parente et indique la ou les clés publiques correspondant à la ou aux clés privées utilisées pour auto signer le RRset DNSKEY au sommet de la zone fille déléguée. L'administrateur de la zone fille, à son tour, utilise la ou les clés privées correspondant à une ou plusieurs des clés publiques dans ce RRset DNSKEY pour signer les données de la zone fille. La chaîne d'authentification normale est donc DNSKEY->[DS->DNSKEY]*->RRset, où "*" note zéro, une ou plusieurs sous-chaînes DS->DNSKEY. DNSSEC permet des chaînes d'authentification plus complexes, telles que des couches supplémentaires de RR DNSKEY signant d'autres RR DNSKEY au sein d'une zone.

Un résolveur à capacité de sécurité construit normalement cette chaîne d'authentification à partir de la racine de la hiérarchie du DNS en descendant jusqu'aux zones terminales sur la base de la connaissance configurée de la clé publique par la racine. Les politiques locales peuvent cependant aussi permettre à un résolveur à capacité de sécurité d'utiliser une ou plusieurs clés publiques configurées (ou hachages de clés publiques) autres que la clé publique racine, peuvent ne pas fournir de connaissance configurée de la clé publique racine, ou peuvent empêcher le résolveur d'utiliser des clés publiques particulières pour des raisons arbitraires, même si ces clés publiques sont correctement signées avec des signatures vérifiables. DNSSEC fournit des mécanismes par lesquels un résolveur à capacité de sécurité peut déterminer si une signature de RRset est "valide" au sein de la signification de DNSSEC. En dernière analyse cependant, l'authentification des clés et des données du DNS sont toutes deux une question de politique locale, qui peut étendre ou même subroger les extensions de protocole définies dans le présent ensemble de documents. Voir à la Section 5 pour des précisions.

3.2 Authentification de la non existence de nom et de type

Le mécanisme de sécurité décrit au paragraphe 3.1 ne fournit qu'un moyen de signer les RRset existants dans une zone. Le problème de la fourniture de réponses négatives avec le même niveau d'authentification et d'intégrité exige l'utilisation d'un nouvel autre type d'enregistrement de ressource, l'enregistrement NSEC. L'enregistrement NSEC permet à un résolveur à capacité de sécurité d'authentifier une réponse négative pour la non existence aussi bien d'un nom que d'un type avec le même mécanisme que celui utilisé pour authentifier les autres réponses du DNS. L'utilisation des enregistrements NSEC exige une représentation canonique et un ordre des noms de domaine dans les zones. Les chaînes d'enregistrements NSEC décrivent explicitement les trous, ou "espaces vides", entre les noms de domaines dans une zone et font la liste des types de RRset présents sur les noms existants. Chaque enregistrement NSEC est signé et authentifié en utilisant les mécanismes décrits au paragraphe 3.1.

4. Services non fournis par la sécurité du DNS

Le DNS a été conçu à l'origine avec l'hypothèse qu'il retournerait la même réponse à toute interrogation sans considération de celui qui pourrait l'avoir formulée, et que toutes les données dans le DNS seraient donc visibles. En conséquence, DNSSEC n'est pas conçu pour fournir la confidentialité, des listes de contrôle d'accès, ou d'autres moyens de différenciation entre les interrogateurs.

DNSSEC ne fournit aucune protection contre les attaques de déni de service. Les résolveurs à capacité de sécurité et les serveurs de noms à capacité de sécurité sont vulnérables à une classe supplémentaire d'attaques de déni de service fondées sur les opérations cryptographiques. Prière de se reporter à la Section 12 pour les détails.

Les extensions de sécurité du DNS fournissent l'authentification des données et de leur origine pour les données du DNS. Les mécanismes mentionnés ci-dessus ne sont pas conçus pour protéger des opérations telles que les transferts de zone et la mise à jour dynamique ([RFC2136], [RFC3007]). Les schémas d'authentification de message décrits dans la [RFC2845] et la [RFC2931] visent des opérations de sécurité qui relèvent de ces transactions.

5. Portée de l'ensemble des documents DNSSEC et problèmes du dernier bond

Les spécifications de cet ensemble de documents définissent le comportement des signataires de zone et serveurs de noms et résolveurs à capacité de sécurité de telle façon que les entités validantes puissent sans ambiguïté déterminer l'état des données.

Un résolveur validant peut déterminer les quatre états suivants :

Sûr : le résolveur validant a une ancre de confiance, une chaîne de confiance, et est capable de vérifier toutes les signatures dans les réponse.

Non sûr : le résolveur validant a une ancre de confiance, une chaîne de confiance, et, à un certain point de délégation, une preuve signée de la non existence d'un enregistrement de DS. Cela indique que des branches ultérieures de l'arborescence sont d'une insécurité prouvée. Un résolveur validant peut avoir une politique locale pour marquer des parties de l'espace du domaine comme non sûr.

Fautif : le résolveur validant a une ancre de confiance et une délégation sûre qui indique que les données subsidiaires sont signées, mais que la réponse a échoué à les valider pour une raison quelconque : signatures manquantes, signatures périmées, signatures avec des algorithmes non pris en charge, données manquantes dont le RR NSEC pertinent dit qu'elles devraient être présentes, et ainsi de suite.

Indéterminé : il n'y a pas d'ancre de confiance qui indiquerait qu'une portion spécifique de l'arborescence est sûre. C'est le mode de fonctionnement par défaut.

La présente spécification ne définit que la façon dont les serveurs de noms à capacité de sécurité peuvent signaler aux résolveurs de bout non validants que des données fautives ont été trouvées (en utilisant le RCODE=2, "Défaillance de serveur" ; voir la [RFC4035]).

Il y a un mécanisme pour que les serveurs à capacité de sécurité signalent aux résolveurs de bout à capacité de sécurité que les données sont sûres (en utilisant le bit AD ; voir la [RFC4035]).

La présente spécification ne définit pas un format pour communiquer pourquoi les réponses se sont trouvées fautives ou marquées comme non sûres. Le mécanisme de signalisation actuel ne fait pas la distinction entre les états indéterminé et non sûr.

Une méthode pour signaler les codes d'erreur et politiques évolués entre résolveurs de bout à capacité de sécurité et serveurs de noms récurrents à capacité de sécurité est un sujet d'étude pour des travaux à venir, comme l'est l'interface entre un résolveur à capacité de sécurité et les applications qui l'utilisent. Noter cependant, que le manque de spécification de telles communications n'interdit pas le déploiement de zones signées ou le déploiement de serveurs de noms récurrents à capacité de sécurité qui interdise la propagation de données fautives aux applications.

6. Considérations sur les résolveurs

Un résolveur à capacité de sécurité doit être capable d'effectuer les fonctions cryptographiques nécessaires pour vérifier les signatures numériques en utilisant au moins le ou les algorithmes de mise en œuvre obligatoire. Les résolveurs à capacité de sécurité doivent aussi être capables de former une chaîne d'authentification à partir d'une zone nouvellement apprise pour remonter jusqu'à une clé d'authentification, comme décrit ci-dessus. Ce processus peut requérir des interrogations supplémentaires aux zones DNS intermédiaires pour obtenir les enregistrements DNSKEY, DS, et RRSIG nécessaires. Un résolveur à capacité de sécurité devrait être configuré avec au moins une ancre de confiance comme point de départ pour tenter d'établir les chaînes d'authentification.

Si un résolveur à capacité de sécurité est séparé des serveurs de noms d'autorité pertinents par un serveur récurrent ou par une sorte quelconque d'appareil intermédiaire agissant comme mandataire pour le DNS, et si le serveur de noms récurrent ou l'appareil intermédiaire n'a pas de capacité de sécurité, le résolveur à capacité de sécurité peut n'être pas capable de fonctionner en mode sécurisé. Par exemple, si les paquets d'un résolveur à capacité de sécurité sont acheminés à travers un appareil de traduction d'adresse réseau (NAT, *network address translation*) qui comporte un mandataire DNS qui n'a pas de capacité de sécurité, le résolveur à capacité de sécurité peut trouver difficile ou impossible d'obtenir ou valider des données de DNS signées. Le résolveur à capacité de sécurité peut connaître un moment particulièrement difficile à essayer d'obtenir des RR DS dans un tel cas, car les RR DS ne suivent pas les règles usuelles du DNS sur la propriété des RR aux coupures de zone. Noter que ce problème n'est pas spécifique des NAT : tout logiciel DNS oublieux de la sécurité entre le résolveur à capacité de sécurité et les serveurs de noms d'autorité va interférer avec DNSSEC.

Si un résolveur à capacité de sécurité doit s'appuyer sur une zone non signée ou sur un serveur de nom qui n'a pas de capacité de sécurité, le résolveur peut n'être pas capable de valider les réponses du DNS et aura besoin d'une politique locale sur la base de laquelle accepter les réponses non vérifiées.

Un résolveur à capacité de sécurité devrait prendre en compte une période de validation de signature lors de la détermination du TTL des données dans son antémémoire, pour éviter de mettre en antémémoire des données signées au

delà de la période de validité de la signature. Cependant, il devrait aussi permettre la possibilité que la propre horloge du résolveur à capacité de sécurité soit erronée. Et donc, un résolveur à capacité de sécurité qui fait partie d'un serveur de noms récurrent à capacité de sécurité devra faire très attention au bit DNSSEC "vérification désactivée" (CD) de la ([RFC4034]). Ceci afin d'éviter de bloquer le passage de signatures valides vers d'autres résolveurs à capacité de sécurité qui sont clients de ce serveur de noms récurrent. Voir dans la [RFC4035] comment un serveur récurrent sécurisé traite les interrogations avec le bit CD établi.

7. Considérations sur les résolveurs de bout

Bien qu'il ne soit pas strictement exigé qu'il en soit ainsi par le protocole, la plupart des interrogations du DNS proviennent des résolveurs de bout. Les résolveurs de bout, par définition, sont des résolveurs DNS minimaux qui utilisent le mode d'interrogation récurrent pour se décharger de la plus grande partie du travail de résolution du DNS sur un serveur de noms récurrent. Étant donné l'utilisation largement répandue des résolveurs de bout, l'architecture de DNSSEC doit tenir compte des résolveurs de bout, mais les caractéristiques de sécurité nécessaires dans un résolveur de bout diffèrent à certains égards de celles nécessaires dans un résolveur itératif à capacité de sécurité.

Même un résolveur de bout oublieux de la sécurité peut bénéficier de DNSSEC si les serveurs de noms récurrents qu'il utilise sont à capacité de sécurité, mais pour que le résolveur de bout puisse faire confiance aux services DNSSEC, il doit pouvoir se fier à la fois aux serveurs de noms récurrents en question et aux canaux de communication entre lui-même et ces serveurs de noms. La première de ces questions est une affaire de politique locale : par nature, un résolveur de bout oublieux de la sécurité n'a pas d'autre choix que de se mettre à la merci des serveurs de noms récurrents qu'il utilise, puisqu'il n'effectue pas les vérifications de validité de DNSSEC de lui-même. La seconde question exige quelque sorte de mécanisme de sécurité du canal ; un bon usage des mécanismes d'authentification de transaction du DNS, tel que SIG(0) ([RFC2931]) ou TSIG ([RFC2845]) devrait suffire, comme le ferait un usage approprié d'IPsec. Des mises en œuvre particulières peuvent avoir d'autres choix à leur disposition, tels que des mécanismes d'interprocessus de communication spécifiques du système d'exploitation. La confidentialité n'est pas nécessaire pour ce canal, mais l'intégrité des données et l'authentification du message le sont.

Un résolveur de bout à capacité de sécurité qui fait confiance à la fois à ses serveurs de noms récurrents et à ses canaux de communication avec eux peut choisir d'examiner le réglage du bit Données authentifiées (AD) dans l'en-tête de message des messages de réponse qu'il reçoit. Le résolveur de bout peut utiliser ce bit fanion comme indication pour découvrir si le serveur de noms récurrent a été capable de valider les signatures pour toutes les données dans les sections Réponse et Autorité de la réponse.

Il y a une étape de plus qu'un résolveur de bout à capacité de sécurité peut franchir si, pour une raison quelconque, il n'est pas capable d'établir une relation de confiance utile avec les serveurs de noms récurrents qu'il utilise : il peut effectuer sa propre validation de signature en établissant le bit Vérification désactivée (CD, *Checking Disabled*) dans ses messages d'interrogation. Un résolveur de bout validant est donc capable de traiter les signatures DNSSEC comme des relations de confiance entre les administrateurs de zone et le résolveur de bout lui-même.

8. Considérations sur les zones

Il y a plusieurs différences entre les zones signées et les zones non signées. Une zone signée contiendra des enregistrements relatifs à la sécurité supplémentaires (RRSIG, DNSKEY, DS, et NSEC). Les enregistrements RRSIG et NSEC peuvent être générés par un processus de signature avant de desservir la zone. Les enregistrements RRSIG qui accompagnent les données de zone ont des périodes de commencement et d'expiration définies qui établissent une période de validité des signatures et des données de zone que couvrent les signatures.

8.1 Valeurs de TTL contre période de validité de RRSIG

Il est important de noter la distinction entre une valeur de TTL de RRset et la période de validité d'une signature spécifiée par le RR RRSIG qui couvre ce RRset. DNSSEC ne change pas la définition ou la fonction de la valeur du TTL, qui est destiné à maintenir la cohérence des bases de données dans les antémémoires. Un résolveur à antémémoire purge les RRset de son antémémoire dès la fin de la période spécifiée par les champs TTL de ces RRset, sans considérer si le résolveur est ou non à capacité de sécurité.

D'un autre côté, les champs de commencement et d'expiration dans le RR RRSIG ([RFC4034]) spécifient la période durant laquelle la signature peut être utilisée pour valider le RRset couvert. Les signatures associées aux données de zone signée ne sont valides que pour la période spécifiée par ces champs dans les RR RRSIG en question. Les valeurs de TTL ne

peuvent pas étendre la période de validité des RRset signés dans l'antémémoire d'un résolveur, mais le résolveur peut utiliser la durée restante avant l'expiration de la période de validité de signature d'un RRset signé comme limite supérieure du TTL du RRset signé et de son RR RRSIG associé dans l'antémémoire du résolveur.

8.2 Nouvelles questions de dépendance temporelle pour les zones

Les informations dans une zone signée ont une dépendance au temps qui n'existait pas dans le protocole DNS d'origine. Une zone signée exige une maintenance régulière pour s'assurer que chaque RRset dans la zone a un RR RRSIGN actuel valide. La période de validité de signature d'un RR RRSIG est un intervalle durant lequel la signature pour un RRset signé particulier peut être considérée valide, et les signatures des différents RRset dans une zone peuvent arriver à expiration à des moments différents. Resigner un ou plusieurs RRset dans une zone changera un ou plusieurs RR RRSIG, ce qui à son tour va exiger d'incrémenter le numéro de série SOA de la zone pour indiquer qu'est survenu un changement dans la zone et de resigner le RRset SOA lui-même. Et donc, resigner un RRset dans une zone peut aussi déclencher des messages NOTIFY du DNS et des opérations de transfert de zone.

9. Considérations sur les noms des serveurs

Un serveur de noms à capacité de sécurité devrait comporter les enregistrements DNSSEC appropriés (RRSIG, DNSKEY, DS et NSEC) dans toutes les réponses aux interrogations provenant de résolveurs qui ont signalé leur accord pour recevoir de tels enregistrements via l'utilisation du bit DO dans l'en-tête EDNS, sous réserve des limitations de taille de message. Parce que l'inclusion de ces RR DNSSEC pourrait facilement causer la troncature du message UDP et le repli sur TCP, un serveur de noms à capacité de sécurité doit aussi prendre en charge le mécanisme EDNS "charge utile UDP de l'envoyeur".

Si possible, la moitié privée de chaque paire de clé DNSSEC devrait être conservée hors ligne, mais cela ne sera pas possible pour une zone dans laquelle la mise à jour dynamique du DNS a été activée. Dans le cas de la mise à jour dynamique, le serveur maître principal pour la zone devra resigner la zone lorsqu'elle est mise à jour, de sorte que la clé privée correspondant à la clé de signature de zone devra être gardée en ligne. C'est un exemple d'une situation dans laquelle la capacité à séparer le RRset DNSKEY de la zone en une ou des clés de signature de zone et une ou des clés de signature de clés peut être utile, car la ou les clés de signature de clés peuvent toujours dans ce cas être conservées hors ligne et peuvent avoir une durée de vie utile plus longue que la ou les clés de signature de zone.

Par lui-même, DNSSEC n'est pas suffisant pour protéger l'intégrité d'une zone entière durant les opérations de transfert de zone, car même une zone signée contient des données non signées, qui ne sont pas d'autorité si la zone a des descendants. Donc, les opérations de maintenance de zone vont exiger des mécanismes supplémentaires (très vraisemblablement quelque forme de sécurité du canal, telle que TSIG, SIG(0), ou IPsec).

10. La famille des documents pour la sécurité du DNS

L'ensemble de documents DNSSEC peut être partagé en plusieurs groupes principaux, dans l'orbite plus large des documents de base du protocole du DNS.

Le terme "ensemble de documents de protocole DNSSEC" se réfère aux trois documents qui forment le cœur des extensions de sécurité du DNS :

1. Introduction et exigences pour la sécurité du DNS (le présent document)
2. Enregistrements de ressource pour les extensions de sécurité au DNS [RFC4034]
3. Modifications de protocole pour les extensions de sécurité au DNS [RFC4035]

De plus, tout document qui ajouterait ou changerait les extensions centrales de sécurité du DNS entrerait dans cette catégorie. Cela inclut tous travaux futurs sur les communications entre les résolveurs de bout à capacité de sécurité et les serveurs de noms récurrents amonts à capacité de sécurité.

L'ensemble de documents "Spécification d'algorithme de signature numérique" se réfère au groupe de documents qui décrivent comment devraient être mis en œuvre les algorithmes de signature numérique spécifiques pour aller avec le format d'enregistrement de ressource DNSSEC. Chaque document de cet ensemble traite d'un algorithme de signature numérique spécifique. Prière de se reporter à l'appendice sur "Algorithme DNSSEC et types de résumés" dans la [RFC4034] pour voir la liste des algorithmes qui ont été définis lors de la rédaction de ce cœur de spécification.

L'ensemble de documents "Protocole d'authentification de transaction" se réfère au groupe de documents qui traitent de l'authentification du message DNS, y compris l'établissement de la clé secrète et sa vérification. Bien qu'il ne fasse pas

strictement partie de la spécification DNSSEC telle que définie dans cet ensemble de documents, ce groupe est mentionné à cause de ses relations avec DNSSEC.

Le dernier ensemble de documents, "Nouveaux usages de sécurité", se réfère aux documents qui cherchent à utiliser les extensions proposées pour la sécurité du DNS pour d'autres objets en rapport avec la sécurité. DNSSEC ne fournit aucune sécurité directe pour ces nouvelles utilisations mais peut être utilisé pour les prendre en charge. Les documents qui entrent dans cette catégorie incluent ceux qui décrivent l'utilisation du DNS dans la mémorisation et la distribution de certificats ([RFC2538]).

11. Considérations relatives à l'IANA

Ce document de généralités n'introduit à aucune nouvelles considérations relatives à l'IANA. Prière de se reporter à la[RFC4034] pour une revue complète des considérations relatives à l'IANA introduites par DNSSEC.

12. Considérations pour la sécurité

Le présent document introduit des extensions pour la sécurité du DNS et décrit l'ensemble de documents qui contiennent les nouveaux enregistrements de sécurité et les modifications au protocole du DNS. Les extensions fournissent l'authentification de l'origine des données et l'intégrité des données en utilisant des signatures numériques sur des ensembles d'enregistrements de ressource. La présente section expose les limitations de ces extensions.

Pour qu'un résolveur à capacité de sécurité valide une réponse du DNS, toutes les zones le long du chemin allant du point de confiance de départ à la zone contenant les zones de réponse doivent être signées, et tous les serveurs de noms et résolveurs impliqués dans le processus de résolution doivent avoir la capacité de sécurité, telle que définie dans le présent ensemble de documents. Un résolveur à capacité de sécurité ne peut pas vérifier les réponses provenant d'une zone non signée, d'une zone non desservie par un serveur de noms à capacité de sécurité, ou de toutes données du DNS que le résolveur ne peut obtenir qu'au travers d'un serveur de noms récurrent qui n'a pas la capacité de sécurité. Si il y a une coupure dans la chaîne d'authentification qui fait qu'un résolveur à capacité de sécurité ne peut pas obtenir et valider les clés d'authentification dont il a besoin, le résolveur à capacité de sécurité ne peut alors pas valider les données de DNS affectées.

Le présent document expose brièvement les autres méthodes pour ajouter à la sécurité d'une interrogation du DNS, comme d'utiliser un canal sécurisé par IPsec ou d'utiliser un mécanisme d'authentification de transaction du DNS tel que TSIG ([RFC2845]) ou SIG(0) ([RFC2931]), mais la sécurité des transactions ne fait pas en soi partie de DNSSEC.

Par définition, un résolveur de bout à capacité de sécurité non validant n'effectue pas de lui-même de validation de signature DNSSEC et est donc vulnérable à la fois aux attaques contre (et par) les serveurs de noms récurrents à capacité de sécurité qui effectuent ces vérifications en son nom et aux attaques sur ses communications avec ces serveurs de noms récurrents à capacité de sécurité. Les résolveurs de bout à capacité de sécurité non validants devraient utiliser certaines formes de sécurité du canal pour se défendre contre cette dernière menace. La seule défense connue contre la première de ces menaces serait que le résolveur de bout à capacité de sécurité effectue sa propre validation de signature, ce qui voudrait dire, encore par définition, que ce ne serait plus un résolveur de bout à capacité de sécurité non validant.

DNSSEC ne protège pas contre les attaques de déni de service. DNSSEC rend le DNS vulnérable à une nouvelle classe d'attaques de déni de service fondées sur des opérations cryptographiques contre les résolveurs à capacité de sécurité et les serveurs de noms à capacité de sécurité, car un attaquant peut tenter d'utiliser les mécanismes de DNSSEC pour consommer les ressources d'une victime. Cette classe d'attaques prend au moins deux formes. Un attaquant peut être capable de consommer les ressources de code de validation de signature d'un résolveur à capacité de sécurité en touchant aux RR RRSIG dans les messages de réponse ou en construisant des chaînes de signature d'une complexité inutile. Un attaquant peut aussi être capable de consommer les ressources d'un serveur de noms à capacité de sécurité qui prend en charge la mise à jour dynamique du DNS en envoyant un flux de messages de mise à jour qui force le serveur de noms à capacité de sécurité à resigner des RRset dans la zone plus fréquemment qu'il ne serait autrement nécessaire.

Suite à un choix délibéré de conception, DNSSEC ne fournit pas de confidentialité.

DNSSEC introduit la capacité qu'un élément hostile énumère tous les noms d'une zone en suivant la chaîne NSEC. Les RR NSEC attestent des noms qui n'existent pas dans une zone en faisant la liaison de nom existant en nom existant suivant l'ordre canonique de tous les noms dans une zone. Et donc, un attaquant peut interroger ces RR NSEC en séquence pour obtenir tous les noms dans une zone. Bien que ce ne soit pas une attaque contre le DNS lui-même, elle pourrait permettre à un attaquant de cartographier les hôtes du réseau ou d'autres ressources en énumérant les contenus d'une zone.

DNSSEC introduit une complexité supplémentaire significative au DNS et donc introduit de nombreuses opportunités nouvelles pour la mise en œuvre de bogues et de zones mal configurées. En particulier, l'activation de la validation de signature DNSSEC dans un résolveur peut être cause que des zones légitimes entières deviennent effectivement inaccessibles par suite d'erreurs de configuration ou de bogues de DNSSEC.

DNSSEC ne protège pas contre la manipulation de données de zone non signée. Les données qui ne sont pas d'autorité aux coupures de zone (RR glus et NS dans la zone parente) ne sont pas signées. Cela ne pose pas de problème lors de la validation de la chaîne d'authentification, mais cela signifie bien que les données qui ne sont pas d'autorité sont elles-mêmes vulnérables aux manipulations durant les opérations de transfert de zone. Et donc, alors que DNSSEC peut fournir l'authentification d'origine des données et l'intégrité des données pour les RRset, il ne peut pas le faire pour les zones, et d'autres mécanismes (tels que TSIG, SIG(0), ou IPsec) doivent être utilisés pour protéger les opérations de transfert de zone.

Prière de se reporter aux [RFC4034] et [RFC4035] pour les considérations supplémentaires sur la sécurité.

13. Remerciements

Le présent document a été créé à partir des apports et des idées des membres du groupe de travail Extensions au DNS. Bien qu'il soit impossible de faire une liste explicite de tous ceux qui ont apporté leurs contributions durant la décade pendant laquelle DNSSEC a été développé, les éditeurs souhaitent remercier particulièrement les personnes suivantes pour leurs contributions et leurs commentaires sur cet ensemble de documents : Jaap Akkerhuis, Mark Andrews, Derek Atkins, Roy Badami, Alan Barrett, Dan Bernstein, David Blacka, Len Budney, Randy Bush, Francis Dupont, Donald Eastlake, Robert Elz, Miek Gieben, Michael Graff, Olafur Gudmundsson, Gilles Guette, Andreas Gustafsson, Jun-ichiro Itojun Hagino, Phillip Hallam-Baker, Bob Halley, Ted Hardie, Walter Howard, Greg Hudson, Christian Huitema, Johan Ihren, Stephen Jacob, Jelte Jansen, Simon Josefsson, Andris Kalnozols, Peter Koch, Olaf Kolkman, Mark Kosters, Suresh Krishnaswamy, Ben Laurie, David Lawrence, Ted Lemon, Ed Lewis, Ted Lindgreen, Josh Littlefield, Rip Loomis, Bill Manning, Russ Mundy, Thomas Narten, Mans Nilsson, Masataka Ohta, Mike Patton, Rob Payne, Jim Reid, Michael Richardson, Erik Rozendaal, Marcos Sanz, Pekka Savola, Jakob Schlyter, Mike StJohns, Paul Vixie, Sam Weiler, Brian Wellington et Suzanne Woolf.

Il ne fait pas de doute que la liste ci-dessus est incomplète. Nos excuses à tous ceux qui ont été oubliés.

14. Références

14.1 Références normatives

[RFC1034] P. Mockapetris, P., "Noms de domaines - Concepts et facilités", STD 13, novembre 1987.

[RFC1035] P. Mockapetris, "Noms de domaines – Mise en œuvre et spécification", STD 13, novembre 1987.

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

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

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

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

[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.)*

[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.

14.2 Références pour information

[RFC2136] P. Vixie, S. Thomson, Y. Rekhter et J. Bound, "Mises à jour dynamiques dans le système de noms de domaine (DNS UPDATE)", avril 1997.

[RFC2181] R. Elz et R. Bush, "Clarifications pour la spécification du DNS", juillet 1997. *(Information)*

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

[RFC2538] D. Eastlake 3rd, O. Gudmundsson, "Mémorisation des certificats dans le système des noms de domaines (DNS)", mars 1999. (*Obsolète, voir* RFC4398) *(P.S.)*

[RFC2845] P. Vixie et autres, "Authentification de transaction de clé secrète pour DNS (TSIG)", mai 20000 (*MàJ par* RFC3645) *(P.S.)*

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

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

[RFC3008] B. Wellington, "Autorité de signature de sécurité du système de noms de domaines (DNSSEC)", novembre 2000. (*Obsolète, voir* RFC4035, RFC4033, RFC4034) (MàJ RFC2535) (*MàJ par* RFC3658) *(P.S.)*

[RFC3090] E. Lewis, "Précision à l'extension de sécurité du DNS sur l'état de zone", mars 2001. (*Obsolète, voir* RFC4033, RFC4034, RFC4035) *(P.S.)*

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

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

[RFC3833] D. Atkins, R. Austein, "Analyse des menaces contre le système des noms de domaines (DNS)", août 2004. *(Information)*

[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.)*

Adresse des auteurs

Roy Arends	Rob Austein	Matt Larson
Telematica Instituut	Internet Systems Consortium	VeriSign, Inc.
Brouwerijstraat 1	950 Charter Street	21345 Ridgetop Circle
7523 XC Enschede	Redwood City, CA 94063	Dulles, VA 20166-6503
NL	USA	USA
mél : roy.arends@telin.nl	mél : sra@isc.org	mél : mlarson@verisign.com

Dan Massey	Scott Rose
Colorado State University	National Institute for Standards and Technology
Department of Computer Science	100 Bureau Drive
Fort Collins, CO 80523-1873	Gaithersburg, MD 20899-8920
USA	USA
mél : massey@cs.colostate.edu	mél : scott.rose@nist.gov

Déclaration de copyright

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.