rfc4033

Introduction à la sécurité DNS et aux pré-requis

Les DNS Security Extensions (DNSSEC) sont une collection de nouveaux enregistrements et modifications de protocole qui ajoutent un authentification de l'origine des données et l'intégrité des données à DNS.

Définition des termes DNSSEC important

Authentication Chain Une séquence alternée de RRsets de clé publique DNS (DNSKEY) et de RRset de Delegation Signer (DS) forment une chaîne de donnée signée, et chaque lien dans la chaîne étant garant de la suivante. Un RR DNSKEY est utilisé pour vérifier la signature couvrant un RR DS et permet au RR DS d'être authentifié. Le RR DS contient un hash d'un autre RR DNSKEY et ce nouveau RR DNSKEY en retour authentifie un autre RRset DNSKEY et , en retour, certains RR DNSKEY dans ce jeu peuvent être utilisés pour authentifiier un autre RR DS, et ainsi de suite jusqu'à ce que la fin de la chaîne se termine avec un RR DNSKEY dont la clé privée correspondante signe la donnée DNS souhaitée. Par exemple, le RRset DNSKEY root peut être utilisé pour authentifier le RRset DS pour "example.". Le RRset DS "example." contient un hash qui matche une DNSKEY "example.", et la clé privée correspondante à ce DNSKEY signe le RRset DNSKEY "example." Les RRset DNSKEY signe les données enregistré tel que "www.example." et les RR DS pour les délégation comme "subzone.example."

Authentication key Une clé publique qu'un résolveur a vérifié et peut ainsi l'utiliser pour authentifier les données. Un résolveur peut obtenir les clés d'authentification de 3 manières. D'abord, le résolveur est généralement configuré pour connaître au moins une clé publique ; cette donnée configurée est généralement soit la clé publique elle-même ou un hash de la clé publique tel que trouvé dans le RR DS. Ensuite, le résolveur peut utiliser une clé publique authentifiée pour vérifier un RR DS et le RR DNSKEY pour lequel le RR DS réfère. Enfin, le résolveur peut être capable de déterminer qu'une nouvelle clé publique a été signée par la clé privée correspondante à une autre clé publique que le résolveur a vérifié. Noter que le résolveur doit toujours être guidé par la stratégie locale quand il décide d'authentifier une nouvelle clé publique même si la stratégie locale est simplement pour authentifier une nouvelle clé publique pour laquelle le résolveur est capable de vérifier la signature.

Authoritative RRset Dans le contexte d'une zone particulière, un RRset est authoritatif si et seulement si le nom propriétaire du RRset est dans le sous-jeu de l'espace de nom qui est au niveau ou sous le zone apex et au niveau ou sous la séparation de la zone de ses enfant, s'il y en a. Tous les RRsets dans la zone apex sont authoritatifs, excepté pour certains RRsets à ce nom de domaine qui, si présent, appartient au parent de cette zone. Ces RRset peuvent inclure un RRset DS, le RRset NSEC référençant ce RRset DS (le NSEC parental), et les RR RRSIG associés avec ces RRset, tous étant authoritatif dans la zone parente. Similairement, si cette zone contient des points de délégation, seul le RRset NSEC parent, les RRsets DS, et tou RR RRSIG associés avec ces RRsets sont autoritatifs pour cette zone

Delegation Point Terme utilisé pour décrire le nom côté parent d'une coupure de zone. C'est à dire, le point de délégation pour "foo.example" serait le nœud foo.example dans la zone "example" (opposé à l'apex de zone de la zone foo.example").

Island of Security Termet utilisé pour décrire une zone signée et déléguée qui n'a pas de chaîne d'authentification de son parent déléguant. C'est à dire qu'il n'y a pas de RR DS contenant un hash d'un RR DNSKEY pour l'île dans la zone du parent déléguant. Une île de sécurité est désservie par des serveurs de nom sécurisés et peut fournir des chaînes d'authentification à toute zone enfant déléguée. Les réponses d'une île de sécurité ou ses descendants peut seulement être authentifié si ses clés d'authentification peuvent être authentifiés par un moyen de confiance en dehors du protocole DNS

Key Signing Key Une clé d'authentification qui correspond à une clé privée utilisée pour signer une ou plusieurs autres clé d'authentification pour une zone donnée. Typiquement, la clé privée correspondant à une KSK va signer une clé de signature de zone, qui en retour a une clé privée correspondante qui va signer les données de la zone. La stratégie locale peut nécessiter que la clé de signature de zone soit changée fréquemment, alors que la KSK peut avoir une période de validité plus longue pour fournir un point d'entrée sécurisé plus stable dans la zone. Désigner une clé d'authentification comme KSK est purement un problème opérationnel : La validation DNSSEC ne distingue pas les KSK et les autres clé d'authentification DNSSEC, et il est possible d'utiliser une seul clé pour signer les clé et signer la zone.

Non-Validation Security-Aware Stub Resolver Un résolveur sécurisé qui valide un ou plusieurs serveurs de noms récursifs sécurisés pour effectuer plus de tâches discutés dans ce document. En particulier, un tel résolveur est une entité qui envoie des

requêtes DNS, reçois les réponses DNS, et est capable d'établir un canal sécurisé approprié vers un serveur récursif sécurisé qui fournir ces services à la demande.

Non-Validating Sub Resolver Un terme plus simple pour Non-Validation Security-Aware Stub Resolver

Security-Aware Name Server Une entité agissant dans le rôle d'un serveur de noms qui comprend les extensions de sécurité DNS définis dans ce document. En particulier, un serveur de nom sécurisé est une entité qui reçois des requêtes DNS, envoie des réponses DNS, supporte l'extension EDNS0 et le bit D0, et supporte les types RR et bits d'en-tête de messages définis dans ce document.

Security-Aware Recursive Name Server Une entité qui agit comme serveur de nom sécurisé et résolveur sécurisé.

Security-Aware Resolver Une entité agissant dans le rôle d'un résolveur qui comprend les extensions de sécurité DNS pour fournir des services additionnels. Ces résolveurs peuvent être soit validateurs soit non-validateurs, dépendant si le résolveur vérifie les signatures DNSSEC par lui-même ou fait confiance à un serveur de nom sécurisé pour le faire.

Security-Oblivious <anything} tout ce qui n'est pas sécurisé

Signed Zone Une zone dont les RRset sont signés et qui contiennent des enregistrements DNSKEY, RRSIG, NSEC et optionnellement DS

Trust Anchor Un RR DNSKEY configuré ou un hash RR DS d'un RR DNSKEY. Un résolveur sécurisé validant utilise cette clé publique ou le hash comme point de départ pour construire la chaîne d'authentification d'une réponse DNS. En général, un résolveur validateur obtient les valeurs initiales de ses ancres de confiance via un moyen sécurisé en dehors du protocole DNS. La présence d'une ancre de confiance implique également que le résolveur s'attende à ce que la zone vers laquelle l'ancre de confiance soit signée.

Unsigned Zone Une zone qui n'est pas signée

Validating Security-Aware Stub Resolver Un résolveur sécurisé qui envoie des requêtes en mode récursif mais qui valide la signature par lui-même au lieu de simplement faire confiance à un serveur de nom sécurisé.

Validating Stub Resolver Un terme plus simple pour Validating Security-Aware Stub Resolver

Zone Apex Terme utilisé pour décrire le nom d'une coupure de zone côté client

Zone Signing Key Une clé d'authentification qui correspond à une clé privée utilisée pour signer une zone. Typiquement, une ZSK fait partie du même RRset DNSKEY que la KSK dont la clé privée correspondante signe ce RRset DNSKEY, mais la ZSK est utilisée dans un but différent et peut être différente de la KSK en autre, sur sa durée de vie.

Services fournis par la sécurité DNS

Les extensions de sécurité DNS fournissent l'authentification de l'origine des données et l'intégrité des données, incluant les mécanismes pour authentifier le refus de l'existance de données DNS.

Ces mécanismes nécessitent de changer le protocole DNS. DNSSEC ajoute 4 nouveaux types d'enregistement de ressource : Resource Record Signature (RRSIG), DNS Publik Key (DNSKEY), Delegation Signer (DS), et Next Secure (NSEC). Il ajoute également 2 nouveaux bits d'en-tête : Checking Disables (CD) et Authenticated Data (AD). Pour supporter des tailles de messages DNS plus grands, DNSSEC exige le support EDNS0. Finallement, DNSSEC nécessite le support pour le bit d'en-tête DNSSEC OK (DO) pour qu'un résolveur sécurisé puissent indiquer dans ses requêtes qu'il souhaite reçevoir les RR DNSSEC dans les réponses.

Authentification de l'origine des données et intégrité des données

DNSSEC fournis l'authentification en associant des signature numérique générées cryptographiquement avec les RRset DNS. Ces signatures numérique sont stockées dans un nouvel enregistrement de ressource, l'enregistrement RRSIG. Généralement, il y a une seule clé privée qui signe les données d'une zone, mais plusieurs clés sont possibles. Par exemple, il peut y avoire des clés pour chaque algorithme de signature. Si un résolveur sécurisé apprend un clé publique de zone, il peut authentifier les données signées de cette zone. Un concept DNSSEC important est que la clé qui signe les données d'une zone est associée avec la zone elle-même et pas avec les serveurs de nom ayant autorité sur la zone. (Les clé publique pour les mécanismes d'authentification de transaction DNS peuvent également apparaître dans les zone, mais DNSSEC lui-même est concerné par la sécurité des données DNS, par la sécurité des canaux de transaction DNS. Les clés associées avec la sécurité des transaction peuvent être stockés dans des types RR différents)

Un résolveur sécurisé peut apprendre une clé publique d'une zone soit en ayant une ancre de confiance configuré dans le résolveur ou par résolution normale DNS, auquel cas les clé publiques sont stockées dans un nouveau type d'enregistrement de ressource, le RR DNSKEY.

Noter que les clés privées utilisée pour signer les donées de la zone doivent être conservé de manière sécurisés et devraient être stockés hors-line. Pour découvrir un clé publique de manière sûre via la résolution DNS, la clé cible elle-même doit être signée par une clé d'authentification configurée ou une autre clé qui a été authentifiée précédemment. Les résolveurs sécurisés authentifient les information de zone en formant une chaîne d'auhentification depuis une nouvelle clé publique apprise vers une clé publique authentifiée connue, qui en retour a été soit configurée dans le résolveur ou doit avoir été apprise et vérifiée précédemment. Donc, le résolveur doit être configuré avec au moins un trust anchor.

Si l'ancre de confiance configurée est une clé de signature de zone, elle authentifie la zone associée ; si la clé configurée est une clé de signature de clé, elle authentifie une clé de signature de zone. Si l'ancre de confiance configuré est le hash d'une clé au lieu de la clé elle-même, le résolveur peut obtenir la clé via une requête DNS. Pour aider les résoleurs à établir cette chaîne d'authentification, les serveurs de noms tentent d'envoyer les signatures nécessaire à authentifier les clé publique de la zone dans le message de réponse DNS avec la clé publique elle-même.

Le type RR Delegation Signer (DS) simplifie certaines tâches administratives en signant les délégation entre les limites administratives. Le RRset DS réside au point de délégation dans une zone parent et indique les clé publique correspondante aux clé privées utilisée pour signer les RRset DNSKEY dans l'apex de zone enfant déléguée. L'administrateur de la zone enfant, en retour, utilise les clés privée correspondantes à une ou plusieurs des clé publique dans ce RRset DNSKEY pour signer les données de la zone enfant. La chaîne d'authentification est donc DNSKEY->[DS>DNSKEY]*->RRset, où '*' dénote 0 ou plusieurs sous-chaînes DS->DNSKEY. DNSSEC permet des chaînes d'authentification plus complexes, tels que des couches additionnelles de RR DNSKEY signant d'autres RR DNSKEY dans une zone.

Un résolveur sécurisé construit normalement cette chaîne d'authentification depuis la racine de la hiérarchie DNS jusqu'aux zones basés sur une connaissance configurée de la clé publique pour root. La stratégie locale, cependant, peut également permettre au résolveur d'utilisen une ou plusieurs clé publique configurées (ou hash de ces clé) autre que la clé publique root, peuvent ne pas fournir de connaissance configuré de la clé publique root, ou peuvent empêcher le résolveur d'utiliser des clé publique particulières pour des raisons arbitraires, même si ces clés publique sont signées correctement et vérifiables. DNSSEC fournis des mécanismes par lesquels un résolveur peut déterminer si la signature d'un RRset est valide. Dans l'analyse finale, cependant, authentifier les clé DNS et les donnée est sujet à la stratégie locale, qui peut étendre ou même remplacer les extensions de protocole définis dans ce document.

Authentifier les noms et la non-existence de type

Le mécanisme de sécurisé décris ci-dessus ne fournis qu'une manière de signer des RRset exsistant dans une zone. Le problème des réponses négatives avec le même niveau d'intégrité et d'authentification exige l'utilisation d'un nouveau type d'enregistrement de ressource, NSEC. NSEC permet à un résolveur d'authentifier une réponse négative depuis soit le nom, ou la non-existance du type avec les même mécanisme utilisés pour authentifier les autres réponses DNS. L'utilisation des enregistrements NSEC nécessite une représentation canonique et d'ordre pour les noms de domaine dans les zones. Les chaînes d'enregistrement NSEC décrivent explicitement les gaps, ou espace vides, entre les noms de domaine dans une zone et la liste des types de RRset présent aux noms existant. Chaque enregistrement NSEC est signé et authentifié en utilisant les mécanismes décris plus haut.

Services non-fournis par la sécurité DNS

DNS a été conçus à l'origine avec la supposition que DNS retourne la même réponse à une requête donnée sans regarder qui a émis la requête, et que toutes les données dans DNS est donc visible. DNSSEC n'est pas conçus pour fournir la confidentialité, les listes de contrôle d'accès, ou d'autres moyens de différencier les questionneurs.

DNSSEC ne fournis pas de protection contre les attack DOS. Les résolveurs et les serveurs de nom sécurisé sont vulnérables à uen classe d'attaque DOS additionnel basé sur les opérations cryptographiques.

Les extensions de sécurité DNS fournissent l'authentification de l'origine des données DNS. Les mécanismes définis plus haut ne sont pas conçus pour protéger es opérations telles que les transferts de zone et les mises à jours dynamiques. Les schéma d'authentification de message décris dans les rfc2845 et rfc3007 adressent les opérations de sécurité pour ces transactions.

Périmètre du document et problème Last Hop

La spécification dans ce jeu de document définis le comportement pour les signataires de zone et les serveurs de nom sécurisés et les résolveurs qui valident les entités peuvent déterminer de manière non-ambigües l'état des données. Un résolveur validateur peut déterminer les 4 états suivants :

Secure Le résolveur validant a une ancre de confiance, a une chaîne de confiance, et est capable de vérifier toutes les signatures dans la réponse.

Insecure Le résolveur validant a une ancre de confiance, une chaîne de confiance, et, à certains points de délégation, la preuve signées de la non-existance d'un enregistrement DS. Celà indique que les branches sous-jacents dans l'arborescence sont probablement non-sécurisés. Un résolveur peut avoir une stratégie local pour marquer les parties de l'espace de domaine comme insécure.

Bogus Le résolveur validant a une ancre de confiance et une délégation sécurisée indique que les données subsidiaires sont signées, mais la réponse échoue la validation : signatures manquantes, signatures expirées, signatures avec des algorithmes non-supportés, données manquantes, etc.

Indeterminés Il n'y a pas d'ancre de confiance qui indique qu'une portion spécifique de l'arborescence est sécurisé. C'est le mode d'opération par défaut.

Cette spécification définis seulement comment les serveurs de nom sécurisés peuvent signaler aux résolveurs non-validateurs que les données trouvés sont à l'état bogus (en utilisant RCODE=2 "Server Failure")

Il y a un mécanisme pour les serveurs de nom sécurisés pour signaler aux résolveurs sécurisé que les données sont sécurisés (en utilisant le bit AD)

Cette spécification ne définis pas de format pour communiquer la raison des réponses bogus ou insecure.

Une méthode pour signaler les codes d'erreur avancés et les stratégies entre un résolveur sécurisé et les serveurs de noms récursifs est un sujet pour un travail future, tout comme l'interface entre un résolveur sécurisé et les applications qui l'utilisent. Noter, cependant, que le manque de spécification d'une telle communication n'empêche pas de déployer des zones signées ou le déploiement de serveurs de noms récursifs sécurisés qui empêchent la propagation de données bogus aux applications.

Considérations du résolveur

Un résolveur sécurisé doit être capable d'effectuer des fonctions cryptographiques nécessaires à la vérification de signatures numérique en utilisant au moins les algorithmes obligatoire. Ces résolveurs doivent être capable de former une chaîne d'authentification depuis une nouvelle zone apprise vers une clé authentifiée, tel que décris plus haut. Ce processus peut nécessiter des requêtes additionnelles aux zones intermédiaires pour obtenir les enregistrements DNSKEY, DS, et RRSIG. Un résolveur devrait être configuré avec au moins une ancre de confiance comme point de départ depuis lequel il tente d'établir les chaînes d'authentification.

Si un résolveur est séparé des serveurs de nom autoritatifs par un serveur de nom récursif ou par un périphérique intermédiaire qui agit comme proxy pour DNS, et si le serveur de nom récursif ou le périphérique intermédiaire n'est pas sécurisé, le résolveur n'est pas capable d'opérer dans un mode sécurisé. Par exemple, si les paquets d'un résolveur sont routés via un NAT qui inclus un proxy DNS qui n'est pas sécurisé, le résolveur peut avoir des difficultés ou l'impossibilité d'obtenir ou valider la données DNS signée.

Si un résolveur sécurisé doit faire confiance à une zone non-signée ou un serveur de nom qui n'est pas sécurisé, le résolveur n'est pas capable de valider les réponses DNS et à besoin d'une stragégie locale pour accepter les réponses non-vérifiées

Un résolveur sécurisé doit prendre en compte la période de validité en déterminant le TTL des données en cache, pour éviter que les données signées en cache soient au-delà de la période de validité de la signature. Cependant, il devrait être permis que l'horloge du résolveur soit fausse. Donc, un résolveur qui fait partie d'un serveur de nom récursif doit faire attention aux bit CD. Cela permet d'éviter le blocage des signatures valide via d'autres résolveurs qui sont clients de ce serveur de nom récursif.

Considérations du résolveur cache

Bien que non strictement requis par le protocole, beaucoups de requêtes DNS ont pour origine les résolveurs cache. Ces résolveurs, par définition, sont des résolveurs minimals qui utilisent les requête récursives pour décharger le travaille de la résolution DNS à un serveur de nom récursif. L'architecture DNSSEC doit prendre en compte les résolveurs cache, mais les fonctionnalités de sécurité dans le résolveur cache diffèrent de ceux nécessaires dans un résolveur itératif sécuris.

Même un résolveur cache non sécurisé peut bénéficier de DNSSEC si les serveurs de noms récursifs qu'il utilise sont sécurisés, mais pour que le résolveur cache puisse s'appuyer sur les services DNSSEC, le résolveur doit faire confiance à serveurs de nom récursifs en question et aux canaux de communication entre lui et ces serveurs de nom. Le premier de ces problème est un problème de stratégie locale : un résolveur non-sécurisé n'a pas le choix mais se place lui-même à la merci des serveurs de noms récursifs qu'il utilise, vu qu'il ne valide pas DNSSEC. Le second problème nécessite un mécanisme de canal sécurisé ; l'utilisation des mécanismes d'authentification de transaction sécurisé comme SIG(0) ou TSIG est suffisant, et est approprié avec IPsec. Les implémentations peuvent avoir d'autres choix disponible, tels que des mécanisme de communication interprocess spécifiques à l'OS. La confidentialité n'est pas nécessaire pour ce canal, mais l'intégrité des données et l'authentification des messages le sont.

Un résolveur sécurisé fait confiance aux serveurs de noms sécurisé et ses canaux de communication et peut choisir d'examiner le bit AD dans l'en-tête des messages qu'il reçoit. Le résolveur peut utiliser ce flag pour voir si le serveur de nom récursif est capable de valider les signatures pour toutes les données dans les sections d'autorité et de réponse

Il y a une étape de plus qu'un résolveur sécurisé peut effectuer, s'il n'est pas capable d'établir une relation de confiance avec les serveurs de nom récursifs qu'il utilise : il peut effectuer sa propre validation de signature en définissant le bit CD dans ses requêtes. Un résolveur est capable de traiter les signatures DNSSEC comme relation de confiance entre les administrateurs de zone et le résolveur lui-même.

Considérations de zone

Il y a de nombreuses différences entre des zones signées et non-signées. Une zone signée contient des enregistrements liées à la sécurité additionnels (RRSIG, DNSKEY, DS, et NSEC). Les enregistrements RRSIG et NSEC peuvent être générées par un procéssus de signature avec de servir la zone. Les enregistrements RRSIG qui accompagnent les données de zone ont une date de création et d'expiration définis qui établissent une période de validité pour les signatures et les données de zone que les signatures couvrent.

Valeurs TTL vs Période de validité RRSIG

Il est important de noter la distinction entre la valeur TTL des RRset et la période de validité de signature spécifiée par le RR RRSIG couvrant ce RRset. DNSSEC ne change par la définition ou la fonction de la valeur TTL, qui est prévue pour maintenir la cohérence de la base dans les caches. Un résolveur cache purge les RRest de ses caches à la fin de la période spécifiée par les champs TTL et ces RRsets, sans regarder si le résolveur est sécurisé.

Les champs de création et d'expiration dans le RR RRSIG, spécifient la période durant laquelle la signature peut être utilisée pour valider les RRset couvert. Les signatures associées avec les données de zone signées sont seulement valides pour la période de temps spécifiés par ces champs dans les RR RRSIG en question. Les valeurs TTL ne peuvent pas étendre la période de validit des RRset signés dans le cache du résolveur, mais le résolveur peut utiliser le temps restant avant l'expiration du la période de validité de la signature d'un RRset comme limite supérieur pour le TTL du RRset signé et ses RR RRSIG associés dans le cache.

Problème de dépendance temporelle pour les zones

L'information dans une zone signée a une dépendance temporelle qui n'existe pas dans le protocole DNS original. Une zone signée nécessite une maintenance régulière pour s'assurer que chaque RRset dans la zone a un RR RRSIG valide. La période de validité de signature d'un RR RRSIG est un interval durant lequel la signature pour un RRset signé particulier peut être considéré comme valide, et les

signatures des différents RRset dans une zone peuvent expirer à des moments différents. Resigner un ou plusieurs RRset dans une zone va changer un ou plusieurs RR RRSIG, qui en retour nécessite d'incrémenter le numéro de série SOA de la zone pour indiquer qu'une zone a changé et resigner le RRset SOA lui-même. Donc, resigner un RRset dans une zone peut également déclencher des messages DNS NOTIFY et des opération de transfert de zone.

Considérations de serveur de nom

Un serveur de nom sécurisé devrait inclure les enregistrements DNSSEC appropriés (RRSIG, DNSKEY, DS, et NSEC) dans toutes les réponses aux requêtes des résolveurs qui ont signalé leur volonté de recevoir de tels enregistrement via l'utilisation du bit DO dans l'en-tête EDNS, sujet aux limitations de taille de message. À cause de l'ajout de ces RR DNSSEC pouvant facilement tronquer le message UDP et retourner en TCP, un serveur de nom sécurisé doit également supporter le mécanisme UPD "sender's UDP payload".

Si possible, la partie privée de chaque paire de clé DNSSEC devrait être conservée hors-ligne, mais ce n'est pas possible pour une zone pour laquelle les mises à jours dynamiques sont permis. Dans le cas des mises à jours dynamiques, le serveur maître primaire pour la zone doit resigner la zone quand elle est mise à jours, dont la clé privée correspondant à la ZSK doit être online. C'est une exemple de situation dans laquelle la capacité de séparer le RRset DNSKEY de la zone en ZSK et KSK peut être utile, vu que la KSK peut rester offline et peut avoir une durée de vie plus longue que les ZSK.

Par lui-même, DNSSEC n'est pas suffisant pour protéger l'intégrité d'une zone durant les opérations de transfert de zone, vu que même une zone signée contient des données non-signées, non-authoritatives si la zone a des enfants. Donc, les opérations de maintenance de zone nécessitent des mécanismes additionnels (tels que TSIG, SIG(0) ou IPsec)

Famille de document de sécurité DNS

Le jeu de document DNSSEC peut être partitionné en plusieurs groupes sous les documents du protocole DNS de base. Les jeu de document de protocole DNSSEC réfère à 3 documents qui forment le cœur des extensions de sécurité DNS :

1. Introduction et exigents pour la sécurité DNS (ce document)
2. Enregistrements de ressource pour les extensions de sécurité DNS (rfc4034)
3. Modification de protocole pour les extensions de sécurité DNS (rfc4035)

Le jeu de document de spécification d'algorithme de signature numérique réfère au groupe de documents qui décrivent comme les algorithmes de signature numérique devraient être implémentés dans DNSSEC. Voir la rfc4034 pour la liste des algorithmes définis.

Le jeu de documents de protocole d'authentification de transaction réfère au groupe de documents qui gérènt l'authentification des messages DNS, incluant l'établissement et la vérification des clé secrètes.

Je jeu de document d'utilisation des nouvelles sécurités réfère aux documents qui visent à utiliser les extensions de sécurité DNS proposés pour d'autres but de sécurité. DNSSEC ne fournis pas de sécurité directe pour ces nouvelles utilisations mais peuvent être utilisé pour les supporter. Les documents qui rentre dans cette catégorie incluent l'utilisation de DNS dans le stockage et la distribution de certificats