Groupe de travail Réseau
Request for Comments : 2930
Catégorie : En cours de normalisation

D. Eastlake 3, Motorola
September 2000
Traduction Claude Brière de L'Isle

Établissement de clé secrète pour le DNS (RR TKEY)

Statut du présent mémoire
Le présent document spécifie un protocole de l'Internet en cours de normalisation pour la communauté de l'Internet, et appelle à des discussions et suggestions pour son amélioration. Prière de se référer à l'édition en cours des "Normes officielles des protocoles de l'Internet" (STD 1) pour connaître l'état de la normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

Résumé
La [RFC2845] donne un moyen pour authentifier les interrogations et les réponses du système des noms de domaines (DNS, *Domain Name System*) en utilisant des clés secrètes partagées via l'enregistrement de ressource (RR, *Resource Record*) Signature de transaction (TSIG) . Cependant, elle ne fournit pas de mécanisme pour établir de telles clés autrement que par échange manuel. Le présent document décrit un RR Clé de transaction (TKEY, *Transaction Key*) qui peut être utilisé dans un certain nombre de différents modes pour établir des clés secrètes partagées entre un résolveur et un serveur DNS.

Remerciements
Les commentaires et les idées des personnes suivantes (par ordre alphabétique) ont été incorporés ici et elles en sont vivement remerciées : Olafur Gudmundsson (TIS), Stuart Kwan (Microsoft), Ed Lewis (TIS), Erik Nordmark (SUN),et Brian Wellington (Nominum).

Table des matières

1. Introduction....2
1.1 Vue générale du contenu....2
2. Enregistrement de ressource TKEY....2
2.1 Champ Nom....3
2.2 Champ TTL....3
2.3 Champ Algorithme....3
2.4 Champs Création et Expiration....3
2.5 Champ Mode....3
2.6 Champ Erreur....4
2.7 Champs Taille de clé et Données de clé....4
2.8 Champs Autre taille et Autres données....4
3. Considérations générales sur TKEY....4
4. Échange via interrogation de résolveur....5
4.1 Interrogation pour clés échangées par Diffie-Hellman....5
4.2 Interrogation pour suppression de TKEY....6
4.3 Interrogation pour établissement par GSS-API....6
4.4 Interrogation pour clés allouées par le serveur....6
4.5 Interrogation pour clés allouées par le résolveur....7
5. Inclusion spontanée par le serveur....7
5.1 Suppression de clé spontanée par le serveur....7
6. Méthodes de chiffrement....7
7. Considérations relatives à l'IANA....8
8. Considérations pour la sécurité....8
Références....8
Adresse de l'auteur....9
Déclaration complète de droits de reproduction....9

1. Introduction

Le système des noms de domaines (DNS) est une base de données hiérarchique, répartie, largement disponible, utilisée pour une transposition bidirectionnelle entre noms de domaines et adresses, pour l'acheminement de la messagerie électronique et pour d'autres informations [RFC1034], [RFC1035]. Il a été étendu pour pourvoir à la sécurité des clés publiques et à la mise à jour dynamique [RFC2535], [RFC2136]. On suppose que le lecteur est familiarisé avec ces RFC.

La [RFC2845] fournit un moyen pour authentifier efficacement les messages du DNS en utilisant des clés secrètes partagées via l'enregistrement de ressource (RR) TSIG mais elle ne fournit pas de mécanisme pour établir de telles clés autrement que par échange manuel. Le présent document spécifie un RR TKEY qui peut être utilisé dans un certain nombre de modes différents pour établir et supprimer de telles clés secrètes partagées entre un résolveur et un serveur DNS.

Noter que TKEY établit le matériel de clés et que les TSIG qui l'utilisent sont associés aux serveurs ou résolveurs DNS. Elles ne sont pas associées aux zones. Elles peuvent être utilisées pour authentifier les interrogations et les réponses mais elles ne fournissent pas l'origine des données DNS sur la base de la zone ni le déni d'authentification [RFC2535].

Certains modes de TKEY effectuent le chiffrement qui peut affecter leur statut d'export ou d'import pour certains pays. Les modes affectés spécifiés dans le présent document sont le mode alloué par le serveur et le mode alloué par le résolveur.

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

Dans tous les cas, le terme "résolveur" inclut la partie d'un serveur qui peut faire des interrogations de transfert de zone pleines et incrémentaires [RFC1995], transmettre des interrogations récurrentes, etc.

1.1 Vue générale du contenu

La Section 2 spécifie le RR TKEY et donne une description de ses champs constitutifs.
La Section 3 décrit les principes généraux du fonctionnement de TKEY.
La Section 4 expose l'accord sur les clés et leur suppression via les demandes DNS avec le code de fonctionnement Interrogation *(Query)* pour le type de RR TKEY. Cette méthode est applicable à tous les modes TKEY actuellement définis, bien que dans certains cas, ce ne soit pas ce qu'on appellerait intuitivement une "interrogation".
La Section 5 expose l'inclusion spontanée des RR TKEY dans les réponses par les serveurs qui ne sont actuellement utilisés que pour la suppression de clés.
La Section 6 décrit les méthodes de chiffrement pour transmettre les informations de clé secrète. Dans le présent document, elles ne sont utilisées que pour le mode alloué par le serveur et pour le mode alloué par le résolveur.
La Section 7 couvre les considérations relatives à l'allocation par l'IANA des modes TKEY.
Finalement, la Section 8 fournit les considérations obligatoires sur la sécurité.

2. Enregistrement de ressource TKEY

L'enregistrement de ressource TKEY a la structure indiquée ci-dessous. Son code de type de RR est 249.

Champ	**Type**	**Commentaire**
NAME	domaine	voir la description ci-dessous
TTYPE	u_int16_t	TKEY = 249
CLASS	u_int16_t	ignoré,DEVRAIT être 255 (ANY)
TTL	u_int32_t	ignoré, DEVRAIT être zéro
RDLEN	u_int16_t	taille de RDATA
RDATA		
Algorithme :	domaine	
Création :	u_int32_t	
Expiration :	u_int32_t	
Mode :	u_int16_t	
Erreur :	u_int16_t	
Taille de clé :	u_int16_t	
Données de clé :	flux d'octets	
Autre taille :	u_int16_t	
Autres données :	flux d'octets	non défini par cette spécification

2.1 Champ Nom

Le champ Nom se rapporte à la dénomination des clés. Sa signification diffère quelque peu selon le mode et le contexte, comme on l'explique dans les sections suivantes.

Sur tout serveur ou résolveur DNS, une seule chaîne d'octets de matériel de clé peut être en place pour un nom de clé particulier. Toute tentative d'établir un autre ensemble de matériel de clé sur un serveur pour un nom existant retourne une erreur BADNAME.

Pour un TKEY avec un nom qui n'est pas racine qui apparaît dans une interrogation, le nom du RR TKEY DEVRAIT être un domaine localement unique chez le résolveur, de moins de 128 octets de long en codage réseau, et ayant une signification pour que le résolveur distingue les clés et/ou les sessions d'accord de clés. Pour les TKEY qui apparaissent dans une réponse à une interrogation, le nom du RR TKEY DEVRAIT être un domaine unique au monde alloué par le serveur.

Un stratégie raisonnable de dénomination de clés est la suivante :
Si la clé est générée par suite d'une interrogation avec une racine comme nom de possesseur, le serveur DEVRAIT alors créer un nom de domaine unique au monde, pour qu'il soit le nom de la clé, en mettant en suffixe une étiquette pseudo aléatoire [RFC1750] avec un nom de domaine du serveur. Par exemple 89n3mDgX072pp.server1.example.com. Si la génération d'un nouveau nom pseudo aléatoire dans chaque cas est une charge de calcul excessive ou une perte d'entropie, un numéro de série en préfixe peut être ajouté à un nom fixe pseudo aléatoire généré au démarrage du serveur DNS, comme 1001.89n3mDgX072pp.server1.example.com.

Si la clé est générée par suite d'une interrogation avec un nom non racine, disons 789.resolver.example.net, utiliser alors l'enchaînement de cela avec un nom du serveur. Par exemple 789.resolver.example.net.server1.example.com.

2.2 Champ TTL

Le champ TTL n'a pas de signification dans les RR TKEY. Il DEVRAIT toujours être de zéro pour être sûr que les plus anciennes mises en œuvre du DNS ne mettent pas en antémémoire les RR TKEY.

2.3 Champ Algorithme

Le nom de l'algorithme a la forme d'un nom de domaine avec la même signification que dans la [RFC2845]. L'algorithme détermine comment le matériel de clé secrète sur lequel on s'est accordé pour utiliser le RR TKEY est en fait utilisé pour déduire les clés spécifiques de l'algorithme.

2.4 Champs Création et Expiration

L'heure de création et l'heure d'expiration sont en nombre de secondes depuis le 1er janvier 1970 00 h GMT en ignorant les secondes sautées, traité comme modulo 2**32 en utilisant l'arithmétique d'anneau [RFC1982]. Dans les messages entre un résolveur DNS et un serveur DNS où ces champs sont significatifs, ce sont l'intervalle de validité exigé pour le matériel de clé demandé, ou l'intervalle de validité du matériel de clé fourni.

Pour éviter des interprétations différentes des heures de création et d'expiration dans les RR TKEY, les résolveurs et serveurs qui les échangent doivent avoir la même idée de l'heure qu'il est. Une façon de le faire est de suivre le protocole NTP [RFC2030] mais cette synchronisation horaire ou toute autre utilisée à cette fin DOIT être sécurisée.

2.5 Champ Mode

Le champ Mode spécifie le schéma général de l'accord de clé ou l'objet du message DNS TKEY. Les serveurs et résolveurs conformes à la présente spécification DOIVENT mettre en œuvre le mode d'accord de clé Diffie-Hellman et le mode de suppression de clé pour les interrogations. Tous les autres modes sont FACULTATIFS. Un serveur qui prend en charge TKEY et qui reçoit une demande TKEY avec un mode qu'il n'accepte pas retourne l'erreur BADMODE. Les valeurs suivantes de l'octet Mode sont définies, disponibles, ou réservés :

Valeur	Description
0	réservé, voir la section 7
1	allocation par le serveur
2	échange Diffie-Hellman
3	négociation GSS-API4 allocation par le résolveur
5	suppression de clé
6-65534	disponible, voir la section 7
65535	réservé, voir la section 7

2.6 Champ Erreur

Le champ Code d'erreur est un RCODE étendu. Les valeurs suivantes sont définies :

Valeur	Description
0	pas d'erreur
1-15	RCODE non étendu
16	BADSIG (TSIG)
17	BADKEY (TSIG)
18	BADTIME (TSIG)
19	BADMODE
20	BADNAME
21	BADALG

Lorsque le champ Erreur TKEY est différent de zéro dans une réponse à une interrogation TKEY, le champ RCODE de l'en-tête DNS n'indique pas d'erreur. Cependant, il est possible si une TKEY est spontanément incluse dans une réponse que le RR TKEY et le champ Erreur de l'en-tête DNS aient des codes d'erreur différents de zéro sans rapport entre eux.

2.7 Champs Taille de clé et Données de clé

Le champ Taille des données de clé est un entier non signé de 16 bits dans l'ordre du réseau, qui spécifie la taille du champ de données d'échange de clé en octets. La signification de ces données dépend du mode.

2.8 Champs Autre taille et Autres données

Les champs Autre taille et Autres données ne sont pas utilisés dans la présente spécification mais pourraient être utilisés dans de futures extensions. Le champ RDLEN DOIT être égal à la longueur de la section RDATA jusqu'à la fin de Autres données sinon le RR sera considéré comme mal formé et rejeté.

3. Considérations générales sur TKEY

TKEY est un méta-RR qui n'est pas mémorisé ni mis en antémémoire dans le DNS et qui n'apparaît pas dans les fichiers de zone. Il prend en charge divers modes pour l'établissement et la suppression des informations de clés secrètes entre les résolveurs et serveurs DNS. L'établissement de telles clés partagées exige que l'état soit maintenu aux deux extrémités et l'exigence que l'allocation des ressources maintienne de tels états peut requérir un accord mutuel. En l'absence de volonté de fournir un tel état, les serveurs DOIVENT retourner des erreurs telles que NOTIMP ou REFUSED face à des tentatives d'utilisation de TKEY et les résolveurs ont toute liberté pour ignorer les RR TKEY qu'ils reçoivent.

Le matériel de clé secrète partagée développé en utilisant TKEY est une pure séquence d'octets. Les moyens par lesquels ce matériel de clé secrète partagée échangé via TKEY est en fait utilisé dans un algorithme TSIG particulier dépend de l'algorithme et est défini en connexion avec cet algorithme. Par exemple, voir dans la [RFC2104] comment le matériel de clé secrète accepté de TKEY est utilisé dans l'algorithme HMAC-MD5 ou d'autres algorithmes HMAC.

Il NE DOIT PAS y avoir plus d'un RR TKEY dans une interrogation ou réponse DNS.

Sauf en mode GSS-API, les réponses TKEY DOIVENT toujours avoir l'authentification de transaction DNS pour protéger l'intégrité de toutes données de clé, des codes d'erreur, etc. Cette authentification DOIT utiliser une clé secrète précédemment établie (TSIG) ou publique (SIG(0) [RFC2931]) et NE DOIT PAS utiliser de clé que la réponse à vérifier fournit elle-même.

Les interrogations TKEY DOIVENT être authentifiées pour tous les modes excepté GSS-API et, dans quelques circonstances, le mode d'allocation par le serveur. En particulier, si l'interrogation pour une clé allouée par un serveur est qu'une clé affirme un certain privilège, comme d'autorité de mise à jour, l'interrogation doit alors être authentifiée pour éviter les mystifications. Cependant, si la clé est juste destinée à la sécurité d'une transaction, la mystification conduirait au pire à un déni de service. L'authentification d'interrogation DEVRAIT utiliser un authentificateur établi de clé secrète (TSIG) si il en est de disponible. Autrement, elle doit utiliser une signature de clé publique (SIG(0)). Elle NE DOIT PAS utiliser de clé que l'interrogation fournirait elle-même.

En l'absence de l'authentification TKEY requise, une erreur NOTAUTH DOIT être retournée.

Pour éviter les attaques en répétition, il est nécessaire qu'une réponse ou interrogation TKEY ne soit pas valide si elle est répétée dans les 2**32 secondes (environ 136 ans) ou un de ses multiples, ultérieurement. Pour réaliser cela, le matériel de clé utilisé dans tout RR TSIG ou SIG(0) qui authentifie un message TKEY NE DOIT PAS avoir une durée de vie de plus de 2**31 - 1 s (environ 68 ans). Donc, sur les tentatives de répétition, le RR TSIG ou SIG(0) authentifiant ne sera pas vérifiable du fait de l'expiration de la clé et la répétition va échouer.

4. Échange via interrogation de résolveur

Une méthode pour qu'un résolveur et un serveur se mettent d'accord sur du matériel de clé secrète partagée à utiliser dans TSIG est par des demandes DNS provenant du résolveur qui sont syntaxiquement des interrogations DNS pour le type TKEY. De telles interrogations DOIVENT être accompagnées par un RR TKEY dans la section informations supplémentaires pour indiquer le mode utilisé, ainsi que par d'autres informations si nécessaire.

Les interrogations de type TKEY NE DEVRAIENPAS avoir de fanion les marquant comme récurrentes et les serveurs PEUVENT ignorer le bit d'en-tête récurrent dans les interrogations TKEY qu'ils reçoivent.

4.1 Interrogation pour clés échangées par Diffie-Hellman

L'échange de clés Diffie-Hellman (DH) est un moyen par lequel deux parties peuvent déduire des informations de secret partagé sans exiger aucun secret du message qu'ils échangent [Schneier]. Des dispositions ont été prises pour la mémorisation des clés publiques DH dans le DNS [RFC2539].

Un résolveur envoie une interrogation pour un TKEY Type accompagné par un RR TKEY dans la section des informations supplémentaires spécifiant le mode Diffie-Hellman et accompagné par un RR KEY lui aussi dans la section des informations supplémentaires, spécifiant une clé Diffie-Hellman de résolveur. Le champ Algorithme du RR TKEY est réglé à l'algorithme d'authentification que le résolveur projette d'utiliser. Les "données de clé" fournies dans le TKEY sont utilisées comme nom occasionnel aléatoire [RFC1750] pour éviter de déduire toujours le même matériel de clé pour la même paire de KEY DH.

La réponse du serveur contient une TKEY dans sa section Réponse avec le mode Diffie-Hellman. Les "données de clé" fournies dans cette TKEY sont utilisées comme nom occasionnel supplémentaire pour éviter de déduire toujours le même matériel de clés pour la même paire de clés DH. Si le champ Erreur de la TKEY n'est pas à zéro, l'interrogation a échoué pour la raison donnée. FORMERR est donné si l'interrogation n'incluait pas de clé DH, et BADKEY est donné si l'interrogation incluait une clé DH incompatible.

Si le champ Erreur de la TKEY est à zéro, le RR KEY Diffie-Hellman fourni par le résolveur DEVRAIT être mis en écho dans la section des informations supplémentaires et un RR KEY Diffie-Hellman de serveur sera aussi présent dans la section réponse de la réponse. Les deux parties peuvent alors calculer la même quantité de secret partagé à partir de la paire de clés Diffie-Hellman utilisée [Schneier] (pourvu que ces clés DH utilisent le même générateur et modulo) et des données dans les RR TKEY. Les données du RR TKEY sont mélangées avec le résultat DH comme suit :

1048/0

matériel de clé = OUX (valeur DH, MD5 (données d'interrogation | valeur DH) | MD5 (données du serveur | valeur DH))

où OUX est une opération OU exclusif et "|" est l'enchaînement de flux d'octet. Le plus court de ces deux opérandes pour OUX est justifié à gauche par octet et bourré d'octets de valeur zéro pour correspondre à la longueur de l'autre opérande. "Valeur DH" est la valeur Diffie-Hellman déduite des RR KEY. Les données d'interrogation et les données de serveur sont les valeurs envoyées dans les champs de données du RR TKEY. Ces noms occasionnels "données d'interrogation" et "données de serveur" reçoivent en suffixe la valeur DH, résumée par MD5, les résultats sont concaténés, puis traités par l'opérateur OUX avec la valeur DH.

Les heures de création et d'expiration dans le RR TKEY d'interrogation sont celles demandées pour le matériel de clé. Les heures de création et d'expiration dans le RR TKEY de réponse sont la période maximum pendant laquelle le serveur va considérer que le matériel de clé est valide. Les serveurs peuvent "pré expirer" les clés de sorte que ceci n'est pas garanti.

4.2 Interrogation pour suppression de TKEY

Les clés établies via TKEY peuvent être traitées comme des états conditionnels. Comme les transactions du DNS sont générées par le résolveur, celui-ci peut simplement jeter les clés, quoique il pourrait devoir passer par un autre échange de clés si il a ultérieurement besoin d'une clé. De même, le serveur peut éliminer les clés bien qu'il en résulte une erreur à réception d'une interrogation avec un TSIG qui utilisé la clé éliminée.

Pour éviter de tenter de s'appuyer dans les demandes sur des clés qui ne sont plus en service, les serveurs DOIVENT mettre en œuvre la suppression de clé par laquelle le serveur "élimine" une clé à réception de la part d'un résolveur d'une demande authentifiée de suppression pour un RR TKEY avec le nom de la clé. Si le serveur n'a pas d'enregistrement de clé portant ce nom, il retourne BADNAME.

Les interrogations TKEY de suppression de clé DOIVENT être authentifiées. Cette authentification PEUT être un RR TSIG qui utilise la clé à éliminer.

Pour les clés allouées par l'interrogateur et les clés Diffie-Hellman, le serveur DOIT vraiment "éliminer" tous les états actifs associés à la clé. Pour les clés allouées par le serveur, celui-ci PEUT simplement marquer la clé comme n'étant plus retenue par le client et peut la renvoyer en réponse à une interrogation future pour du matériel de clé alloué par le serveur.

4.3 Interrogation pour établissement par GSS-API

Ce mode est décrit dans un autre document en préparation auquel on devrait se reporter pour sa description complète. En gros, le résolveur et le serveur peuvent échanger des interrogations et des réponses pour le TKEY Type avec un RR TKEY qui spécifie le mode GSS-API dans la section des informations supplémentaires et un jeton GSS-API dans la portion Données de clé du RR TKEY.

Toutes les questions de possible chiffrement de parties des données du jeton GSS-API qui pourraient être transmises sont traitées par le niveau GSS-API. De plus, le niveau GSS-API fournit sa propre authentification de sorte que ce mode d'interrogation et réponse TKEY PEUT être, bien qu'il n'ait pas besoin de le faire, authentifié avec un RR TSIG ou un RR SIG(0) [RFC2931].

Les heures de création et d'expiration dans un RR TKEY en mode GSS-API sont ignorées.

4.4 Interrogation pour clés allouées par le serveur

Facultativement, le serveur peut allouer du matériel de clé pour le résolveur. Il envoie au résolveur en chiffré sous une clé publique du résolveur. Voir à la section 6 la description des méthodes de chiffrement.

Un résolveur envoie une interrogation pour une TKEY Type accompagnée d'un RR TKEY qui spécifie le mode "allocation par le serveur" et un RR TKEY de résolveur à utiliser pour chiffrer la réponse, tous deux dans la section des informations supplémentaires. Le champ Algorithme de la TKEY est réglé à l'algorithme d'authentification que le résolveur prévoit d'utiliser. Il est RECOMMANDÉ que toutes "données de clé" fournies dans le RR TKEY d'interrogation par le résolveur soient fortement mélangées par le serveur avec un aléa généré par le serveur [RFC1750] pour déduire le matériel de clé à utiliser. Le RR KEY qui apparaît dans l'interrogation n'a pas besoin d'être accompagné par un RR SIG(KEY). Si l'interrogation est authentifiée par le résolveur avec un RR TSIG [RFC2845] ou un RR SIG(0) et si cette authentification est vérifiée, toute SIG(KEY) fournie alors dans l'interrogation DEVRAIT être ignorée. Le RR KEY dans une telle interrogation DEVRAIT avoir un nom qui corresponde au résolveur mais il est seulement essentiel que ce soit une clé publique pour laquelle le résolveur a la clé privée correspondante afin qu'il puisse déchiffrer les données de la réponse.

La réponse du serveur contient un RR TKEY dans sa section Réponse avec le mode alloué par le serveur et fait écho au RR KEY fourni dans l'interrogation dans sa section des informations supplémentaires.

Si le champ Erreur de la TKEY de réponse est à zéro, la portion Données de clé du RR TKEY de la réponse sera les données de clé allouées par le serveur chiffrées avec la clé publique figurant dans le RR KEY fourni par le résolveur. Dans ce cas, le nom de possesseur du RR TKEY de la réponse sera le nom de clé alloué par le serveur.

Si le champ Erreur de la TKEY de réponse est différent de zéro, l'interrogation a échoué pour la raison donnée. FORMERR est donné si l'interrogation ne spécifiait pas de clé de chiffrement.

Les heures de création et d'expiration dans le RR TKEY de l'interrogation sont celles demandées pour le matériel de clé. Les heures de création et d'expiration dans le TKEY de réponse sont la période maximum pendant laquelle le serveur va considérer le matériel de clé comme valide. Les serveurs peuvent "pré expirer" les clés, de sorte que ceci ne constitue pas une garantie.

Le RR KEY de résolveur DOIT être authentifié, au moyen de l'authentification de cette interrogation avec une TSIG ou SIG(0) ou la signature de la clé du résolveur avec une SIG(KEY). Autrement, un attaquant pourrait falsifier une clé de résolveur pour laquelle il connaît la clé privée, et par ce moyen, l'attaquant pourrait obtenir une clé secrète partagée valide du serveur.

4.5 Interrogation pour clés allouées par le résolveur

Facultativement, un serveur peut accepter des clés allouées par un résolveur. Le matériel de clé DOIT être chiffré avec une clé de serveur pour la protection durant la transmission comme décrit à la Section 6.

Le résolveur envoie une interrogation TKEY avec un RR TKEY qui spécifie le matériel de clé chiffré et un RR KEY qui spécifie la clé publique du serveur utilisée pour chiffrer les données, tous deux dans la section des informations supplémentaires. Le nom de la clé et les données de clé sont complètement contrôlées par le résolveur qui envoie et un nom de clé unique au monde DEVRAIT être utilisé. Le RR KEY utilisé DOIT être un de ceux dont le serveur a la clé privée correspondante, ou il ne sera pas capable de déchiffrer le matériel de clé et va retourner une erreur FORMERR. Il est aussi important qu'aucune partie qui n'est pas de confiance (de préférence aucune autre partie que le serveur) ait la clé privée correspondant au RR KEY parce que, si c'était le cas, elle pourrait capturer les messages au serveur, apprendre le secret partagé, et simuler des TSIG valides.

L'heure de création et d'expiration du RR TKEY d'interrogation donne la période pendant laquelle l'interrogateur à l'intention de considérer le matériel de clé comme valide. Le serveur peut retourner un intervalle de temps plus court pour annoncer qu'il ne veut pas conserver l'état aussi longtemps et peut dans tous les cas faire périmer les clés.

Ce mode d'interrogation DOIT être authentifié avec une TSIG ou SIG(0). Autrement, un attaquant pourrait simuler une interrogation TKEY allouée par un résolveur, et ainsi il pourrait spécifier une clé secrète partagée qui serait acceptée, utilisée, et honorée par le serveur.

5. Inclusion spontanée par le serveur

Un serveur DNS peut inclure spontanément un RR TKEY comme informations supplémentaires dans les réponses. Cela ne DEVRAIT être fait que si le serveur sait que l'interrogateur comprend la TKEY et a cette option de mise en œuvre. Cette technique peut être utilisée pour supprimer une clé et peut être spécifié pour les modes qui seront définis à l'avenir. Un inconvénient de cette technique est qu'il n'y a pas de moyen pour le serveur d'obtenir d'indication d'erreur ou de succès en retour et, dans le cas de UDP, aucun moyen même de savoir si la réponse DNS a atteint le résolveur.

5.1 Suppression de clé spontanée par le serveur

Un serveur peut facultativement dire à un client qu'il a supprimé une clé secrète en incluant spontanément un RR TKEY dans la section des informations supplémentaires d'une réponse avec le nom de la clé et en spécifiant le mode de suppression de la clé. Une telle réponse DEVRAIT être authentifiée. Si elle est authentifiée, elle "supprime" la clé qui porte ce nom. Les heures de création et d'expiration du RR TKEY de suppression sont ignorées. L'échec par un client à recevoir ou traiter correctement de telles informations supplémentaires dans une réponse signifierait que le client pourrait utiliser une clé que le serveur avait éliminée et il obtiendrait alors une indication d'erreur.

Pour les clés Diffie-Hellman et celles allouées par le serveur, le client DOIT "éliminer" l'état actif associé à la clé. Pour les clés allouées par l'interrogateur, celui-ci PEUT simplement marquer la clé comme n'étant plus retenue par le serveur et peut la réutiliser dans une interrogation future spécifiant du matériel de clé alloué par l'interrogateur.

6. Méthodes de chiffrement

Pour les modes d'accord de clé alloué par le serveur et alloué par le résolveur, le matériel de clé est envoyé au sein du champ données de clé d'un RR TKEY chiffré avec la clé publique dans un RR KEY d'accompagnement [RFC2535]. Ce RR KEY DOIT

être pour un algorithme de clé publique où les clés publique et privée peuvent être utilisées pour le chiffrement et le déchiffrement correspondant qui récupère les données chiffrées à l'origine. Le RR KEY DEVRAIT correspondre à un nom pour le résolveur/serveur qui déchiffre de telle sorte que le processus de déchiffrement ait accès à la clé privée correspondante pour déchiffrer les données. Le matériel de clé secrète qui est envoyé va généralement être très court, habituellement moins de 256 bits, parce que c'est adéquat pour une très forte protection avec les algorithmes modernes de hachage de clé ou de clé symétrique.

Si le RR KEY spécifie l'algorithme RSA, le matériel de clé est alors chiffré selon la description du chiffrement RSAES-PKCS1-v1_5 dans PKCS#1 [RFC2437]. (Noter que le matériel de clé secrète envoyé est directement chiffré en RSA en format PKCS#1. Il n'est pas "enveloppé" dans un autre algorithme symétrique.) Dans le cas peu vraisemblable où le matériel de clé ne tiendrait pas dans un seul module RSA de la clé publique choisie, des blocs de chiffrement RSA supplémentaires sont inclus. La longueur de chaque bloc est claire d'après la clé publique RSA spécifiée et le bourrage RSAES-PKCS1-v1_5 précise quelle partie des données chiffrées est en fait le matériel de clé et quelle partie est du formatage ou le bourrage exigé d'au moins huit octets d'aléa [RFC1750].

7. Considérations relatives à l'IANA

La présente section est à interpréter comme prévu dans la [RFC2434].

Les valeurs du champ Mode 0x0000 et 0xFFFF sont réservées.

Les valeurs du champ Mode de 0x0001 à 0x00FF, et de 0XFF00 à 0XFFFE ne peuvent être allouées que par action de normalisation de l'IETF.

Les valeurs du champ Mode de 0x0100 à 0x0FFF et de 0xF0000 à 0xFEFF sont allouées par approbation de l'IESG ou consensus de l'IETF.

Les valeurs du champ Mode de 0x1000 à 0xEFFF sont allouées sur la base de la spécification exigée définie dans la [RFC2434].

Les valeurs de Mode ne devraient pas être changées lorsque le statut de leur utilisation change. Par exemple, une valeur de mode allouée sur la base de la seule fourniture d'une spécification ne devrait pas être changée ultérieurement simplement parce que le statut de cette utilisation a changé sur la voie de la normalisation.

Les allocations suivantes sont documentées ici :

RR Type 249 pour TKEY.

Modes TKEY 1 à 5 comme donné au paragraphe 2.5.

Valeurs d'erreur de RCODE étendues de 19, 20, et 21 comme donné au paragraphe 2.6.

8. Considérations pour la sécurité

Cette spécification est toute entière concernée par l'établissement sûr d'un secret partagé entre les clients et les serveurs DNS pour la prise en charge de SIG [RFC2845].

La protection contre le déni de service via l'utilisation de TKEY n'est pas fournie.

Références

[RFC1034] P. Mockapetris, "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.

[RFC1750] D. Eastlake, 3rd et autres, "Recommandations d'aléa pour la sécurité", décembre 1994. *(Voir la RFC4086)*

[RFC1982] R. Elz, R. Bush, "Arithmétique des numéros de série", août 1996. (*MàJ* RFC1034, RFC1035) *(P.S.)*

[RFC1995] M. Ohta, "Transferts de zone par incréments dans le DNS", août 1996.

[RFC2030] D. Mills, "Protocole simple de l'heure du réseau (SNTP) version 4 pour IPv4, IPv6 et OSI", octobre 1996. *(Rendue*

obsolète par la RFC4330)

[RFC2104] H. Krawczyk, M. Bellare, R. Canetti, "HMAC : Hachage de clés pour l'authentification de message", février 1997.

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

[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.

[RFC2434] T. Narten et H. Alvestrand, "Lignes directrices pour la rédaction d'une section Considérations relatives à l'IANA dans les RFC", BCP 26, octobre, 1998. *(Rendue obsolète par la RFC5226)*

[RFC2437] B. Kaliski et J. Staddon, "PKCS n° 1 : Spécifications de la cryptographie RSA version 2.0", octobre 1998. *(Obsolète, voir RFC3447) (Information)*

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

[RFC2539] D. Eastlake 3rd, "Mémorisation des clés Diffie-Hellman dans le système des noms de domaines (DNS)", mars 1999.

[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.)*

[Schneier] Bruce Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C", 1996, John Wiley and Sons

Adresse de l'auteur

Donald E. Eastlake 3rd
Motorola
140 Forest Avenue
Hudson, MA 01749 USA
téléphone : +1 978-562-2827 (dom) / +1 508-261-5434 (bureau)
Fax : +1 508-261-4447 (bureau)
mél : Donald.Eastlake@motorola.com

Déclaration complète de droits de reproduction

Remerciement
Le financement de la fonction d'éditeur des RFC est actuellement assuré par la Internet Society.