Internet Engineering Task Force (IETF)
Request for Comments : 8945
STD 93
RFC rendues obsolètes : 2845, 4635
Catégorie : Sur la voie de la normalisation
ISSN : 2070-1721
Traduction Claude Brière de L'Isle

F. Dupont, ISC
S. Morris
P. Vixie, Farsight
D. Eastlake 3rd, Futurewei
O. Gudmundsson, Cloudflare
B. Wellington, Akamai
novembre 2020

Authentification de transaction de clé secrète pour le DNS (TSIG)

Résumé
Le présent document décrit un protocole pour l'authentification au niveau de la transaction utilisant des secrets partagés et un hachage unidirectionnel. Il peut être utilisé pour authentifier des mises à jour dynamiques d'une zone du DNS comme venant d'un client approuvé ou pour authentifier des réponses comme venant d'un serveur de noms approuvé.

Aucune recommandation n'est faite ici pour distribuer les secrets partagés ; on s'attend à ce qu'un administrateur de réseau configure statiquement les serveurs de noms et les clients en utilisant un mécanisme hors bande.

Le présent document rend obsolètes les RFC 2845 et 4635.

Statut de ce mémoire
Ceci est un document de l'Internet sur la voie de la normalisation.

Le présent document a été produit par l'équipe d'ingénierie de l'Internet (IETF). Il représente le consensus de la communauté de l'IETF. Il a subi une révision publique et sa publication a été approuvée par le groupe de pilotage de l'ingénierie de l'Internet (IESG). Tous les documents approuvés par l'IESG ne sont pas candidats à devenir une norme de l'Internet ; voir la Section 2 de la RFC5741.

Les informations sur le statut actuel du présent document, tout errata, et comment fournir des réactions sur lui peuvent être obtenues à http://www.rfc-editor.org/info/rfc8945 .

Table des matières

1. Introduction

1.1 Fondements

Le système des noms de domaines (DNS, *Domain Name System*) ([RFC1034], [RFC1035]) est un système de bases de données hiérarchiques dupliquées réparties qui fournissent des informations fondamentales pour les opérations de l'Internet, comme la traduction de nom en adresse et les informations pour le traitement de la messagerie.

Le présent document spécifie l'utilisation d'un code d'authentification de message (MAC, *Message Authentication Code*) généré en utilisant certaines fonctions de hachage chiffré, pour fournir un moyen efficace d'authentification en point à point et de vérification d'intégrité pour les transactions du DNS. Ces transactions incluent les demandes et les réponses de mise à jour du DNS pour lesquelles cela peut fournir une solution de remplacement légère au protocole de mise à jour dynamique sûre du DNS décrit par la [RFC3007].

Une autre utilisation de ce mécanisme est de protéger les transferts de zone. Dans ce cas, les données couvertes vont être le transfert de zone entier incluant tous les enregistrements de glu envoyés. Le protocole décrit par DNSSEC ([RFC4033], [RFC4034], [RFC4035]) ne protège pas les enregistrements glu ni les enregistrements non signés.

Le mécanisme d'authentification proposé ici fournit une authentification simple et efficace entre les clients et les serveurs, en utilisant des clés secrètes partagées pour établir une relation de confiance entre deux entités. Ces clés doivent être protégées d'une manière similaire à celle des clés privées, à moins qu'un tiers se fasse passer pour une des parties prévues (en falsifiant le MAC). La proposition ne convient pas pour l'authentification générale de serveur à serveur et pour les serveurs qui parlent à de nombreux autres serveurs, car la gestion de clés devient ingérable lorsque le nombre de clés partagées augmente de façon quadratique. Mais il convient pour de nombreux résolveurs sur des hôtes qui ne parlent qu'à quelques serveurs récurrents.

1.2 Vue d'ensemble du protocole

L'authentification de transaction de clé secrète utilise des signatures sur les messages envoyés entre les parties impliquées (par exemple, résolveur et serveur). Elles sont appelées des "signatures de transaction", ou TSIG. Pour des raisons historiques, dans ce document, elles sont appelées des codes d'authentification de message (MAC, *Message Authentication Code*).

L'utilisation de TSIG suppose un accord préalable entre les deux parties impliquées (par exemple, résolveur et serveur) sur tous algorithmes et clés à utiliser. La façon dont cet accord est obtenu sort du domaine d'application de ce document.

Un échange de messages DNS implique l'envoi d'une interrogation et la réception d'un ou plusieurs messages DNS en réponse. Pour l'interrogation, le MAC est calculé sur la base du hachage du contenu et de la clé de TSIG acceptée. Le MAC pour la réponse est similaire mais inclut aussi le MAC de l'interrogation au titre du calcul. Lorsque une réponse comporte plusieurs paquets, le calcul du MAC associé au second paquet et aux suivants inclut dans ses entrées le MAC pour le paquet précédant. De cette façon, il est possible de détecter toute interruption de la suite de paquets, mais pas sa termination prématurée.

Le MAC est contenu dans un enregistrement de ressource TSIG inclus dans la section supplémentaire du message DNS.

1.3 Historique du document

TSIG était à l'origine spécifié dans la [RFC2845]. En 2017, deux mises en œuvre de serveur de noms suivant strictement ce document (et la [RFC4635] qui s'y rapporte) se sont trouvées avoir des problèmes de sécurité relatifs à cette caractéristique ([CVE-2017-3142], [CVE-2017-3143], [CVE-2017-11104]). Les mises en œuvre ont été corrigées, mais pour éviter des problèmes similaires à l'avenir, les deux documents ont été mis à jour et fusionnés, produisant cette spécification révisée pour TSIG.

Bien que les mises en œuvre de TSIG en accord avec la présente RFC assurent une sécurité améliorée, il n'y a pas de changement de l'interopérabilité. TSIG sur le réseau est toujours le même mécanisme que décrit dans la [RFC2845] ; seule la sémantique de vérification a été changée. Voir les détails au paragraphe 10.1.

2. Mots clés

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119], [RFC8174] quand, et seulement quand ils apparaissent tout en majuscules, comme montré ci-dessus.

3. Numéros alloués

Le présent document définit le type d'enregistrement de ressource (RR, *Resource Record*) et la valeur associée :

TSIG (250)

De plus, le document définit aussi les RCODE DNS et les noms associés :
16 (BADSIG) *(mauvaise signature)*
17 (BADKEY) *(mauvaise clé)*
18 (BADTIME) *(mauvaise heure)*
22 (BADTRUNC) *(mauvaise troncature)*

(Voir au paragraphe 2.3 de la [RFC6895] l'allocation de la valeur 16 à BADSIG.)

Ces RCODE peuvent apparaître dans le champ "Erreur" d'un RR TSIG.

4. Format de RR TSIG

4.1 Type de RR TSIG

Pour assurer l'authentification de la clé secrète, on utilise un type de RR dont le mnémonique est TSIG et dont le code de type est 250. TSIG est un méta-RR et NE DOIT PAS être mis en antémémoire. Les RR TSIG sont utilisés pour l'authentification entre des entités du DNS qui ont établi une clé secrète partagée. Les RR TSIG sont calculés de façon dynamique pour couvrir une transaction DNS particulière et ne sont pas des RR du DNS au sens usuel.

Comme les RR TSIG se rapportent à une demande/réponse DNS, il ne sert à rien de les mémoriser ou de les retransmettre ; donc, le RR TSIG est éliminé une fois qu'il a été utilisé pour authentifier un message DNS.

4.2 Format d'enregistrement TSIG

Les champs du RR TSIG sont décrits ci-après. Tous les entiers multi-octets dans l'enregistrement sont envoyés dans l'ordre des octets du réseau (voir le paragraphe 2.3.2 de la [RFC1035]).

Nom : nom de la clé utilisée, dans la syntaxe de nom de domaine. Le nom devrait refléter les noms des hôtes et identifier de façon univoque la clé parmi un ensemble de clés que ces deux hôtes peuvent partager à tout moment. Par exemple, si les hôtes A.site.exemple et B.exemple.net partagent une clé, les possibilités pour le nom de la clé incluent <id>.A.site.exemple, <id>.B.exemple.net, et <id>.A.site.exemple.B.exemple.net. Il devrait être possible que plus d'une clé soient utilisées simultanément parmi un ensemble d'hôtes interagissants. Cela permet une rotation périodique des clés selon les pratiques de fonctionnement des hôtes, ainsi que l'agilité d'algorithme indiquée par la [RFC7696].

Le nom peut être utilisé comme indice local de la clé impliquée, mais il est recommandé qu'elle soit unique au monde. Lorsque une clé est juste partagée entre deux hôtes, son nom a seulement besoin d'être significatif entre eux, mais il est recommandé que le nom de la clé soit mnémonique et incorpore les noms des agents ou des ressources participants comme suggéré ci-dessus.

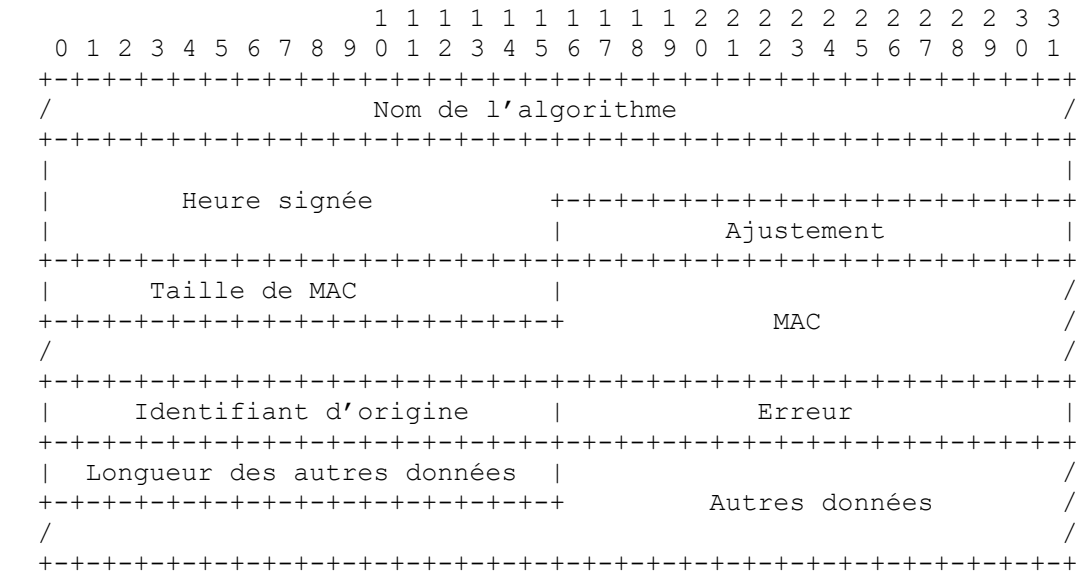
Type : ce DOIT être TSIG (250 : Signature de transaction).

Classe : ce DOIT être ANY.

TTL : ce DOIT être 0.

RDLENGTH : (variable)

RDATA : les RDATA pour un RR TSIG consistent en un certain nombre de champs, décrits ci-dessous :



Le contenu des champs RDATA est :

Nom d'algorithme : séquence d'octets qui identifie l'algorithme TSIG dans la syntaxe de nom de domaine. (Les noms permis sont énumérés dans le Tableau 3.) Le nom est mémorisé dans le format de nom DNS du réseau comme décrit dans la [RFC1034]. Selon la [RFC3597], ce nom NE DOIT PAS être compressé.

Heure signée : entier non signé de 48 bits contenant l'heure de signature du message en secondes depuis 00:00 le 1er janvier 1970 UTC, en ignorant les sauts de secondes.

Ajustement : entier non signé de 16 bits qui spécifie la différence d'heure permise en secondes dans le champ Heure signée.

Taille de MAC : entier non signé de 16 bits qui donne la longueur du champ MAC en octets. La troncature est indiquée par une taille de MAC inférieure à la taille du hachage chiffré produit par l'algorithme spécifié par le Nom d'algorithme.

MAC : séquence d'octets dont le contenu est défini par l'algorithme TSIG utilisé, éventuellement tronqué comme spécifié par la taille de MAC. La longueur de ce champ est donnée par la taille de MAC. Le calcul du MAC est précisé au paragraphe 4.3.

Identifiant d'origine : entier non signé de 16 bits contenant l'identifiant de message du message de demande d'origine. Pour un RR TSIG sur une demande, il est réglé égal à l'identifiant du message DNS. Dans une TSIG attachée à une réponse -- ou dans des cas comme la transmission d'une demande de mise à jour dynamique – le champ contient l'identifiant de la demande DNS originale.

Erreur : dans les réponses, entier non signé de 16 bits contenant le RCODE étendu couvrant le traitement TSIG. Dans les demandes, ce DOIT être zéro.

Longueur des autres données : entier non signé de 16 bits qui spécifie la longueur du champ Autres données en octets.

Autres données : données supplémentaires relevant de l'enregistrement TSIG. Dans les réponses, il va être vide (c'est-à-dire, Longueur des autres données va être zéro) sauf si le contenu du champ Erreur est BADTIME, et dans ce cas, il va être un entier non signé de 48 bits contenant l'heure actuelle du serveur comme nombre de secondes depuis 00:00 le 1er janvier 1970 UTC, en ignorant les sauts de secondes (voir le paragraphe 5.2.3). Le présent document n'accorde aucune signification à ce contenu dans les demandes.

4.3 Calcul du MAC

Quand on génère ou vérifie le contenu d'un enregistrement TSIG, les données mentionnées dans le reste de ce paragraphe sont passées, dans l'ordre mentionné ci-dessous, comme entrées au calcul de MAC. Les données sont passées dans l'ordre des octets du réseau ou format du réseau, comme approprié et sont entrées dans la fonction de hachage comme une séquence d'octets continue sans séparateur ou bourrage entre les champs.

4.3.1 MAC de demande

Inclus seulement dans le calcul d'un MAC pour un message de réponse (ou le premier message dans une réponse multi-messages) le MAC de demande validé DOIT être inclus dans le calcul de MAC. Si le MAC de demande échoue à la validation, un message d'erreur non signé DOIT être retourné (paragraphe 5.3.2).

Le MAC de la demande, comportant les champs suivants, est résumé dans le format du réseau :

Champ	Type	Description
Taille de MAC	Entier non signé de 16 bits	dans l'ordre des octets du réseau
Données de MAC	Séquence d'octets	exactement comme transmises

Tableau 1 : MAC de demande

Des considérations particulières s'appliquent au calcul de TSIG pour le second message et les suivants dans une réponse qui consiste en plusieurs messages DNS (par exemple, un transfert de zone). Elles sont décrites au paragraphe 5.3.1.

4.3.2 Message DNS

Dans le calcul de MAC, le message DNS complet dans le format du réseau est utilisé.

Lors de la création d'un message sortant, la TSIG est fondée sur le contenu du message avant que le RR TSIG ait été ajouté à la section supplémentaire et avant que le ARCOUNT de l'en-tête du message DNS ait été incrémenté pour inclure le RR TSIG.

Quand on vérifie un message entrant, la TSIG est vérifiée par rapport au message après la suppression du RR TSIG, le ARCOUNT décrémenté, et l'identifiant de message remplacé par l'identifiant d'origine du message provenant de la TSIG si ces identifiants diffèrent. (Cela pourrait arriver, par exemple, lors de la transmission d'une demande de mise à jour

dynamique.)

4.3.3 Variables TSIG

Certaines informations présentes dans le RR TSIG sont aussi incluses dans le résumé. Ajouter ces données fournit une protection supplémentaire contre une tentatice d'interférer avec le message.

Source	Nom du champ	Notes
TSIG RR	NOM	nom de clé, en format canonique du réseau
TSIG RR	CLASSE	DOIT être ANY
TSIG RR	TTL	DOIT être 0
TSIG RDATA	Nom d'algorithme	en format canonique du réseau
TSIG RDATA	Heure signée	dans l'ordre des octets du réseau
TSIG RDATA	Ajustement	dans l'ordre des octets du réseau
TSIG RDATA	Erreur	dans l'ordre des octets du réseau
TSIG RDATA	Longueur des autres données	dans l'ordre des octets du réseau
TSIG RDATA	Autres données	exactement comme transmises

Tableau 2 : Variables TSIG

Le RR RDLENGTH et la taille de MAC de RDATA MAC ne sont pas inclus dans les entrées du calcul de MAC, car il n'est pas garanti qu'elles soient connaissables avant la génération du MAC.

Le champ Identifiant d'origine n'est pas inclus dans ce paragraphe, car il lui a déjà été substitué l'identifiant de message dans l'en-tête DNS et son hachage.

Pour chaque type d'étiquette, il doit y avoir un "format canonique du réserau" défini qui spécifie comment exprimer une étiquette sans ambiguïté. Pour le type d'étiquette 00, ceci est défini au paragraphe 6.2 de la [RFC4034]. L'utilisation de types d'étiquettes autres que 00 n'est pas défini pour la présente spécification.

4.3.3.1 Valeur de temps utilisées dans les calculs TSIG

Les données résumées incluent les deux valeurs de temporisateur dans l'en-tête TSIG afin de défendre contre les attaques en répétition. Si ce n'était pas fait, un attaquant pourrait répéter de vieux messages mais mettre à jour les champs Heure signée et Ajustement pour faire paraître le message comme étant nouveau. Les deux champs sont collectivement nommés "temporisateurs TSIG", et pour les besoins du calcul de MAC, ils sont hachés dans leur format du réseau, dans l'ordre suivant : d'abord Heure signée, ensuite Ajustement.

5. Détails du protocole

5.1 Génération de TSIG sur les demandes

Une fois l'enregistrement sortant construit, le client effectue le calcul du hachage chiffré (code d'authentification de message haché (HMAC)) ajoute un enregistrement TSIG avec le MAC calculé à la section supplémentaire (incrémentant le ARCOUNT pour refléter le RR supplémentaire) et transmet la demande au serveur. Cet enregistrement TSIG DOIT être le seul RR TSIG dans le message et DOIT être le dernier enregistrement dans la section de données supplémentaires. Le client DOIT mémoriser le MAC et le nom de la clé provenant de la demande en attendant une réponse.

Les composants du résumé pour une demande sont :
Message DNS (demande)
Variables TSIG (demande)

5.2 Traitement des demandes par le serveur

Si un message entrant contient un enregistrement TSIG, il DOIT être le dernier enregistrement dans la section supplémentaire. Plusieurs enregistrements TSIG ne sont pas permis. Si plusieurs enregistrements TSIG sont détectés ou si un enregistrement TSIG est présent dans une autre position, le message DNS est éliminé et une réponse avec RCODE 1 (FORMERR) DOIT être retournée. À réception d'un message avec exactement un RR TSIG correctement placé, une copie

du RR TSIG est mémorisée et le RR TSIG est retiré du message DNS et décrémenté dans le ARCOUNT de l'en-tête du message DNS.

Si le RR TSIG ne peut pas être interprété, le serveur DOIT considérer le message comme corrompu et retourner une FORMERR au serveur. Autrement, il est EXIGÉ du serveur qu'il retourne un RR TSIG dans la réponse.

Pour valider le RR TSIG reçu, le serveur DOIT effectuer les vérifications suivantes dans cet ordre :
1. Vérifier la clé
2. Vérifier le MAC
3. Vérifier les valeurs d'heure
4. Vérifier la politique de troncature

5.2.1 Vérification de clé et traitement des erreurs

Si un serveur non transmetteur ne reconnaît pas la clé ou l'algorithme utilisé par le client (ou reconnaît l'algorithme mais ne le met pas en œuvre) le serveur DOIT générer une réponse d'erreur avec RCODE 9 (NOTAUTH) et TSIG ERROR 17 (BADKEY). Cette réponse DOIT être non signée comme spécifié au paragraphe 5.3.2. Le serveur DEVRAIT enregistrer l'erreur. (Des considérations particulières s'appliquent aux serveurs transmetteurs ; voir le paragraphe 5.5.)

5.2.2 Vérification de MAC et traitement des erreurs

En utilisant les informations de la TSIG, le serveur DOIT vérifier le MAC en faisant ses propres calculs et en comparant le résultat au MAC reçu. Si le MAC ne se vérifie pas, le serveur DOIT générer une réponse d'erreur comme spécifié au paragraphe 5.3.2 avec RCODE 9 (NOTAUTH) et TSIG ERROR 16 (BADSIG). Cette réponse DOIT être non signée, comme spécifié au paragraphe 5.3.2. Le serveur DEVRAIT enregistrer l'erreur.

5.2.2.1 MAC tronqué

Quand l'espace est un problème et que la force de la longueur entière d'un MAC n'est pas nécessaire, il est raisonnable de tronquer le hachage chiffré et d'utiliser la valeur tronquée pour l'authentification. Le HMAC SHA-1 tronqué à 96 bits est une option disponible dans plusieurs protocoles de l'IETF, incluant IPsec et TLS. Cependant, bien que cette option soit conservée pour la rétro compatibilité, elle peut ne pas fournir un niveau de sécurité approprié pour tous les cas dans l'environnement moderne. Dans ces cas, il est préférable d'utiliser un algorithme de hachage comme SHA-256-128, SHA-384-192, ou SHA-512-256 [RFC4868].

Le traitement d'un MAC tronqué a les règles suivantes :

Si le champ Taille de MAC est supérieur à la longueur du résultat du hachage chiffré : ce cas NE DOIT PAS être généré et, si il est reçu, DOIT causer l'élimination du message DNS et le retour du RCODE 1 (FORMERR).

Si le champ Taille de MAC est égal à la longueur du résultat du hachage chiffré : le résultat entier du hachage chiffré est présent et utilisé.

Si le champ Taille de MAC est inférieur au plus grand de 10 (octets) et de la moitié de la longueur de la fonction de hachage utilisée : à l'exception de certains messages d'erreur TSIG décrits au paragraphe 5.3.2, où il est permis que la taille de MAC soit zéro, ce cas NE DOIT PAS être généré et, si il est reçu, DOIT causer l'élimination du message DNS et le retour du RCODE 1 (FORMERR).

Autrement : cela est envoyé quand le signataire a tronqué le résultat du hachage chiffré à une longueur admissible, comme décrit dans la [RFC2104], en prenant les octets initiaux et en éliminant les octets de queue. La troncature TSIG peut seulement être à un nombre entier d'octets. À réception d'un message DNS avec troncature comme indiquée, le MAC calculé en local est tronqué de façon similaire, et seulement les valeurs tronquées sont comparées pour l'authentification. Le MAC de demande utilisé pour calculer le MAC de TSIG pour une réponse est le MAC de demande tronqué.

5.2.3 Vérification de l'heure et traitement des erreurs

Si l'heure du serveur est en-dehors de l'intervalle de temps spécifié dans la demande (qui est la valeur de Heure signée plus/moins la valeur de Ajustement) le serveur DOIT générer une réponse d'erreur avec RCODE 9 (NOTAUTH) et TSIG

ERROR 18 (BADTIME). Le serveur DEVRAIT aussi mettre en antémémoire la plus récente valeur de Heure signée dans un message généré par une clé et DEVRAIT retourner BADTIME si un message reçu plus tard a une valeur de Heure signée antérieure. Une réponse indiquant une erreur BADTIME DOIT être signée par la même clé que la demande. Elle DOIT inclure l'heure actuelle du client dans le champ Heure signée, l'heure actuelle du serveur (un entier non signé de 48 bits) dans le champ Autres données, et 6 dans le champ Longueur des autres données. Ceci est fait pour que le client puisse vérifier un message avec une erreur BADTIME sans que la vérification échoue à cause d'une autre erreur BADTIME. De plus, le champ Ajustement DOIT être réglé à la valeur d'ajustement reçue du client. Les données signées sont spécifiées au paragraphe 5.3.2. Le serveur DEVRAIT enregistrer l'erreur.

Mettre en antémémoire la plus récente valeur d'heure signée et rejeter les demandes avec une heure plus ancienne pourrait conduire à valider des messages qui seraient rejetés si le transit à travers le réseau conduisait à des paquets UDP arrivant dans un ordre différent de celui dans lequel ils ont été envoyés. Les mises en œuvre devrait être conscientes de cette possibilité et être prêtes à la traiter, par exemple, en retransmettant les demandes rejetées avec une nouvelle TSIG une fois que les demandes en instance ont été achevées ou que le temps donné par leur valeur d'heure signée plus la valeur d'ajustement est passée. Si les mises en œuvre réessayent les demandes dans ce cas, une limite DEVRAIT être placée sur le nombre maximum d'essais.

5.2.4 Vérification de troncature et traitement des erreurs

Si une TSIG est reçue avec la troncature qui est permise par le paragraphe 5.2.2.1 mais si le MAC est trop court pour la politique locale en vigueur, un RCODE 9 (NOTAUTH) et une TSIG ERROR 22 (BADTRUNC) DOIVENT être retournés. Le serveur DEVRAIT enregistrer l'erreur.

5.3 Génération de TSIG sur les réponses

Quand un serveur a généré une réponse à une demande signée, il signe la réponse en utilisant le même algorithme et la même clé. Le serveur NE DOIT PAS générer une réponse signée à une demande si la clé est invalide (par exemple, le nom de la clé ou de l'algorithme sont inconnus) ou si le MAC échoue à la validation ; voir au paragraphe 5.3.2 les détails de la réponse dans ces cas.

Il NE DOIT PAS non plus générer une réponse signée à une demande non signée, sauf dans le cas d'une réponse à une demande TKEY non signée d'un client si la clé secrète est établie sur le côté du serveur après que le serveur a traité la demande du client. Signer des réponses à des demandes TKEY non signées DOIT être explicitement spécifié dans la description de l'algorithme d'établissement d'une clé secrète individuelle [RFC3645].

Les composants de résumé utilisés pour générer une TSIG sur une réponse sont :
MAC de demande
Message DNS (réponse)
Variables TSIG (réponse)

(Ce calcul est différent pour le second message et les suivants dans une réponse multi-messages ; voir ci-dessous.)

Si l'ajout de l'enregistrement TSIG va causer la troncature du message, le serveur DOIT altérer la réponse pour qu'une TSIG puisse être incluse. Cette réponse contient seulement la question et un enregistrement TSIG, a le bit TC établi, et a un RCODE de 0 (NOERROR). À ce point, le client DEVRAIT réessayer la demande en utilisant TCP (conformément au paragraphe 4.2.2 de la [RFC1035]).

5.3.1 TSIG sur connexions TCP

Une session TCP DNS, comme un transfert de zone, peut inclure plusieurs messages DNS. Utiliser une TSIG sur une telle connexion peut protéger la connexion d'une attaque et assurer l'intégrité des données. La TSIG DOIT être incluse dans tous les messages DNS de la réponse. Pour la rétro compatibilité, un client qui reçoit des messages DNS et vérifie la TSIG DOIT accepter jusqu'à 99 messages intermédiaires sans TSIG et DOIT vérifier que le premier et le dernier message contiennent une TSIG.

Le premier message est traité comme une réponse standard (voir le paragraphe 5.3) mais les messages qui suivent ont les composants de résumé suivants :
MAC antérieur (courrant)

Messages DNS (tous les messages non signés depuis la dernière TSIG)
Temporisateurs TSIG (du message en cours)

Le "MAC antérieur" est le MAC provenant de la TSIG attachée au dernier message contenant une TSIG. "Messages DNS" comporte l'enchaînement (dans l'ordre du message) de tous les messages après le dernier message qui incluait une TSIG et inclut le message en cours. Les "Temporisateurs TSIG" comprennent les champs Heure signée et Ajustement (dans cet ordre) appartenant au message pour lequel la TSIG a été créée ; cela signifie que les enregistrements successifs de TSIG dans le flux vont avoir des valeurs d'Heure signée non décroissantes. Noter que seuls les temporisateurs sont inclus dans le second message et les suivants, pas toutes les variables TSIG.

Cela permet au client de détecter rapidement quand la session a été altérée ; à ce point, il peut clore la connexion et réessayer. Si la vérification de la TSIG d'un client échoue, le client DOIT clore la connexion. Si le client ne reçoit pas les enregistrements de TSIG assez fréquemment (comme spécifié ci-dessus) il DEVRAIT supposer que la connexion a été capturée, et il DEVRAIT clore la connexion. Le client DEVRAIT traiter cela de la même façon qu'il ferait de tout autre transfert interrompu (bien que le comportement exact ne soit pas spécifié).

5.3.2 Génération de TSIG sur des retours d'erreur

Quand un serveur détecte une erreur relative à la clé ou au MAC dans la demande entrante, le serveur DEVRAIT renvoyer un message d'erreur non signé (Taille de MAC == 0 et MAC vide). Il NE DOIT PAS renvoyer un message d'erreur signé.

Si une erreur relative à la période de validité de la TSIG est détectée ou si le MAC est trop court pour la politique locale, le serveur DEVRAIT renvoyer un message d'erreur signé. Les composants du résumé sont :
MAC de demande (si le MAC de demande s'est validé)
Message DNS (réponse)
Variables TSIG (réponse)

La raison pour laquelle le MAC de demande n'est pas inclus dans ce MAC dans certains cas est de rendre possible au client de vérifier l'erreur. Si l'erreur n'est pas une erreur de TSIG, la réponse DOIT être générée comme spécifié au paragraphe 5.3.

5.4 Traitement de réponse par le client

Quand un client reçoit une réponse d'un serveur et s'attend à voir une TSIG, il vérifie d'abord si le RR TSIG est présent dans la réponse. Sinon, la réponse est traitée comme ayant une erreur de format et est éliminée.

Si le RR TSIG est présent, le client effectue les mêmes vérifications que décrites au paragraphe 5.2. Si le RR TSIG est non signé comme spécifié au paragraphe 5.3.2 ou ne se valide pas, le message DOIT être éliminé sauf si le RCODE est 9 (NOAUTH). Dans ce cas, le client DEVRAIT tenter de vérifier la réponse comme si c'était une erreur de TSIG, comme décrit dans les paragraphes qui suivent.

Sans égard au RCODE, un message contenant un RR TSIG non signé comme spécifié au paragraphe 5.3.2 ou qui échoue à la vérification NE DEVRAIT PAS être considéré comme une réponse acceptable, car il peut avoir été usurpé ou manipulé. Le client DEVRAIT plutôt enregistrer une erreur et continuer d'attendre une réponse signée jusqu'à ce que la demande arrive en fin de temporisation.

5.4.1 Traitement d'erreur de clé

Si un RCODE sur une réponse est 9 (NOTAUTH) mais si la TSIG de réponse se valide et si la clé de TSIG est reconnue par le client mais est différente de celle utilisée sur la demande, c'est alors une erreur relative à la clé. Le client PEUT réessayer la demande en utilisant la clé spécifiée par le serveur. Cependant, cela ne devrait jamais se produire car un serveur NE DOIT PAS signer une réponse avec une clé différente de celle utilisée pour signer la demande.

5.4.2 Traitement d'erreur de MAC

Si la réponse RCODE est 9 (NOTAUTH) et si TSIG ERROR est 16 (BADSIG), c'est une erreur relative au MAC, et les clients PEUVENT réessayer la demande avec un nouvel identifiant de demande, mais il serait préférable d'essayer une clé

partagée différente si il en est une disponible. Les clients DEVRAIENT garder trace du nombre d'erreurs de MAC associé à chaque clé. Les clients DEVRAIENT enregistrer cet événement.

5.4.3 Traitement d'erreur de temps

Si le RCODE de réponse est 9 (NOTAUTH) et la TSIG ERROR est 18 (BADTIME) ou si l'heure courante ne rentre pas dans la gamme spécifiée dans l'enregistrement TSIG, c'est alors une erreur relative à l'heure. C'est une indication que les horloges du client et du serveur ne sont pas synchronisées. Dans ce cas, le client DEVRAIT enregistrer l'événement. Les résolveurs du DNS NE DOIVENT PAS ajuster d'horloge de client sur la base d'erreurs BADTIME, mais l'heure du serveur dans le champ Autres données DEVRAIT être enregistré.

5.4.4 Traitement d'erreur de troncature

Si le RCODE de réponse est 9 (NOTAUTH) et l'erreur de TSIG est 22 (BADTRUNC) c'est une erreur relative à la troncature. Le client PEUT réessayer avec une moindre troncature jusqu'au résultat HMAC complet (aucune troncature), en utilisant la troncature utilisée dans la réponse comme indication de ce que la politique du serveur permet (Section 7). Les clients DEVRAIENT enregistrer cet événement.

5.5 Considérations particulières pour les serveurs de transmission

Un serveur qui agit comme serveur de transmission d'un message DNS DEVRAIT vérifier l'existence d'un enregistrement TSIG. Si le nom sur la TSIG n'est pas celui d'un secret que le serveur partage avec le générateur, le serveur DOIT transmettre le message inchangé, y compris la TSIG. Si le nom de la TSIG est celui d'une clé que ce serveur partage avec le générateur, il DOIT traiter la TSIG. Si la TSIG réussit toutes les vérifications, le serveur transmetteur DOIT, si possible, inclure une TSIG de son cru à la destination ou au prochain transmetteur. Si aucune sécurité de transaction n'est disponible à la destination et si le message est une interrogation, et si la réponse correspondante a le fanion AD (voir la [RFC4035]) établi, le transmetteur DOIT mettre le fanion AD à zéro avant d'ajouter la TSIG à la réponse et de retourner le résultat au système d'où il a reçu l'interrogation.

6. Algorithmes et identifiants

Le seul algorithme de résumé de message spécifié dans la première version de ces spécifications [RFC2845] était "HMAC-MD5" (voir les [RFC1321] et [RFC2104]). Bien qu'une révision de sa sécurité il y a quelques années [RFC6151] ait conclu que "il peut n'être pas urgent de supprimer HMAC-MD5 des protocoles existants", avec la disponibilité de solutions de remplacement plus sûres, l'opportunité a été saisie de rendre facultative la mise en œuvre de cet algorithme.

La [RFC4635] a ajouté la prise en charge obligatoire dans TSIG de SHA-1 [FIPS180-4] [RFC3174]. Des collisions de SHA-1 ont été démontrées [SHA1SHAMBLES], de sorte que les considérations sur la sécurité de MD5 décrites à la Section 2 de la [RFC6151] s'appliquent de façon similaire à SHA-1. Bien que la prise en charge de hmac-sha1 dans TSIG soit toujours obligatoire pour des raisons de compatibilité, les utilisations existantes DEVRAIT être remplacées par hmac-sha256 ou d'autres algorithmes de résumé SHA-2 ([FIPS180-4], [RFC3874], [RFC6234]).

L'utilisation de TSIG entre deux agents du DNS est par accord mutuel. Cet accord peut inclure la prise en charge d'algorithmes supplémentaires et des critères d'acceptabilité de quels algorithmes et troncatures, sous réserve des restrictions et lignes directrices du paragraphe 5.2.2.1. L'accord de clés peut être le mécanisme TKEY [RFC2930] ou autre méthode mutuellement acceptable.

Les mises en œuvre qui prennent en charge TSIG DOIVENT aussi mettre en œuvre HMAC SHA1 et HMAC SHA256 et PEUVENT mettre en œuvre gss-tsig et les autres algorithmes mentionnés ci-dessous. SHA-1 tronqué à 96 bits (12 octets) DEVRAIT être mis en œuvre.

Nom d'algorithme	Mise en œuvre	Utilisation
HMAC-MD5.SIG-ALG.REG.INT	PEUT	NE DOIT PAS
gss-tsig	PEUT	PEUT
hmac-sha1	DOIT	NON RECOMMANDÉ
hmac-sha224	PEUT	PEUT

hmac-sha256	DOIT	RECOMMANDÉ
hmac-sha256-128	PEUT	PEUT
hmac-sha384	PEUT	PEUT
hmac-sha384-192	PEUT	PEUT
hmac-sha512	PEUT	PEUT
hmac-sha512-256	PEUT	PEUT

Tableau 3 : Algorithmes pour les mises en œuvre qui prennent en charge TSIG

7. Politique de troncature TSIG

Comme noté ci-dessus, deux agents DNS (par exemple, un résolveur et un serveur) doivent s'accorder mutuellement pour utiliser TSIG. Implicites dans de tels "accords" sont les critères d'acceptabilité des clés, algorithmes, et (avec les extensions du présent document) les troncatures. Les politiques locales PEUVENT exiger le rejet des TSIG, même si elles utilisent un algorithme dont la mise en œuvre est obligatoire.

Quand une politique locale permet l'acceptation d'une TSIG avec un algorithme particulier et une quantité de troncature non zéro particulière, elle DEVRAIT aussi permettre l'utilisation de cet algorithme avec une moindre truncature (un MAC plus long) jusqu'au résultat complet de hachage chiffré.

Sans considération de la longueur inférieure de MAC tronqué acceptable spécifiée par la politique locale, une réponse DEVRAIT être envoyée avec un MAC au moins aussi long que dans la demande correspondante. Noter que si la demande spécifiait une longueur de MAC supérieure à la longueur du résultat du hachage chiffré, elle sera rejetée par les règles de traitement (paragraphe 5.2.2.1, cas 1).

Les mises en œuvre qui permettent plusieurs algorithmes et/ou troncatures acceptables DEVRAIENT permettre que leur liste soit ordonnée par force présumée et DEVRAIENT permettre que différentes troncatures pour le même algorithme soient traitées comme des entités séparées dans cette liste. Quand elles sont mises en œuvre ainsi, les politiques DEVRAIENT accepter un algorithme et une troncature présumés plus forts que la force minimale exigée par la politique.

8. Secrets partagés

Les clés secrètes sont des informations très sensibles et toutes les mesures disponibles devraient être prises pour les protéger sur tout hôte sur lequel elles sont mémorisées. Généralement, de tels hôtes ont besoin d'être physiquement protégés. Si ils sont des machines multi-utilisateurs, un grand soin devrait être apporté à ce que des utilisateurs non privilégiés n'aient pas d'accès au matériel de chiffrement. Les résolveurs fonctionnent souvent sans privilèges, ce qui signifie que tous les utilisateurs d'un hôte vont être capables de voir toutes les données de configuration qui sont utilisées par le résolveur.

Un serveur de noms fonctionne généralement avec des privilèges, ce qui signifie que les données de configuration n'ont pas besoin d'être visibles à tous les utilisateurs de l'hôte. Pour cette raison, un hôte qui met en œuvre l'authentification fondée sur la transaction devrait probablement être configuré avec un "résolveur de bout" et une antémémoire locale d'un serveur de noms transmetteur. Cela pose un problème particulier pour la [RFC2136], qui dépend autrement de clients qui communiquent seulement avec les serveurs de noms d'autorité d'une zone.

L'utilisation de forts secrets partagés aléatoires est essentielle pour la sécurité de TSIG. Voir dans la [RFC4086] une discussion de cette question. Le secret DEVRAIT être au moins aussi long que le résultat du hachage chiffré [RFC2104].

9. Considérations relatives à l'IANA

L'IANA tient un registre des noms d'algorithmes à utiliser comme "Noms d'algorithmes", comme défini au paragraphe 4.2 [IANA-TSIG]. Les noms d'algorithmes sont des chaînes de texte codées en utilisant la syntaxe d'un nom de domaine. Il n'y a pas de structure pour les noms, et les noms d'algorithmes sont comparés comme si ils étaient des noms DNS, c'est-à-dire que leur comparaison est insensible à la casse. Les précédentes spécifications ([RFC2845] et [RFC4635]) définissaient

des valeurs pour les algorithmes HMAC-MD5 et certains HMAC-SHA. L'IANA a aussi enregistré "gss-tsig" comme identifiant pour l'authentification TSIG où les opérations cryptographiques sont déléguées au service générique de sécurité (GSS, *Generic Security Service*) [RFC3645]. Le présent document ajoute aux algorithmes permis, et le registre a été mis à jour avec les noms mentionnés dans le Tableau 3.

De nouveaux algorithmes sont alloués en utilisant la politique de revue par l'IETF définie dans la [RFC8126]. Le nom d'algorithme HMAC-MD5.SIG-ALG.REG.INT ressemble à un nom de domaine pleinement qualifié pour des raisons historiques ; les autres noms d'algorithmes sont des noms simples, d'un seul composant.

L'IANA tient un registre des RCODE *(codes d'erreur)* (voir [IANA-RCODE], incluant des "valeurs d'erreur TSIG" à utiliser pour les valeurs de "Erreur" comme défini au paragraphe 4.2. Le présent document définit le RCODE comme décrit à la Section 3. Les nouveaux codes d'erreur seront alloués et spécifiés comme dans la [RFC6895].

10. Considérations sur la sécurité

L'approche spécifiée ici est beaucoup moins coûteuse en calcul que les signatures spécifiées dans DNSSEC. Tant que la clé secrète partagée n'est pas compromise, une forte authentification est fournie entre deux systèmes DNS, par exemple, pour le dernier bond d'un serveur de nom local au résolveur de l'utilisateur ou entre serveur de noms primaire et secondaire.

Les recommandations pour choisir et maintenir des clés secrètes se trouvent dans la [RFC2104]. Si l'hôte client a été compromis, le serveur devrait suspendre l'utilisation de tous les secrets connus de ce client. Si possible, les secrets devraient être mémorisés sous une forme chiffrée. Les secrets ne devraient jamais être transmis en clair sur aucun réseau. Le présent document ne traite pas la question de comment distribuer les secrets, sauf à mentionner la possibilité d'une configuration manuelle et l'utilisation de TKEY [RFC2930]. Les secrets NE DEVRAIENT PAS être partagés par plus de deux entités ; tout partage supplémentaire permettrait à toute partie qui connaît la clé de se faire passer pour une autre de ces parties auprès des membres du groupe.

Ce mécanisme n'authentifie pas les données de source, seulement leur transmission entre deux parties qui partagent un secret. Les données de source originales peuvent venir d'un maître de zone compromis ou peuvent être corrompues durant le transit entre un authentique maître de zone et un "transmetteur qui met en antémémoire". Cependant, si le serveur effectue de bonne foi toutes les vérifications de la sécurité de DNSSEC, alors seulement les données dont la sécurité est vérifiée vont être disponibles au client.

Une valeur d'ajustement qui est trop large peut laisser le serveur ouvert à des attaques en répétition. Une valeur d'ajustement trop étroite peut causer des défaillances si les machines ne sont pas synchronisées ou si il y a des délais inattendus du réseau. La valeur RECOMMANDÉE dans la plupart des situations est de 300 secondes.

Pour prévenir les attaques de croisement d'algorithme, il DEVRAIT seulement y avoir un algorithme associé à tout nom de clé.

Dans plusieurs cas où des erreurs sont détectées, un message d'erreur non signé doit être retourné. Cela peut permettre à un attaquant d'usurper ou manipuler ces réponses. Le paragraphe 5.4 recommande d'enregistrer cela comme des erreurs et de continuer d'attendre une réponse signée jusqu'à ce que la demande arrive en fin de temporisation.

Bien que la force d'un algorithme détermine sa sécurité, il y a eu des arguments pour dire qu'une certaine troncature peut renforcer un MAC en réduisant les informations disponibles à un attaquant. Cependant, une troncature excessive affaiblit clairement l'authentification en réduisant le nombre de bits qu'un attaquant doit essayer pour casser l'authentification en force brute [RFC2104].

Des progrès significatifs ont été faits récemment en cryptanalyse des fonctions de hachage des types utilisés ici. Bien que les résultats ne devraient pas jusqu'à présent affecter HMAC, le plus fort algorithme SHA-256 est rendu obligatoire par précaution.

Voir aussi la section des considérations sur la sécurité de la [RFC2104] d'où sont tirées les limites de troncature de la présente RFC.

10.1 Problèmes corrigés dans ce document

Quand on signe un message de réponse du DNS en utilisant TSIG, le calcul de MAC utilise le MAC du message de demande comme entrée pour mettre cryptographiquement en relation la réponse et la demande. La spécification originale de TSIG [RFC2845] exigeait que les valeurs d'heures soient vérfiées avant le MAC de la demande. Si l'heure était invalide, certaines mises en œuvre échouaient à effectuer les autres vérifications et pouvaient utiliser un MAC de demande invalide dans la réponse signée.

Le présent document rend obligatoire que le MAC de demande soit considéré comme invalide jusqu'à ce qu'il ait été validé ; jusque là, toute réponse doit être non signée. Pour cette raison, le MAC de demande est maintenant vérifié avant les valeurs d'heures.

10.2 Pourquoi pas DNSSEC ?

Le DNS a été étendu par DNSSEC ([RFC4033], [RFC4034], et [RFC4035]) pour fournir l'authentification de l'origine des données et la distribution de clé publique, toutes fondées sur la cryptographie de clé publique et des signatures numériques fondées sur des clés publiques. Pour être pratique, cette forme de sécurité exige généralement des capacités extensives de mise en antémémoire locale des clés et le suivi de l'authentification à travers plusieurs clés et signatures jusqu'à une clé de confiance pré- configurée en local.

Une difficulté du schéma DNSSEC est que les mises en œuvre courantes du DNS incluent des simples résolveurs"de bout" qui n'ont pas d'antémémoires. Ces résolveurs s'appuient normalement sur un serveur DNS sur un autre hôte qui met en antémémoire. Il n'est pas pratique pour de tels résolveurs de bout d'effectuer l'authentification générale DNSSEC et ils vont naturellement dépendre de l'antémémoire de leur serveur DNS pour effectuer ces services pour eux. Pour faire cela en toute sécurité il faut une communication sécurisée des demandes et des réponses. DNSSEC fournit des signatures de transaction de clé publique pour prendre cela en charge, mais la génération de ces signatures est très coûteuse en calcul. En général, cela exige la même logique complexe de clé publique qui est impraticable pour les extrémités.

Un second domaine où l'utilisation des mécanismes directement fondés sur la clé publique DNSSEC peut être impraticable est l'authentification des demandes de mise à jour dynamique [RFC2136]. DNSSEC fournit des signatures de demande mais avec DNSSEC, comme avec les signatures de transaction, elles exigent une cryptographie de clé publique coûteuse en calcul et une logique d'authentification complexe. La mise à jour dynamique sécurisée du système des noms de domaine [RFC3007] décrit comment différentes clés sont utilisées dans les zones mises à jour dynamiquement.

11. Références

11.1 Références normatives

[FIPS180-4] National Institute of Standards and Technology, "Secure Hash Standard (SHS)", FIPS PUB 180-4, DOI 10.6028/NIST.FIPS.180-4, août 2015, <https://doi.org/10.6028/NIST.FIPS.180-4>.

[RFC1034] P. Mockapetris, "Noms de domaines - Concepts et facilités", STD 13, novembre 1987. (*MàJ par* RFC1101, 1183, 1348, 1876, 1982, 2065, 2181, 2308, 2535, 4033, 4034, 4035, 4343, 4035, 4592, 5936, 8020, 8482, 8767)

[RFC1035] P. Mockapetris, "Noms de domaines – Mise en œuvre et spécification", STD 13, novembre 1987. (*MàJ par* RFC1101, 1183, 1348, 1876, 1982, 1995, 1996, 2065, 2136, 2181, 2137, 2308, 2535, 2673, 2845, 3425, 3658, 4033, 4034, 4035, 4343, 5936, 5966, 6604, 7766, 8482, 8767)

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. DOI 10.17487/RFC2119, *(MàJ par* RFC8174)

[RFC2845] P. Vixie et autres, "Authentification de transaction de clé secrète pour DNS (TSIG)", mai 2000, DOI 10.17487/RFC2845, (*MàJ par* RFC3645 *; remplacée par* RFC8945 *; P.S.)*

[RFC3597] A. Gustafsson, "Traitement des types inconnus d'enregistrement de ressource du DNS ", septembre 2003, DOI 10.17487/RFC3597, *(P.S.)*

[RFC4635] D. Eastlake 3rd, "Identifiants d'algorithme TSIG SHA (Algorithme de hachage sécurisé) de HMAC (Code

d'authentification de message haché)", août 2006, DOI 10.17487/RFC4635, *(P.S. ; remplacée par* RFC8945*)*

[RFC8174] B. Leiba, "Ambiguïté des mots clés en majuscules ou minuscules dans la RFC2119", DOI 10.17487/RFC8174, mai 2017. BCP14. *(MàJ RFC*2119)

11.2 Références pour information

[CVE-2017-11104] Common Vulnerabilities and Exposures, "CVE-2017-11104: Improper TSIG validity period check may allow TSIG forgery", juin 2017, <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11104>.

[CVE-2017-3142] Common Vulnerabilities and Exposures, "CVE-2017-3142: An error in TSIG authentication may permit unauthorized zone transfers", juin 2017, <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3142>.

[CVE-2017-3143] Common Vulnerabilities and Exposures, "CVE-2017-3143: An error in TSIG authentication may permit unauthorized dynamic updates", juin 2017, <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3143>.

[IANA-RCODE] IANA, "DNS RCODEs", <https://www.iana.org/assignments/dns-parameters/>.

[IANA-TSIG] IANA, "TSIG Algorithm Names", <https://www.iana.org/assignments/tsig-algorithm-names/>.

[RFC1321] R. Rivest, "Algorithme de résumé de message MD5", avril 1992, DOI 10.17487/RFC1321, *(Information)*

[RFC2104] H. Krawczyk, M. Bellare et R. Canetti, "HMAC : Hachage de clés pour l'authentification de message", février 1997, DOI 10.17487/RFC2104.

[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, DOI 10.17487/RFC2136.

[RFC2930] D. Eastlake 3rd, "Établissement de clés secrètes pour le DNS (TKEY RR)", septembre 2000, DOI 10.17487/RFC2930, *(P.S.)*

[RFC3007] B. Wellington, "Mise à jour dynamique sécurisée du système des noms de domaine (DNS)", novembre 2000, DOI 10.17487/RFC3007.

[RFC3174] D. Eastlake 3rd et P. Jones, "Algorithme US de hachage sécurisé n° 1 (SHA1)", septembre 2001, DOI 10.17487/RFC3174. *(Info, MàJ par 4634 et 6234)*

[RFC3645] S. Kwan et autres, "Algorithme générique de service de sécurité pour l'authentification de transaction de clé secrète pour le DNS (GSS-TSIG)", octobre 2003, DOI 10.17487/RFC3645, (*MàJ* RFC2845) *(P.S.)*

[RFC3874] R. Housley, "SHA-224 : une fonction de hachage unidirectionnelle à 224 bits", septembre 2004, DOI 10.17487/RFC3874, *(Information)*

[RFC4033] R. Arends, et autres, "Introduction et exigences pour la sécurité du DNS", mars 2005, DOI 10.17487/RFC4033

[RFC4034] R. Arends et autres, "Enregistrements de ressources pour les extensions de sécurité au DNS", mars 2005, DOI 10.17487/RFC4034, (*MàJ par* RFC9077)

[RFC4035] R. Arends et autres, "Modifications du protocole pour les extensions de sécurité du DNS", mars 2005, DOI 10.17487/RFC4035, *(P.S. ; MàJ par* RFC8198, 9077)

[RFC4086] D. Eastlake 3rd, J. Schiller, S. Crocker, "Exigences d'aléa pour la sécurité", juin 2005, BCP0106, DOI 10.17487/RFC4086, (*Remplace* RFC1750)

[RFC4868] S. Kelly, S. Frankel, "Utilisation de HMAC-SHA-256, HMAC-SHA-384, et HMAC-SHA-512 avec IPsec",

mai 2007, DOI 10.17487/RFC4868, *(P.S.)*

[RFC6151] S. Turner, L. Chen, "Mise à jour des considérations de sécurité pour les algorithmes de résumé de message MD5 et le HMAC-MD5", mars 2011, DOI 10.17487/RFC6151, (*MàJ* RFC1321, RFC2104) *(Information)*

[RFC6234] D. Eastlake 3rd, T. Hansen, "Algorithmes US de hachage sécurisé (SHA et HMAC fondé sur SHA et HKDF)", mai 2011, DOI 10.17487/RFC6234, *(Remplace la* RFC4634 ; *MàJ la* RFC3174 ; *Information)*

[RFC6895] D. Eastlake 3rd, "Considérations de l'IANA sur le système des noms de domaine (DNS)", BCP0042, avril 2013, DOI 10.17487/RFC6895, (*Remplace* RFC6195 ; *MàJ* RFC1183, 2845, 2930, 3597)

[RFC7696] R. Housley, "Lignes directrices pour la gestion des algorithmes cryptographiques d'application obligatoire", novembre 2015. BCP 201, DOI 10.17487/RFC7696.

[RFC8126] M. Cotton, B. Leiba, T. Narten, "Lignes directrices pour la rédaction d'une section de considérations relatives à l'IANA dans les RFC", juin 2017. BCP 26, DOI 10.17487/RFC8126, *(Remplace* RFC5226)

[SHA1SHAMBLES] Leurent, G. and T. Peyrin, "SHA-1 is a Shambles", janvier 2020, <https://eprint.iacr.org/2020/014.pdf>.

Remerciements

Le problème de sécurité traité par ce document a été rapporté par Clément Berthaux de Synacktiv.

Peter van Dijk, Benno Overeinder, Willem Toroop, Ondrej Sury, Mukund Sivaraman, et Ralph Dolmans ont participé aux discussions qui ont amené à ce document. Mukund Sivaraman, Martin Hoffman, et Tony Finch ont fait des suggestions extrêmement utiles concernant la structure et la formulation du document mis à jour.

Stephen Morris tient à remercier Internet Systems Consortium du soutien de sa participation à la création de ce document.

Adresse des auteurs

Francis Dupont
Internet Systems Consortium, Inc.
PO Box 360
Newmarket, NH 03857
United States of America
mél : Francis.Dupont@fdupont.fr

Stephen Morris
United Kingdom
mél : sa.morris8@gmail.com

Paul Vixie
Farsight Security Inc
Suite 180
177 Bovet Road
San Mateo, CA 94402 USA
mél : paul@redbarn.org

Donald E. Eastlake 3rd
Futurewei Technologies
2386 Panoramic Circle
Apopka, FL 32703
United States of America
mél : d3e3e3@gmail.com

Olafur Gudmundsson
Cloudflare
United States of America
mél : olafur+ietf@cloudflare.com

Brian Wellington
Akamai
United States of America
mél : bwelling@akamai.com