

Groupe de travail Réseau  
**Request for Comments : 2536**  
 Catégorie : En cours de normalisation

D. Eastlake, IBM  
 mars 1999  
 Traduction Claude Brière de L'Isle

## Clés DSA et SIG dans le système des noms de domaines (DNS)

### Statut de ce mémoire

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

### Notice de copyright

Copyright (C) The Internet Society (1999). Tous droits réservés.

### Résumé

On décrit une méthode standard pour mémoriser les clés et signatures d'algorithme de signature numérique du gouvernement des USA dans le système des noms de domaines, qui utilise les enregistrements de ressource KEY et SIG du DNS.

### Table des Matières

1. Introduction.....	1
2. Enregistrements de ressource KEY de DSA.....	1
3. Enregistrements de ressource SIG du DSA.....	2
4. Considérations de performances.....	2
5. Considérations pour la sécurité.....	2
6. Considérations pour l'IANA.....	3
Références.....	3
Adresse de l'auteur.....	3
Déclaration complète de droits de reproduction.....	3

## 1. Introduction

Le système des noms de domaines (DNS, *Domain Name System*) est le système mondial hiérarchisé à copies réparties pour l'adressage de l'Internet, les mandataires de messagerie, et autres informations. Le DNS a été étendu pour inclure des signatures numériques et des clés de chiffrement comme décrit dans la [RFC2535]. Le DNS peut donc maintenant être sécurisé et peut être utilisé pour une distribution sûre de clés.

Le présent document décrit comment mémoriser les clés et signatures d'algorithme de signature numérique (DSA, *Digital Signature Algorithm*) du gouvernement américain dans le DNS. On suppose une certaine familiarité avec l'algorithme américain de signature numérique [Schneier]. La mise en œuvre de DSA est obligatoire pour la sécurité du DNS.

## 2. Enregistrements de ressource KEY de DSA

Les clés publiques DSA sont mémorisées dans le DNS comme des enregistrements de ressource (RR, *resource record*) KEY qui utilisent le numéro d'algorithme 3 [RFC2535]. La structure de la portion spécifique de l'algorithme de la partie RDATA de ce RR est montrée ci-dessous. Ces champs, de Q à Y sont la partie "clé publique" du RR KEY DSA.

La période de validité de la clé n'est pas dans le RR KEY mais est indiquée par le ou les RR SIG qui signent et authentifient le ou les RR KEY à ce nom de domaine.

Champ	Taille
T	1 octet
Q	20 octets
P	64 + T*8 octets
G	64 + T*8 octets
Y	64 + T*8 octets

Comme décrit dans [FIPS 186] et [Schneier], T est un paramètre de taille de clé choisi de telle sorte que  $0 \leq T \leq 8$ . (La signification pour l'algorithme 3 de l'octet T supérieur à 8 est réservée et le reste de la portion de RDATA peut avoir un format différent dans ce cas.) Q est un nombre premier choisi au moment de la génération de la clé tel que  $2^{159} < Q < 2^{160}$ , de sorte que Q est toujours long de 20 octets et, comme les autres champs, est mémorisé dans l'ordre "gros boutien" du réseau. P, G, et Y sont calculés comme indiqué par l'algorithme FIPS 186 de génération de clé [Schneier]. P est dans la gamme  $2^{511+64T} < P < 2^{512+64T}$  et est donc long de  $64 + 8 \cdot T$  octets. G et Y sont des quantités modulo P et peuvent donc avoir jusqu'à la même longueur que P et sont des champs de taille allouée fixée avec le même nombre d'octets que P.

Durant le processus de génération de clés, un nombre aléatoire X doit être généré de telle façon que  $1 \leq X \leq Q-1$ . X est la clé privée et est utilisée dans l'étape finale de la génération de clé publique dans laquelle Y est calculé comme

$$Y = G^{**}X \text{ mod } P$$

### 3. Enregistrements de ressource SIG du DSA

La portion signature de la zone RDATA du RR SIG, lorsque on utilise l'algorithme US de signature numérique, est montré ci-dessous avec les champs dans l'ordre dans lequel ils apparaissent. Voir dans la [RFC2535] les champs RDATA du RR SIG qui précèdent la signature elle-même.

Champ	Taille
T	1 octet
R	20 octets
S	20 octets

Les données signées sont déterminées comme spécifié dans la [RFC2535]. Les étapes suivantes sont alors effectuées, comme spécifié dans [FIPS 186], où Q, P, G, et Y sont comme spécifié dans la clé publique [Schneier] :

hachage = SHA-1 ( données )

Générer un K aléatoire tel que  $0 < K < Q$ .

$R = ( G^{**}K \text{ mod } P ) \text{ mod } Q$

$S = ( K^{**}(-1) * (\text{hachage} + X \cdot R) ) \text{ mod } Q$

Comme Q fait 160 bits, R et S ne peuvent pas être supérieurs à 20 octets, qui est l'espace alloué.

T est copié de la clé publique. Il n'est pas logiquement nécessaire dans le SIG mais est présent afin que les valeurs de  $T > 8$  puissent plus facilement être utilisées comme échappement pour les versions étendues de DSA ou autres algorithmes, comme ils seront spécifié ultérieurement.

### 4. Considérations de performances

Les vitesses générales de génération de signature sont en gros similaires pour RSA [RFC2537] et DSA. Avec un pré calcul suffisant, la génération de signature avec DSA est plus rapide qu'avec RSA. La génération de clé est aussi plus rapide pour DSA. Cependant, la vérification de signature est d'un ordre de grandeur inférieur à celle de RSA lorsque l'exposant public RSA est choisi petit, comme recommandé pour les RR KEY utilisés dans l'authentification de données du système des noms de domaine (DNS).

Les mises en œuvre actuelles du DNS sont optimisées pour les petits transferts, normalement de moins de 512 octets tout compris. Bien que de plus gros transferts soient effectués correctement et que des travaux soient en cours pour rendre plus efficaces les plus gros transferts, il est toujours conseillé pour l'instant de faire des efforts raisonnables pour minimiser la taille de ensembles de RR KEY mémorisés au sein du DNS dans la mesure de la sécurité adéquate. Il faut se souvenir que dans une zone sécurisée, au moins un RR SIG d'authentification sera aussi retourné.

### 5. Considérations pour la sécurité

Beaucoup des considérations générales de sécurité de la [RFC2535] s'appliquent. Les clés récupérées auprès du DNS ne devraient pas être considérées comme de confiance à moins que (1) elles aient été obtenues de façon sûre d'un résolveur sécurisé ou vérifiées de façon indépendante par l'utilisateur, et que (2) ce résolveur sécurisé et l'obtention sécurisée ou la

vérification indépendante se conforment à des politiques de sécurité acceptables pour l'utilisateur. Comme avec tous les algorithmes de chiffrement, l'évaluation de la force de clé nécessaire est essentielle et dépend de la politique locale.

La limitation de la taille de clé à un maximum de 1024 bits (  $T = 8$  ) dans la norme de DSA actuelle peut limiter la sécurité du DSA. Pour des applications particulièrement critiques, les mises en œuvre sont invitées à examiner toute la gamme des algorithmes et tailles de clé disponibles.

DSA suppose la capacité à générer fréquemment des nombres aléatoires de haute qualité. Voir des lignes directrices dans la [RFC1750]. DSA a été conçu de telle sorte que si on utilise des nombres manipulés plutôt qu'aléatoires, des canaux dissimulés à très large bande passante sont possibles. Voir [Schneier] et les recherches plus récentes. La divulgation d'une clé privée DSA entière dans seulement deux signatures DSA a été démontrée. DSA ne fournit la sécurité que si on utilise des mises en œuvre de confiance, incluant la génération de nombres aléatoires de confiance.

## 6. Considérations pour l'IANA

L'allocation d'une signification aux valeurs du paramètre T qui ne sont pas définies ici exige une action de normalisation de l'IETF. Il est prévu que les valeurs non allouées ici soient utilisées pour couvrir de futures extensions de la norme DSS.

## Références

- [FIPS 186] U.S. Federal Information Processing Standard: Digital Signature Standard.
- [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. (*MàJ par la RFC6604*)
- [RFC1750] D. Eastlake, 3<sup>rd</sup> et autres, "Recommandations d'[aléa pour la sécurité](#)", décembre 1994. (*Info., remplacée par la RFC4086*)
- [RFC2535] D. Eastlake, 3<sup>rd</sup>, "Extensions de sécurité du système des noms de domaines", mars 1999. (*Obsolète, voir RFC4033, RFC4034, RFC4035*) (P.S.)
- [RFC2537] D. Eastlake 3<sup>rd</sup>, "Clés RSA/MD5 et SIG dans le système des noms de domaines (DNS)", mars 1999. (*Obsolète, voir RFC3110*) (P.S.)
- [Schneier] Schneier, B., "Applied Cryptography Second Edition: protocols, algorithms, and source code in C", 1996.

## Adresse de l'auteur

Donald E. Eastlake 3rd  
IBM  
65 Shindegan Hill Road  
RR #1  
Carmel, NY 10512  
USA  
téléphone : +1-914-784-7913 (bureau)  
                  +1-914-276-2668 (domicile)  
fax : +1-914-784-3833 (w-fax)  
mél : [dee3@us.ibm.com](mailto:dee3@us.ibm.com)

## Déclaration complète de droits de reproduction

Copyright (C) The Internet Society (1999). Tous droits réservés.

Ce document et les traductions de celui-ci peuvent être copiés et diffusés, et les travaux dérivés qui commentent ou expliquent autrement ou aident à sa mise en œuvre peuvent être préparés, copiés, publiés et distribués, partiellement ou en

totalité, sans restriction d'aucune sorte, à condition que l'avis de copyright ci-dessus et ce paragraphe soit inclus sur toutes ces copies et œuvres dérivées. Toutefois, ce document lui-même ne peut être modifié en aucune façon, par exemple en supprimant le droit d'auteur ou les références à l'Internet Society ou d'autres organisations Internet, sauf si c'est nécessaire à l'élaboration des normes Internet, auquel cas les procédures pour les droits de reproduction définis dans les processus des normes pour l'Internet doivent être suivies, ou si nécessaire pour le traduire dans des langues autres que l'anglais.

Les permissions limitées accordées ci-dessus sont perpétuelles et ne seront pas révoquées par la Société Internet, ses successeurs ou ayants droit.

Ce document et les renseignements qu'il contient sont fournis "TELS QUELS" et l'INTERNET SOCIETY et l'INTERNET ENGINEERING TASK FORCE déclinent toute garantie, expresse ou implicite, y compris mais sans s'y limiter, toute garantie que l'utilisation de l'information ici présente n'enfreindra aucun droit ou aucune garantie implicite de commercialisation ou d'adaptation à un objet particulier.

**Remerciement**

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