Groupe de travail Réseau
Request for Comments : 4398
RFC rendue obsolète : 2538
Catégorie : Sur la voie de la normalisation

S. Josefsson
mars 2006

Traduction Claude Brière de L'Isle

Mémorisation de certificats dans le système des noms de domaines (DNS)

Résumé
Les clés publiques de chiffrement sont fréquemment publiées, et leur authenticité est démontrée par des certificats. Un enregistrement de ressource (RR, *resource record*) CERT est défini afin que de tels certificats et les listes de révocation de certificat qui s'y rapportent puissent être mémorisées dans le système des noms de domaines (DNS).

Le présent document rend obsolète la RFC 2538.

Table des matières

1. Introduction

Les clés publiques sont fréquemment publiées sous la forme d'un certificat, et leur authenticité est couramment démontrée par des certificats et les listes de révocation de certificats (CRL, *certificate revocation list*) qui s'y rapportent. Un certificat est un lien, par une signature numérique cryptographique, d'une clé publique, d'un intervalle de validité et/ou des conditions, d'une identité, d'une autorisation, ou d'autres informations. Une liste de révocation de certificats est une liste des certificats qui sont révoqués, et des informations connexes, tous signés par le signataire (producteur) des certificats

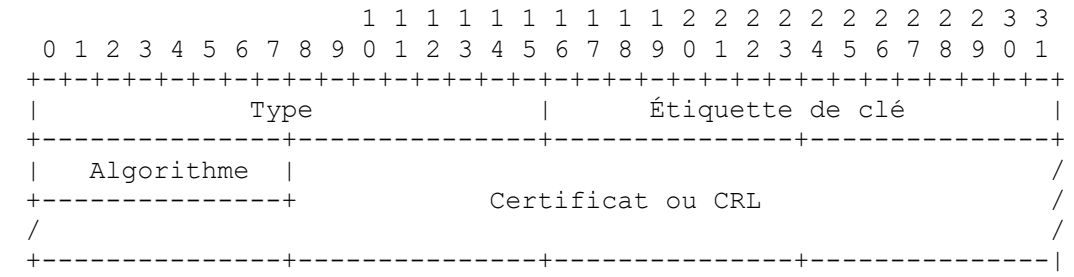
révoqués. Des exemples sont les certificats/CRL X.509 dans le système de répertoire X.500 ou les certificats/révocations OpenPGP utilisés par le logiciel OpenPGP.

La Section 2 spécifie un enregistrement de ressource CERT (RR) pour la mémorisation des certificats dans le système des noms de domaines [RFC1034], [RFC1035]. La Section 3 discute des noms appropriés de possesseur pour les RR CERT. Les Sections 4, 7, et 8 couvrent respectivement les performances, la sécurité, et les considérations relatives à l'IANA. La Section 9 explique les changements que le présent document apporte à la RFC 2538.

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].

2. Enregistrement de ressource CERT

L'enregistrement de ressource (RR) CERT a la structure ci-dessous. Son code de type de RR est 37.



Le champ Type est le type de certificat comme défini au paragraphe 2.1.

Le champ Étiquette de clé est la valeur de 16 bits calculée pour la clé incorporée dans le certificat, en utilisant l'algorithme d'étiquette de clé RRSIG décrit dans l'Appendice B de la [RFC4034]. Ce champ est utilisé comme une mesure d'efficacité pour saisir les RR CERT qui peuvent être applicables à une clé particulière. L'étiquette de clé peut être calculée pour la clé en question, et ensuite seulement les RR CERT qui ont la même étiquette de clé seront examinés. Noter que deux clés différentes peuvent avoir la même étiquette de clé. Cependant, la clé DOIT être transformée au format qu'elle aurait comme portion de clé publique d'un RR DNSKEY avant le calcul de l'étiquette de clé. Ceci n'est possible que si la clé est applicable à un algorithme et se conforme aux limites (comme de taille de clé) définies pour la sécurité du DNS. Si ce n'est pas le cas, le champ Algorithme DOIT être à zéro et le champ Étiquette est sans objet et DEVRAIT être zéro.

Le champ Algorithme a la même signification que dans les RR DNSKEY et RRSIG [RFC4034], sauf qu'un champ Algorithme de zéro indique que l'algorithme est inconnu d'un DNS sûr, ce qui peut être simplement le résultat de ce que l'algorithme n'a pas été normalisé pour DNSSEC [RFC4033].

2.1 Valeurs de type de certificat

Les valeurs suivantes sont définies ou réservées :

Valeur	Mnémonique	Type de certificat
0		Réservé
1	PKIX	X.509 selon PKIX
2	SPKI	certificat SPKI
3	PGP	paquet OpenPGP
4	IPKIX	URL d'un objet de données X.509
5	ISPKI	URL d'un certificat SPKI
6	IPGP	empreinte digitale et URL d'un paquet OpenPGP
7	ACPKIX	certificat d'attribut
8	IACPKIX	URL d'un certificat d'attribut
9-252		disponible pour allocation par l'IANA
253	URI	URI privé
254	OID	OID privé

255	Réservé
256-65279	disponible pour allocation par l'IANA
65280-65534	Expérimental
65535	Réservé

Ces valeurs représentent le contenu initial du registre de l'IANA ; voir la Section 8.

Le type PKIX est réservé pour indiquer un certificat X.509 conforme au profil défini par le groupe de travail PKIX de l'IETF [RFC3280]. La section Certificat va commencer par un OID d'un octet non signé et ensuite d'un OID X.500 indiquant la nature du reste de la section Certificat (voir au paragraphe 2.3). (Note : les certificats X.509 n'incluent pas leur OID de désignation de type de répertoire X.500 comme préfixe.)

Les types SPKI et ISPKI sont réservés pour indiquer le format de certificat SPKI [RFC2693], à utiliser lorsque les documents relatifs à SPKI quitteront le statut de "expérimental". Le format de ces deux types de RR CERT devra être spécifié ultérieurement.

Le type PGP indique un paquet OpenPGP comme décrit dans la [RFC2440] et ses extensions et successeurs. C'est utilisé pour transférer le matériel de clé publique et les signatures de révocation. Les données sont binaires et NE DOIVENT PAS être codées en ASCII. Une mise en œuvre DEVRAIT traiter les clés publiques transférables comme décrit au paragraphe 10.1 de la [RFC2440], mais elle PEUT traiter des paquets OpenPGP supplémentaires.

Le type ACPKIX indique un format de certificat d'attribut [RFC3281].

Les types IPKIX et IACPKIX indiquent un URL qui va servir le contenu qui aurait été dans le champ "certificat", "CRL", ou "URL" du type correspondant (respectivement PKIX ou ACPKIX).

Le type IPGP contient à la fois une empreinte digitale OpenPGP pour la clé en question, ainsi qu'un URL. La portion certificat du RR CERT IPGP est définie comme une empreinte digitale de un octet, suivie par l'empreinte digitale OpenPGP, suivie par l'URL. L'empreinte digitale OpenPGP est calculée comme défini dans la [RFC2440]. Une empreinte digitale de longueur zéro ou un URL de longueur zéro sont légaux, et indiquent des données IPGP seulement d'URL ou des données IPGP seulement d'empreinte digitale, respectivement. Une empreinte digitale de longueur zéro et un URL de longueur zéro n'ont pas de signification et sont invalides.

Les types IPKIX, ISPKI, IPGP, et IACPKIX sont connus comme "indirects". Ces types DOIVENT être utilisés quand le contenu est trop gros pour tenir dans le RR CERT et PEUVENT être utilisés à la discrétion de la mise en œuvre. Ils NE DEVRAIENT PAS être utilisés lorsque le message DNS fait 512 octets ou moins et pourrait donc tenir dans un paquet UDP.

Le type privé URI indique un format de certificat défini par un URL absolu. La portion certificat du RR CERT DOIT commencer par un URI terminé par un nul [RFC3986], et les données après le nul sont le certificat de format privé lui-même. L'URI DEVRAIT être tel qu'une restitution à partir de lui conduise à la documentation sur le format du certificat. La reconnaissance des types de certificats privés n'a pas besoin de se fonder sur l'égalité d'URI mais peut utiliser diverses formes de schémas de correspondance de sorte que, par exemple, des informations de sous type ou de version peuvent aussi être codées dans l'URI.

Le type OID privé indique un certificat de format privé spécifié par un préfixe d'OID ISO. La section certificat va commencer par un OID d'un octet non signé et ensuite un OID codé en BER qui indique la nature du reste de la section certificat. Ce peut être un format de certificat X.509 ou un autre format. Les certificats X.509 qui se conforment au profil PKIX de l'IETF DEVRAIENT être indiqués par le type PKIX, et non par le type OID privé. La reconnaissance des types de certificats privés n'a pas besoin de se fonder sur l'égalité des OID mais peut utiliser diverses formes de schémas de correspondance de tels préfixes d'OID.

2.2 Représentation textuelle des RR CERT

La portion RDATA d'un RR CERT a le champ Type comme un entier décimal non signé ou comme un symbole mnémonique dont la liste figure au paragraphe 2.1 ci-dessus.

Le champ Étiquette de clé est représenté par un entier décimal non signé.

Le champ Algorithme est représenté par un entier décimal non signé ou un symbole mnémonique de la liste de la

[RFC4034].

La portion certificat/CRL représentée en base 64 [RFC3548] peut être divisée en tout nombre de sous chaînes séparées par des espaces, jusqu'à un seul chiffre en base-64, qui sont enchaînés pour obtenir la signature complète. Ces sous chaînes peuvent s'étendre sur plusieurs lignes en utilisant les parenthèses standard.

Noter que la portion certificat/CRL peut avoir des sous champs internes, mais ceux-ci n'apparaissent pas dans la représentation du fichier maître. Par exemple, avec le type 254, il y aura une taille d'OID, un OID, et ensuite le certificat/CRL proprement dit. Cependant, une seule chaîne logique en base-64 apparaîtra dans la représentation textuelle.

2.3 OID X.509

Les OID ont été définis en connexion avec le répertoire X.500 pour les certificats d'utilisateur, les certificats d'autorité de certification, la révocation des autorités de certification, et la révocation des certificats d'utilisateur. Le tableau suivant fait la liste des OID, de leur codage en BER, et de leur format hexadécimal préfixé de longueur pour les RR CERT :

id-at-userCertificate = { joint-iso-ccitt(2) ds(5) at(4) 36 } == 0x 03 55 04 24
id-at-cACertificate = { joint-iso-ccitt(2) ds(5) at(4) 37 } == 0x 03 55 04 25
id-at-authorityRevocationList = { joint-iso-ccitt(2) ds(5) at(4) 38 } == 0x 03 55 04 26
id-at-certificateRevocationList = { joint-iso-ccitt(2) ds(5) at(4) 39 } == 0x 03 55 04 27

3. Noms de possesseur appropriés pour les RR CERT

Il est recommandé que les RR CERT de certificat soient mémorisés sous un nom de domaine en rapport avec leur sujet, c'est-à-dire, le nom de l'entité destinée à contrôler la clé privée correspondant à la clé publique qui est certifiée. Il est recommandé que les RR CERT de liste de révocation de certificat soient mémorisées sous un nom de domaine en rapport avec leur producteur.

Certaines des lignes directrices suivantes peuvent résulter en des noms DNS qui ont des caractères exigeant des guillemets conformément au paragraphe 5.1 de la [RFC1035].

Le choix du nom sous lequel sont mémorisés les RR CERT est important pour les clients qui effectuent les interrogations de CERT. Dans certaines situations, les clients peuvent ne pas connaître toutes les informations sur l'objet RR CERT qu'ils veulent restituer. Par exemple, un client peut ne pas connaître le nom de sujet d'un certificat X.509, ou l'adresse de messagerie électronique du possesseur d'une clé OpenPGP. De plus, le client peut ne connaître que le nom d'hôte d'un service qui utilise les certificats X.509 ou l'identifiant de clé d'une clé OpenPGP.

Donc, deux lignes directrices sont définies pour le nom de possesseur : les noms de possesseur fondés sur le contenu, et les noms de possesseur fondés sur l'objet. Un nom de possesseur fondé sur le contenu est déduit du contenu des données du RR CERT ; par exemple, le champ Sujet dans un certificat X.509 ou le champ Identifiant d'utilisateur dans les clés OpenPGP. Un nom de possesseur fondé sur l'objet est un nom qu'un client qui récupère des RR CERT devrait déjà connaître ; par exemple, le nom d'hôte d'un service protégé par X.509 ou l'identifiant de clé d'une clé OpenPGP. Le nom de possesseur fondé sur le contenu et celui fondé sur l'objet peuvent être le même ; par exemple, quand un client cherche une clé fondée sur l'adresse "From: " d'un message électronique entrant.

Les mises en œuvre DEVRAIENT utiliser les lignes directrices de nom de possesseur fondé sur l'objet décrites dans le présent document et PEUVENT utiliser les RR CNAME des noms de possesseur fondés sur le contenu (ou d'autres noms) qui pointent sur le nom de possesseur fondé sur l'objet.

Noter que ce paragraphe décrit une transposition fondée sur l'application de l'espace de noms utilisé dans un certificat en l'espace de noms utilisé par le DNS. Le DNS n'implique aucune relation entre les enregistrements de ressource CERT sur la base des similarités ou différences du ou des noms de possesseur DNS des enregistrements de ressource CERT. Par exemple, si plusieurs étiquettes sont utilisés quand on transpose un identifiant CERT en un nom de domaine, il faut alors faire attention à bien comprendre les synthèses d'enregistrement de caractères génériques.

3.1 Noms de RR CERT X.509 fondés sur le contenu

Certaines versions de X.509, comme le profil PKIX de X.509 [RFC3280], permettent que plusieurs noms soient associés à

des sujets et producteurs sous "Nom de remplacement de sujet" et "Nom de remplacement de producteur". Par exemple, le profil PKIX a de tels noms de remplacement avec une spécification ASN.1 comme suit :

```
GeneralName ::= CHOIX {
    otherName                   [0]   OtherName,
    rfc822Name                  [1]   IA5String,
    dNSName                     [2]   IA5String,
    x400Address                 [3]   ORAddress,
    directoryName               [4]   Name,
    ediPartyName                [5]   EDIPartyName,
    uniformResourceIdentifier   [6]   IA5String,
    iPAddress                   [7]   OCTET STRING,
    registeredID                [8]   OBJECT IDENTIFIER }
```

Les localisations recommandées des mémorisations de CERT sont les suivantes, en ordre de priorité :

1. Si un nom de domaine est inclus dans l'identification d'un certificat ou CRL, cela devrait être utilisé.
2. Si un nom de domaine n'est pas inclus mais si une adresse IP est incluse, la traduction de cette adresse IP en le nom de domaine inverse approprié devrait être utilisé.
3. Si aucun de ci-dessus n'est utilisé, mais si un URI contenant un nom de domaine est présent, ce nom de domaine devrait être utilisé.
4. Si aucun de ci-dessus n'est inclus mais si un nom de chaîne de caractères est inclus, il devrait alors être traité comme décrit ci-dessous pour les noms OpenPGP.
5. Si aucun de ci-dessus ne s'applique, le nom distinctif (DN) devrait alors être transposé en un nom de domaine comme spécifié dans la [RFC2247].

Exemple 1 : un certificat X.509v3 est produit à /CN=John Doe /DC=Doe/ DC=com/DC=xy/O=Doe Inc/C=XY/ avec les noms de remplacement de sujet de (a) chaîne "John (l'homme) Doe", (b) nom de domaine john-doe.com, et (c) URI <https://www.secure.john-doe.com:8080/>. Les localisations de mémorisation recommandées seraient, par ordre de priorité :

1. john-doe.com,
2. www.secure.john-doe.com,
3. Doe.com.xy.

Exemple 2 : un certificat X.509v3 est produit à /CN=James Hacker/ L=Basingstoke/O=Widget Inc/C=GB/ avec les noms de remplacement de sujet de (a) nom de domaine widget.foo.exemple, (b) l'adresse IPv4 10.251.13.201, et (c) la chaîne "James Hacker <hacker@mail.widget.foo.exemple>". Les localisations de mémorisation recommandées seraient, par ordre de priorité :

1. widget.foo.exemple,
2. 201.13.251.10.in-addr.arpa,
3. hacker.mail.widget.foo.exemple.

3.2 Noms de RR CERT X.509 fondés sur l'objet

Du fait de la difficulté pour les clients qui ne possèdent pas déjà un certificat pour reconstruire le nom de possesseur fondé sur le contenu, les noms de possesseurs fondés sur l'objet sont recommandés dans ce paragraphe. Les recommandations pour les noms de possesseur fondés sur l'objet varient selon le scénario. Le tableau qui suit résume les lignes directrices sur le nom de possesseur de RR CERT X.509 fondé sur l'objet à utiliser avec S/MIME [RFC3851], SSL/TLS [RFC2246], et IPsec [RFC4301]:

Scénario	**Nom de possesseur**
Certificat S/MIME	Traduction standard d'une adresse de messagerie RFC2822. Exemple : un certificat S/MIME pour "postmaster@exemple.org" va utiliser une traduction standard de noms d'hôte du nom du possesseur, "postmaster.exemple.org".
Certificat TLS	Nom d'hôte du serveur TLS.
Certificat IPsec	Nom d'hôte de la machine IPsec et/ou, pour les adresses IPv4 ou IPv6, le nom de domaine pleinement qualifié dans le domaine inverse approprié.

Un autre approche pour IPsec est de mémoriser les clés publiques brutes [RFC4025].

3.3 Noms de RR CERT OpenPGP fondés sur le contenu

Les clés signées OpenPGP (certificats) utilisent une chaîne de caractères générale Identifiant d'utilisateur [RFC2440]. Cependant, il est recommandé par OpenPGP que de tels noms incluent l'adresse de messagerie [RFC2822] de la partie concernée, comme dans "Leslie Exemple <Leslie@hôte.exemple>". Si un tel format est utilisé, le CERT devrait être sous la traduction standard de l'adresse de messagerie en un nom de domaine, qui serait "leslie.hôte.exemple" dans ce cas. Si aucun nom de la RFC2822 ne peut être extrait de la chaîne de nom, aucun nom de domaine spécifique n'est recommandé.

Si un usager a plus d'une adresse de messagerie, le type de CNAME peut être utilisé pour réduire la quantité de données mémorisées dans le DNS. Par exemple :

```
$ORIGIN example.org.
smith       IN CERT PGP 0 0 <OpenPGP binary>
john.smith  IN CNAME smith
js          IN CNAME smith
```

3.4 Noms de RR CERT OpenPGP fondés sur l'objet

Les applications qui reçoivent un paquet OpenPGP contenant des données chiffrées ou signées mais ne connaissent pas l'adresse de messagerie de l'envoyeur auront des difficultés à construire le nom correct du possesseur et ne peuvent pas utiliser les lignes directrices sur le nom de possesseur fondées sur le contenu. Cependant, ces clients connaissent habituellement l'empreinte digitale de la clé ou l'identifiant de clé. L'identifiant de clé se trouve dans les paquets OpenPGP, et l'empreinte digitale de clé se trouve habituellement dans les données auxiliaires qui peuvent être disponibles. Dans ce cas, l'utilisation d'un nom de possesseur identique à l'empreinte digitale de clé et l'identifiant de clé exprimé en hexadécimal [RFC3548] est recommandé. Par exemple :

```
$ORIGIN example.org.
0424D4EE81A0E3D119C6F835EDA21E94B565716F IN CERT PGP ...
F835EDA21E94B565716F                IN CERT PGP ...
B565716F                        IN CERT PGP ...
```

Si le même matériel de clé est mémorisé pour plusieurs noms de possesseur, l'utilisation du CNAME peut aider à éviter des duplications de données. Noter que le CNAME n'est pas toujours applicable, parce qu'il transpose un nom de possesseur en l'autre pour tous les objets, ce qui peut être sous optimal quand deux clés avec le même identifiant de clé sont mémorisées.

3.5 Noms de possesseur pour IPKIX, ISPKI, IPGP, et IACPKIX

Ces types sont mémorisés sous les mêmes noms de possesseur, à la fois fondé sur l'objet et sur le contenu, comme les types PKIX, SPKI, PGP, et ACPKIX.

4. Considérations de performances

Le protocole du système des noms de domaines (DNS) a été conçu pour de petits transferts, normalement de moins de 512 octets. Bien que de plus gros transferts s'effectuent correctement et que des travaux soient en cours pour rendre les plus grands transferts plus efficaces, il est toujours conseillé pour l'instant que tous les efforts raisonnables soient faits pour minimiser la taille des certificats mémorisés dans le DNS. Les mesures qui peuvent être prises à cette fin peuvent inclure d'utiliser le moins possible de champs facultatifs ou d'extensions et d'utiliser des valeurs de champ courtes pour les champs nécessaires de longueur variable.

Le champ RDATA dans le protocole DNS peut seulement contenir des données de 65535 octets (64kbit) ou moins. Cela signifie que chaque RR CERT NE DOIT PAS contenir plus de 64 kbit de charge utile, même si le certificat ou liste de révocation de certificats correspondant est plus grand. Le présent document traite cela en définissant les types de données "indirects" pour chaque type normal.

Déployer des RR CERT pour prendre en charge des messages électroniques signés numériquement change les schémas

d'accès des recherches sur le DNS de recherches par domaine en recherches par utilisateur. Si des messages électroniques signés numériquement et une recherche de clé/certificat fondée sur les RR CERT sont déployés à large échelle, cela peut conduire à une charge accrue sur le DNS, avec des conséquences potentielles sur les performances et l'efficacité de la mise en antémémoire. On ne sait pas si cette augmentation de charge sera ou non notable.

5. Contributeurs

La majorité de ce document est copiée textuellement de la RFC 2538, rédigée par Donald Eastlake 3rd et Olafur Gudmundsson.

6. Remerciements

Merci à David Shaw et Michael Graff de leurs contributions aux travaux antérieurs qui ont motivé, et servi d'inspiration pour le présent document.

Ce document a été amélioré par les suggestions et commentaires de Olivier Dubuisson, Scott Hollenbeck, Russ Housley, Peter Koch, Olaf M. Kolkman, Ben Laurie, Edward Lewis, John Loughney, Allison Mankin, Douglas Otis, Marcos Sanz, Pekka Savola, Jason Sloderbeck, Samuel Weiler, et Florian Weimer. Cette liste est sans doute incomplète. Mes excuses à tous les oubliés.

7. Considérations sur la sécurité

Par définition, les certificats contiennent leur propre signature d'authentification. Donc, il est raisonnable de mémoriser les certificats dans des zones non sécurisées du DNS ou de restituer les certificats du DNS sans mettre en œuvre les vérifications de sécurité du DNS ou de les différer dans un souci d'efficacité. On peut se fier aux résultats si la chaîne de certificats est vérifiée jusqu'à une clé de confiance connue et si cela est conforme à la politique de sécurité de l'utilisateur.

Autrement, si les certificats sont restitués d'une zone sûre du DNS avec les certifications de sécurité du DNS activées, et sont vérifiés par la sécurité du DNS, la clé au sein du certificat restitué peut être considérée comme de confiance sans vérifier si la chaîne de certificats se conforme à la politique de sécurité de l'utilisateur.

Si une organisation choisit de produire des certificats pour ses employés, en plaçant des RR CERT dans le DNS par nom de possesseur, et si DNSSEC (avec NSEC) est utilisé, il est possible à quelqu'un d'avoir la liste de tous les employés de l'organisation. Ceci n'est généralement pas considéré comme désirable, pour la même raison que les listes téléphoniques internes aux entreprises sont rarement rendues publiques et sont mêmes plutôt confidentielles.

Utiliser le type URI introduit un autre niveau d'indiscrétion qui peut ouvrir une nouvelle vulnérabilité. Une méthode pour sécuriser cela est d'inclure un hachage du certificat dans l'URI lui-même.

Si DNSSEC est utilisé, alors la non existence d'un RR CERT, et par conséquent, les certificats ou les listes de révocation de certificats peuvent être certifiés en toute sécurité. Sans DNSSEC, ceci n'est pas possible.

8. Considérations relatives à l'IANA

L'IANA a créé un nouveau registre pour le RR CERT : types de certificat. Le contenu initial de ce registre est :

N°	Type	Signification	Référence
0	Réservé		RFC 4398
1	PKIX	X.509 selon PKIX	RFC 4398
2	SPKI	Certificat SPKI	RFC 4398
3	PGP	Paquet OpenPGP	RFC 4398
4	IPKIX	URL d'un objet de données X.509	RFC 4398
5	ISPKI	URL d'un certificat SPKI	RFC 4398
6	IPGP	Empreinte digitale et URL d'un paquet OpenPGP	RFC 4398

7	ACPKIX	Certificat d'attribut	RFC 4398
8	IACPKIX	URL d'un certificat d'attribut	RFC 4398
9-252	Disponible pour l'allocation par l'IANA sur action de normalisation de l'IETF		
253	URI	URI privé	RFC 4398
254	OID	OID privée	RFC 4398
255	Réservé		RFC 4398
256-65279	Disponible pour l'allocation par l'IANA sur consensus de l'IETF		
65280-65534	Expérimental		RFC 4398
65535	Réservé		RFC 4398

Les types de certificats de 0x0000 à 0x00FF et de 0xFF00 à 0xFFFF ne peuvent être alloués que par une action de normalisation de l'IETF [RFC2434]. Le présent document alloue les valeurs 0x0001 à 0x0008, 0x00FD et 0x00FE. Les types de certificats de 0x0100 à 0xFEFF sont alloués par consensus de l'IETF [RFC2434] sur la base d'un document RFC du type de certificat. La disponibilité des types privés sous 0x00FD et 0x00FE devrait satisfaire la plupart des exigences de types propriétaires ou privés.

Le RR CERT réutilise le registre des numéros d'algorithme de sécurité du DNS. En particulier, le RR CERT exige que le numéro d'algorithme 0 reste réservé, comme décrit à la Section 2. L'IANA fait référence au RR CERT comme à un utilisateur de ce registre et de la valeur 0, en particulier.

9. Changements par rapport à la RFC 2538

1. Changements rédactionnels pour se conformer aux nouvelles exigences pour les documents, incluant de partager la section des références en deux parties, et mise à jour des références pour pointer sur les dernières versions, et ajout de références supplémentaires.
2. Amélioration de la terminologie. Par exemple, remplacement de "PGP" par "OpenPGP", pour s'aligner sur la RFC2440.
3. Au paragraphe 2.1, précision que les données de clé publique OpenPGP sont binaires, et n'ont pas le format ASCII, et référence au paragraphe 10.1 de la RFC 2440 sur la façon de traiter les clés OpenPGP, et reconnaissance que les mises en œuvre peuvent traiter des types de paquet supplémentaires.
4. Précision que les entiers dans le format de représentation sont décimaux.
5. Remplacement de KEY/SIG par DNSKEY/RRSIG etc, pour s'aligner sur la terminologie de DNSSEC bis. Référence améliorée pour les calculs d'algorithme d'étiquette de clé.
6. Ajout d'exemples qui suggèrent l'utilisation de CNAME pour réduire la consommation de bande passante.
7. À la Section 3, ajout du dernier paragraphe qui discute des noms de possesseur "fondés sur le contenu" et "fondés sur l'objet". Ajout du paragraphe 3.2 sur les noms de possesseur de CERT X.509 fondés sur l'objet, et du paragraphe 3.4 sur les noms de possesseur de CERT OpenPGP fondés sur l'objet.
8. Ajout des considérations de taille.
9. Les types SPKI ont été réservés, jusqu'à ce que les RFC 2692/2693 quittent le statut de expérimental.
10. Ajout des types indirects IPKIX, ISPKI, IPGP, et IACPKIX.
11. Un registre IANA des valeurs de type CERT a été créé.

10. Références

10.1 Références normatives

[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. *(MàJ par* RFC8174)

[RFC2247] S. Kille et autres, "Utilisation des domaines dans les noms distinctifs LDAP/X.500", janvier 1998.

[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)

[RFC2440] J. Callas, L. Donnerhacke, H. Finney et R. Thayer, "Format de message OpenPGP", novembre 1998. *(Obs. voir* 4880)

[RFC2822] P. Resnick, "Format de message Internet", avril 2001. *(Remplace la* RFC0822, STD 11, *Remplacée par* RFC5322)

[RFC3280] R. Housley, W. Polk, W. Ford et D. Solo, "Profil de certificat d'infrastructure de clé publique X.509 et de liste de révocation de certificat (CRL) pour l'Internet", avril 2002. *(Obsolète, voir* RFC5280)

[RFC3281] S. Farrell et R. Housley, "Profil de certificat d'attribut Internet pour l'autorisation", avril 2002. *(Obsolète, voir* RFC5755)

[RFC3986] T. Berners-Lee, R. Fielding et L. Masinter, "Identifiant de ressource uniforme (URI) : Syntaxe générique", STD 66, janvier 2005.

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

[RFC4034] R. Arends et autres, "Enregistrements de ressources pour les extensions de sécurité au DNS", mars 2005.

10.2 Références pour information

[RFC2246] T. Dierks et C. Allen, "Protocole TLS version 1.0", janvier 1999. *(P.S. ; MàJ par* RFC7919)

[RFC2693] C. Ellison, B. Frantz, B. Lampson, R. Rivest, B. Thomas, T. Ylonen, "Théorie des certificats SPKI", septembre 1999. *(Expérimentale)*

[RFC3548] S. Josefsson, "Codages de données Base16, Base32, et Base64", juillet 2003. *(Obsolète, voir* 4648) *(Info)*

[RFC3851] B. Ramsdell, "Spécification du message d'extensions de messagerie Internet multi-objets/sécurisé (S/MIME) version 3.1", juillet 2004. *(Obsolète, voir* RFC5751)

[RFC4025] M. Richardson, "Méthode pour mémoriser le matériel de clés IPsec dans le DNS", mars 2005. *(P.S.)*

[RFC4301] S. Kent et K. Seo, "Architecture de sécurité pour le protocole Internet", décembre 2005. *(P.S.) (Remplace la* RFC2401)

Appendice A. Conditions de copie

Adresse de l'auteur

Simon Josefsson

mél : simon@josefsson.org

Déclaration complète de droits de reproduction

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