Groupe de travail Réseau
Request for Comments : 4985
Catégorie : sur la voie de la normalisation

S. Santesson, Microsoft
août 2007
Traduction Claude Brière de L'Isle

Nom de remplacement de sujet d'infrastructure de clé publique X.509 pour l'Internet pour exprimer un nom de service

Statut du présent mémoire
Le présent document spécifie un protocole de l'Internet sur la voie de la 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 "Protocoles officiels de l'Internet" (STD 1) pour voir l'état de normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.
(La présente traduction incorpore les errata 2520, 2395, 2396, 2397, 2399)

Résumé
Le présent document définit une nouvelle forme de nom à inclure dans le champ otherName d'une extension de nom de remplacement de sujet qui permet à un sujet de certificat d'être associé aux composants de nom de service et de nom de domaine d'un enregistrement de ressource de service DNS.

Table des Matières

1. Introduction

Le présent document spécifie une forme de nom à inclure dans les certificats X.509 qui peuvent être utilisés par un consommateur de certificat pour vérifier qu'un certain hôte est autorisé à fournir un service spécifique au sein d'un domaine.

La [RFC2782] définit un enregistrement de ressource (RR, *Resource Record*) du DNS pour spécifier la localisation des services (RR SRV) qui permet aux clients de demander un service/protocole spécifiquec pour un domaine spécifique et de revenir aux noms de tous serveurs disponibles.

Les formes de nom existantes dans les certificats X.509 prennent en charge l'authentification d'un nom d'hôte. Ceci est utile quand le nom de l'hôte est connu par le client avant l'authentification.

Quand un nom d'hôte serveur est découvert par une interrogation de recherche de RR du DNS sur la base du nom de service, le client peut devoir authentifier l'autorisation du serveur pour fournir le service demandé en plus du nom d'hôte du serveur.

Bien que les serveurs du DNS puissent avoir la capacité de fournir des informations de confiance, il peut y avoir de

nombreuses autres situations où le lien entre le nom de l'hôte et le service fourni doive être pris en charge par des accréditifs supplémentaires.

La forme actuelle de nom de remplacement de sujet dNSName GeneralName ne permet d'exprimer les noms d'hôte du DNS que dans la "syntaxe de nom préférée", comme spécifié dans la [RFC1034]. Cette définition n'est donc pas assez large pour permettre l'expression d'un service en rapport avec ce domaine.

1.1 Terminologie

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. Définitions de noms

Cette section définit le nom SRVName *(nom de service)* comme une forme de otherName *(autre nom)* dans la structure GeneralName *(nom général)* d'un SubjectAltName *(nom de sujet de remplacement)* défini dans la [RFC3280].

IDENTIFIANT D'OBJET id-on-dnsSRV ::= { id-on 7 }

SRVName ::= IA5String (SIZE (1..MAX))

Le SRVName, si il est présent, DOIT contenir un nom de service et un nom de domaine sous la forme suivante :

_Service.Name

Le contenu des composants de cette forme de nom DOIT être cohérent avec la définition correspondante de ces composants dans un RR SRV conformément à la [RFC2782].

Le contenu de ces composants est :

Service : le nom symbolique du service désiré, comme défini dans les numéros alloués [RFC3232] ou en local. Un souligné (_) est ajouté devant l'identifiant de service pour éviter les collisions avec les étiquettes du DNS qui existent dans la nature. Certains services largement utilisés, en particulier POP, n'ont pas un seul nom universel. Si les numéros alloués désignent le service indiqué, ce nom est le seul nom permis dans le composant de service de cette forme de nom. Le service est insensible à la casse.

Nom : un nom de domaine du DNS, représentant un domaine pour lequel le producteur de certificat a attesté que le sujet certifié est un fournisseur légitime du service identifié. Si le nom de domaine est un nom de domaine internationalisé (IDN, *Internationalized Domain Name*) alors le codage en forme ASCII DEVRA être fait comme défini à la Section 3.

Même si cette forme de nom se fonde sur la définition de l'enregistrement de ressource de service (RR SRV) de la [RFC2782] et peut être utilisée pour améliorer l'authentification ultérieure de la découvert de service fondée sur le DNS, la présente norme ne définit aucune nouvelle condition ni exigence concernant l'utilisation de RR SRV pour la découverte de service ou sur quand et où une telle utilisation est appropriée.

Le format d'un RR DNS, conformément à la RFC 2782, inclut aussi un composant protocole (_Service._Proto.Name). Ce composant de protocole n'est pas inclus dans le SRVName spécifié dans le présent document. L'objet du SRVName est limité à l'autorisation d'une fourniture de service au sein d'un domaine. Il sort du domaine d'application de SRVName de fournir des moyens de vérifier que l'hôte utilise un protocole prévu. En omettant le composant de protocole du SRVName, deux importants avantages sont obtenus :

* Un certificat avec un seul SRVName peut être produit à un hôte qui offre plusieurs solutions de remplacement de protocole.

* Les règles de traitement des contraintes de nom (spécifiées à la Section 4) sont significativement moins complexes à

définir sans le composant de protocole.

Un SRVName présent dans un certificat NE DOIT PAS être utilisé pour identifier un hôte en l'absence d'une des conditions suivantes :

* l'utilisation de cette forme de nom est spécifiée par le protocole de sécurité utilisé et le service identifié a un nom de service défini selon la RFC 2782, ou ;
* l'utilisation de cette forme de nom est configurée par la politique locale.

3. Noms de domaine internationalisés

IA5String est limité au jeu de caractères ASCII. Pour s'accommoder des noms de domaine internationalisés dans la structure actuelle, les mises en œuvre conformes DOIVENT convertir les noms de domaine internationalisés au format de codage compatible ASCII (ACE, *ASCII Compatible Encoding*) comme spécifié à la Section 4 de la [RFC3490] avant de mémoriser la partie Nom du SRVName. Précisément, les mises en œuvre conformes DOIVENT effectuer l'opération de conversion spécifiée à la Section 4 de la [RFC3490], avec les éclaircissements suivants :

* dans l'étape 1, le nom de domaine DEVRA être considéré comme une "chaîne mémorisée". C'est-à-dire, le fanion AllowUnassigned *(non alloués permis)* NE DEVRA PAS être établi ;
* dans l'étape 3, établir le fanion appelé "UseSTD3ASCIIRules" *(utiliser les règles ASCII du STD 3)* ;
* dans l'étape 4, traiter chaque étiquette avec l'opération "ToASCII" ; et
* dans l'étape 5, changer tous les séparateurs d'étiquette en U+002E (point).

Dans la comparaison pour égalité des noms du DNS, les mises en œuvre conformes DOIVENT effectuer une confrontation exacte insensible à la casse sur le nom de domaine entier. Quand on évalue les contraintes de nom, les mises en œuvre conformes DOIVENT effectuer une confrontation exacte insensible à la casse étiquette par étiquette.

Les mises en œuvre DEVRAIENT convertir les IDN en Unicode avant l'affichage. Précisément, les mises en œuvre conformes DEVRAIENT effectuer l'opération de conversion spécifiée à la Section 4 de la [RFC3490], avec les éclaircissements suivants :

* dans l'étape 1, le nom de domaine DEVRA être considéré comme une "chaîne mémorisée". C'est-à-dire, le fanion AllowUnassigned NE DEVRA PAS être établi ;

* dans l'étape 3, établir le fanion appelé "UseSTD3ASCIIRules";

* dans l'étape 4, traiter chaque étiquette avec l'opération "ToUnicode" ; et

* sauter l'étape 5.

Note : les mises en œuvre DOIVENT permettre des exigences d'espace augmentées pour les IDN. Une étiquette IDN ACE va commencer par les quatre caractères supplémentaires "xn--" et peut exiger jusqu'à cinq caractères ASCII pour spécifier un seul caractère international.

4. Règles de correspondance de contraintes de nom

Des contraintes de noms, comme spécifiées dans la RFC 3280, PEUVENT être appliquées au SRVName en ajoutant la restriction de nom dans l'extension de nom sous la forme d'un SRVName.

Les restrictions de SRVName sont exprimées comme un SRVName complet (_mail.exemple.com), juste un nom de service (_mail), ou juste comme un nom DNS (exemple.com). La restriction de nom de la partie Nom de service et la partie Nom DNS du SRVName sont traitées séparément.

Si un nom de service est inclus dans la restriction, alors cette restriction ne peut être satisfaite que par un SRVName qui inclut un nom de service correspondant. Si la restriction a un nom de service absent, alors cette restriction est satisfaite par tout SRVName qui correspond à la partie Domaine de la restriction.

Les restrictions sur un nom DNS sont exprimées comme hôte.exemple.com. Tout nom DNS qui peut être construit en ajoutant simplement des sous domaines du côté gauche du nom satisfait la partie Nom DNS de la contrainte de nom. Par

exemple, www.hôte.exemple.com satisferait la contrainte (hôte.exemple.com) mais pas 1hôte.exemple.com.

Exemples :

Contrainte de noms

Restriction de SRVName	**SRVName correspondant**	**SRVName non correspondant**
exemple.com	_mail.exemple.com _ntp.exemple.com _mail.1.exemple.com	_mail.1exemple.com
_mail	_mail.exemple.com _mail.1exemple.com	_ntp.exemple.com
_mail.example.com	_mail.exemple.com _mail.1.exemple.com	_mail.1exemple.com _ntp.exemple.com

5. Considérations sur la sécurité

L'allocation de services aux hôtes peut subir des changements. Les mises en œuvre devraient être conscientes du besoin de révoquer les vieux certificats qui ne reflètent plus l'allocation actuelle des services et donc s'assurer que tous les certificats produits sont à jour.

Quand des certificats X.509 améliorés avec la forme de nom spécifiée dans la présente norme sont utilisés pour améliorer l'authentification de la découverte de service sur la base d'une interrogation d'un RR SRV auprès d'un serveur du DNS, toutes les considérations de sécurité de la RFC 2782 s'appliquent.

6. 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)

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

[RFC2782] A. Gulbrandsen, P. Vixie et L. Esibov, "Enregistrement de ressource DNS pour la spécification de la localisation des services (DNS SRV)", février 2000.

[RFC3232] J. Reynolds, "Numéros alloués : la RFC 1700 est remplacée par une base de données en ligne", janvier 2002.

[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)

[RFC3490] P. Faltstrom et autres, "Internationalisation des noms de domaine dans les applications (IDNA)", mars 2003. (*Remplacée par les* RFC5890 et 5891, *P.S.*)

Appendice A. Syntaxe ASN.1

Comme dans la RFC 2459, les modules ASN.1 sont fournis dans deux variantes différentes de la syntaxe ASN.1.

Cette Section décrit les objets de données utilisés par les composants d'infrastructure de clé publique (PKI, *Public Key Infrastructure*) conformes dans une syntaxe "de style ASN.1". Cette syntaxe est un hybride des syntaxes ASN.1 de 1988 et de 1993. La syntaxe ASN.1 de 1988 est augmentée du type UTF8String UNIVERSAL de 1993.

La syntaxe ASN.1 ne permet pas l'inclusion des déclarations de type dans le module ASN.1, et la norme d'ASN.1 de 1993 ne permet pas l'utilisation des nouveaux types UNIVERSAL dans les modules qui utilisent la syntaxe de 1988. Par suite, ce module ne se conforme à aucune des versions de la norme ASN.1.

L'Appendice A.1 peut être analysé par un analyseur ASN.1 de 1988 en remplaçant les définitions pour les types UNIVERSAL par le fourre-tout "ANY" de 1988.

L'Appendice A.2 peut être analysé "tel quel" par un analyseur ASN.1 conforme à la version 1997.

En cas de discordances entre ces modules, celui de 1988 est normatif.

Appendice A.1. Module ASN.1 1988

```
PKIXServiceNameSAN88 {iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) id-
mod(0) id-mod-dns-srv-name-88(39) }

ÉTIQUETTES EXPLICITES DE DÉFINITION ::=

DÉBUT

-- EXPORTE TOUT --

IMPORTE

-- UTF8String, / Déplacer les tirets avant les barres obliques si UTF8String n'est pas résolu avec le compilateur

id-pkix
        DE PKIX1Explicit88 { iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7)
        id-mod(0) id-pkix1-explicit(18) }                ; d'après la [RFC3280]

--Identifiant et syntaxe d'objet Nom de service
-- IDENTIFIANT D'OBJET id-pkix  ::= {1 3 6 1 5 5 7}

IDENTIFIANT D'OBJET id-on ::= { id-pkix 8 }

IDENTIFIANT D'OBJET  id-on-dnsSRV ::= { id-on 7 }

SRVName ::= IA5String (SIZE (1..MAX))

FIN
```

Appendice A.2. Module ASN.1 1993

```
PKIXServiceNameSAN93 {iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) id-
mod(0) id-mod-dns-srv-name-93(40) }

ÉTIQUETTES EXPLICITES DE DÉFINITION ::=

DÉBUT

-- EXPORTE TOUT --

IMPORTE

id-pkix
        DE PKIX1Explicit88 { iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7)
        id-mod(0) id-pkix1-explicit(18) } ;
         -- d'après la [RFC3280]

-- La définition de GeneralName en utilisant la syntaxe ASN.1 de 1993 inclut :
```

```
OTHER-NAME ::= TYPE-IDENTIFIER

-- Identifiant d'objet Nom de service

IDENTIFIANT D'OBJET id-on ::= { id-pkix 8 }

IDENTIFIANT D'OBJET id-on-dnsSRV ::= { id-on 7 }

-- Nom de service

srvName OTHER-NAME ::= { SRVName IDENTIFIED BY { id-on-dnsSRV }}

SRVName ::= IA5String (SIZE (1..MAX))

FIN
```

Adresse de l'auteur

Stefan Santesson
Microsoft
Tuborg Boulevard 12
2900 Hellerup
Denmark

mél : stefans@microsoft.com

Déclaration complète de droits de reproduction

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