Groupe de travail Réseau
Request for Comments : 4043
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

D. Pinkas, Bull
T. Gindin, IBM
mai 2005

Identifiant permanent d'infrastructure de clé publique X.509 Internet

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

Résumé
Le présent document définit une nouvelle forme de nom, appelé identifiant permanent, qui peut être inclus dans l'extension subjectAltName *(nom sujet de remplacement)* d'un certificat de clé publique produit à une entité.

L'identifiant permanent est une caractéristique facultative qui peut être utilisée par une autorité de certification (CA, *Certification Authority*) pour indiquer que deux certificats ou plus se rapportent à la même entité, même si elles contiennent un nom de sujet différent ou des noms différents dans l'extension subjectAltName, ou si le nom ou l'affiliation de cette entité mémorisé dans le sujet ou une autre forme de nom dans l'extension subjectAltName a changé.

Le nom sujet, porté dans le champ Subject, n'est unique que pour chaque entité sujette certifiée par cette CA comme défini par le champ Nom du producteur. Cependant, la nouvelle forme de nom peut porter un nom unique pour chaque entité sujette certifiée par une CA.

Table des Matières

1. Introduction

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].

La présente spécification se fonde sur la [RFC3280], qui définit les formats et la sémantique des certificats sous-jacents nécessaires pour une pleine mise en œuvre de la présente norme.

Le champ Sujet d'un certificat de clé publique identifie l'entité associée à la clé publique mémorisée dans le champ Clé

publique sujette. Les noms et identités d'un sujet peuvent être portés dans le champ Sujet et/ou l'extension subjectAltName. Lorsque le champ Sujet n'est pas vide, il DOIT contenir un nom distinctif (DN, *distinguished name*) X.500. Le DN DOIT être unique pour chaque entité sujette certifiée par une seule CA comme défini par le champ Nom du producteur.

Le nom sujet change chaque fois qu'un des composants de ce nom change. Il y a plusieurs raisons pour qu'un tel changement survienne.

Pour les employés d'une entreprise ou organisation, la personne peut passer à une position différentes au sein de la même entreprise et va donc entrer dans une autre unité d'organisation. Inclure l'unité d'organisation dans le nom peut cependant être très utile pour permettre aux consommateurs d'assertions (RP, *relying party*) qui utilisent ce certificat d'identifier le bon individu.

Pour les citoyens, un individu peut changer de nom par un processus légal, en particulier par suite de mariage *(dans certains pays peut-être mais ce n'est pas le cas en France où, sauf décision du Conseil d'État, l'état civil est intangible)*.

Tout sujet de certificat identifié par une localisation géographique peut se délocaliser et changer au moins une partie de ses attributs de localisation (par exemple, le nom du pays, l'état ou la région, la ville, ou la rue).

Un identifiant permanent consiste en une valeur d'identifiant allouée au sein d'un certain espace de dénomination par l'organisation qui est d'autorité pour cet espace de dénomination. L'organisation qui alloue la valeur d'identifiant peut être la CA qui a produit le certificat ou une organisation différente appelée une autorité d'allocation.

Une autorité d'allocation peut être un gouvernement, une agence gouvernementale, une corporation, ou toute autre sorte d'organisation. Elle DOIT avoir un identifiant unique pour la distinguer de toute autre autorité de cette sorte. Dans la présente norme, cet identifiant DOIT être un identifiant d'objet.

Un identifiant permanent peut être utile dans trois contextes : le contrôle d'accès, la non répudiation et les enregistrements de vérification *(audit records)*.

Pour le contrôle d'accès, l'identifiant permanent peut être utilisé dans une liste de contrôle d'accès (ACL, *Access Control List*) au lieu du DN ou de toute autre forme de nom et n'aurait pas besoin d'être changé, même si le nom sujet de l'entité change. Pour la non répudiation, l'identifiant permanent peut être utilisé pour relier différentes transactions à la même entité, même lorsque le nom sujet de l'entité change.

Pour les enregistrements de vérification, l'identifiant permanent peut être utilisé pour relier différents enregistrements de vérification à la même entité, même lorsque le nom sujet de l'entité change.

Pour deux certificats qui ont tous deux été vérifiés comme valides conformément à une certaine politique de validation et qui contiennent un identifiant permanent, ces certificats se rapportent à la même entité si leur identifiant permanent correspond, quel que puisse être le contenu du DN ou autres composants du subjectAltName.

Comme l'utilisation des identifiants permanents peut entrer en conflit avec la confidentialité, les CA DEVRAIENT annoncer aux acheteurs de certificats l'utilisation des identifiant permanents dans les certificats.

2. Définition d'un identifiant permanent

Cet identifiant permanent est un nom défini comme une forme de otherName *(autre nom)* de la structure "GeneralName" *(nom général)* dans "SubjectAltName", comme défini dans [X.509] et la [RFC3280].

Une CA qui inclut un identifiant permanent dans un certificat certifie que tout certificat de clé publique contenant les mêmes valeurs pour cet identifiant se réfère à la même entité.

L'utilisation d'un identifiant permanent est FACULTATIVE. L'identifiant permanent est défini comme suit :

```
IDENTIFIANT D'OBJET   id-on-permanentIdentifier   ::= { id-on 3 }
      PermanentIdentifier ::=  SEQUENCE {
        identifierValue    UTF8String            FACULTATIF,
                    -- si absent, on utilise l'attribut serialNumber, si un tel attribut est présent dans le DN sujet.
        assigner          IDENTIFIANT D'OBJET      FACULTATIF
                    -- si absent, l'alloueur est le producteur de certificat.
  }
```

Le champ identifierValue *(valeur d'identifiant)* est facultatif.

Lorsque le champ identifierValue est présent, identifierValue accepte une syntaxe : UTF8String *(chaîne UTF 8)*.

Lorsque le champ identifierValue est absent, la valeur de l'attribut serialNumber *(numéro de série)* (comme défini au paragraphe 5.2.9 de [X.520]) provenant du plus profond RDN du DN sujet est alors la valeur à prendre comme identifierValue. Dans ce cas, il DOIT y avoir au moins un attribut serialNumber dans le DN sujet, autrement, l'identifiant permanent NE DEVRA PAS être utilisé.

Le champ Assigner est facultatif.

Lorsque le champ Assigner est présent, il est alors un OID qui identifie un espace de dénomination, c'est-à-dire, à la fois une autorité d'allocation et le type de ce champ. De façon caractéristique, le préfixe de l'OID identifie l'autorité d'allocation, et un suffixe est utilisé pour identifier le type d'identifiant permanent.

Lorsque le champ Assigner est absent, l'identifiant permanent est alors localement unique pour la CA.

Les diverses combinaisons sont détaillées ci-dessous :

1. Les deux champs Assigner et identifierValue sont présents : identifierValue est la valeur pour ce type d'identifiant. Le champ Assigner identifie l'autorité d'allocation et le type d'identifiant permanent qui est identifié. L'identifiant permanent est unique au monde parmi toutes les CA. Dans ce cas, deux identifiants permanents de ce type correspondent si et seulement si leurs champs Assigner correspondent et si le contenu du champ identifierValue dans les deux identifiants permanents consistent en les mêmes codets Unicode présentés dans le même ordre.

2. Le champ Assigner est absent et le champ identifierValue est présent : l'autorité d'allocation est la CA qui a produit le certificat. identifierValue est donnée par la CA et l'identifiant permanent est seulement local pour la CA qui a produit le certificat. Dans ce cas, deux identifiants permanents de ce type correspondent si et seulement si le DN du producteur dans les certificats qui le contiennent correspond en utilisant la règle distinguishedNameMatch, comme défini dans X.501, et les deux valeurs du champ identifierValue consistent en les mêmes codets Unicode présentés dans le même ordre.

3. Les deux champs Assigner et identifierValue sont absents: Si il y a un ou plusieurs RDN contenant un attribut serialNumber (seul ou accompagné d'autres attributs) alors la valeur contenue dans le numéro de série d'un plus profond de ces RDN DEVRA être utilisée comme valeur d'identifiant ; autrement, la définition de l'identifiant est invalide et l'identifiant permanent NE DEVRA PAS être utilisé. L'identifiant permanent n'est local que pour la CA qui a produit le certificat. Dans ce cas, deux identifiants permanents de ce type correspondent si et seulement si le DN du producteur qui est dans les certificats qui les contiennent correspond et si les attributs de numéro de série au sein des DN sujets de ces mêmes certificats correspondent aussi en utilisant la règle caseIgnoreMatch.

4. Le champ Assigner est présent et le champ Valeur d'identifiant est absent : si il y a un ou plusieurs RDN contenant un attribut Numéro de série (seul ou accompagné d'autres attributs) la valeur contenue dans le numéro de série du plus profond de ces RDN DEVRA alors être utilisée comme valeur d'identifiant ; autrement, la définition d'identifiant permanent est invalide et l'identifiant permanent NE DEVRA PAS être utilisé. Le champ Assigner identifie l'autorité d'allocation et le type d'identifiant permanent qui est identifié. L'identifiant permanent est unique au monde parmi toutes les CA. Dans ce cas, deux identifiants permanents de ce type correspondent si et seulement si leurs champs Assigner correspondent et si le contenu des attributs serialNumber au sein des DN sujets de ces mêmes certificats correspond en utilisant la règle caseIgnoreMatch.

Note : L'arc complet de l'identifiant d'objet utilisé pour identifier la forme de nom de l'identifiant permanent est déduit en utilisant :

```
IDENTIFIANT D'OBJET id-pkix ::= { iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5)
                                  pkix(7) }
IDENTIFIANT D'OBJET id-on  ::= { id-pkix 8 }   -- autres formes de nom
```

3. Considérations relatives à l'IANA

Aucune action de l'IANA n'est nécessaire. Cependant, un numéro d'entreprise privée peut être utilisé pour construire un OID pour le champ Assigner (voir l'Annexe B.1.).

4. Considérations sur la sécurité

Une certaine entité peut avoir à un moment ou à des moments différents plusieurs formes d'identités. Si l'identifiant permanent est localement unique pour la CA (c'est-à-dire, si le champ Assigner n'est pas présent) deux certificats provenant de la même CA peuvent être comparés.

Lorsque deux certificats contiennent des identifiants permanents identiques, un consommateur d'assertions peut déterminer qu'ils se réfèrent à la même entité.

Si l'identifiant permanent est unique au monde parmi toutes les CA (c'est-à-dire, si le champ Assigner est présent) deux certificats provenant de CA différentes peuvent alors être comparés. Quand ils contiennent deux identifiants permanents identiques, le consommateur d'assertions peut alors déterminer qu'ils se réfèrent à la même entité. Il est de la responsabilité de la CA de vérifier que l'identifiant permanent qui est inclus dans le certificat se réfère au sujet certifié.

L'identifiant permanent identifie l'entité, sans considération de toute extension d'attribut. Lorsque un certificat de clé publique contient des extensions d'attributs, l'identifiant permanent, si il est présent, ne devrait pas être utilisé pour les besoins du contrôle d'accès mais seulement à des fins de vérification. La raison en est que comme ces attributs peuvent changer, l'accès pourrait être accordé sur des attributs qui étaient présents à l'origine dans un certificat produit à cette entité mais ne sont plus présents dans le certificat actuel.

Les noms de sujets dans les certificats sont choisis par la CA productrice et sont obligatoirement uniques pour chaque CA ; de sorte qu'il ne peut pas y avoir de collision de noms entre noms sujets provenant de la même CA. Un tel nom peut être un nom d'entité d'extrémité lorsque le certificat est un certificat feuille, ou un nom de CA, lorsque c'est un certificat de CA.

Comme un nom n'est unique que vers sa CA supérieure, sauf si certaines contraintes de dénomination sont utilisées, un nom ne sera garanti d'être unique au monde que lorsque il est considéré d'inclure une séquence de tous les noms des CA supérieures. Donc, deux certificats qui sont produits sous le même DN producteur et qui contiennent la même extension d'identifiant permanent sans un champ Assigner ne se réfèrent pas nécessairement à la même entité.

Des vérifications supplémentaires doivent être effectuées, par exemple, vérifier si les valeurs de clé publique des deux CA qui ont produit les certificats à comparer sont identiques ou si la séquence des noms de CA dans le chemin de certification de l'ancre de confiance à la CA est identique.

Lorsque les vérifications ci-dessus échouent, les identifiants permanents peuvent quand même correspondre si il y a eu un retour à zéro des clés de CA. Dans ce cas, la vérification est plus compliquée.

La certification de différentes CA avec le même DN par différentes CA a d'autres conséquences négatives dans diverses parties de la PKI, en particulier en rendant la structure IssuerAndSerialNumber du paragraphe 10.2.4 de la[RFC3852] ambiguë.

L'identifiant permanent permet aux organisations de créer des liens entre différents certificats associés à une entité produits avec ou sans périodes de validité qui se chevauchent. Cette capacité de lier différents certificats peut entrer en conflit avec la confidentialité. Il est donc important qu'une CA divulgue clairement aux sujets potentiels de ces certificats tous plans de production de certificats qui incluent un identifiant permanent.

5. Références

5.1 Références normatives

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

[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)

[RFC3629] F. Yergeau, "UTF-8, un format de transformation de la norme ISO 10646", STD 63, novembre 2003.

[X.501] Recommandation UIT-T X.501 | ISO 9594-2: 2001, "Technologie de l'information - Interconnexion des systèmes ouverts - L'Annuaire : Modèles", février 2001.

5.2 Références pour information

[RFC3852] R. Housley, "Syntaxe de message cryptographique (CMS)", juillet 2004. *(Obsolète, voir la* RFC5652)

[X.509] Recommandation UIT-T X.509 (1997 E), "Technologie de l'information - Interconnexion des systèmes ouverts - L'Annuaire : cadre d'authentification", juin 1997.

[X.520] Recommandation UIT-T X.520, "Technologie de l'information - Interconnexion des systèmes ouverts - L'Annuaire : Types d'attribut choisis", juin 1997.

[X.660] Recommandation UIT-T X.660, "Technologie de l'information - Interconnexion des systèmes ouverts - Procédures pour le fonctionnement des autorités d'enregistrement OSI : Procédures générales", 1992.

[X.680] Recommandation UIT-T X.680, "Technologie de l'information – notation n° i de syntaxe abstraite", 1997.

Appendice A. Syntaxe ASN.1

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

Cette section décrit les objets de données utilisés par les composants de PKI 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 1988 est augmentée du type UNIVERSAL 1993 UTF8String.

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

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

L'Appendice A.2 peut être analysé "tel quel" par un analyseur ASN.1 conforme au modèle 1997.

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

A.1 Module ASN.1 1988

PKIXpermanentidentifier88 {iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) id-mod(0) id-mod-perm-id-88(28) }

ÉTIQUETTES DE DÉFINITION EXPLICITES ::=

DÉBUT

-- EXPORTE TOUT --

IMPORTE

-- UTF8String, / retirer les tirets devant la barre oblique si UTF8String n'est pas résolu par le compilateur.
-- Le contenu de ce type est conforme à la [RFC3629].

```
    id-pkix
        FROM PKIX1Explicit88 { iso(1) identified-organization(3)
        dod(6) internet(1) security(5) mechanisms(5) pkix(7)
        id-mod(0) id-pkix1-explicit(18) } ;
        -- from [RFC3280]
```

-- Identifiant d'objet et syntaxe d'identifiant permanent

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

IDENTIFIANT D'OBJET  id-on-permanentIdentifier   ::= { id-on 3 }

 PermanentIdentifier ::= SEQUENCE {
    identifierValue    UTF8String            FACULTATIF,
                -- si absent, on utilise l'attribut serialNumber, si un tel attribut est présent dans le DN sujet.
       assigner          IDENTIFIANT D'OBJET      FACULTATIF
                -- si absent, l'alloueur est le producteur de certificat.
 }

FIN
```

A.2 Module ASN.1 1993

```
PKIXpermanentidentifier93 {iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) id-
mod(0) id-mod-perm-id-93(29) }

ÉTIQUETTES DE DÉFINITION EXPLICITES ::=

DÉBUT

-- EXPORTE TOUT --

IMPORTE

   id-pkix
      FROM 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]

   ATTRIBUTE
      FROM InformationFramework {joint-iso-itu-t ds(5) module(1) informationFramework(1) 4};
       -- d'après [X.501]

-- Identifiants d'objet Identifiant permanent

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

IDENTIFIANT D'OBJET  id-on-permanentIdentifier ::= { id-on 3 }

-- identifiant permanent

ATTRIBUT    permanentIdentifier ::= {
       WITH SYNTAX     PermanentIdentifier
       ID              id-on-permanentIdentifier }

  PermanentIdentifier ::= SEQUENCE {
     identifierValue    UTF8String            FACULTATIF,
                -- si absent, on utilise l'attribut serialNumber, si un seul tel attribut est présent dans le DN sujet.
     assigner          IDENTIFIANT D'OBJET      FACULTATIF
                -- si absent, l'alloueur est le producteur de certificat.
}

FIN
```

Appendice B. OID pour les organisations

Afin de construire un OID pour le champ Assigner, les organisations doivent d'abord avoir un OID enregistré pour elles-mêmes. Un tel OID doit être obtenu d'une autorité d'enregistrement conformément à [X.660]. Dans certains cas, les OID sont fournis gratuitement. Dans d'autres cas, une redevance unique est exigée. La principale différence tient à la nature des informations qui sont collectées au moment de l'enregistrement et à la façon dont la précision de ces informations est vérifiée.

B.1 Utilisation de l'IANA (Internet Assigned Numbers Authority)

Le formulaire de demande de numéro d'entreprise privée dans la liste des OID de l'IANA est : http://www.iana.org/cgi-bin/enterprise.pl

Actuellement, l'IANA attribue gratuitement les numéros. Le préfixe d'entreprise privée enregistrée par l'IANA est : iso.org.dod.internet.private.enterprise (1.3.6.1.4.1)

Ces numéros sont utilisés, entre autres choses, pour définir les MIB privées SNMP.

Les allocations officielles sous cet OID sont mémorisées dans le fichier IANA "enterprise-numbers" disponible à : http://www.iana.org/assignments/enterprise-numbers

B.2 Utilisation d'un membre de l'ISO

L'ISO a défini la structure d'OID de façon telle que chaque pays membre de l'ISO ait son propre OID unique. Chaque membre de l'ISO est donc libre d'allouer son propre espace d'arc en dessous.

Les organisations et entreprises peuvent contacter les membres de l'ISO lorsque leur organisation ou entreprise est constituée pour obtenir un OID d'organisation/entreprise.

Actuellement, les membres de l'ISO n'allouent pas gratuitement les OID d'organisation/entreprise.

La plupart d'entre eux ne publient pas de registre de ces OID qu'ils ont alloué, interdisant parfois l'accès aux organisations enregistrées ou préférant facturer les recherches demande par demande. L'utilisation des OID des organisations membres de l'ISO qui ne publient pas un tel registre peut imposer des coûts supplémentaires aux CA qui ont besoin de s'assurer que l'OID correspond à l'organisation enregistrée.

Par exemple, AFNOR (Association Française de Normalisation - organisation française membre de l'ISO) a défini un arc pour allouer des OID aux entreprises : {iso (1) member-body (2) fr (250) type-org (1) organisation (n)}

B.3 Utilisation d'un ICD de BSI pour spécifier un schéma d'identification nouveau ou existant

Le désignateur de code international (ICD, *International Code Designator*) est utilisé pour identifier de façon univoque un schéma d'identification d'organisation conforme à la norme ISO 6523. ISO 6523 est une norme qui définit la structure appropriée d'un identifiant et la procédure d'enregistrement pour un ICD. La conjonction de l'ICD avec un identifiant produit par l'autorité d'enregistrement est unique au monde.

La structure de base du code contient les composants suivants :
- une valeur d'ICD : le désignateur de code international produit au schéma d'identification rend l'identifiant unique au monde (jusqu'à 4 chiffres),
- l'organisation, généralement une entreprise ou une organisation gouvernementale (jusqu'à 35 caractères),
- une partie d'organisation (OPI, *Organization Part Identifier*). Un identifiant alloué à une partie d'organisation (facultatif, jusqu'à 35 caractères).

L'ICD est aussi équivalent à un identifiant d'objet (OID) sous l'arc {1(iso). 3(identified organization)}.

Au nom de l'ISO, l'institut britannique de normalisation (BSI, *British Standards Institution*) est l'autorité d'enregistrement pour les organisations sous l'arc {iso (1) org(3)}. Cela signifie que BSI enregistre les codes d'autorités productrices (organisations) par valeurs d'ICD qui sont équivalents aux OID de la forme {iso (1) org(3) icd(xxxx)}. La valeur d'identifiant correspondante est la valeur de code du schéma identifié par icd(xxxx).

Par exemple, l'ICD 0012 a été alloué à l'association européenne des fabricants informatiques (ECMA, *European Computer Manufacturers Association*). Donc l'OID pour ECMA est {iso(1) org(3) ecma(12)}.

Pour s'enregistrer auprès de BSI, une "autorité de parrainage" doit se porter garante pour l'organisation candidate. L'enregistrement n'est pas gratuit. Les autorités de parrainage reconnues sont : les comités ou sous comités techniques de l'ISO, les membres de l'ISO ou les organisations internationales qui ont un statut de liaison avec l'ISO ou avec un de ses comités ou sous comités techniques.

Un exemple d'autorité de parrainage est l'association EDIRA (EDI/EC Registration Authority, web: http://www.edira.org, email:info@edira.org).

La liste numérique de tous les ICD qui ont été attribués est publiée sur la page du site :
http://www.edira.org/documents.htm#icd-List

Note : l'IANA possède le code ICD 0090, mais (vraisemblablement) n'a pas l'intention de l'utiliser à présent.

Adresse des auteurs

Denis Pinkas
Bull
Rue Jean-Jaures BP 68
78340 Les Clayes-sous-Bois
FRANCE
mél : Denis.Pinkas@bull.net

Thomas Gindin
IBM Corporation
6710 Rockledge Drive
Bethesda, MD 20817
USA
mél : tgindin@us.ibm.com

Déclaration complète de droits de reproduction

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