PKIX Working Group
INTERNET-DRAFT
Expires: March 2005
Target category: Standard Track

D. Pinkas (Bull)
T. Gindin (IBM)
September 2004

Internet X.509 Public Key Infrastructure Permanent Identifier

<draft-ietf-pkix-pi-11.txt>

Status of this Memo

Abstract

This document define a new form of name, called permanent identifier, that may be included in the subjectAltName extension of a public key certificate issued to an entity.

The permanent identifier is an optional feature that may be used by a CA to indicate that two or more certificates relate to the same entity, even if they contain different subject name (DNs) or different names in the subjectAltName extension, or if the name or the affiliation of that entity stored in the subject or another name form in the subjectAltName extension has changed.

The subject name, carried in the subject field, is only unique for each subject entity certified by the one CA as defined by the issuer name field. However, the new name form can carry a name that is unique for each subject entity certified by a CA.

Table of Contents

1 Introduction

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

This specification is based on RFC 3280, which defines underlying certificate formats and semantics needed for a full implementation of this standard.

The subject field of a public key certificate identifies the entity associated with the public key stored in the subject public key field. Names and identities of a subject may be carried in the subject field and/or the subjectAltName extension. Where subject field is non-empty, it MUST contain an X.500 distinguished name (DN). The DN MUST be unique for each subject entity certified by a single CA as defined by the issuer name field.

The subject name changes whenever any of the components of that name gets changed. There are several reasons for such a change to happen.

> For employees of a company or organization, the person may get a different position within the same company and thus will move from one organization unit to another one. Including the organization unit in the name may however be very useful to allow the relying parties (RP's) using that certificate to

identify the right individual.

For citizens, an individual may change their name by legal processes, especially as a result of marriage.

Any certificate subject identified by geographical location may relocate and change at least some of the location attributes (e.g. country name, state or province, locality, or street).

A permanent identifier consists of an identifier value assigned within a given naming space by the organization which is authoritative for that naming space. The organization assigning the identifier value may be the CA that has issued the certificate or a different organization called an Assigner Authority.

An Assigner Authority may be a government, a government agency, a corporation, or any other sort of organization. It MUST have a unique identifier to distinguish it from any other such authority. In this standard, that identifier MUST be an object identifier.

A permanent identifier may be useful in three contexts: access control, non-repudiation and audit records.

For access control, the permanent identifier may be used in an ACL (Access Control List) instead of the DN or any other form of name and would not need to be changed, even if the subject name of the entity changes.
For non-repudiation, the permanent identifier may be used to link different transactions to the same entity, even when the subject name of the entity changes.

For audit records, the permanent identifier may be used to link different audit records to the same entity, even when the subject name of the entity changes.

For two certificates which have been both verified to be valid according to a given validation policy and which contain a permanent identifier, those certificates relate to the same entity if their permanent identifiers match, whatever the content of the DN or other subjectAltName components may be.

Since the use of permanent identifiers may conflict with privacy, CAs SHOULD advertise to purchasers of certificates the use of permanent identifiers in certificates.

2. Definition of a Permanent Identifier

This Permanent Identifier is a name defined as a form of otherName from the GeneralName structure in SubjectAltName.

A CA which includes a permanent identifier in a certificate is certifying that any public key certificate containing the same values for that identifier refers to the same entity.

The use of a permanent identifier is OPTIONAL. The permanent identifier is defined as follows:

```
id-on-permanentIdentifier   OBJECT IDENTIFIER ::= { id-on 3 }
```

```
     PermanentIdentifier ::=     SEQUENCE {
        identifierValue    UTF8String             OPTIONAL,
                        -- if absent, use a serialNumber attribute,
                        -- if there is such an attribute present
                        -- in the subject DN
        assigner           OBJECT IDENTIFIER      OPTIONAL
                        -- if absent, the assigner is
                        -- the certificate issuer
}
```

The identifierValue field is optional.

When the identifierValue field is present, then the identifierValue supports one syntax: UTF8String.

When the identifierValue field is absent, then the value of the serialNumber attribute from the deepest RDN of the subject DN is the value to be taken for the identifierValue. In such a case, there MUST be at least one serialNumber attribute in the subject DN, otherwise the PermanentIdentifier SHALL NOT be used.

The assigner field is optional.

When the assigner field is present, then it is an OID which identifies a naming space, i.e. both an Assigner Authority and the type of that field. Characteristically, the prefix of the OID identifies the Assigner Authority, and a suffix is used to identify the type of permanent identifier.

When the assigner field is absent, then the permanent identifier is locally unique to the CA.

The various combinations are detailed below:

1- Both the assigner and the identifierValue fields are present:

The identifierValue is the value for that type of identifier. The assigner field identifies the Assigner Authority and the type of permanent identifier being identified.

The permanent identifier is globally unique among all CAs. In such a case, two permanent identifiers of this type match if and only if their assigner fields match and the contents of the identifierValue field in the two permanent identifiers consist of the same Unicode code points presented in the same order.

2 - The assigner field is absent and the identifierValue field is present:

The Assigner Authority is the CA that has issued the certificate. The identifierValue is given by the CA and the permanent identifier is only local to the CA that has issued the certificate.

In such a case, two permanent identifiers of this type match if and only if the issuer DN's in the certificates which contain them match using the distinguishedNameMatch rule, as defined in X.501 , and the two values of the identifierValue field consist of the same Unicode code points presented in the same order.

3 - Both the assigner and the identifierValue fields are absent:

If there are one or more RDNs containing a serialNumber attribute (alone or accompanied by other attributes), then the value contained in the serialNumber of the deepest such RDN SHALL be used as the identifierValue; otherwise, the Permanent Identifier definition is invalid and the Permanent Identifier SHALL NOT be used.

The permanent identifier is only local to the CA that has issued the certificate. In such a case, two permanent identifiers of this type match if and only if the issuer DN's in the certificates which contain them match and the serialNumber attributes within the subject DN's of those same certificates also match using the caseIgnoreMatch rule.

4 - The assigner field is present and the identifierValue field is absent:

If there are one or more RDNs containing a serialNumber attribute (alone or accompanied by other attributes), then the value contained in the serialNumber of the deepest such RDN SHALL be used as the identifierValue; otherwise, the Permanent Identifier definition is invalid and the Permanent Identifier SHALL not be used.

The assigner field identifies the Assigner Authority and the type of permanent identifier being identified.

The permanent identifier is globally unique among all CAs. In such a case, two permanent identifiers of this type match if and only if their assigner fields match and the contents the serialNumber attributes within the subject DN's of those same certificates match using the caseIgnoreMatch rule.

Note: the full arc of the object identifier used to identify the permanent identifier name form is derived using:

```
id-pkix OBJECT IDENTIFIER ::= { iso(1) identified-organization(3)
   dod(6) internet(1) security(5) mechanisms(5) pkix(7) }

id-on OBJECT IDENTIFIER ::= { id-pkix 8 }   -- other name forms
```

3. IANA Considerations

No IANA actions are necessary. However, a Private Enterprise Number may be used
to construct an OID for the assigner field (see Annex B1).

4. Security considerations

A given entity may have at an instant of time or at different instants of time multiple forms of identities. If the permanent identifier is locally unique to the CA (i.e. the assigner field is not present), then two certificates from the same CA can be compared.

When they contain two identical permanent identifiers, then a relying party may determine that they refer to the same entity.

If the permanent identifier is globally unique among all CAs (i.e. the assigner field is present), then two certificates from different CAs can be compared. When they contain two identical permanent identifiers, then a relying party may determine that they refer to the same entity. It is the responsibility of the CA to verify that the permanent identifier being included in the certificate refers to the subject being certified.

The permanent identifier identifies the entity, irrespective of any attribute extension. When a public key certificate contains attribute extensions, the permanent identifier, if present, should not be used for access control purposes but only for audit purposes. The reason is that since these attributes may change, access could be granted on attributes that were originally present in a certificate issued to that entity but are no longer present in the current certificate.

Subject names in certificates are chosen by the issuing CA and are mandated to be unique for each CA; so there can be no name collision between subject names from the same CA. These names may be an end-entity name when the certificate is a leaf certificate, or a CA name, when it is a CA certificate.

Since a name is only unique towards its superior CA, unless some naming constraints are being used, a name would only be guaranteed to be globally unique when considered to include a sequence of all the names of the superior CAs. Thus, two certificates that are issued under the same issuer DN and which contain the same permanent identifier extension without an assigner field do not necessarily refer to the same entity.

Additional checks need to be done, e.g. to check if the public key values of the two CAs which have issued the certificates to be compared are identical or if the sequence of CA names in the certification path from the trust anchor to the CA are identical.

When the above checks fail, the permanents identifiers may still match if there has been a CA key rollover. In such a case the

checking is more complicated.

The certification of different CAs with the same DN by different CAs has other negative consequences in various parts of the PKI, notably rendering the IssuerAndSerialNumber structure in [RFC 3852] section 10.2.4 ambiguous.

The permanent identifier allows organizations to create links between different certificates associated with an entity issued with or without overlapping validity periods. This ability to link different certificates may conflict with privacy. It is therefore important that a CA clearly disclose any plans to issue certificates which include a permanent identifier to potential subjects of those certificates.

5. References

5.1. Normative

[RFC 3667] S. Bradner. BCP 78. IETF Rights in Contributions, February 2004.

[RFC 3668]. S. Bradner. BCP 79. Intellectual Property Rights in IETF Technology, February 2004.

[RFC 2119] S. Bradner, "Key words for use in RFCs to Indicate Requirement Levels", March 1997.

[RFC 3280] R. Housley, W. Ford, W. Polk, and D. Solo, "Internet X.509 Public Key Infrastructure: Certificate and CRL Profile", April 2002.

[Unicode] The Unicode Consortium, "The Unicode Standard, Version 3.2.0" is defined by "The Unicode Standard, Version 3.0" (Reading, MA, Addison-Wesley, 2000. ISBN 0-201-61633-5), as amended by the "Unicode Standard Annex #27: Unicode 3.1" (http://www.unicode.org/reports/tr27/) and by the "Unicode Standard Annex #28: Unicode 3.2" (http://www.unicode.org/reports/tr28/).

[ISO10646] Universal Multiple-Octet Coded Character Set (UCS) - Architecture and Basic Multilingual Plane, ISO/IEC 10646-1: 1993.

[UTF-8] RFC 2279. F. Yergeau. UTF-8, a transformation format of ISO 10646, January 1998.

[X.501] ITU-T Rec X.501 | ISO 9594-2: 2001 Information technology. Open Systems Interconnection. The Directory: Models

5.2. Informative

[RFC 3852] R.Housley. Cryptographic Message Syntax (CMS), July 2004.

[X.509] ITU-T Recommendation X.509 (1997 E): Information Technology

- Open Systems Interconnection - The Directory: Authentication Framework, June 1997.

[X.520] ITU-T Recommendation X.520: Information Technology - Open Systems Interconnection - The Directory: Selected Attribute Types, June 1997.

[X.660] ITU-T Recommendation X.660: Information Technology - Open Systems Interconnection - Procedures for the Operation of OSI Registration Authorities: General Procedures, 1992.

[X.680] ITU-T Recommendation X.680: Information Technology - Abstract Syntax Notation One, 1997.

6. Author's Addresses

Denis Pinkas
Bull
Rue Jean-Jaur s. BP 68
78340 Les Clayes-sous-Bois
FRANCE
Email: Denis.Pinkas@bull.net

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

7. Intellectual Property Rights

APPENDIX A. ASN.1 syntax

As in RFC 2459, ASN.1 modules are supplied in two different variants of the ASN.1 syntax.

This section describes data objects used by conforming PKI components in an "ASN.1-like" syntax. This syntax is a hybrid of the 1988 and 1993 ASN.1 syntaxes. The 1988 ASN.1 syntax is augmented with 1993 the UNIVERSAL Type UTF8String.

The ASN.1 syntax does not permit the inclusion of type statements in the ASN.1 module, and the 1993 ASN.1 standard does not permit use of the new UNIVERSAL types in modules using the 1988 syntax. As a result, this module does not conform to either version of the ASN.1 standard.

Appendix A.1 may be parsed by an 1988 ASN.1-parser by replacing the definitions for the UNIVERSAL Types with the 1988 catch-all "ANY".

Appendix A.2 may be parsed by an 1993 ASN.1-parser by removing the UTF8String choice from the definition of IdentifierValue in the module. Appendix A.2 may be parsed "as is" by an 1997-compliant ASN.1 parser.

In case of discrepancies between these modules, the 1988 module is the normative one.

APPENDIX A.1. 1988 ASN.1 Module

```
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) }

DEFINITIONS EXPLICIT TAGS ::=

   BEGIN

   -- EXPORTS ALL --

   IMPORTS

-- UTF8String, / move hyphens before slash if UTF8String does not
-- resolve with your compiler
-- The content of this type conforms to RFC 2279.

        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 [RFC 3280]


   -- Permanent identifier Object Identifier and Syntax

   id-on   OBJECT IDENTIFIER ::= { id-pkix 8 }

   id-on-permanentIdentifier   OBJECT IDENTIFIER ::= { id-on 3 }

   PermanentIdentifier ::= SEQUENCE {
        identifierValue    UTF8String             OPTIONAL,
                        -- if absent, use the serialNumber attribute
                        -- if there is a single such attribute present
                        -- in the subject DN
        assigner           OBJECT IDENTIFIER      OPTIONAL
                        -- if absent, the assigner is
                        -- the certificate issuer
}

END
```

APPENDIX A.2. 1993 ASN.1 Module

```
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) }

   DEFINITIONS EXPLICIT TAGS ::=

   BEGIN

   -- EXPORTS ALL --

   IMPORTS

        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 [RFC 3280]

        ATTRIBUTE
              FROM InformationFramework {joint-iso-itu-t ds(5) module(1)
              informationFramework(1) 4};
               -- from [X.501]

   -- Permanent identifier Object Identifiers

   id-on   OBJECT IDENTIFIER ::= { id-pkix 8 }

   id-on-permanentIdentifier   OBJECT IDENTIFIER ::= { id-on 3 }

   -- Permanent Identifier

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

   PermanentIdentifier ::= SEQUENCE {
        identifierValue    UTF8String             OPTIONAL,
                         -- if absent, use the serialNumber attribute
                         -- if there is a single such attribute present
                         -- in the subject DN
        assigner           OBJECT IDENTIFIER      OPTIONAL
                         -- if absent, the assigner is
                         -- the certificate issuer
}


END
```

APPENDIX B. OID's for organizations

In order to construct an OID for the assigner field, organizations need first to have a registered OID for themselves. In some cases, OID's are provided for free. In other cases a one-time fee is required. The main difference lies in the nature of the information that is collected at the time of registration and how this information is verified for its accuracy.

B.1. Using IANA (Internet Assigned Numbers Authority)

The application form for a Private Enterprise Number in the IANA's OID list is: http://www.iana.org/cgi-bin/enterprise.pl.

Currently IANA assigns numbers for free. The IANA-registered Private Enterprises prefix is: iso.org.dod.internet.private.enterprise (1.3.6.1.4.1)

These numbers are used, among other things, for defining private SNMP MIBs.

The official assignments under this OID are stored in the IANA file "enterprise-numbers" available at:
http://www.iana.org/assignments/enterprise-numbers

B.2. Using an ISO member body

ISO has defined the OID structure in a such a way so that every ISO member-body has its own unique OID. Then every ISO member-body is free to allocate its own arc space below.

Organizations and enterprises may contact the ISO member-body where their organization or enterprise is established to obtain an organization/enterprise OID.

Currently, ISO members do not assign organization/enterprise OID's for free.

Most of them do not publish registries of such OID's which they have assigned, sometimes restricting the access to registered organizations or preferring to charge inquirers for the assignee of an OID on a per-inquiry basis. The use of OID's from an ISO member organization which does not publish such a registry may impose extra costs on the CA that needs to make sure that the OID corresponds to the registered organization.

As an example, AFNOR (Association Francaise de Normalisation - the French organization that is a member of ISO) has defined an arc to allocate OID's for companies:

{iso (1) member-body (2) fr (250) type-org (1) organisation (n)}

B.3. Using an ICD (International Code Designator) from British Standards Institution to specify a new or an existing identification scheme

The International Code Designator (ICD) is used to uniquely identify an ISO 6523 compliant organization identification scheme. ISO 6523 is a standard that defines the proper structure of an identifier and the registration procedure for an ICD. The conjunction of the ICD with an identifier issued by the registration authority is worldwide unique.

The basic structure of the code contains the following components:

- the ICD value: The International Code Designator issued to the identification scheme makes the identifier worldwide unique (up to 4 digits),

- the Organization, usually a company or governmental body (up to 35 characters),

- an Organization Part (OPI - Organization Part Identifier). An identifier allocated to a particular Organization Part (optional, up to 35 characters)

The ICD is also equivalent to an object identifier (OID) under the arc {1(iso). 3(identified organization)}.

On behalf of ISO, British Standards Institution (BSI) is the Registration Authority for organizations under the arc {iso (1) org(3)}. This means BSI registers code issuing authorities (organizations) by ICD values which are equivalent to OIDs of the form {iso (1) org(3) icd(xxxx)}. The corresponding IdentifierValue is the code value of the scheme identified by icd(xxxx).

As an example, the ICD 0012 was allocated to European Computer Manufacturers Association: ECMA. Thus the OID for ECMA is {iso(1) org(3) ecma(12)}.

For registration with BSI, a "Sponsoring Authority" has to vouch for the Applying organization. Registration is not free. Recognized "Sponsoring Authorities" are: ISO Technical Committees or (Sub)Committees, Member Bodies of ISO or International Organizations having a liaison status with ISO or with any of its Technical (Sub)Committees.

An example of a Sponsoring Authority is the EDIRA Association (EDI/EC Registration Authority, web: http://www.edira.org, email:info@edira.org).

The numerical list of all ICDs that have been issued is posted on its webpage: http://www.edira.org/documents.htm#icd-List

Note: IANA owns ICD code 0090, but that (presumably) it isn't intending

to use it for the present purpose.

Full Copyright Statement