PKIX Working Group
INTERNET-DRAFT
Expires: August, 2002
Target category: Standard Track

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

February, 2002

Internet X.509 Public Key Infrastructure

Permanent Identifier

<draft-ietf-pkix-pi-03.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 the certificate relates to the same entity even if the name or the affiliation of that entity has changed.

The subject name when carried in the subject field is only unique for each subject entity certified by the one CA as defined by the issuer name field. This new form of name also can carry a name that is unique for each subject entity certified by any CA.

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.

Please send comments on this document to the ietf-pkix@imc.org mailing list.

1 Introduction

This specification is one part of a family of standards for the X.509 Public Key Infrastructure (PKI) for the Internet. It is based on RFC 2459, 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 it is non-empty, the subject field 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 (RPÆs) using that certificate to identify the right individual.
>
> For citizens, an individual may change their name by legal processes, especially women 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 may be useful both in the context of access control and of non repudiation.

> 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.

When two certificates from the same CA contain the same permanent identifier value, then these certificates relate to the same entity, whatever the content of the DN or other subjectAltName components may be.

When two certificates from different CAÆs contain both the same permanent identifier value and the same type of permanent identifier from a given Assigner Authority, then these

certificates relate to the same entity, whatever the content of the DN or other subjectAltName components may be.

2. Definition of a Permanent Identifier

A CA which includes a permanent identifier in a certificate is certifying that any public key certificate containing that identifier refers to the same entity, whatever the content of the DN or other subjectAltName components may be.

The use of a permanent identifier is optional. This name is defined as a form of otherName from the GeneralName structure in SubjectAltName. The permanent identifier is defined as follows:

```
id-on-permanentIdentifier   AttributeType ::= { id-on 2 }

  PermanentIdentifier ::=     SEQUENCE {
     identifierValue                    IdentifierValue,
     identifierType                     IdentifierType OPTIONAL
  }

  IdentifierValue ::= CHOICE {
         iA5String            IA5String,
         uTF8String           UTF8String
  }

  IdentifierType ::= CHOICE {
         registeredOID                  OBJECT IDENTIFIER,
         uniformResourceIdentifier      IA5String,
         intluniformResourceIdentifier  UTF8String
```

}

The IdentifierType field, when present, identifies both the organization responsible for assigning the content of the identifier field and the type of that field.

When the IdentifierType field is missing, then it is assumed that the organization responsible for assigning the content of the identifier field is the CA itself and that there is only one type of such identifier for the CA.

Two forms of values are supported for the IdentifierValue: IA5String or UTF8String.

The IdentifierType field may contain a registeredOID in the form of :

a) an Object Identifier (i.e. an OID), or
b) a permanent URI using IA5String, or
c) a permanent URI using UTF8String.

Characteristically, when an OID is used, the prefix of the OID identifies the organization, and a suffix is used to identify the type of permanent identifier being identified. Essentially the same thing is true of URIÆs.

If identifierType is missing, then the permanent identifier is locally unique to the CA.

If identifierType is present, then the permanent identifier is globally unique among all CAÆs.

Note: the full arc of the object identifier 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. 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. identifierType 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 CAÆs (i.e. identifierType is present), then two certificates from different CAÆs can be compared. When they contain two identical permanent identifiers, then a relying party may determine that they refer to the same entity.

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 more present in the current certificate.

4. References

[RFC 2026] S. Bradner, ôThe Internet Standards Process û Revision 3 ©, November 1996.

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

[RFC 2459] R. Housley, W. Ford, W. Polk, and D. Solo, "Internet X.509 Public Key Infrastructure: Certificate and CRL Profile", January 1999.

[X.501] ITU-T Recommendation X.501 (1997 E): Information Technology - Open Systems Interconnection - The Directory: Models, June 1997.

[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 û 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.

5. AuthorÆs Addresses

Denis Pinkas
Bull,
68, Route de Versailles
78434 Louveciennes Cedex
FRANCE
Email: Denis.Pinkas@bull.net

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

6 Intellectual Property Rights

APPENDIX

ASN.1 definitions

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-permanent-identifier-88(14) }

DEFINITIONS EXPLICIT TAGS ::=

   BEGIN

   -- EXPORTS ALL --

   IMPORTS

        id-pkix, AttributeType,
                FROM PKIX1Explicit88 {iso(1) identified-organization(3)
                dod(6) internet(1) security(5) mechanisms(5) pkix(7)
                id-mod(0) id-pkix1-explicit-88(1)}

   -- Object Identifiers

-- Externally defined OIDs

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

   -- permanent identifier

   id-on-permanentIdentifier   AttributeType ::= { id-on 2 }

     PermanentIdentifier ::=     SEQUENCE {
        identifierValue                      IdentifierValue,
        identifierType                       IdentifierType OPTIONAL
     }

     IdentifierValue ::= CHOICE {
            iA5String            IA5String,
            uTF8String           UTF8String
     }

     IdentifierType ::= CHOICE {
            registeredOID                    OBJECT IDENTIFIER,
            uniformResourceIdentifier        IA5String,
            intluniformResourceIdentifier    UTF8String
     }

END
```

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-permanent-identifier-93(15) }

   DEFINITIONS EXPLICIT TAGS ::=

   BEGIN

   -- EXPORTS ALL --

   IMPORTS

id-pkix, ATTRIBUTE
       FROM PKIX1Explicit93 {iso(1) identified-organization(3) dod(6)
       internet(1) security(5) mechanisms(5) pkix(7) id-mod(0)
       id-pkix1-explicit-93(3)};

   -- Object Identifiers

-- Externally defined OIDs

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

-- Locally defined OIDs

id-on-permanentIdentifier     OBJECT IDENTIFIER ::= { id-on 2 }

   -- permanent identifier

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

     PermanentIdentifier ::=     SEQUENCE {
        identifierValue                     IdentifierValue,
        identifierType                      IdentifierType OPTIONAL
     }

     IdentifierValue ::= CHOICE {
            iA5String            IA5String,
            uTF8String           UTF8String
     }
```

```
     IdentifierType ::= CHOICE {
            registeredOID                   OBJECT IDENTIFIER,
            uniformResourceIdentifier       IA5String,
            intluniformResourceIdentifier   UTF8String
     }

END
```


B. OIDÆs for organizations

In order to obtain an OID for an identifier type, organizations need first to have a registered OID for themselves (or must use a permanent URI). In some cases, OIDÆs 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:
ftp://ftp.isi.edu/in-notes/iana/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 OIDÆs for free.

Most of them do not publish registries of such OIDÆs 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 OIDÆs 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 OIDÆs for companies:

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

C. Full Copyright Statement