Information technology — Open Systems Interconnection — The Directory: Public-key and attribute certificate frameworks

TECHNICAL CORRIGENDUM 3

Technologies de l'information — Interconnexion de systèmes ouverts (OSI) — L’annuaire: Cadre général des certificats de clé publique et d’attribut

RECTIFICATIF TECHNIQUE 3

Technical Corrigendum 3 to ISO/IEC 9594-8:2005 was prepared by Joint Technical Committee ISO/IEC JTC 1, Information technology, Subcommittee SC 6, Telecommunications and information exchange between systems, in collaboration with ITU-T. The identical text is published as Rec. ITU-T X.509 (2005)/Cor.3 (02/2011).
Technical Corrigendum 3

(covers resolution to defect reports 332, 333, 334, 344, 348 and 352)

1) Correction of the defects reported in defect report 332
In the CertificateExtensions module of Annex A, change:

```plaintext
id-ce-nameConstraint  OBJECT IDENTIFIER  ::=  {id-ce 30}
```

to:

```plaintext
id-ce-nameConstraints   OBJECT IDENTIFIER  ::=  {id-ce 30}
```

2) Correction of the defects reported in defect report 333
Delete subclause 15.1.2.5 and renumber 15.1.2.6 to 15.1.2.5.
Replace the last part of subclause 15.5.2.5 starting with "The indirect issuer matching rule ..." with:

The presence of this extension within an attribute certificate may be determined by applying the extensionPresenceMatch matching rule.

Add a new subclause 17.3.5:

17.3.5 Extension presence match

The Extension Presence Match rule compares for equality a presented object identifier value identifying a particular extension with the extensions component of a certificate.

```plaintext
extensionPresenceMatch  MATCHING-RULE ::= {
  SYNTAX   OBJECT IDENTIFIER
  ID       id-mr-extensionPresenceMatch }
```

This matching rule returns TRUE if the certificate contains the particular extension.

3) Correction of the defects reported in defect report 334
In 17.2.9, change:

```plaintext
id-at-xMLProtPrivPolicy
```

to:

```plaintext
id-at-xmlPrivPolicy
```

Make the same change to Annex A.

4) Correction of the defects reported in defect report 344
In 3.3, add the following new definitions:

**end-entity certificate**: An attribute or public-key certificate issued to an end-entity.

**end-entity attribute certificate**: An attribute certificate issued to an end-entity.
end-entity public-key certificate: A public-key certificate issued to an end-entity.  

In 7.3, 8.6.2.2, 8.6.2.7 and 11.3.10 replace "user certificate" with "end-entity certificate".

In 11.2.1, update as shown:

A user may obtain one or more end-entity public-key certificates from one or more CAs. The userCertificate attribute type contains the end-entity public-key certificates a user has obtained from one or more CAs.

5) Correction of the defects reported in defect report 348

Replace definitions 3.3.59 and 3.3.60 with the text below:

3.3.59 trust: Entity X is said to trust entity Y for a set of activities if and only if entity X relies upon entity Y behaving in a particular way with respect to the activities.

3.3.60 trust anchor: A trust anchor is an entity that is trusted by a certificate using system and used for validating certificates in certification paths.

3.3.61 trust anchor information: Trust anchor information is at least the: distinguished name of the trust anchor, associated public key, algorithm identifier, public key parameters (if applicable), and any constraints on its use including a validity period. The trust anchor information may be provided in any format, such as a self-signed certificate, a normal CA public-key certificate, a to-be-signed certificate, or a TrustAnchorInfo as defined by IETF RFC 5914.

6) Correction of the defects reported in defect report 352

Change the first paragraph of 11.1.6 to:

The PKI cert path object class is used in defining entries for objects that contain PKI paths. It will generally be used in conjunction with entries that include auxiliary object class structural pkiCA or pkiUser.