Telecommunications and Information Exchange Between Systems

ISO/IEC JTC 1/SC 6

Document Number:	N14285
Date:	2010-04-28
Replaces:	
Document Type:	Text for DCOR ballot
Document Title:	Text for DCOR ballot, ISO/IEC 9594-8:2005 Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks, ITU-T X.509 (2005)
Document Source:	SC 6/WG 8 Geneva meeting
Project Number:	
Document Status:	SC 6 P-members are requested to ballot on this DCOR text through the e-balloting system (www.iso.org/jtc1/sc6) no later than 2010-07-28.
Action ID:	LB
Due Date:	2010-07-28
No. of Pages:	3

ISO/IEC JTC1/SC6 Secretariat Ms. Jooran Lee, KSA (on behalf of KATS)

Korea Technology Center #701-7 Yeoksam-dong, Gangnam-gu, Seoul, 135-513, Republic of Korea ;

Telephone: +82 2 6009 4808 ; Facsimile: +82 2 6009 4819 ; Email : jooran@kisi.or.kr

INTERNATIONAL STANDARD
ITU-T RECOMMENDATION

ITU-T X.509 (2005) | ISO/IEC 9594-8:2005
Information technology – Open Systems Interconnection –
The Directory: Public-key and attribute certificate frameworks

Technical Corrigendum 3

(covering 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*

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

to:

```
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 the subclause 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.

```
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

```
id-at-xMLPprotPrivPolicy
```

to:

```
id-at-xmlPrivPolicy
```

Make the same change to Annex A

4) Correction of the defects reported in defect report 344

In 3.4, 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 the definitions 3.4.64 and 3.4.64 with below text.

3.4.64 **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.

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

3.4.66 **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 constrains 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 draft-ietf-pkix-ta-format-03 (to be replaced by the proper RFC-number).

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**.