INTERNATIONAL STANDARD ISO/IEC 9594-8:2005
TECHNICAL CORRIGENDUM 4

Published 2012-09-15

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION • МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ПО СТАНДАРТИЗАЦИИ • ORGANISATION INTERNATIONALE DE NORMALISATION
INTERNATIONAL ELECTROTECHNICAL COMMISSION • МЕЖДУНАРОДНАЯ ЭЛЕКТРОТЕХНИЧЕСКАЯ КОМИССИЯ • COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

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

TECHNICAL CORRIGENDUM 4

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

RECTIFICATIF TECHNIQUE 4

Technical Corrigendum 4 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.4 (04/2012).

ICS 35.100.70 **Ref. No. ISO/IEC 9594-8:2005/Cor.4:2012(E)**

Published in Switzerland

INTERNATIONAL STANDARD

RECOMMENDATION ITU-T

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

Technical Corrigendum 4

(covering resolution to defect reports 353, 362, 365, 366, 368, 369, 372 and 373)

1) Correction of the defects reported in defect report 353

In Annex A, replace the definition for **`CertificatePair`** *data type with:*

```
CertificatePair ::= SEQUENCE {
  issuedToThisCA   [0]  Certificate OPTIONAL,
  issuedByThisCA   [1]  Certificate OPTIONAL }
  (WITH COMPONENTS { ..., issuedToThisCA PRESENT} |
   WITH COMPONENTS { ..., issuedByThisCA PRESENT})
```

2) Correction of the defects reported in defect report 362

Add clause 2.3 as follows:

2.3 Recommendations

– ITU-T Recommendation X.1252 (2010), *Baseline identity management terms and definitions.*

Insert the following new clause 3.2 after clause 3.1 and renumber subsequent clauses accordingly:

3.2 Baseline identity management terms and definitions

The following term is defined in Rec. ITU-T X.1252:

a) **trust**: The firm belief in the reliability and truth of information or in the ability and disposition of an entity to act appropriately, within a specified context.

Delete the 'trust' definition from clause 3.3 (now clause 3.4) and renumber subsequent clauses accordingly.

For consistency purposes, modify the first paragraph of clause 18.2.1, Obtaining public-key certificates from the directory, as shown:

Certificates are held within directory entries as attributes of type UserCertificate, CACertificate and CrossCertificatePair. These attribute types are known to the Directory. These attributes can be operated on using the same protocol operations as other attributes. The definition of these types can be found in clause 3~~3.3~~; the specification of these attribute types is defined in clause 11.2.

3) Correction of the defects reported in defect report 365

Update the definition for end-entity as shown:

3.~~3~~4.27 end-entity: Either a public-key certificate subject that uses its private key for purposes other than signing certificates, or an attribute certificate holder that uses its attributes to gain access to a resource~~, or an entity that is a relying party~~.

4) Correction of the defects reported in defect report 366

In clause 7, replace the text for the issuer field to:

The **`issuer`** field shall hold the distinguished name of the CA that issued the public-key certificate. It shall hold a non-empty distinguished name.

In clause 7, replace the text for the subject field to:

The **`subject`** field shall identify the entity associated with the public-key found in the **`subjectPublicKey`** component of the **`subjectPublicKeyInfo`** field. If the public-key certificate is for an end-entity, then the distinguished name may be an empty sequence providing that the **`subjectAltName`** extension is present and flagged as critical. Otherwise, it shall be a non-empty distinguished name (see 8.3.2.1).

Change NOTE 2 in clause 8.3.2.1 as shown

> NOTE 2 – If this extension field is present and is flagged critical, the **`subject`** field of ~~the~~ an end-entity public-key certificate may contain a null name (e.g., a sequence of zero relative distinguished names) in which case the subject is identified only by the name or names in this extension.

Delete the NOTE in clause 8.3.2.2.

5) Correction of the defects reported in defect report 368

Update the first paragraph of clause 6 as shown:

This Directory Specification defines a framework for obtaining and trusting a public key of an entity in order to encrypt information to be decrypted by that entity, or in order to verify the digital signature of that entity. The framework includes the issuance of a public-key certificate by a Certification Authority (CA) and the validation of that public-key certificate by the ~~certificate user~~*relying party*, i.e., the entity relying on the content of the public-key certificate. The validation includes:

- establishing a trusted path of public-key certificates between a trusted entity called a *trust anchor* ~~the certificate user~~ and the public-key certificate subject, i.e., the entity for which the public-key certificate has been issued;

6) Correction of the defects reported in defect report 369

Replace the definition for certification path with:

3.~~3~~4.19 certification path: An ordered list of one or more public-key certificates, starting with a public-key certificate signed by the trust anchor, and ending with the public key certificate to be validated. All intermediate public-key certificates, if any, are CA-certificates in which the subject of the preceding certificate is the issuer of the following certificate.

7) Correction of the defects reported in defect report 372

In clause 8.4.2.3 and Annex A, update the **`PolicyConstraintsSyntax`** *as shown:*

```
PolicyConstraintsSyntax ::= SEQUENCE {
  requireExplicitPolicy  [0]  SkipCerts OPTIONAL,
  inhibitPolicyMapping   [1]  SkipCerts OPTIONAL,
  ... }
   (WITH COMPONENTS {..., requireExplicitPolicy PRESENT } |
    WITH COMPONENTS {..., inhibitPolicyMapping  PRESENT } )
```

Add a new paragraph right under the ASN1:

At least one of the **`requireExplicitPolicy`** and **`inhibitPolicyMapping`** components shall be present.