



INTERNATIONAL STANDARD ISO/IEC 9594-8:1998
TECHNICAL CORRIGENDUM 1

Published 2000-12-15

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: Authentication framework

TECHNICAL CORRIGENDUM 1

Technologies de l'information — Interconnexion de systèmes ouverts (OSI) — L'Annuaire: Cadre d'authentification

RECTIFICATIF TECHNIQUE 1

Technical Corrigendum 1 to International Standard ISO/IEC 9594-8:1998 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 6, *Telecommunications and information exchange between systems*.

Withdrawn

INTERNATIONAL STANDARD

ITU-T RECOMMENDATION

INFORMATION TECHNOLOGY – OPEN SYSTEMS INTERCONNECTION –
THE DIRECTORY: AUTHENTICATION FRAMEWORK

TECHNICAL CORRIGENDUM 1

1) Resolution to defect report 9594/200

Subclause 12.6.2

Add the following at the end of the paragraph beginning with "If this extension is flagged critical ...":

"Where the distribution points are used to distribute CRL information for all revocation reason codes and all certificates issued by the CA include the **crlDistributionPoint** as a critical extension, the CA is not required to also publish a full CRL at the CA entry."

2) Resolution to defect report 9594/201

Subclause 12.6.3.1

Move the second sentence of the second paragraph "If this field is absent ...CRL issuer." to the first paragraph immediately before the sentence "This field is defined as follows:"

Add a paragraph break following the relocated sentence, making "This field is defined as follows:" as an independent paragraph immediately before the ASN.1.

3) Resolution to defect report 9594/212

Subclause 12.7.6

Add the following to subclause 12.7.6:

"g) **authorityKeyIdentifier** matches if the value of this component in the stored attribute value equals that in the presented value; there is no match if the stored attribute value contains no authority key identifier extension or if not all components in the presented value are present in the stored attribute value."

4) Resolution to defect report 9594/213

Subclause 12.7.6 d)

Replace the text of 12.7.6 d) with the following:

"d) **reasonFlags** matches if any of the bits that are set in the presented value are also set in the **onlySomeReasons** components of the issuing distribution point extension of the stored attribute value; there is also a match if the stored attribute value contains no **reasonFlags** in the issuing distribution point extension, or if the stored attribute value contains no issuing distribution point extension;

NOTE – Even though a CRL matches on a particular value of **reasonFlags**, the CRL may not contain any revocation notices with that reason code."

5) Resolution to defect report 9594/218

Subclause 12.7.2 j)

Replace the text of 12.7.2 j) with the following:

- "j) **policy** matches if at least one member of the **CertPolicySet** presented appears in the certificate policies extension in the stored attribute value; there is no match if there is no certificate policies extension in the stored attribute value;"

6) Resolution to defect report 9594/220

Subclause 11.2, Note 3

In Note 3, in the second sentence, replace "shall be absent" with "may be absent".

*In Note 3, at the beginning of the 3rd sentence, replace "This may permit" with "If **version** is absent, this may permit".*

*In Note 3, at the beginning of the 4th sentence, replace "An implementation that supports version 2 (or greater) CRLs may" with "An implementation that supports version 2 (or greater) CRLs, in the absence of **version**, may also ...".*

7) Resolution to defect report 9594/185

Clause 8

*Add the following text immediately following the ASN.1 for **certificatePair**:*

"The **cACertificate** attribute of a CA's directory entry shall be used to store self-issued certificates (if any) and certificates issued to this CA by CAs in the same realm as this CA.

The **forward** elements of the **crossCertificatePair** attribute of a CA's directory entry shall be used to store all, except self-issued certificates issued to this CA. Optionally, the **reverse** elements of the **crossCertificatePair** attribute, of a CA's directory entry may contain a subset of certificates issued by this CA to other CAs. When both the **forward** and the **reverse** elements are present in a single attribute value, issuer name in one certificate shall match the subject name in the other and vice versa, and the subject public key in one certificate shall be capable of verifying the digital signature on the other certificate and vice versa.

When a **reverse** element is present, the forward element value and the reverse element value need not be stored in the same attribute value; in other words, they can be stored in either a single attribute value or two attribute values.

In the case of v3 certificates, none of the above CA certificates shall include a **basicConstraints** extension with the **cA** value set to **FALSE**.

The definition of realm is purely a matter of local policy."