INTERNATIONAL STANDARD ISO/IEC 9594-8:1998
TECHNICAL CORRIGENDUM 2

Published 2002-06-15

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 2

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

RECTIFICATIF TECHNIQUE 2

Technical Corrigendum 2 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.*

ICS 35.100.70 **Ref. No. ISO/IEC 9594-8:1998/Cor.2:2002(E)**

INTERNATIONAL STANDARD
ITU-T RECOMMENDATION

Information technology – Open Systems Interconnection – The Directory: Authentication framework

TECHNICAL CORRIGENDUM 2

NOTE – This Technical Corrigendum covers Draft Technical Corrigenda 8 and 9.

1) Defect reports resolved by Draft Technical Corrigendum 8

(covering resolutions to defect reports 226, 227 and 240)

1.1) This corrects the defects reported in defect report 226

In 11.2, delete the 2nd paragraph:

The production of a certificate … compromise unlikely.

1.2) This corrects the defects reported in defect report 227

In 12.2.2.1, add the following 2 sentences to the end of the paragraph that begins with "Certification authorities shall assign…":

The **keyIdentifier** form can be used to select CA certificates during path construction. The **authorityCertIssuer**, **authoritySerialNumber** pair can only be used to provide preference to one certificate over others during path construction.

1.3) This corrects the defects reported in defect report 240

The following corrections should be made to the 1997 edition **authenticationFramework** *module in Annex A:*

1) *Add* **id-mr** *to the list of objects imported from* **UsefulDefinitions** *module in the* **authenticationFramework** *module.*

2) *Add* **AttributeType**, **Attribute**, *and* **MATCHING-RULE** *to the set of objects imported into the* **authenticationFramework** *module from the* **InformationFramework** *module.*

3) *Add* **GeneralNames** *to the set of objects imported into the* **authenticationFramework** *module from the* **CertificateExtensions** *module.*

4) *Add the following definition to the* **authenticationFramework** *module because this is imported into other modules in the X.500 series of Recommendations, but had never been included in the 1997 text of this Recommendation:*

```
HASH {ToBeHashed}          ::=     SEQUENCE {
    algorithmIdentifier                AlgorithmIdentifier,
    hashValue                          BIT STRING ( CONSTRAINED BY {
        -- must be the result of applying a hashing procedure to the DER-encoded octets --
        -- of a value of --ToBeHashed } ) }
```

5) *Add the following OID assignments in the* **authenticationFramework** *module:*

```
id-at-attributeCertificateRevocationList OBJECT IDENTIFIER ::= {id-at 59}

id-mr-attributeCertificateMatch OBJECT IDENTIFIER ::= {id-mr 42}
```

6) *Add* **Time** *to the set of objects imported into the* **certificateExtensions** *module from the* **authenticationFramework** *module.*

7) *In the* **certificateExtensions** *module, and in the main text of 12.7.2 replace:*

```
CertPolicySet ::= SEQUENCE (1..MAX) OF CertPolicyId
```

with:

```
CertPolicySet ::= SEQUENCE SIZE (1..MAX) OF CertPolicyId
```

2) Defect reports resolved by Draft Technical Corrigendum 9

(covering resolutions to defect reports 244, 256, 257 and 258)

2.1) This corrects the defects reported in defect report 244

In clause 8:

In the paragraph that begins "The **extensions** field allows addition of new ...", *add the following two sentences to the end of the paragraph:*

When a certificate-using implementation recognizes and is able to process an extension, then the certificate-using implementation shall process the extension regardless of the value of the criticality flag. Note that any extension that is flagged non-critical will cause inconsistent behaviour between certificate-using systems that will process the extension and certificate-using systems that do not recognize the extension will ignore it.

Add the following immediately after the paragraph that begins "If unknown elements appear within the extension …"*:*

A CA has three options with respect to an extension:

i) it can exclude the extension from the certificate;

ii) it can include the extension and flag it non-critical;

iii) it can include the extension and flag it critical.

A validation engine has two possible actions to take with respect to an extension:

i) it can ignore the extension and accept the certificate (all other things being equal);

ii) it can process the extension and accept or reject the certificate depending on the content of the extension and the conditions under which processing is occuring (e.g. the current values of the path processing variables).

Some extensions can only be marked critical. In these cases, a validation engine that understands the extension processes it and acceptance/rejection of the certificate is dependent (at least in part) on the content of the extension. A validation engine that does not understand the extension rejects the certificate.

Some extensions can only be marked non-critical. In these cases, a validation engine that understands the extension processes it and acceptance/rejection of the certificate is dependent (at least in part) on the content of the extension. A validation engine that does not understand the extension accepts the certificate (unless factors other than this extension cause it to be rejected).