INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.509

Corrigendum 2

(02/2001)

SERIES X: DATA NETWORKS AND OPEN SYSTEM COMMUNICATIONS
Directory

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

Technical Corrigendum 2

ITU-T Recommendation X.509 (1997) – Corrigendum 2

(Formerly CCITT Recommendation)

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS AND OPEN SYSTEM COMMUNICATIONS

PUBLIC DATA NETWORKS	
Services and facilities	X.1–X.19
Interfaces	X.20–X.49
Transmission, signalling and switching	X.50–X.89
Network aspects	X.90–X.149
Maintenance	X.150–X.179
Administrative arrangements	X.180–X.199
OPEN SYSTEMS INTERCONNECTION	
Model and notation	X.200–X.209
Service definitions	X.210–X.219
Connection-mode protocol specifications	X.220–X.229
Connectionless-mode protocol specifications	X.230–X.239
PICS proformas	X.240–X.259
Protocol Identification	X.260–X.269
Security Protocols	X.270–X.279
Layer Managed Objects	X.280–X.289
Conformance testing	X.290–X.299
INTERWORKING BETWEEN NETWORKS	
General	X.300–X.349
Satellite data transmission systems	X.350–X.369
IP-based networks	X.370–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	**X.500–X.599**
OSI NETWORKING AND SYSTEM ASPECTS	
Networking	X.600–X.629
Efficiency	X.630–X.639
Quality of service	X.640–X.649
Naming, Addressing and Registration	X.650–X.679
Abstract Syntax Notation One (ASN.1)	X.680–X.699
OSI MANAGEMENT	
Systems Management framework and architecture	X.700–X.709
Management Communication Service and Protocol	X.710–X.719
Structure of Management Information	X.720–X.729
Management functions and ODMA functions	X.730–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	
Commitment, Concurrency and Recovery	X.850–X.859
Transaction processing	X.860–X.879
Remote operations	X.880–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999

For further details, please refer to the list of ITU-T Recommendations.

INTERNATIONAL STANDARD ISO/IEC 9594-8
ITU-T RECOMMENDATION X.509

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

TECHNICAL CORRIGENDUM 2

Source

Corrigendum 2 to ITU-T Recommendation X.509 (1997) was prepared by ITU-T Study Group 7 (2001-2004) and approved on 2 February 2001. An identical text is also published as Technical Corrigendum 2 to ISO/IEC 9594-8.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementors are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database.

CONTENTS

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).

Some extensions can be marked critical or 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, regardless of the criticality flag. A validation engine that does not understand the extension accepts the certificate if the extension is marked non-critical (unless factors other than this extension cause it to be rejected) and rejects the certificate if the extension is marked critical.

When a CA considers including an extension in a certificate, it does so with the expectation that its intent will be adhered to wherever possible. If it is necessary that the content of the extension be considered prior to any reliance on the certificate, a CA would flag the extension critical. This must be done with the realization that any validation engine that does not process the extension will reject the certificate (probably limiting the set of applications that can verify the certificate). The CA may mark certain extensions non-critical to achieve backward compatibility with validation applications that cannot process the extensions. Where the need for backward compatibility and interoperability with validation applications incapable of processing the extensions is more vital than the ability of the CA to enforce the extensions, then these optionally critical extensions would be marked non-critical. It is most likely that CAs would set optionally critical extensions as non-critical during a transition period while the verifiers' certificate processing applications are upgraded to ones that can process the extensions.

In clause 12.1:

In the paragraph that begins "In a certificate or CRL, an extension is flagged ..."*, add the following immediately after the third sentence that ends with* "... ignoring the extension"*:*

If an extension is flagged non-critical, a certificate-using system that does recognize the extension, shall process the extension.

In clause 12.2.2.3:

In the paragraph that begins "If the extension is flagged non-critical ..."*, replace the second sentence with the following:*

If this extension is present, and the certificate-using system recognizes and processes the **keyUsage** extension type, then the certificate using system shall ensure that the certificate shall be used only for a purpose for which the corresponding key usage bit is set to one.

In clause 12.2.2.4:

In the paragraph that begins "If the extension is flagged non-critical ..."*, replace the second sentence with the following:*

If this extension is present, and the certificate-using system recognizes and processes the **extendedKeyUsage** extension type, then the certificate using system shall ensure that the certificate shall be used only for one of the purposes indicated.

In clause 12.4.2.1:

In the 4th paragraph following the ASN.1, replace: "If this extension is present and is flagged critical then:" *with the following:*

If this extension is present and is flagged critical, or is flagged non-critical but is recognized by the certificate-using system, then:

In clause 12.4.2.2:

Replace the last sentence "If this extension is present and is flagged critical ..." *with the following:*

If this extension is present and is flagged critical, or is flagged non-critical but is recognized by the certificate-using system, then the certificate-using system shall check that the certification path being processed is consistent with the value in this extension.

2.2) This corrects the defects reported in defect report 256

In clause 8:

In the first paragraph of the description of the cross certificate pair attribute (that begins "The **forward** elements …"*), add the following as a new 3rd sentence:*

If a CA issues a certificate to another CA, and the subject CA is not a subordinate to the issuer CA in a hierarchy, then the issuer CA must place that certificate in the **reverse** element of the **crossCertificatePair** attribute of its own directory entry.

2.3) This corrects the defects reported in defect report 257

In clause 8 in the ASN.1 construct **CertificatePair***:*

Replace **forward** *with* **issuedByThisCA** *and*
Replace **reverse** *with* **issuedToThisCA** *and make changes to the associated text as outlined below.*

In the descriptive text, throughout ITU-T X.509, update the text accordingly to reflect these new terms. This includes the following specific clauses:

- *general descriptive text in clause 8;*
- *ASN.1 and descriptive text for the cross certificate pair attribute in clause 8;*
- *ASN.1 and descriptive text for the associated matching rules in clauses 12.7.3 and 12.7.4, and*
- *the duplicate ASN.1 constructs in Annex A.*

Also, add the following text to the end of the paragraph that begins "The **forward** elements ..."*:*

The term **forward** was used in previous editions for **issuedByThisCA**, and the term **reverse** was used in previous editions for **issuedToThisCA**.

2.4) This corrects the defects reported in defect report 258

In clause 8, add the following as a new paragraph at the end of the clause, immediately before the first subclause 8.1:

Each certificate in a certification path shall be unique. No certificate may appear more than once in a value of **theCACertificates** component of **CertificationPath** or in a value of **certificate** in the **CrossCertificates** component of **ForwardCertificationPath**.

In clause 12.4.3 add the following Note immediately after bullet a), "a set of certificates":

NOTE – Each certificate in a certification path is unique. A path that contains the same certificate two or more times is not a valid certification path.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series B	Means of expression: definitions, symbols, classification
Series C	General telecommunication statistics
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	TMN and network maintenance: international transmission systems, telephone circuits, telegraphy, facsimile and leased circuits
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks and open system communications**
Series Y	Global information infrastructure and Internet protocol aspects
Series Z	Languages and general software aspects for telecommunication systems

Geneva, 2002