International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.509

Corrigendum 3

(02/2011)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Directory

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

Technical Corrigendum 3

Recommendation ITU-T X.509 (2005) – Technical Corrigendum 3

ITU-T

ITU International Telecommunication Union

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

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.379
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.889
Generic applications of ASN.1	X.890–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	X.1000–X.1099
SECURE APPLICATIONS AND SERVICES	X.1100–X.1199
CYBERSPACE SECURITY	X.1200–X.1299
SECURE APPLICATIONS AND SERVICES	X.1300–X.1399
CYBERSECURITY INFORMATION EXCHANGE	X.1500–X.1598

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

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

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

Technical Corrigendum 3

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T X.509	1988-11-25	
2.0	ITU-T X.509	1993-11-16	7
3.0	ITU-T X.509	1997-08-09	7
3.1	ITU-T X.509 (1997) Technical Cor. 1	2000-03-31	7
3.2	ITU-T X.509 (1997) Technical Cor. 2	2001-02-02	7
3.3	ITU-T X.509 (1997) Technical Cor. 3	2001-10-29	7
3.4	ITU-T X.509 (1997) Technical Cor. 4	2002-04-13	17
3.5	ITU-T X.509 (1997) Technical Cor. 5	2003-02-13	17
3.6	ITU-T X.509 (1997) Technical Cor. 6	2004-04-29	17
4.0	ITU-T X.509	2000-03-31	7
4.1	ITU-T X.509 (2000) Technical Cor. 1	2001-10-29	7
4.2	ITU-T X.509 (2000) Technical Cor. 2	2002-04-13	17
4.3	ITU-T X.509 (2000) Technical Cor. 3	2004-04-29	17
4.4	ITU-T X.509 (2000) Technical Cor. 4	2007-01-13	17
5.0	ITU-T X.509	2005-08-29	17
5.1	ITU-T X.509 (2005) Cor. 1	2007-01-13	17
5.2	ITU-T X.509 (2005) Cor. 2	2008-11-13	17
5.3	ITU-T X.509 (2005) Cor. 3	2011-02-13	17
6.0	ITU-T X.509	2008-11-13	17
6.1	ITU-T X.509 (2008) Cor. 1	2011-02-13	17

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). 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.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

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 not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

CONTENTS

INTERNATIONAL STANDARD
RECOMMENDATION ITU-T

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 subclause 15.5.2.5 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 3.3, 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 definitions 3.3.59 *and* 3.3.60 *with the text below:*

3.3.59 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.

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

3.3.61 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 constraints 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 IETF RFC 5914.

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**.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
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	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
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, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2011