International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.509

Corrigendum 1

(05/2015)

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 1

Recommendation ITU-T X.509 (2012) – Technical Corrigendum 1

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.1599
CLOUD COMPUTING SECURITY	X.1600–X.1699

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 1

Summary

Technical Corrigendum 1 to Rec. ITU-T X.509 | ISO/IEC 9594-8 covers the following:

– Resolution to defect reports 389, 390,393, 394, 395, 397, 398, 399, 400, 401, 402, 403, 404 and 405).

History

Edition	Recommendation	Approval	Study Group	Unique ID[*]
1.0	ITU-T X.509	1988-11-25		11.1002/1000/2999
2.0	ITU-T X.509	1993-11-16	7	11.1002/1000/3000
3.0	ITU-T X.509	1997-08-09	7	11.1002/1000/4123
3.1	ITU-T X.509 (1997) Technical Cor. 1	2000-03-31	7	11.1002/1000/5033
3.2	ITU-T X.509 (1997) Technical Cor. 2	2001-02-02	7	11.1002/1000/5311
3.3	ITU-T X.509 (1997) Technical Cor. 3	2001-10-29	7	11.1002/1000/5559
3.4	ITU-T X.509 (1997) Technical Cor. 4	2002-04-13	17	11.1002/1000/6025
3.5	ITU-T X.509 (1997) Technical Cor. 5	2003-02-13	17	11.1002/1000/6236
3.6	ITU-T X.509 (1997) Technical Cor. 6	2004-04-29	17	11.1002/1000/7285
4.0	ITU-T X.509	2000-03-31	7	11.1002/1000/5034
4.1	ITU-T X.509 (2000) Technical Cor. 1	2001-10-29	7	11.1002/1000/5560
4.2	ITU-T X.509 (2000) Technical Cor. 2	2002-04-13	17	11.1002/1000/6026
4.3	ITU-T X.509 (2000) Technical Cor. 3	2004-04-29	17	11.1002/1000/7284
4.4	ITU-T X.509 (2000) Technical Cor. 4	2007-01-13	17	11.1002/1000/8637
5.0	ITU-T X.509	2005-08-29	17	11.1002/1000/8501
5.1	ITU-T X.509 (2005) Cor. 1	2007-01-13	17	11.1002/1000/9051
5.2	ITU-T X.509 (2005) Cor. 2	2008-11-13	17	11.1002/1000/9591
5.3	ITU-T X.509 (2005) Cor. 3	2011-02-13	17	11.1002/1000/11042
5.4	ITU-T X.509 (2005) Cor. 4	2012-04-13	17	11.1002/1000/11577
6.0	ITU-T X.509	2008-11-13	17	11.1002/1000/9590
6.1	ITU-T X.509 (2008) Cor. 1	2011-02-13	17	11.1002/1000/11043
6.2	ITU-T X.509 (2008) Cor. 2	2012-04-13	17	11.1002/1000/11578
6.3	ITU-T X.509 (2008) Cor. 3	2012-10-14	17	11.1002/1000/11736
7.0	ITU-T X.509	2012-10-14	17	11.1002/1000/11735
7.1	ITU-T X.509 (2012) Cor. 1	2015-05-29	17	11.1002/1000/12474

[*] To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

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 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/.

INTERNATIONAL STANDARD
ITU-T RECOMMENDATION

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

Technical Corrigendum 1

(Covering resolution to defect reports 389, 390,393, 394, 395, 397, 398, 399, 400, 401, 402, 403, 404 and 405)

1) Correction of the defects reported in defect report 389

Replace clause 3.5.61 with the following:

3.5.61 self-issued attribute certificate: An attribute certificate where the issuer and the holder are the same attribute authority. An attribute authority might use a self-issued attribute certificate, for example, to publish policy information.

2) Correction of the defects reported in defect report 390

Delete the last paragraph of clause 8.6.2.

3) Correction of the defects reported in defect report 393

Replace the last paragraph of clause 8.5.2.9 with:

The scope of a CRL containing this extension is extended to include the revocation status of revoked certificates that expired after the date specified in **`ExpiredCertsOnCRL`** or at that date. The revocation status of a certificate shall not be updated once the certificate has expired.

4) Correction of the defects reported in defect report 394

Add the following references to clause 2.4

– IETF RFC 5914 (2010), *Trust Anchor Format*.

Add a new definition to clause 3.5:

3.5.68 trust anchor store: A trust anchor information collection at a relying party for one or more trust anchors.

Replace clause 7.5 with:

7.5 Trust anchor

An entity is a trust anchor for a particular relying party for one or more purposes, typically including certificate validation. A trust anchor is identified by trust anchor information. Trust anchor information includes a public key and some associated data. This trust anchor information is configured into the relying party in a trust anchor store. A relying party may have configured information about multiple trust anchors into one or more trust anchor stores.

A trust anchor may be a CA that issues public-key certificates and certificate revocation lists (CRLs) (see clause 7.10). The relying party may then use the trust anchor information for public-key certificate and CRL validation.

A trust anchor may also function as an end entity by signing other types of information such as software packages, time stamps, responses to online certificate status protocol (OCSP) requests (see IETF RFC 6960), etc.

A CA may be a trust anchor for some entities with respect to particular public-key certificates, but may otherwise be an ordinary CA.

NOTE 1 – As an example, entities within a company may trust all the public-key certificates issued by the company CA. This CA is then the trust anchor for these local relying parties with respect to locally issued public-key certificates. However, by use of name constraints, it might not be a trust anchor with respect to public-key certificates issued outside the company. Likewise, relying parties outside the company may not consider the company CA as the trust anchor for any public-key certificates.

NOTE 2 – The term trust anchor is seen as synonymous with the term root-CA. In a strict hierarchy, the CA at the top of the hierarchy may be the root CA and it may also be a trust anchor. However, in more complex environments, it may not be possible

> to identify a root CA. Even when it is possible to identify a root CA, a relying party may not necessarily consider it a trust anchor. An intermediate CA may instead take that role.

IETF RFC 5914 defines trust anchor information as a choice between three alternatives:

```
TrustAnchorChoice ::= CHOICE {
  certificate     Certificate,
  tbsCert     [1] EXPLICIT TBSCertificate,
  taInfo      [2] EXPLICIT TrustAnchorInfo }
```

The **`certificate`** alternative specifies a public-key certificate that can be either a self-signed certificate or a public-key certificate.

The **`tbsCert`** alternative specifies an unsigned public-key certificate as defined in clause 7.2.

NOTE 3 – This alternative is deprecated by this Specification and therefore not considered further.

The **`taInfo`** alternative specify a special trust anchor information format defined by IETF RFC 5914.

In case the trust anchor information is not used for signing public-key certificates, it shall be an end-entity public-key certificate.

5) Correction of the defects reported in defect report 395

Add the following to the references in clause 2.4:

- IETF RFC 3492 (2003), *Punycode: A Bootstring encoding of Unicode for Internationalized Domain Names in Applications (IDNA).*
- IETF RFC 5890 (2010), *Internationalized Domain Names for Applications (IDNA): Definitions and Document Framework.*

Add the following abbreviations to clause 4:

FQDN	Fully-Qualified Domain Name
IDN	Internationalized Domain Name
LDH	Letters, Digits, Hyphen

Replace the text for the ***`dNSName`*** *in clause 8.3.2.1 with:*

- the **`dNSName`** alternative shall be a fully-qualified domain name (FQDN). The domain name shall be in the syntax as specified by section 2.3.1 of IETF RFC 5890 meaning that a domain name is a sequence of labels in the letters, digits, hyphen (LDH) format separated by dots.

  A label may be in one of two formats:

  a) All characters in the label are from the Basic Latin collection as defined by ISO/IEC 10646 (i.e., having code points in the ranges 002D, 0030-0039, 0041-005A and 0061-007A) and it does not start with "xn--". The maximum length is 63 octets.

  b) It is an A-label as defined in IETF RFC 5890, i.e., it starts with the "xn--" and is a U-label converted to valid ASCII characters as in item a) using the Punycode algorithm defined by IETF RFC 3492. The converted string shall be maximum 59 octets. To be valid, it shall be possible for an A-label to be converted to a valid U-label. The U-label is as also defined in IETF RFC 5890.

  NOTE 1 – An A-label is normally not human-readable.

6) Correction of the defects reported in defect report 397

In clause 7.10, replace the explanatory text for the ***`version`*** *component with:*

The **`version`** field shall indicate the version of the encoded revocation list. If the **`extensions`** component is present in the revocation list, the version shall be **`v2`**. If the **`extensions`** component is not present, the version shall either be absent or present as **`v2`**.

> NOTE 1 – In the first and the second editions of this specification, the version component was always absent. In the third, fourth, fifth and sixth editions of this specification, the version shall be v2, if the extensions component flagged as critical is present in the revocation list. Or the version may either be absent or present as v2, if no extensions component flagged as critical is present in the revocation list.

Delete current Note 4.

Renumber the remaining notes from clause 7.10.

7) Correction of the defects reported in defect report 398

Update the ASN.1 in clause 8.6.2.2 as shown:

```
IssuingDistPointSyntax ::= SEQUENCE {
  -- If onlyContainsUserPublicKeyCerts and onlyContainsCACerts are both FALSE,
  -- the CRL covers both public-key certificate types
  distributionPoint              [0]  DistributionPointName OPTIONAL,
  onlyContainsUserPublicKeyCerts [1]  BOOLEAN DEFAULT FALSE,
  onlyContainsCACerts            [2]  BOOLEAN DEFAULT FALSE,
  onlySomeReasons                [3]  ReasonFlags OPTIONAL,
  indirectCRL                    [4]  BOOLEAN DEFAULT FALSE,
  onlyContainsAttributeCerts     [5]  BOOLEAN OPTIONAL, -- Use is strongly deprecated
  ... }
```

After the first paragraph after the ASN.1, add a new paragraph:

If **`onlyContainsAttributeCerts`** is **`TRUE`**, the CRL only contains revocations for attribute certificates. This component is deprecated and should not be included. Instead, the **`aAissuingDistributionPoint`** extension should be used.

> NOTE 1 – This component was introduced into the fourth edition of this Specification and removed again in the fifth edition. Each of these two actions has caused compatibility problems. This component has been reintroduced into the sixth edition in a way to remove any compatibility issues.

In the penultimate paragraph of clause 8.6.2.2, renumber current NOTE as NOTE 2.

8) Correction of the defects reported in defect report 399

C.1 Introduction

Replace the third paragraph of C.1:

This annex is written for revocation status checking of public-key certificates using CRLs, Full and Complete End-Entity CRLs (EPRLs) and CA Revocation Lists (CARLs). However, this description can also be applied to revocation status checking of attribute certificates using Attribute Certificate Revocation Lists (ACRL) and Attribute Authority Revocation Lists (AARL). For the purposes of this annex, ACRL can be considered in place of CRL, EPRL can be full and complete end-entity ACRL, and AARL in place of CARL. Similarly, the directory attributes identified in clause C.4 shall be mapped to those for the AARL and ACRL and the fields identifying certificate types in the Issuing Distribution Point extension can be mapped to those applicable to PMI.

with:

This annex is written for revocation status checking of public-key certificates using CRLs, full and complete end-entity certificate revocation lists (EPRLs) and certification authority revocation lists (CARLs). However, this description may also be applied to revocation status checking of attribute certificates. For the purposes of this annex, privilege verifier may be considered in place of relying party, attribute certificate revocation lists (ACRLs) may be considered in place of CRLs, full and complete end-entity attribute certifications lists (ACRLs) in place of EPRLs, and attribute authority revocation lists (AARLs) in place of CARLs. Similarly, the directory attributes types **`certificateRevocationList`** and **`authorityRevocationList`** identified in clause C.4 may be mapped into **`attributeCertificateRevocationList`** and **`attributeAuthorityRevocationList`** and the **`issuingDistributionPoint`** extension may be mapped into the **`aAissuingDistributionPoint`** extension.

C.1.1 CRL types

Update the following as shown:

CRLs of one or more of the following types may be available to a relying party, based on the revocation aspects of the policy of the certificate issuing authority:

- Full and complete CRL;
- Full and complete end-entity public-key certificate revocation list ~~CRL~~ (EPRL);
- Full and complete certification authority ~~CA R~~revocation ~~L~~list (CARL);

- Distribution Point CRL, EPRL or CARL;
- Indirect CRL, EPRL or CARL (ICRL);
- Delta CRL, EPRL or CARL;
- Indirect dCRL, EPRL or CARL.

9) Correction of the defects reported in defect report 400

*In clause 8.3.2.1, replace the text for the **`iPAddress`** alternative of the **`GeneralName`** data type with:*

- the **`iPAddress`** alternative is an Internet Protocol address defined in accordance with IETF RFC 791 for IPv4 (four octets) or in accordance with IETF 2460 for IPv6 (16 octets).

10) Correction of the defects reported in defect report 401

*In clause 7.2, replace the **`ALGORITHM`** information object class with:*

```
ALGORITHM ::= CLASS {
  &Type           OPTIONAL,
  &id             OBJECT IDENTIFIER UNIQUE }
WITH SYNTAX {
  [PARMS          &Type]
  IDENTIFIED BY  &id }
```

In Annex B, replace the **`rsa`**, *the* **`MD5Algorithm`** `and` *the* **`sha1Algorithm`** *type object classes with:*

```
rsa ALGORITHM ::= {PARMS           KeySize
                   IDENTIFIED BY  id-ea-rsa
}

mD5Algorithm ALGORITHM ::= { PARMS NULL
IDENTIFIED BY {iso(1) member-body(2) us(840) rsadsi(113549) digestAlgorithm(2) md5(5)}}


sha1Algorithm ALGORITHM ::= { PARMS NULL
IDENTIFIED BY {iso(1) identified-organization(3) oiw(14) secsig(3) algorithm(2) 26}}
```

11) Correction of the defects reported in defect report 402

Replace the first paragraph of clause 8.2.2.1 with:

This extension, which may be used as either a public-key certificate extension or CRL extension, identifies the public key to be used to verify the signature on this public-key certificate or CRL. It enables distinct keys used by the same CA used for signing public-key certificates to be distinguished (e.g., as key updating occurs) and it enables distinct keys used by the same CRL issuer to be distinguished. This extension is defined as follows:

12) Correction of the defects reported in defect report 403

In clause 7.2, add the following to the second paragraph after the ASN.1 (starting with "The TBSCertificate data type ...":

It shall be encoded using the DER.

In clause 12.1:

Change **`AttributeCertificateInfo`** *to* **`TBSAttributeCertificate`**:

Add a new paragraph after the ASN.1:

The **`TBSAttributeCertificate`** data type is the unsigned attribute certificate and is referred to as a to-be-signed attribute certificate. It shall be encoded using the DER.

Add the following note after the above-mentioned new paragraph and renumber the remaining notes in this clause accordingly:

NOTE 1 – Some specifications may specify that a public-key certificate may be transmitted in a non-DER encoding, i.e., in BER encoding without the DER restrictions, but the signature then has to be generated over a DER encoded value of the **`TSBCertificate`** data type. An otherwise valid signature will then fail the signature validation if the relying party does not decode the public-key certificate and then DER encode it before validating the signature. It is a local policy decision whether in this case to fail the validation or to re-encode the public-key certificate.

13) Correction of the defects reported in defect report 404

Add the following to clause 3.5, after clause 3.5.54, and renumber subsequent clauses accordingly:

3.5.55 registration authority: Those aspects of the responsibilities of a certification authority that are related to identification and authentication of the subject of a public-key certificate to be issued by that certification authority. A registration authority may either be a separate entity or be an integrated part of the certification authority.

NOTE – This definition is different in scope from the one defined in Rec. ITU-T X.660 | ISO/IEC 9834-1.

14) Correction of the defects reported in defect report 405

In clause 8.2.2.3, delete the following ASN.1:

```
subjectKeyIdentifier EXTENSION ::= {
  SYNTAX         SubjectKeyIdentifier
  IDENTIFIED BY  id-ce-subjectKeyIdentifier }

SubjectKeyIdentifier ::= KeyIdentifier
```

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	Environment and ICTs, climate change, e-waste, energy efficiency; 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, 2015