

Recommendation

ITU-T X.509 (2019) Cor. 2 (10/2023)

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 2

ITU-T X-SERIES RECOMMENDATIONS

Data networks, open system communications and security

PUBLIC DATA NETWORKS	X.1-X.199
OPEN SYSTEMS INTERCONNECTION	X.200-X.299
INTERWORKING BETWEEN NETWORKS	X.300-X.399
MESSAGE HANDLING SYSTEMS	X.400-X.499
DIRECTORY	X.500-X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600-X.699
OSI MANAGEMENT	X.700-X.799
SECURITY	X.800-X.849
OSI APPLICATIONS	X.850-X.899
OPEN DISTRIBUTED PROCESSING	X.900-X.999
INFORMATION AND NETWORK SECURITY	X.1000-X.1099
SECURE APPLICATIONS AND SERVICES (1)	X.1100-X.1199
CYBERSPACE SECURITY	X.1200-X.1299
SECURE APPLICATIONS AND SERVICES (2)	X.1300-X.1499
CYBERSECURITY INFORMATION EXCHANGE	X.1500-X.1599
CLOUD COMPUTING SECURITY	X.1600-X.1699
QUANTUM COMMUNICATION	X.1700-X.1729
DATA SECURITY	X.1750-X.1799
IMT-2020 SECURITY	X.1800-X.1819

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

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

Technical Corrigendum 2

Summary

Corrigendum 2 to ITU-T X.509 (2019) | ISO/IEC 9594-8:2020 covers resolution to defect reports 434 and 435.

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	2003-02-13	17	11.1002/1000/15258
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

* To access the Recommendation, type the URL <https://handle.itu.int/> in the address field of your web browser, followed by the Recommendation's unique ID.

7.1	ITU-T X.509 (2012) Cor. 1	2015-05-29	17	11.1002/1000/12474
7.2	ITU-T X.509 (2012) Cor. 2	2016-04-29	17	11.1002/1000/12844
7.3	ITU-T X.509 (2012) Cor. 3	2016-10-14	17	11.1002/1000/13032
8.0	ITU-T X.509	2016-10-14	17	11.1002/1000/13031
9.0	ITU-T X.509	2019-10-14	17	11.1002/1000/14033
9.1	ITU-T X.509 (2019) Cor. 1	2021-10-14	17	11.1002/1000/14791
9.2	ITU-T X.509 (2019) Cor. 2	2023-10-29	17	11.1002/1000/15705

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/software copyrights, 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 appropriate ITU-T databases available via the ITU-T website at <http://www.itu.int/ITU-T/ipr/>.

© ITU 2023

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

INTERNATIONAL STANDARD
ITU-T RECOMMENDATION

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

Technical Corrigendum 2

(Covering resolution to defect reports 434 and 435)

1) Correction of the defects reported in defect report 434

Replace the definition of the role attribute type in 16.5.1 with:

```
role ATTRIBUTE ::= {
  WITH SYNTAX   RoleSyntax
  LDAP-SYNTAX   ldapRoleSyntax.&id
  LDAP-NAME     {"role"}
  LDAP-DESC     "LDAP role"
  ID            id-at-role }
```

Replace the definition of xmlPrivilegeInfo in 16.7 with:

```
xmlPrivilegeInfo ATTRIBUTE ::= {
  WITH SYNTAX   UTF8String --contains XML-encoded privilege information
  LDAP-SYNTAX   directoryString.&id
  LDAP-NAME     {"xmlPrivInfo"}
  LDAP-DESC     "XML Privilege Info"
  ID            id-at-xMLPrivilegeInfo }
```

Replace the definition of permission attribute in 16.8.1 with:

```
permission ATTRIBUTE ::= {
  WITH SYNTAX           DualStringSyntax
  EQUALITY MATCHING RULE dualStringMatch
  LDAP-SYNTAX           ldapDualStringSyntax.&id
  LDAP-NAME             {"permission"}
  LDAP-DESC             "LDAP permission"
  ID                    id-at-permission }
```

Replace the definition of dualStringMatch matching rule in 16.8.2 with:

```
dualStringMatch MATCHING-RULE ::= {
  SYNTAX           DualStringSyntax
  LDAP-SYNTAX       ldapDualStringSyntax.&id
  LDAP-NAME         {"permission"}
  LDAP-DESC         "LDAP permission match"
  ID                id-mr-dualStringMatch }
```

Replace the definition of the PMI user object class in 19.1.1 with:

```
pmiUser OBJECT-CLASS ::= {
  SUBCLASS OF {top}
  KIND        auxiliary
  MAY CONTAIN {attributeCertificateAttribute}
  LDAP-NAME   {"pmiUser"}
  LDAP-DESC   "Privilege holder"
  ID          id-oc-pmiUser }
```

Replace the definition of the PMI AA object class in 19.1.2 with:

```
pmiAA OBJECT-CLASS ::= { -- a PMI AA
  SUBCLASS OF {top}
  KIND        auxiliary
  MAY CONTAIN {aACertificate |
               attributeCertificateRevocationList |
               eeAttrCertificateRevocationList |
               attributeAuthorityRevocationList}
```

```

LDAP-NAME      {"pmiAA"}
LDAP-DESC      "Privilege authority"
ID             id-oc-pmiAA }

```

Replace the definition of the PMI SOA object class in 19.1.3 with:

```

pmiSOA OBJECT-CLASS ::= { -- a PMI Source of Authority
  SUBCLASS OF {top}
  KIND        auxiliary
  MAY CONTAIN {attributeCertificateRevocationList |
               eeAttrCertificateRevocationList |
               attributeAuthorityRevocationList |
               attributeDescriptorCertificate}
  LDAP-NAME    {"pmiSOA"}
  LDAP-DESC    "Source of authority"
  ID           id-oc-pmiSOA }

```

Replace the definition of the Attribute certificate CRL distribution point object class in 19.1.4 with:

```

attCertCRLDistributionPt OBJECT-CLASS ::= {
  SUBCLASS OF {top}
  KIND        auxiliary
  MAY CONTAIN {attributeCertificateRevocationList |
               eeAttrCertificateRevocationList |
               attributeAuthorityRevocationList}
  LDAP-NAME    {"ACRL distribution point"}
  ID           id-oc-attCertCRLDistributionPts }

```

Replace the definition of the Attribute certificate PMI delegation path object class in 19.1.5 with:

```

pmiDelegationPath OBJECT-CLASS ::= {
  SUBCLASS OF {top}
  KIND        auxiliary
  MAY CONTAIN {delegationPath}
  LDAP-NAME    {"pmiDelegationPath"}
  LDAP-DESC    "Privilege delegation path"
  ID           id-oc-pmiDelegationPath }

```

Replace the definition of the privilege policy object class in 19.1.6 with:

```

privilegePolicy OBJECT-CLASS ::= {
  SUBCLASS OF {top}
  KIND        auxiliary
  MAY CONTAIN {privPolicy}
  LDAP-NAME    {"privilegePolicy"}
  LDAP-DESC    "Privilege policy"
  ID           id-oc-privilegePolicy }

```

Replace the definition of the protected privilege policy object class in 19.1.7 with:

```

protectedPrivilegePolicy OBJECT-CLASS ::= {
  SUBCLASS OF {top}
  KIND        auxiliary
  MAY CONTAIN {protPrivPolicy}
  LDAP-NAME    {"protectedPrivilegePolicy"}
  LDAP-DESC    "Protected privilege policy"
  ID           id-oc-protectedPrivilegePolicy }

```

Replace the definition of attributeCertificateAttribute attribute type in 19.2.1 with:

```

attributeCertificateAttribute ATTRIBUTE ::= {
  WITH SYNTAX      AttributeCertificate
  EQUALITY MATCHING RULE attributeCertificateExactMatch
  LDAP-SYNTAX      x509AttributeCertificate.&id
  LDAP-NAME        {"attributeCertificateAttribute"}
  LDAP-DESC        "X.509 Attr certificate attribute"
  ID               id-at-attributeCertificate }

```


Replace the definition of *aACertificate* attribute type in 19.2.2 with:

```
aACertificate ATTRIBUTE ::= {
  WITH SYNTAX      AttributeCertificate
  EQUALITY MATCHING RULE  attributeCertificateExactMatch
  LDAP-SYNTAX      x509AttributeCertificate.&id
  LDAP-NAME        {"aACertificate"}
  LDAP-DESC        "X.509 AA certificate"
  ID               id-at-aACertificate }
```

Replace the definition of *attributeDescriptorCertificate* attribute type in 19.2.3 with:

```
attributeDescriptorCertificate ATTRIBUTE ::= {
  WITH SYNTAX      AttributeCertificate
  EQUALITY MATCHING RULE  attributeCertificateExactMatch
  LDAP-SYNTAX      x509AttributeCertificate.&id
  LDAP-NAME        {"AttributeDescriptorCertificate"}
  LDAP-DESC        "X.509 Attr descriptor certificate"
  ID               id-at-attributeDescriptorCertificate }
```

Replace the definition of *delegationPath* attribute type in 19.2.7 with:

```
delegationPath ATTRIBUTE ::= {
  WITH SYNTAX      AttCertPath
  LDAP-SYNTAX      ldapAttCertPath.&id
  LDAP-NAME        {"delegationPath"}
  LDAP-DESC        "LDAP delegation path"
  ID               id-at-delegationPath }
```

Replace the definition of *privPolicy* attribute type in 19.2.8 with:

```
privPolicy ATTRIBUTE ::= {
  WITH SYNTAX      PolicySyntax
  LDAP-SYNTAX      x509PolicySyntax.&id
  LDAP-NAME        {"privPolicy"}
  LDAP-DESC        "X.509 privPolicy"
  ID               id-at-privPolicy }
```

Replace the definition of *protPrivPolicy* attribute type in 19.2.9 with:

```
protPrivPolicy ATTRIBUTE ::= {
  WITH SYNTAX      AttributeCertificate
  EQUALITY MATCHING RULE  attributeCertificateExactMatch
  LDAP-SYNTAX      x509AttributeCertificate.&id
  LDAP-NAME        {"protPrivPolicy"}
  LDAP-DESC        "X.509 prot priv policy"
  ID               id-at-protPrivPolicy }
```

Replace the definition of *xmlPrivPolicy* attribute type in 19.2.10 with:

```
xmlPrivPolicy ATTRIBUTE ::= {
  WITH SYNTAX      UTF8String -- XML-encoded privilege policy information
  LDAP-SYNTAX      directoryString.&id
  LDAP-NAME        {"xmlPrivPolicy"}
  LDAP-DESC        "LDAP XML Priv Policy"
  ID               id-at-xmlPrivPolicy }
```

Replace the definition of *attribute certificate exact match* matching rule in 19.3.1 with:

```
attributeCertificateExactMatch MATCHING-RULE ::= {
  SYNTAX      AttributeCertificateExactAssertion
  LDAP-SYNTAX  attCertExactAssertion.&id
  LDAP-NAME    {"attributeCertificateExactMatch"}
  LDAP-DESC    "Attribute Certificate Exact Match"
  ID           id-mr-attributeCertificateExactMatch }
```

Replace the definition of attribute certificate match matching rule in 19.3.2 with:

```
attributeCertificateMatch MATCHING-RULE ::= {
  SYNTAX      AttributeCertificateAssertion
  LDAP-SYNTAX attCertAssertion.&id
  LDAP-NAME    {"attributeCertificateMatch"}
  LDAP-DESC    "Attribute Certificate Match"
  ID           id-mr-attributeCertificateMatch }
```

Add a new clause 19.4:

19.4 PMI directory syntax definitions

19.4.1 LDAP role syntax

```
ldapRoleSyntax SYNTAX-NAME ::= {
  LDAP-DESC      "LDAP RoleSyntax"
  DIRECTORY SYNTAX RoleSyntax
  ID             id-asx-x509RoleSyntax }
```

A value which has `ldapRoleSyntax` syntax is the specification of a role expressed in a binary encoding such as DER encoding (see also IETF RFC 4522).

19.4.2 LDAP dual string syntax

```
ldapDualStringSyntax SYNTAX-NAME ::= {
  LDAP-DESC      "LDAP DualStringSyntax"
  DIRECTORY SYNTAX DualStringSyntax
  ID             id-asx-x509DualStringSyntax }
```

A value which has `ldapDualStringSyntax` syntax is the specification of a dual string expressed in a binary encoding such as DER encoding (see also IETF RFC 4522).

19.4.3 X.509 attribute certificate syntax

```
x509AttributeCertificate SYNTAX-NAME ::= {
  LDAP-DESC      "X.509 AttributeCertificate"
  DIRECTORY SYNTAX AttributeCertificate
  ID             id-asx-x509AttributeCertificateSyntax }
```

A value which has LDAP `x509AttributeCertificate` syntax is the specification of an attribute certificate expressed in a binary encoding such as DER encoding (see also IETF RFC 4522).

19.4.4 LDAP attribute certification path

```
ldapAttCertPath SYNTAX-NAME ::= {
  LDAP-DESC      "LDAP AttCertPath"
  DIRECTORY SYNTAX AttCertPath
  ID             id-asx-x509AttCertPath }
```

A value which has `ldapAttCertPath` syntax is the specification of an attribute certification path expressed in a binary encoding such as DER encoding (see also IETF RFC 4522).

19.4.5 LDAP policy Syntax

```
ldapPolicySyntax SYNTAX-NAME ::= {
  LDAP-DESC      "LDAP Policy syntax"
  DIRECTORY SYNTAX PolicySyntax
  ID             id-asx-x509PolicySyntax }
```

A value which has `ldapPolicySyntax` syntax is the specification of a policy syntax expressed in a binary encoding such as DER encoding (see also IETF RFC 4522).

19.4.6 Attribute Certificate Exact Match syntax

```
attCertExactAssertion SYNTAX-NAME ::= {
  LDAP-DESC      "Attribute Certificate Exact Match"
  DIRECTORY SYNTAX AttributeCertificateExactAssertion
  ID             id-asx-attCertExactAssertion }
```

A value of this syntax is a value of the **AttributeCertificateExactAssertion** data type specified in clause 19.3.1 and shall be encoded using the generic string encoding rules specified in IETF RFC 3641.

19.4.7 Attribute Certificate Match syntax

```
attCertAssertion SYNTAX-NAME ::= {
  LDAP-DESC          "Attribute Certificate Match"
  DIRECTORY SYNTAX   AttributeCertificateAssertion
  ID                  id-asx-attCertAssertion }
```

A value of this syntax is a value of the **AttributeCertificateAssertion** data type specified in clause 19.3.2 and shall be encoded using the generic string encoding rules specified in IETF RFC 3641.

Add the following definitions in Annex A at the end of the **AttributeCertificateDefinitions** module.

```
id-asx-x509RoleSyntax          OBJECT IDENTIFIER ::= {id-asx 13}
id-asx-x509DualStringSyntax    OBJECT IDENTIFIER ::= {id-asx 14}
id-asx-x509AttributeCertificateSyntax OBJECT IDENTIFIER ::= {id-asx 15}
id-asx-x509AttCertPath        OBJECT IDENTIFIER ::= {id-asx 16}
id-asx-x509PolicySyntax        OBJECT IDENTIFIER ::= {id-asx 17}
id-asx-attCertExactAssertion   OBJECT IDENTIFIER ::= {id-asx 18}
id-asx-attCertAssertion        OBJECT IDENTIFIER ::= {id-asx 19}
```

Add **id-asx** to the import from the **usefulDefinitions** module in Annex A, clause A.3.

IMPORTS

```
id-at, id-ce, id-mr, id-oc, id-asx
FROM UsefulDefinitions
{joint-iso-itu-t ds(5) module(1) usefulDefinitions(0) 9} WITH SUCCESSORS
```

Add the following entry to the list of normative references in clause 2.4:

- IETF RFC 3641 (2003), *Generic String Encoding Rules (GSER) for ASN.1 Types*.

Add the following entry to the bibliography:

- IETF RFC 4522 (2006), *Lightweight Directory Access Protocol (LDAP): The Binary Encoding Option*.

2) Correction of the defects reported in defect report 435

Add a new subclause 9.6.2.7:

9.6.2.7 No revocation information available extension

In some environments (e.g., where public-key certificates or attribute certificates are issued with very short validity periods), there may not be a need to revoke such certificates. A CA may use this extension to indicate that revocation status information is not provided for this public-key certificate, or an AA may use this extension to indicate that revocation status information is not provided for this attribute certificate. This extension is defined as follows:

```
noRevAvail EXTENSION ::= {
  SYNTAX          NULL
  IDENTIFIED BY   id-ce-noRevAvail }
```

This extension may be present in end-entity public key certificates issued by CAs and in attribute certificates issued by AAs. It shall not be present in CA or AA certificates.

This extension shall always be flagged as non-critical.

If this extension is present in a public-key certificate, a relying party need not seek revocation status information. If this extension is present in an attribute certificate, a privilege verifier need not seek revocation status information.

In 17.2.2.7 update the paragraph right after the **ASN.1** as shown:

This extension may be present in attribute certificates issued by AAs, including SOAs, to entities acting as PMI end entities. This extension shall not be included in public-key certificates or in attribute certificates issued to AAs.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
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	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
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, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems