International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.509

Corrigendum 1
(10/2021)

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 (2019) – 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 (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.

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

Corrigendum 1 to Rec. ITU-T X.509 (2019) | ISO/IEC 9594-8:2020 has successfully been balloted within ISO/IEC and therefore finally been approved by ISO/IEC.

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
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

Keywords

Cryptographic algorithm, object identifier

[*] 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/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/.

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 431 and 432)

1) Correction of the defects reported in defect report 431

Replace the first part of clause 6.2.2 down to and including the paragraph:

The algorithm component shall be an object identifier that uniquely identifies the cryptographic algorithm being defined.

with the following:

The following ASN.1 information object class is used to specify cryptographic algorithms.

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

The `ALGORITHM` information object class has the following fields.

a) The `&Type` field is used to specify those fixed parameters that are necessary for specifying the exact procedure for deploying the cryptographic algorithm being defined. Not all cryptographic algorithms require such parameters. The field is then absent or has the value `NULL`, as determined by the individual cryptographic algorithm specifications.

b) The `&DynParms` field is used to specify those dynamic parameters that determine the value(s) to be exchanged between two communicating entities when invoking the cryptographic algorithm. Not all cryptographic algorithms require dynamic parameters. In this case the `&DynParms` field shall be absent.

c) The `&id` field is used to uniquely identify the class of cryptographic algorithm being defined.

The `AlgorithmWithInvoke` parameterized data type defined as follows is used in situations where the type of cryptographic algorithm is signalled together with its invocation.

```
AlgorithmWithInvoke{ALGORITHM:SupportedAlgorithms} ::= SEQUENCE {
  algorithm        ALGORITHM.&id({SupportedAlgorithms}),
  parameters   [0] ALGORITHM.&Type({SupportedAlgorithms}{@algorithm}) OPTIONAL,
  dynamParms   [1] ALGORITHM.&DynParms({SupportedAlgorithms}{@algorithm}) OPTIONAL,
  ... }
```

The `AlgorithmWithInvoke` parameterized data type has the following components.

a) The `algorithm` component shall hold the object identifier that uniquely identify the cryptographic algorithm being defined.

b) The `parameters` component, when present, shall hold the values of the fixed parameters that further identify the cryptographic algorithm in question. This component shall be present when the `&Type` field is present in the information object for the cryptographic algorithm in question. Otherwise, it shall be absent.

c) The `dynamParms` component, when present, shall hold the value(s) required by the dynamic parameters for the cryptographic algorithm. This component shall be present when the `&DynParms` field is present in the information object for the cryptographic algorithm. Otherwise, it shall be absent.

The `AlgorithmIdentifier` parameterized data type defined as follows is used in situations where the type of cryptographic algorithm is signalled without a corresponding invocation.

```
AlgorithmIdentifier{ALGORITHM:SupportedAlgorithms} ::= SEQUENCE {
  algorithm        ALGORITHM.&id({SupportedAlgorithms}),
  parameters       ALGORITHM.&Type({SupportedAlgorithms}{@algorithm}) OPTIONAL,
  ... }
```

The components of **AlgorithmIdentifier** data type shall be as specified for the corresponding components of the **AlgorithmWithIvoke** parameterized data type.

The **AlgoInvoke** parameterized data type defined as follows is used when the cryptographic algorithm has previously been determined and where only invocation information is required.

```
AlgoInvoke{ALGORITHM:SupportedAlgorithms} ::=
    ALGORITHM.&DynParms({SupportedAlgorithms})
```

2) Correction of the defects reported in defect report 432

In Annex B of Rec. ITU-T X.509 | ISO/IEC 9594-8, replace:

```
sha224WithRSAEncryptionAlgorithm ALGORITHM ::= { -- IETF RFC 5754
  PARMS          NULL
  IDENTIFIED BY sha224WithRSAEncryption }

sha256WithRSAEncryptionAlgorithm ALGORITHM ::= { -- IETF RFC 7427
  PARMS          NULL
  IDENTIFIED BY sha256WithRSAEncryption }

sha384WithRSAEncryptionAlgorithm ALGORITHM ::= { -- IETF RFC 7427
  PARMS          NULL
  IDENTIFIED BY sha384WithRSAEncryption }

sha512WithRSAEncryptionAlgorithm ALGORITHM ::= { -- IETF RFC 7427
  PARMS          NULL
  IDENTIFIED BY sha512WithRSAEncryption }
```

With:

```
sha224RSA ALGORITHM ::= { -- IETF RFC 4055
  PARMS          NULL
  IDENTIFIED BY sha224WithRSAEncryption }

sha256RSA ALGORITHM ::= { -- IETF RFC 4055
  PARMS          NULL
  IDENTIFIED BY sha256WithRSAEncryption }

sha384RSA ALGORITHM ::= { -- IETF RFC 4055
  PARMS          NULL
  IDENTIFIED BY sha384WithRSAEncryption }

sha512RSA ALGORITHM ::= { -- IETF RFC 4055
  PARMS          NULL
  IDENTIFIED BY sha512WithRSAEncryption }
```

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

Printed in Switzerland
Geneva, 2021