INTERNATIONAL STANDARD ISO/IEC 9594-8:2020
TECHNICAL CORRIGENDUM 1

Published 2021-12

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION • МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ПО СТАНДАРТИЗАЦИИ • ORGANISATION INTERNATIONALE DE NORMALISATION
INTERNATIONAL ELECTROTECHNICAL COMMISSION • МЕЖДУНАРОДНАЯ ЭЛЕКТРОТЕХНИЧЕСКАЯ КОМИССИЯ • COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

Information technology — Open systems interconnection —

Part 8:
The Directory: Public-key and attribute certificate frameworks

TECHNICAL CORRIGENDUM 1

Technical Corrigendum 1 to ISO/IEC 9594-8:2020 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 6, *Telecommunications and information exchange between systems,* in collaboration with ITU-T. The identical text is published as ITU-T X.509 (2019)/Cor.1 (10/2021).

ICS 35.100.70 **Ref. No. ISO/IEC 9594-8:2020/Cor.1:2021(E)**

Published in Switzerland

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see https://patents.iec.ch).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by ITU-T [as ITU-T REC. X.509 (2019) – Technical Corrigendum 1 (2020)] and drafted in accordance with its editorial rules, in collaboration with Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 6, *Telecommunications and information exchange between systems.*

A list of all parts in the ISO/IEC 9594 series can be found on the ISO and IEC websites.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

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 }
```