INTERNATIONAL STANDARD

ISO/IEC 9594-8

Ninth edition
2020-11

Information technology — Open systems interconnection —

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

Reference number
ISO/IEC 9594-8:2020(E)

© ISO/IEC 2020



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2020

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

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 (see www.iso.org/directives).

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 http://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.

This document was prepared by ITU-T as ITU-T X.509 (10/2019) 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*.

This ninth edition cancels and replaces the eighth edition (ISO/IEC 9594-8:2017), which has been technically revised.

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

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.

© ISO/IEC 2020 – All rights reserved

CONTENTS

Page

SECTION 1 – General ... 1

1 Scope ... 1

2 Normative references ... 1

2.1 Identical Recommendations | International Standards ... 1

2.2 Paired Recommendations | International Standards equivalent in technical content ... 2

2.3 Recommendations ... 2

2.4 Other references ... 2

3 Definitions ... 3

3.1 OSI Reference Model security architecture definitions ... 3

3.2 Baseline identity management terms and definitions ... 3

3.3 Directory model definitions ... 3

3.4 Access control framework definitions ... 3

3.5 Public-key and attribute certificate definitions ... 3

4 Abbreviations ... 7

5 Conventions ... 8

6 Frameworks overview ... 8

6.1 Digital signatures ... 9

6.2 Public-key cryptography and cryptographic algorithms ... 10

6.3 Distinguished encoding of basic encoding rules ... 12

6.4 Applying distinguished encoding ... 12

6.5 Using repositories ... 13

SECTION 2 – PUBLIC-KEY CERTIFICATE FRAMEWORK ... 14

7 Public keys and public-key certificates ... 14

7.1 Introduction ... 14

7.2 Public-key certificate ... 14

7.3 Public-key certificate extensions ... 17

7.4 Types of public-key certificates ... 18

7.5 Trust anchor ... 18

7.6 Entity relationship ... 19

7.7 Certification path ... 19

7.8 Generation of key pairs ... 21

7.9 Public-key certificate creation ... 21

7.10 Certificate revocation list ... 22

7.11 Uniqueness of names ... 25

7.12 Indirect CRLs ... 25

7.13 Repudiation of a digital signing ... 26

8 Trust models ... 27

8.1 Three-cornered trust model ... 27

8.2 Four cornered trust model ... 27

9 Public-key certificate and CRL extensions ... 28

9.1 Policy handling ... 29

9.2 Key and policy information extensions ... 31

9.3 Subject and issuer information extensions ... 38

9.4 Certification path constraint extensions ... 41

9.5 Basic CRL extensions ... 45

9.6 CRL distribution points and delta CRL extensions ... 52

9.7 Authorization and validation list extensions ... 57

9.8 Alternative cryptographic algorithms and digital signature extensions ... 58

10 Delta CRL relationship to base ... 59

11 Authorization and validation lists ... 60

11.1 Authorization and validation list concept ... 60

© ISO/IEC 2020 – All rights reserved

Page

11.2 The authorizer ... 60
11.3 Authorization and validation list syntax ... 61
11.4 Multiple cryptographic algorithms for authorization and validation list ... 62
12 Certification path processing procedure ... 63
12.1 Path processing inputs ... 63
12.2 Path processing outputs ... 63
12.3 Path processing variables ... 64
12.4 Initialization step ... 64
12.5 Public-key certificate processing ... 65
13 PKI directory schema ... 67
13.1 PKI directory object classes and name forms ... 67
13.2 PKI directory attributes ... 68
13.3 PKI directory matching rules ... 72
13.4 PKI directory syntax definitions ... 77
SECTION 3 – ATTRIBUTE CERTIFICATE FRAMEWORK ... 80
14 Attribute certificates ... 80
14.1 General ... 80
14.2 Attribute certificate syntax ... 81
14.3 Multiple cryptographic algorithms for attribute certificates ... 83
14.4 Delegation paths ... 83
14.5 Attribute certificate revocation lists ... 84
15 Attribute authority, source of authority and certification authority relationship ... 86
15.1 Privilege in attribute certificates ... 87
15.2 Privilege in public-key certificates ... 87
16 PMI models ... 87
16.1 General model ... 87
16.2 Control model ... 89
16.3 Delegation model ... 90
16.4 Group assignment model ... 90
16.5 Roles model ... 91
16.6 Recognition of Authority Model ... 93
16.7 XML privilege information attribute ... 96
16.8 Permission attribute and matching rule ... 97
17 Attribute certificate and attribute certificate revocation list extensions ... 97
17.1 Basic privilege management extensions ... 98
17.2 Privilege revocation extensions ... 101
17.3 Source of authority extensions ... 107
17.4 Role extensions ... 109
17.5 Delegation extensions ... 110
17.6 Recognition of authority extensions ... 114
17.7 Use of alternative digital signature algorithm and digital signature extensions ... 117
18 Delegation path processing procedure ... 118
18.1 Basic processing procedure ... 118
18.2 Role processing procedure ... 119
18.3 Delegation processing procedure ... 119
19 PMI directory schema ... 121
19.1 PMI directory object classes ... 121
19.2 PMI directory attributes ... 123
19.3 PMI general directory matching rules ... 125
Annex A – Public-key and attribute certificate frameworks ... 127
Annex B – Reference definition of cryptographic algorithms ... 155
Annex C Certificate extension attribute types ... 162

 © ISO/IEC 2020 – All rights reserved

Page
C.1 Certificate extension attribute concept ... 162
C.2 Formal specification for certificate extension attribute types ... 162
Annex D – External ASN.1 modules ... 171
Annex E – CRL generation and processing rules ... 180
E.1 Introduction ... 180
E.2 Determine parameters for CRLs ... 181
E.3 Determine CRLs required ... 182
E.4 Obtain CRLs ... 183
E.5 Process CRLs ... 183
Annex F – Examples of delta CRL issuance ... 187
Annex G – Privilege policy and privilege attribute definition examples ... 189
G.1 Introduction ... 189
G.2 Sample syntaxes ... 189
G.3 Privilege attribute example ... 193
Annex H – An introduction to public key cryptography[2)] ... 194
Annex I – Examples of use of certification path constraints ... 196
I.1 Example 1: Use of basic constraints ... 196
I.2 Example 2: Use of policy mapping and policy constraints ... 196
I.3 Use of name constraints extension ... 196
Annex J – Guidance on determining for which policies a certification path is valid ... 205
J.1 Certification path valid for a user-specified policy required ... 205
J.2 Certification path valid for any policy required ... 206
J.3 Certification path valid regardless of policy ... 206
J.4 Certification path valid for a user-specific policy desired, but not required ... 206
Annex K – Key usage certificate extension issues ... 207
Annex L – Deprecated extensions ... 208
L.1 CRL scope extension ... 208
Annex M – Directory concepts ... 211
M.1 Scope ... 211
M.2 The directory attribute concept ... 211
M.3 Basic directory concepts ... 211
M.4 Subtrees ... 212
M.5 Directory distinguished names ... 212
M.6 Directory schema ... 213
Annex N – Considerations on strong authentication ... 214
N.1 Introduction ... 214
N.2 One-way authentication ... 215
N.3 Two-way authentication ... 215
N.4 Three-way authentication ... 216
N.5 Five-way authentication (initiated by A) ... 217
N.6 Five-way authentication (initiated by B) ... 218
Annex O – Alphabetical list of information item definitions ... 220
Annex P – Amendments and corrigenda ... 223
Bibliography ... 224

© ISO/IEC 2020 – All rights reserved

Introduction

Many applications have requirements for security to protect against threats to the communication of information. Virtually all security services are dependent upon the identities of the communicating parties being reliably known, i.e., authenticated.

This Recommendation | International Standard defines a framework for public-key certificates. This framework includes the specification of data objects used to represent the public-key certificates themselves, as well as revocation notices for issued public-key certificates that should no longer be trusted. It defines some critical components of a public-key infrastructure (PKI), but it does not define a PKI in its entirety. However, this Recommendation | International Standard provides the foundation upon which full PKIs and their specifications can be built.

Similarly, this Recommendation | International Standard defines a framework for attribute certificates. This framework includes the specification of data objects used to represent the attribute certificates themselves, as well as revocation notices for issued attribute certificates that should no longer be trusted. It defines some critical components of a privilege management infrastructure (PMI), but it does not define a PMI in its entirety. However, this Recommendation | International Standard provides the foundation upon which full PMIs and their specifications can be built.

Directory schema definitions allow PKI and PMI information to be represented in a directory according to the specification found in the Directory Specifications (Rec. ITU-T X.500 | ISO/IEC 9594-1, Rec. ITU-T X.501 | ISO/IEC 9594-2, Rec. ITU-T X.511 | ISO/IEC 9594-3, Rec. ITU-T X.518 | ISO/IEC 9594-4, Rec. ITU-T X.519 | ISO/IEC 9594-5, Rec. ITU-T X.520 | ISO/IEC 9594-6, Rec ITU-T X.521 | ISO/IEC 9594-7 and Rec. ITU-T X.525 | ISO/IEC 9594-9) or according to the lightweight directory access protocol (LDAP) specification.

This Recommendation | International Standard provides the foundation frameworks upon which industry profiles can be defined by other standards groups and industry forums. Many of the features defined as optional in these frameworks may be mandated for use in certain environments through profiles. This ninth edition technically revises and enhances the eighth edition of this Recommendation | International Standard.

This ninth edition specifies versions 1, 2 and 3 of public-key certificates, versions 1 and 2 of certificate revocation lists and version 2 of attribute certificates.

The extensibility function was added in an earlier edition with version 3 of the public-key certificate and with version 2 of the certificate revocation list and was incorporated into the attribute certificate from its initial inception.

Annex A, which is an integral part of this Recommendation | International Standard, provides the ASN.1 modules which contain all of the definitions associated with the frameworks.

Annex B, which is not an integral part of this Recommendation | International Standard, lists object identifiers assigned to cryptographic algorithms defined by other specifications. It is provided for easy reference and import into other ASN.1 modules.

Annex C, which is an integral part of this Recommendation | International Standard, provides definitions for how certificate extension types may be represented by directory attribute types.

Annex D, which is not an integral part of this Recommendation | International Standard, includes extracts of external ASN.1 modules referenced by this Recommendation | International Standard.

Annex E, which is an integral part of this Recommendation | International Standard, provides rules for generating and processing certificate revocation lists (CRLs).

Annex F, which is not an integral part of this Recommendation | International Standard, provides examples of delta certificate revocation list (CRL) issuance.

Annex G, which is not an integral part of this Recommendation | International Standard, provides examples of privilege policy syntaxes and privilege attributes.

Annex H, which is not an integral part of this Recommendation | International Standard, is an introduction to public-key cryptography.

Annex I, which is not an integral part of this Recommendation | International Standard, contains examples of the use of certification path constraints.

Annex J, which is not an integral part of this Recommendation | International Standard, provides guidance for public-key infrastructure (PKI) enabled applications on the processing of certificate policy while in the certification path validation process.

Annex K, which is not an integral part of this Recommendation | International Standard, provides guidance on the use of the **`contentCommitment`** bit in the **`keyUsage`** certificate extension.

 © ISO/IEC 2020 – All rights reserved

Annex L, which is not an integral part of this Recommendation | International Standard, includes public-key and attribute certificate extensions that have been deprecated.

Annex M, which is not an integral part of this Recommendation | International Standard, gives a short introduction to directory and distinguished name concepts.

Annex N, which is not an integral part of this Recommendation | International Standard, provides some general considerations on strong authentication.

Annex O, which is not an integral part of this Recommendation | International Standard, contains an alphabetical list of information item definitions in this Recommendation | International Standard.

Annex P, which is not an integral part of this Recommendation | International Standard, lists the amendments and defect reports that have been incorporated to form this edition of this Recommendation | International Standard.

© ISO/IEC 2020 – All rights reserved

INTERNATIONAL STANDARD
ITU-T RECOMMENDATION

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

SECTION 1 – GENERAL

1 Scope

This Recommendation | International Standard addresses some of the security requirements in the areas of authentication and other security services through the provision of a set of frameworks upon which full services can be based. Specifically, this Recommendation | International Standard defines frameworks for:

- public-key certificates; and
- attribute certificates.

The public-key certificate framework defined in this Recommendation | International Standard specifies the information objects and data types for a public-key infrastructure (PKI), including public-key certificates, certificate revocation lists (CRLs), trust broker and authorization and validation lists (AVLs). The attribute certificate framework specifies the information objects and data types for a privilege management infrastructure (PMI), including attribute certificates, and attribute certificate revocation lists (ACRLs). This Recommendation | International Standard also provides the framework for issuing, managing, using and revoking certificates. An extensibility mechanism is included in the defined formats for both certificate types and for all revocation list schemes. This Recommendation | International Standard also includes a set of extensions, which is expected to be generally useful across a number of applications of PKI and PMI. The schema components (including object classes, attribute types and matching rules) for storing PKI and PMI information in a directory, are included in this Recommendation | International Standard.

This Recommendation | International Standard specifies the framework for strong authentication, involving credentials formed using cryptographic techniques. It is not intended to establish this as a general framework for authentication, but it can be of general use for applications which consider these techniques adequate.

Authentication (and other security services) can only be provided within the context of a defined security policy. It is a matter for users of an application to define their own security policy.

2 Normative references

The following Recommendations and International Standards contain provisions which, through reference in this text, constitute provisions of this Recommendation | International Standard. At the time of publication, the editions indicated were valid. All Recommendations and Standards are subject to revision, and parties to agreements based on this Recommendation | International Standard are encouraged to investigate the possibility of applying the most recent edition of the Recommendations and Standards listed below. Members of IEC and ISO maintain registers of currently valid International Standards. The Telecommunication Standardization Bureau of the ITU maintains a list of currently valid ITU-T Recommendations.

2.1 Identical Recommendations | International Standards

- Recommendation ITU-T X.411 (1999) | ISO/IEC 10021-4:2003, *Information technology – Message Handling Systems (MHS) – Message Transfer System: Abstract Service Definition and Procedures*.
- Recommendation ITU-T X.500 (2019) | ISO/IEC 9594-1:2020, *Information technology – Open Systems Interconnection – The Directory: Overview of concepts, models and services*.
- Recommendation ITU-T X.501 (2019) | ISO/IEC 9594-2:2020, *Information technology – Open Systems Interconnection – The Directory: Models*.
- Recommendation ITU-T X.511 (2019) | ISO/IEC 9594-3:2020, *Information technology – Open Systems Interconnection – The Directory: Abstract service definition*.
- Recommendation ITU-T X.518 (2019) | ISO/IEC 9594-4:2020, *Information technology – Open Systems Interconnection – The Directory: Procedures for distributed operation*.
- Recommendation ITU-T X.519 (2019) | ISO/IEC 9594-5:2020, *Information technology – Open Systems Interconnection – The Directory: Protocol specifications*.

© ISO/IEC 2020 – All rights reserved

- Recommendation ITU-T X.520 (2019) | ISO/IEC 9594-6:2020, *Information technology – Open Systems Interconnection – The Directory: Selected attribute types*.
- Recommendation ITU-T X.521 (2019) | ISO/IEC 9594-7:2020, *Information technology – Open Systems Interconnection – The Directory: Selected object classes*.
- Recommendation ITU-T X.525 (2019) | ISO/IEC 9594-9:2020, Information technology – Open Systems Interconnection – The Directory: Replication.
- Recommendation ITU-T X.660 (2011) | ISO/IEC 9834-1:2012, *Information technology – Open Systems Interconnection – Procedures for the operation of OSI Registration Authorities: General procedures and top arcs of the International Object Identifier tree*.
- Recommendation ITU-T X.680 (2015) | ISO/IEC 8824-1:2015, Information technology – Abstract Syntax Notation One (ASN.1): *Specification of basic notation*.
- Recommendation ITU-T X.681 (2015) | ISO/IEC 8824-2:2015, *Information technology – Abstract Syntax Notation One (ASN.1): Information object specification*.
- Recommendation ITU-T X.682 (2015) | ISO/IEC 8824-3:2015, Information technology – Abstract Syntax Notation One (ASN.1): *Constraint specification*.
- Recommendation ITU-T X.683 (2015) | ISO/IEC 8824-4:2015, Information technology – Abstract Syntax Notation One (ASN.1): *Parameterization of ASN.1 specifications*.
- Recommendation ITU-T X.690 (2015) | ISO/IEC 8825-1:2015, *Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*.
- Recommendation ITU-T X.812 (1995) | ISO/IEC 10181-3:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Access control framework*.
- Recommendation ITU-T X.813 (1996) | ISO/IEC 10181-4:1997, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Non-repudiation framework*.
- Recommendation ITU-T X.841 (2000) | ISO/IEC 15816:2002, *Information technology – Security techniques – Security information objects for access control*.

2.2 Paired Recommendations | International Standards equivalent in technical content

- Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

  ISO 7498-2:1989, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture*.

2.3 Recommendations

- Recommendation ITU-T X.1252 (2010), *Baseline identity management terms and definitions*.

2.4 Other references

- IETF RFC 791 (1981), *Internet Protocol*.
- IETF RFC 822 (1982), *Standard for the Format of ARPA Internet Text Messages.*
- IETF RFC 1630 (1994), *Universal Resource Identifiers in WWW: A Unifying Syntax for the Expression of Names and Addresses of Objects on the Network as used in the World-Wide Web*.
- IETF RFC 3492 (2003), *Punycode: A Bootstring encoding of Unicode for Internationalized Domain Names in Applications (IDNA)*.
- IETF RFC 4511 (2006), *Lightweight Directory Access Protocol (LDAP): The Protocol*.
- IETF RFC 4523 (2006), *Lightweight Directory Access Protocol (LDAP) Schema Definitions for X.509 Certificates*.
- IETF RFC 5280 (2008), *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*.
- IETF RFC 5890 (2010), *Internationalized Domain Names for Applications (IDNA): Definitions and Document Framework*.
- IETF RFC 5914 (2010), *Trust Anchor Format*.

 © ISO/IEC 2020 – All rights reserved

– IETF RFC 6960 (2013), *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP*.

3 Definitions

For the purposes of this Recommendation | International Standard, the following definitions apply.

3.1 OSI Reference Model security architecture definitions

The following terms are defined in Rec. ITU-T X.800 | ISO 7498-2:

a) authentication exchange;
b) authentication information;
c) confidentiality;
d) credentials;
e) cryptography;
f) data origin authentication;
g) decipherment;
h) digital signature;
i) encipherment; and
j) key;

3.2 Baseline identity management terms and definitions

The following term is defined in Rec. ITU-T X.1252:

a) trust.

3.3 Directory model definitions

The following terms are defined in Rec. ITU-T X.501 | ISO/IEC 9594-2:

a) attribute;
c) directory information tree (DIT);
b) directory system agent;
c) directory user agent (DUA);
d) distinguished name;
e) entry;
f) relative distinguished name;
g) root.

3.4 Access control framework definitions

The following terms are defined in Rec. ITU-T X.812 | ISO/IEC 10181-3:

a) access control decision function (ADF);
b) access control enforcement function (AEF).

3.5 Public-key and attribute certificate definitions

The following terms are defined in this Recommendation | International Standard:

3.5.1 ACRL distribution point: A directory entry or another distribution source for **attribute certificate revocation list**s (ACRLs); an ACRL distributed through an ACRL distribution point may contain revocation entries for only a subset of the full set of attribute certificates issued by one attribute authority (AA) or may contain revocation entries for multiple AAs.

© ISO/IEC 2020 – All rights reserved