This is a preview - click here to buy the full publication

INTERNATIONAL STANDARD

ISO/IEC 9594-8

Eighth edition
2017-05

Information technology — Open Systems Interconnection — The Directory —

Part 8: Public-key and attribute certificate frameworks

Technologies de l'information — Interconnexion de systèmes ouverts (OSI) — L'annuaire —

Partie 8: Cadre général des certificats de clé publique et d'attribut

withdrawn

Reference number
ISO/IEC 9594-8:2017(E)

© ISO/IEC 2017

This is a preview - click here to buy the full publication

withdrawn

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2017, Published in Switzerland

All rights reserved. Unless otherwise specified, 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
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

 © ISO/IEC 2017 – All rights reserved

This is a preview - click here to buy the full publication

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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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).

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).

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

For an explanation on 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 the following URL: www.iso.org/iso/foreword.html.

This eighth edition cancels and replaces the seventh edition (ISO/IEC 9594-8:2014), which has been technically revised.

This document was prepared by ISO/IEC JTC 1, *Information technology*, SC 6, *Telecommunications and information exchange between systems*, in collaboration with ITU-T. The identical text is published as ITU-T X.509 (10/2016).

A list of all parts in the ISO/IEC 9594 series, published under the general title *Information technology — Open Systems Interconnection — The Directory*, can be found on the ISO website.

Withdrawn

© ISO/IEC 2017 – All rights reserved

This is a preview - click here to buy the full publication

CONTENTS

		Page
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	2
3.1	OSI Reference Model security architecture definitions	2
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	11
6.4	Applying distinguished encoding	12
6.5	Using repositories	12
7	Public keys and public-key certificates	13
7.1	Introduction	13
7.2	Public-key certificate	13
7.3	Public-key certificate extensions	15
7.4	Types of public-key certificates	16
7.5	Trust anchor	16
7.6	Entity relationship	17
7.7	Certification path	18
7.8	Generation of key pairs	19
7.9	Public-key certificate creation	19
7.10	Certificate revocation list	20
7.11	Uniqueness of names	22
7.12	Indirect CRLs	22
7.13	Repudiation of a digital signing	24
8	Trust models	24
8.1	Three-cornered trust model	24
8.2	Four cornered trust model	25
9	Public-key certificate and CRL extensions	26
9.1	Policy handling	26
9.2	Key and policy information extensions	29
9.3	Subject and issuer information extensions	35
9.4	Certification path constraint extensions	37
9.5	Basic CRL extensions	41
9.6	CRL distribution points and delta CRL extensions	49
10	Delta CRL relationship to base	53
11	Authorization and validation lists	55
11.1	Authorization and validation list concept	55
11.2	The authorizer	55
11.3	Authorization and validation list syntax	55
11.4	Authorization and validation restrictions	57

Withdrawn

This is a preview - click here to buy the full publication

		Page
12	Certification path processing procedure	57
	12.1 Path processing inputs	57
	12.2 Path processing outputs	58
	12.3 Path processing variables	59
	12.4 Initialization step	59
	12.5 Public-key certificate processing	59
13	PKI directory schema	62
	13.1 PKI directory object classes and name forms	62
	13.2 PKI directory attributes	63
	13.3 PKI directory matching rules	66
	13.4 PKI directory syntax definitions	71
14	Attribute certificates	73
	14.1 Attribute certificate structure	73
	14.2 Delegation paths	76
	14.3 Attribute certificate revocation lists	76
15	Attribute authority, source of authority and certification authority relationship	77
	15.1 Privilege in attribute certificates	79
	15.2 Privilege in public-key certificates	79
16	PMI models	79
	16.1 General model	79
	16.2 Control model	81
	16.3 Delegation model	81
	16.4 Group assignment model	82
	16.5 Roles model	83
	16.6 Recognition of Authority Model	84
	16.7 XML privilege information attribute	88
	16.8 Permission attribute and matching rule	89
17	Attribute certificate and attribute certificate revocation list extensions	89
	17.1 Basic privilege management extensions	90
	17.2 Privilege revocation extensions	93
	17.3 Source of authority extensions	95
	17.4 Role extensions	97
	17.5 Delegation extensions	98
	17.6 Recognition of authority extensions	103
	17.7 Use of basic CRL extension for ACRLs	105
18	Delegation path processing procedure	109
	18.1 Basic processing procedure	109
	18.2 Role processing procedure	110
	18.3 Delegation processing procedure	110
19	PMI directory schema	112
	19.1 PMI directory object classes	113
	19.2 PMI directory attributes	114
	19.3 PMI general directory matching rules	116
20	Protocol support for public-key and privilege management infrastructures	118
	20.1 General syntax	118
	20.2 Wrapping of non-encrypted protocol data units	118
	20.3 Wrapping of encrypted protocol data unit	119
	20.4 Check of PKI-PMI-Wrapper protocol elements	121
	20.5 PKI-PMI-Wrapper error codes	122
21	Authorization and validation list management	123
	21.1 General	123
	21.2 Defined protocol data unit (PDU) types	123
	21.3 Checking of received PDU	123

Withdrawn

This is a preview - click here to buy the full publication

Page

21.4 Authorization and validation management protocol 124
21.5 Certification authority subscription protocol 130

22 Trust broker protocol 137

Annex A – Public-key and attribute certificate frameworks 140

Annex B – Reference definition of cryptographic algorithms 176

Annex C – Certificate extension attribute types 182
C.1 Certificate extension attribute concept 182
C.2 Formal specification for certificate extension attribute types 182

Annex D – External ASN.1 modules 190

Annex E – CRL generation and processing rules 199
E.1 Introduction 199
E.2 Determine parameters for CRLs 200
E.3 Determine CRLs required 201
E.4 Obtain CRLs 202
E.5 Process CRLs 202

Annex F – Examples of delta CRL issuance 206

Annex G – Privilege policy and privilege attribute definition examples 208
G.1 Introduction 208
G.2 Sample syntaxes 208
G.3 Privilege attribute example 212

Annex H – An introduction to public key cryptography[2)] 213

Annex I – Examples of use of certification path constraints 215
I.1 Example 1: Use of basic constraints 215
I.2 Example 2: Use of policy mapping and policy constraints 215
I.3 Use of name constraints extension 215

Annex J – Guidance on determining for which policies a certification path is valid 224
J.1 Certification path valid for a user-specified policy required 224
J.2 Certification path valid for any policy required 225
J.3 Certification path valid regardless of policy 225
J.4 Certification path valid for a user-specific policy desired, but not required 225

Annex K – Key usage certificate extension issues 226

Annex L – Deprecated extensions 227
L.1 CRL scope extension 227

Annex M – Directory concepts 230
M.1 Scope 230
M.2 Basic directory concepts 230
M.3 Directory schema 230
M.4 Directory distinguished names 231
M.5 Subtrees 231

Annex N – Considerations on strong authentication 232
N.1 Introduction 232
N.2 One-way authentication 233
N.3 Two-way authentication 233
N.4 Three-way authentication 234
N.5 Five-way authentication (initiated by A) 235
N.6 Five-way authentication (initiated by B) 236

Annex O – Alphabetical list of information item definitions 238

Annex P – Amendments and corrigenda 241

Bibliography 242

Withdrawn

This is a preview - click here to buy the full publication

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.

Schema definitions are defined for holding PKI and PMI information in a directory according to the specification found in the ITU-T X.500 series of Recommendations | ISO/IEC 9594 (all parts) 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 eighth edition technically revises and enhances the seventh edition of this Recommendation | International Standard.

This eighth 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.

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

Withdrawn

This is a preview - click here to buy the full publication

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.

withdrawn

This is a preview - click here to buy the full publication

INTERNATIONAL STANDARD
ITU-T RECOMMENDATION

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

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 (2016) | ISO/IEC 9594-1:2017, *Information technology – Open Systems Interconnection – The Directory: Overview of concepts, models and services*.

– Recommendation ITU-T X.501 (2016) | ISO/IEC 9594-2:2017, *Information technology – Open Systems Interconnection – The Directory: Models*.

– Recommendation ITU-T X.511 (2016) | ISO/IEC 9594-3:2017, *Information technology – Open Systems Interconnection – The Directory: Abstract service definition*.

– Recommendation ITU-T X.519 (2016) | ISO/IEC 9594-5:2017, *Information technology – Open Systems Interconnection – The Directory: Protocol specifications*.

– Recommendation ITU-T X.520 (2016) | ISO/IEC 9594-6:2017, *Information technology – Open Systems Interconnection – The Directory: Selected attribute types*.

– 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*.

Withdrawn

This is a preview - click here to buy the full publication

– 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.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*.

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

Withdrawn