INTERNATIONAL STANDARD

ISO/IEC 9594-8

Seventh edition
2014-03-01

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

Reference number
ISO/IEC 9594-8:2014(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web 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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

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.

ISO/IEC 9594-8 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 Rec. ITU-T X.509 (10/2012).

This seventh edition cancels and replaces the sixth edition (ISO/IEC 9594-8:2008), which has been technically revised. It also incorporates the Technical Corrigenda ISO/IEC 9594-8:2008/Cor.1:2011, ISO/IEC 9594-8:2008/Cor.2:2012 and ISO/IEC 9594-8:2008/Cor.3:2013.

ISO/IEC 9594 consists of the following parts, under the general title *Information technology — Open Systems Interconnection — The Directory*:

— *Part 1: Overview of concepts, models and services*

— *Part 2: Models*

— *Part 3: Abstract service definition*

— *Part 4: Procedures for distributed operation*

— *Part 5: Protocol specifications*

— *Part 6: Selected attribute types*

— *Part 7: Selected object classes*

— *Part 8: Public-key and attribute certificate frameworks*

— *Part 9: Replication*

CONTENTS

		Page
1	Scope	1
2	Normative references	2
2.1	Identical Recommendations | International Standards	2
2.2	Paired Recommendations | International Standards equivalent in technical content	3
2.3	Recommendations	3
2.4	Other references	3
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	4
3.4	Access control framework definitions	4
3.5	Public-key and attribute certificate definitions	4
4	Abbreviations	7
5	Conventions	8
6	Frameworks overview	8
6.1	Digital signatures	9
6.2	Formal definitions for public-key cryptography	10
6.3	Distinguished encoding of Basic Encoding Rules	10
6.4	Applying distinguished encoding	11
7	Public-keys and public-key certificates	11
7.1	Introduction	11
7.2	Public-key certificate	12
7.3	Public-key certificate extensions	14
7.4	Types of public-key certificates	15
7.5	Trust anchor	15
7.6	Entity relationship	16
7.7	Certification path	16
7.8	Generation of key pairs	18
7.9	Public-key certificate creation	18
7.10	Certificate revocation list	18
7.11	Repudiation of a digital signing	21
8	Public-key certificate and CRL extensions	22
8.1	Policy handling	22
8.2	Key and policy information extensions	25
8.3	Subject and issuer information extensions	31
8.4	Certification path constraint extensions	33
8.5	Basic CRL extensions	37
8.6	CRL distribution points and delta-CRL extensions	46
9	Delta CRL relationship to base	52
10	Certification path processing procedure	53
10.1	Path processing inputs	53
10.2	Path processing outputs	54
10.3	Path processing variables	54
10.4	Initialization step	55
10.5	Certificate processing	55
11	PKI directory schema	57
11.1	PKI directory object classes and name forms	57
11.2	PKI directory attributes	59
11.3	PKI directory matching rules	61
11.4	PKI directory syntax definitions	66

Page

12 Attribute Certificates 68
12.1 Attribute certificate structure 69
12.2 Attribute certification paths 71
13 Attribute Authority, SOA and Certification Authority relationship 71
13.1 Privilege in attribute certificates 73
13.2 Privilege in public-key certificates 73
14 PMI models 73
14.1 General model 73
14.2 Control model 75
14.3 Delegation model 76
14.4 Group assignment model 76
14.5 Roles model 77
14.6 Recognition of Authority Model 78
14.7 XML privilege information attribute 82
14.8 Permission attribute and matching rule 83
15 Privilege management certificate extensions 83
15.1 Basic privilege management extensions 84
15.2 Privilege revocation extensions 87
15.3 Source of Authority extensions 87
15.4 Role extensions 90
15.5 Delegation extensions 91
15.6 Recognition of Authority Extensions 95
16 Privilege path processing procedure 98
16.1 Basic processing procedure 98
16.2 Role processing procedure 99
16.3 Delegation processing procedure 99
17 PMI directory schema 102
17.1 PMI directory object classes 102
17.2 PMI Directory attributes 103
17.3 PMI general directory matching rules 105
18 Directory authentication 107
18.1 Simple authentication procedure 107
18.2 Password policy 109
18.3 Strong Authentication 119
19 Access control 122
20 Protection of Directory operations 122
Annex A – Public-Key and Attribute Certificate Frameworks 123
Annex B – Reference definition of algorithm object identifiers 153
Annex C – CRL generation and processing rules 154
C.1 Introduction 154
C.2 Determine parameters for CRLs 155
C.3 Determine CRLs required 156
C.4 Obtain CRLs 157
C.5 Process CRLs 157
Annex D – Examples of delta CRL issuance 161
Annex E – Privilege policy and privilege attribute definition examples 163
E.1 Introduction 163
E.2 Sample syntaxes 163
E.3 Privilege attribute example 167
Annex F – An introduction to public key cryptography[2)] 168
Annex G – Examples of use of certification path constraints 170

Page

G.1 Example 1: Use of basic constraints 170
G.2 Example 2: Use of policy mapping and policy constraints 170
G.3 Use of Name Constraints Extension 170

Annex H – Guidance on determining for which policies a certification path is valid 179
H.1 Certification path valid for a user-specified policy required 179
H.2 Certification path valid for any policy required 180
H.3 Certification path valid regardless of policy 180
H.4 Certification path valid for a user-specific policy desired, but not required 180

Annex I – Key usage certificate extension issues 181

Annex J – External ASN.1 modules 182

Annex K – Use of Protected Passwords for Bind operations 190

Annex L – Examples of password hashing algorithms 191
L.1 Null Hashing method 191
L.2 MD5 method 191
L.3 SHA-1 method 191

Annex M – Alphabetical list of information item definitions 192

Annex N – Amendments and corrigenda 195

Introduction

This Recommendation | International Standard, together with other Recommendations | International Standards, has been produced to facilitate the interconnection of information processing systems to provide directory services. A set of such systems, together with the directory information which they hold, can be viewed as an integrated whole, called the *Directory*. The information held by the Directory, collectively known as the Directory Information Base (DIB), is typically used to facilitate communication between, with or about objects such as application-entities, people, terminals and distribution lists.

The Directory plays a significant role in Open Systems Interconnection, whose aim is to allow, with a minimum of technical agreement outside of the interconnection standards themselves, the interconnection of information processing systems:

– from different manufacturers;
– under different managements;
– of different levels of complexity; and
– of different ages.

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., authentication.

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

Similarly, this Recommendation | International Standard defines a framework for attribute certificates. That framework includes the specification of data objects used to represent the certificates themselves, as well as revocation notices for issued certificates that should no longer be trusted. The attribute certificate framework defined in this Recommendation | International Standard, while it defines some critical components of a Privilege Management Infrastructure (PMI), it does not define a PMI in its entirety. However, this Recommendation | International Standard provides the foundation upon which full PMIs and their specifications would be built.

Information objects for holding PKI and PMI objects in the Directory and for comparing presented values with stored values are also defined.

This Recommendation | International Standard also defines a framework for the provision of authentication services by the Directory to its users.

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 seventh edition technically revises and enhances the sixth edition of this Recommendation | International Standard.

This seventh edition specifies versions 1, 2 and 3 of public-key certificates and versions 1 and 2 of certificate revocation lists. This edition also specifies 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. This function is specified in clause 7. It is anticipated that any enhancements to this edition can be accommodated using this function and avoid the need to create new versions.

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 an integral part of this Recommendation | International Standard, defines object identifiers assigned to authentication and encryption algorithms, in the absence of a formal register.

Annex C, which is an integral part of this Recommendation | International Standard, provides rules for generating and processing Certificate Revocation Lists.

Annex D, which is not an integral part of this Recommendation | International Standard, provides examples of delta-CRL issuance.

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

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

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

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

Annex I, 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 J, 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 K, which is not an integral part of this Recommendation | International Standard, provides a suggested technique for a Bind protected password.

Annex L, which is not an integral part of this Recommendation | International Standard, gives some examples of password hashing algorithms.

Annex M, 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 N, 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.

INTERNATIONAL STANDARD
RECOMMENDATION ITU-T

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;
- attribute certificates; and
- authentication services.

The public-key certificate framework defined in this Recommendation | International Standard includes a definition of the information objects for a public-key infrastructure (PKI), including public-key certificates and Certificate Revocation Lists (CRLs). The attribute certificate framework includes a definition of the information objects 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 standard extensions for each, 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 objects in the Directory, are included in this Recommendation | International Standard. Other elements of PKI and PMI, beyond these frameworks, such as key and certificate management protocols, operational protocols, additional certificate and CRL extensions are expected to be defined by other standards bodies (e.g., ISO TC 68, IETF, etc.).

The authentication scheme defined in this Recommendation | International Standard is generic and may be applied to a variety of applications and environments.

The Directory makes use of public-key certificates and attribute certificates, and the framework for the Directory's use of these facilities is also defined in this Recommendation | International Standard. Public-key technology, including certificates, is used by the Directory to enable strong authentication and signed operations, and for storage of signed data in the Directory. Attribute certificates can be used by the Directory to enable rule-based access control. Although the framework for these is provided in this Recommendation | International Standard, the full definition of the Directory's use of these frameworks, and the associated services provided by the Directory and its components is supplied in the complete set of ITU-T X.500 series of Recommendations | ISO/IEC 9594 (all parts).

This Recommendation | International Standard, in the Authentication services framework, also:

- specifies the form of authentication information held by the Directory;
- describes how authentication information may be obtained from the Directory;
- states the assumptions made about how authentication information is formed and placed in the Directory;
- defines three ways in which applications may use this authentication information to perform authentication and describes how other security services may be supported by authentication.

This Recommendation | International Standard describes two levels of authentication: simple authentication, using a password as a verification of claimed identity; and strong authentication, involving credentials formed using cryptographic techniques. While simple authentication offers some limited protection against unauthorized access, only strong authentication should be used as the basis for providing secure services. 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 which may be constrained by the services provided by a standard.

It is a matter for standards-defining applications which use the authentication framework to specify the protocol exchanges which need to be performed in order to achieve authentication based upon the authentication information obtained from the Directory. The protocol used by applications to obtain credentials from the Directory is the Directory Access Protocol (DAP), specified in Rec. ITU-T X.519 | ISO/IEC 9594-5.

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 (2012) | ISO/IEC 9594-1:2014, *Information technology – Open Systems Interconnection – The Directory: Overview of concepts, models and services*.
- Recommendation ITU-T X.501 (2012) | ISO/IEC 9594-2:2014, *Information technology – Open Systems Interconnection – The Directory: Models*.
- Recommendation ITU-T X.511 (2012) | ISO/IEC 9594-3:2014, *Information technology – Open Systems Interconnection – The Directory: Abstract service definition*.
- Recommendation ITU-T X.518 (2012) | ISO/IEC 9594-4:2014, *Information technology – Open Systems Interconnection – The Directory: Procedures for distributed operation*.
- Recommendation ITU-T X.519 (2012) | ISO/IEC 9594-5:2014, *Information technology – Open Systems Interconnection – The Directory: Protocol specifications*.
- Recommendation ITU-T X.520 (2012) | ISO/IEC 9594-6:2014, *Information technology – Open Systems Interconnection – The Directory: Selected attribute types*.
- Recommendation ITU-T X.521 (2012) | ISO/IEC 9594-7:2014, *Information technology – Open Systems Interconnection – The Directory: Selected object classes*.
- Recommendation ITU-T X.525 (2012) | ISO/IEC 9594-9:2014, *Information technology – Open Systems Interconnection – The Directory: Replication*.
- Recommendation ITU-T X.660 (2008) | ISO/IEC 9834-1:2008, *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 (2008) | ISO/IEC 8824-1:2008, *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation*.
- Recommendation ITU-T X.681 (2008) | ISO/IEC 8824-2:2008, *Information technology – Abstract Syntax Notation One (ASN.1): Information object specification*.
- Recommendation ITU-T X.682 (2008) | ISO/IEC 8824-3:2008, *Information technology – Abstract Syntax Notation One (ASN.1): Constraint specification*.
- Recommendation ITU-T X.683 (2008) | ISO/IEC 8824-4:2008, *Information technology – Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications*.
- Recommendation ITU-T X.690 (2008) | ISO/IEC 8825-1:2008, *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.691 (2008) | ISO/IEC 8825-2:2008, *Information technology – ASN.1 encoding rules: Specification of Packed Encoding Rules (PER)*.
- 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 CCITT 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 1035 (1987), *Domain names – implementation and specification*.

– 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 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*.