INTERNATIONAL STANDARD

ISO/IEC 9594-8

Information technology — Open systems interconnection —

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

COPYRIGHT PROTECTED DOCUMENT

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.

iTeh STANDARD PREVIEW

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.

ISO/IEC 9594-8:2020
https://standards.iteh.ai/catalog/standards/sist/22f04b84-a5ca-41ae-ac62-

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

CONTENTS

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.

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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*.

– 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*.

– 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.

3.5.2   attribute authority certificate: An attribute certificate for one attribute authority (AA) issued by another AA or by the same AA.

3.5.3   attribute certificate: A data structure, digitally signed by an attribute authority that binds some attribute values with identification information about its holder.

3.5.4   attribute authority (AA): An authority which assigns privileges by issuing attribute certificates or by including them in public-key certificates.

3.5.5   attribute authority revocation list (AARL): A revocation list containing a list of references to attribute certificates issued to attribute authorities (AAs) that are no longer considered valid by the issuing AA.

3.5.6   attribute certificate revocation list (ACRL): A revocation list containing a list of references to attribute certificates that are no longer considered valid by the issuing attribute authority.

3.5.7   attribute certificate validation: The process of ensuring that an attribute certificate was valid at a given time, including possibly the construction and processing of a delegation path, and ensuring that all attribute certificates in that path were valid (e.g., were not expired or revoked) at that given time.

3.5.8   authority: An entity, responsible for the issuance of certificates or of revocation lists. Four types are defined in this Recommendation | International Standard; a certification authority which issues public-key certificates, an attribute authority which issues attribute certificates, a certificate revocation list (CRL) issuer which issues CRLs and an attribute certificate revocation list (ACRL) issuer which issues ACRLs.

3.5.9   authorization and validation list (AVL): A signed list containing information to an AVL entity about potential communications entities and possible restrictions on the communications with such entities.

3.5.10   authorization and validation list entity (AVL entity): An entity, when acting as a relying party, is dependent on an AVL issued by a designated authorizer.

3.5.11   authorizer: An entity trusted by one or more entities operating as authorization and validation list (AVL) entities to create, maintain and sign authorization and validation lists.

3.5.12   base attribute certificate revocation list (base ACRL): An attribute certificate revocation list (ACRL) that is used as the foundation in the generation of a delta attribute certificate revocation list (dACRL).

3.5.13   base certificate revocation list (base CRL): A certificate revocation list (CRL) that is used as the foundation in the generation of a delta certificate revocation list (dCRL).

3.5.14   CA certificate: A public-key certificate for one certification authority (CA) issued by another CA or by the same CA.

3.5.15   certificate policy: A named set of rules that indicates the applicability of a public-key certificate to a particular community and/or class of application with common security requirements. For example, a particular certificate policy might indicate applicability of a type of certificate to the authentication of electronic data interchange transactions for the trading of goods within a given price range.

3.5.16   certification practice statement (CPS): A statement of the practices that a certification authority (CA) employs in issuing certificates.

3.5.17   certificate revocation list (CRL): A signed list indicating a set of public-key certificates that are no longer considered valid by the issuing certification authority (CA). In addition to the generic term certificate revocation list (CRL), some specific CRL types are defined for CRLs that cover particular scopes.

3.5.18   certificate serial number: An integer value, unique within the issuing authority, which is unambiguously associated with a certificate issued by that authority.

3.5.19   certification authority (CA): An authority trusted by one or more entities to create and digital sign public-key certificates. Optionally the certification authority may create the subjects' keys.

3.5.20   certification authority revocation list (CARL): A revocation list containing a list of certification authority (CA) certificates issued to CAs that are no longer considered valid by the issuing CA.

3.5.21   certification path: An ordered list of one or more public-key certificates, starting with a public-key certificate signed by the trust anchor, and ending with the end-entity public-key certificate to be validated. All intermediate public-key certificates, if any, are certification authority (CA) certificates in which the subject of the preceding public-key certificate is the issuer of the following public-key certificate.

3.5.22   CRL distribution point: A directory entry or other distribution source for certificate revocation lists (CRLs); a CRL distributed through a CRL distribution point may contain revocation entries for only a subset of the full set of public-key certificates issued by one certification authority (CA) or may contain revocation entries for multiple CAs.

3.3.23 **cross-certificate**: A certification authority (CA) certificate where the issuer and the subject are different CAs. CAs issue cross-certificates to other CAs as a mechanism to authorize the subject CA's existence.

3.5.24 **delegation**: Conveyance of privilege from one entity that holds such privilege, to another entity.

3.5.25 **delegation path**: An ordered sequence of attribute certificates which, together with authentication of a privilege asserter's identity can be processed to verify the authenticity of a privilege asserter's privilege.

3.5.26 **delta attribute certificate revocation list (dACRL)**: A partial attribute certificate revocation list that only contains entries for attribute certificates that have had their revocation status changed since the issuance of the referenced base attribute certificate revocation list (base ACRL).

3.4.27 **delta-CRL (dCRL)**: A partial revocation list that only contains entries for public-key certificates that have had their revocation status changed since the issuance of the referenced base CRL.

3.5.28 **end entity**: Either a public-key certificate subject that uses its private key for purposes other than signing public-key certificates, or an attribute certificate holder that cannot delegate privileges of the attribute certificate, but uses its attributes only to gain access to a resource.

3.5.29 **end-entity attribute certificate**: An attribute certificate issued to an entity, which then acts as an end entity within a privilege management infrastructure.

3.5.30 **end-entity attribute certificate revocation list (EARL)**: A revocation list containing a list of attribute certificates issued to holders that are not also attribute authorities (AAs) that are no longer considered valid by the certificate issuer.

3.5.31 **end-entity public-key certificate**: A public-key certificate issued to an entity, which then acts as an end entity within a public-key infrastructure.

3.5.32 **end-entity public-key certificate revocation list (EPRL)**: A revocation list containing a list of public-key certificates issued to subjects that are not also certification authorities (CAs), that are no longer considered valid by the certificate issuer.

3.5.33 **environmental variables**: Those aspects of policy required for an authorization decision, that are not contained within static structures, but are available through some local means to a privilege verifier (e.g., time of day or current account balance).

3.5.34 **full attribute certificate revocation list (full ACRL)**: A complete revocation list that contains entries for all attribute certificates that have been revoked for a given scope.

3.5.35 **full CRL**: A complete revocation list that contains entries for all public-key certificates that have been revoked for the given scope.

3.5.36 **hash function**: A (mathematical) function which maps data of arbitrary size into data of a fixed size called a digest.

3.5.37 **holder**: An entity to whom some privilege has been delegated either directly from the source of authority or indirectly through another attribute authority.

3.5.38 **indirect attribute certificate revocation list (iACRL)**: A revocation list whose scope includes attribute certificates issued by one or more attribute authorities (AAs) other than the issuer of the revocation list. The same indirect ACRL is also authoritative for the attribute certificates, if any, issued by the ACRL issuer.

3.5.39 **indirect certificate revocation list (iCRL)**: A revocation list whose scope includes public-key certificates issued by one or more certification authorities (CAs) other than the issuer of the revocation list. The same indirect certificate revocation list (CRL) is also authoritative for the public-key certificates, if any, issued by the CRL issuer.

3.5.40 **intermediate CA**: A certification authority (CA) is acting as an intermediate CA within a certification path when it is the issuer of the next public-key certificate on that certification path.

3.5.41 **key agreement**: A method for negotiating a symmetric key value on-line without transferring the key, even in an encrypted form, e.g., the Diffie-Hellman technique (see ISO/IEC 11770-1 for more information on key agreement mechanisms).

3.5.42 **multiple cryptographic algorithms public-key certificate**: Public-key certificate that for migration purposes includes extensions for an alternative public-key algorithm, an alternative digital signature algorithm and an alternative digital signature.

3.5.43 **object method**: An action that can be invoked on a resource (e.g., a file system may have read, write and execute object methods).