
**Information technology — Open Systems
Interconnection — The Directory —**

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

iTeh STANDARD PREVIEW
*Technologies de l'information — Interconnexion de systèmes ouverts
(OSI) — L'annuaire*
(standards.iteh.ai)
Partie 8: Cadre général des certificats de clé publique et d'attribut

ISO/IEC 9594-8:2014

<https://standards.iteh.ai/catalog/standards/sist/e3aeb7a-a7e8-468c-90cc-0b803a81599b/iso-iec-9594-8-2014>

iTeh STANDARD PREVIEW (standards.iteh.ai)

[ISO/IEC 9594-8:2014](https://standards.iteh.ai/catalog/standards/sist/e3aeb7a-a7e8-468c-90cc-0b803a81599b/iso-iec-9594-8-2014)

<https://standards.iteh.ai/catalog/standards/sist/e3aeb7a-a7e8-468c-90cc-0b803a81599b/iso-iec-9594-8-2014>



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2014

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
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*

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[ISO/IEC 9594-8:2014](#)

<https://standards.iteh.ai/catalog/standards/sist/e3aeb7a-a7e8-468c-90cc-0b803a81599b/iso-iec-9594-8-2014>

CONTENTS

| | <i>Page</i> |
|------|--|
| 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 ISO/IEC 9594-8:2014 15 |
| 7.6 | Entity relationship..... standards.iteh.ai/catalog/standards/sist/e3aeb7a-a7e8-468c-90cc-0b803a81599b/iso-iec-9594-8-2014 16 |
| 7.7 | Certification path..... 0b803a81599b/iso-iec-9594-8-2014 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 |

| | | |
|----|--|-----|
| 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 |

| | <i>Page</i> |
|--|-------------|
| 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 |

iTeh STANDARD PREVIEW (standards.iteh.ai)

[ISO/IEC 9594-8:2014](https://standards.iteh.ai/catalog/standards/sist/e3aeb7a-a7e8-468c-90cc-0b803a81599b/iso-iec-9594-8-2014)

<https://standards.iteh.ai/catalog/standards/sist/e3aeb7a-a7e8-468c-90cc-0b803a81599b/iso-iec-9594-8-2014>

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.

iTeh STANDARD PREVIEW (standards.iteh.ai)

[ISO/IEC 9594-8:2014](https://standards.iteh.ai/catalog/standards/sist/e3aebc7a-a7e8-468c-90cc-0b803a81599b/iso-iec-9594-8-2014)

<https://standards.iteh.ai/catalog/standards/sist/e3aebc7a-a7e8-468c-90cc-0b803a81599b/iso-iec-9594-8-2014>

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[ISO/IEC 9594-8:2014](#)

<https://standards.iteh.ai/catalog/standards/sist/e3aeb7a-a7e8-468c-90cc-0b803a81599b/iso-iec-9594-8-2014>

**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*.

iTeh STANDARD PREVIEW

3 Definitions

(standards.iteh.ai)

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 CCITT Rec. X.800 | ISO 7498-2:

- asymmetric (encipherment);
- authentication exchange;
- authentication information;
- confidentiality;
- credentials;
- cryptography;
- data origin authentication;
- decipherment;
- digital signature;
- encipherment;
- key;
- password;
- peer-entity authentication;
- symmetric (encipherment).

3.2 Baseline identity management terms and definitions

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

- trust: The firm belief in the reliability and truth of information or in the ability and disposition of an entity to act appropriately, within a specified context.

3.3 Directory model definitions

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

- a) attribute;
- b) Directory Information Base;
- c) Directory Information Tree;
- d) Directory System Agent;
- e) Directory User Agent;
- f) distinguished name;
- g) entry;
- h) object;
- i) 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 attribute certificate (AC):** A data structure, digitally signed by an Attribute Authority, that binds some attribute values with identification information about its holder.
- 3.5.2 Attribute Authority (AA):** An authority which assigns privileges by issuing attribute certificates.
- 3.5.3 attribute authority revocation list (AARL):** A revocation list containing a list of references to attribute certificates issued to AAs that are no longer considered valid by the issuing authority.
- 3.5.4 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 authority.
- 3.5.5 authentication token; (token):** Information conveyed during a strong authentication exchange, which can be used to authenticate its sender.
- 3.5.6 authority:** An entity, responsible for the issuance of certificates. Two types are defined in this Recommendation | International Standard; a certification authority which issues public-key certificates and an attribute authority which issues attribute certificates.
- 3.5.7 authority certificate:** A certificate issued to an authority (e.g., either to a certification authority or to an attribute authority).
- 3.5.8 base CRL:** A CRL that is used as the foundation in the generation of a dCRL.
- 3.5.9 CA-certificate:** A public-key certificate for one CA issued by either another CA or by the same CA.
- 3.5.10 certificate policy:** A named set of rules that indicate the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular certificate policy might indicate the applicability of a type of certificate to the authentication of electronic data interchange transactions for the trading of goods within a given price range.
- 3.5.11 certification practice statement (CPS):** A statement of the practices that a CA employs in issuing certificates.
- 3.5.12 certificate revocation list (CRL):** A signed list indicating a set of certificates that are no longer considered valid by the certificate issuer. In addition to the generic term CRL, some specific CRL types are defined for CRLs that cover particular scopes.
- 3.5.13 certificate serial number:** An integer value, unique within the issuing authority, which is unambiguously associated with a certificate issued by that authority.
- 3.5.14 certificate-using system:** An implementation of those functions defined in this Recommendation | International Standard that are used by a relying party.

- 3.5.15 certificate validation:** The process of ensuring that a certificate was valid at a given time, including possibly the construction and processing of a certification path, and ensuring that all certificates in that path were valid (i.e., were not expired or revoked) at that given time.
- 3.5.16 certification authority (CA):** An authority trusted by one or more users to create and assign public-key certificates. Optionally the certification authority may create the subjects' keys.
- 3.5.17 certification authority revocation list (CARL):** A revocation list containing a list of CA-certificates issued to certification authorities that are no longer considered valid by the certificate issuer.
- 3.5.18 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 public key certificate to be validated. All intermediate public-key certificates, if any, are CA-certificates in which the subject of the preceding certificate is the issuer of the following certificate.
- 3.5.19 CRL distribution point:** A directory entry or other distribution source for CRLs; a CRL distributed through a CRL distribution point may contain revocation entries for only a subset of the full set of certificates issued by one CA or may contain revocation entries for multiple CAs.
- 3.5.20 cross-certificate:** A public-key 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.
- 3.5.21 cryptographic system, cryptosystem:** A collection of transformations from plain text into cipher text and vice versa, the particular transformation(s) to be used being selected by keys. The transformations are normally defined by a mathematical algorithm.
- 3.5.22 data confidentiality:** This service can be used to provide the protection of data from unauthorized disclosure. The data confidentiality service is supported by the authentication framework. It can be used to protect against data interception.
- 3.5.23 delegation:** Conveyance of privilege from one entity that holds such privilege, to another entity.
- 3.5.24 delegation path:** An ordered sequence of certificates which together with the authentication of a privilege asserter's identity, can be processed to verify the authenticity of an asserter's privilege.
- 3.5.25 delta-CRL (dCRL):** A partial revocation list that only contains entries for certificates that have had their revocation status changed since the issuance of the referenced base CRL.
- 3.5.26 end-entity:** Either a public-key certificate subject that uses its private key for purposes other than signing certificates, or an attribute certificate holder that uses its attributes to gain access to a resource.
- 3.5.27 end-entity attribute certificate:** An attribute certificate issued to an end-entity.
- 3.5.28 end-entity attribute certificate revocation list (EARL):** A revocation list containing a list of end-entity attribute certificates that are no longer considered valid by the issuing attribute authority.
- 3.5.29 end-entity certificate:** An attribute or public-key certificate issued to an end-entity.
- 3.5.30 end-entity public-key certificate:** A public-key certificate issued to an end-entity.
- 3.5.31 end-entity public-key certificate revocation list (EPRL):** A revocation list containing a list of end-entity public-key certificates that are no longer considered valid by the issuing certification authority.
- 3.5.32 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).
- 3.5.33 full CRL:** A complete revocation list that contains entries for all certificates that have been revoked for the given scope.
- 3.5.34 hash function:** A (mathematical) function which maps values from a large (possibly very large) domain into a smaller range. A "good" hash function is such that the results of applying the function to a (large) set of values in the domain will be evenly distributed (and apparently at random) over the range.
- 3.5.35 holder:** An entity to whom some privilege has been delegated either directly from the Source of Authority or indirectly through another Attribute Authority.
- 3.5.36 indirect CRL (iCRL):** A revocation list that contains at least revocation information about certificates issued by authorities other than that which issued this CRL.