

# DRAFT INTERNATIONAL STANDARD

## ISO/IEC DIS 9594-8

ISO/IEC JTC 1/SC 6

Secretariat: **KATS**

Voting begins on:  
**2020-03-30**

Voting terminates on:  
**2020-06-22**

---

### Information technology — Open systems interconnection —

Part 8:

### The Directory: Public-key and attribute certificate frameworks

ICS: 35.100.70

**iTeh STANDARD PREVIEW**  
(standards.iteh.ai)  
Full standard:  
<https://standards.iteh.ai/catalog/standards/sist/22f04b84-a5ca-41ae-ac62-2d2c137de238/iso-iec-dis-9594-8>

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

This document is circulated as received from the committee secretariat.



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

© ISO/IEC 2020

**iTeh STANDARD PREVIEW**  
(standards.iteh.ai)  
Full standard:  
<https://standards.iteh.ai/catalog/standards/sist/22f04b84-a5ca-41ae-ac62-2d2c137de238/iso-iec-dis-9594-8>



**COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2020

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

ISO copyright office  
CP 401 • Ch. de Blandonnet 8  
CH-1214 Vernier, Geneva  
Phone: +41 22 749 01 11  
Fax: +41 22 749 09 47  
Email: [copyright@iso.org](mailto:copyright@iso.org)  
Website: [www.iso.org](http://www.iso.org)

Published in Switzerland

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

**Summary**

Recommendation ITU-T X.509 | ISO/IEC 9594-8 defines frameworks for public-key infrastructure (PKI) and privilege management infrastructure (PMI). It introduces the basic concept of asymmetric cryptographic techniques. It specifies the following data types: public-key certificate, attribute certificate, certificate revocation list (CRL) and attribute certificate revocation list (ACRL). It also defines several certificates and CRL extensions, and it defines directory schema information allowing PKI and PMI related data to be stored in a directory. In addition, it defines entity types, such as certification authority (CA), attribute authority (AA), relying party, privilege verifier, trust broker and trust anchor. It specifies the principles for certificate validation, validation path, certificate policy, etc. It also includes a specification for authorization validation lists that allow for fast validation and restrictions on communications.

**History**

| Edition | Recommendation                      | Approval   | Study Group | Unique ID*                                                                                                     |
|---------|-------------------------------------|------------|-------------|----------------------------------------------------------------------------------------------------------------|
| 1.0     | ITU-T X.509                         | 1988-11-25 |             | <a href="https://standards.iso.org/standards/catalog/standards/sist/11.1002/1000/2999">11.1002/1000/2999</a>   |
| 2.0     | ITU-T X.509                         | 1993-11-16 | 7           | <a href="https://standards.iso.org/standards/catalog/standards/sist/11.1002/1000/3000">11.1002/1000/3000</a>   |
| 3.0     | ITU-T X.509                         | 1997-08-09 | 7           | <a href="https://standards.iso.org/standards/catalog/standards/sist/11.1002/1000/4123">11.1002/1000/4123</a>   |
| 3.1     | ITU-T X.509 (1997) Technical Cor. 1 | 2000-03-31 | 7           | <a href="https://standards.iso.org/standards/catalog/standards/sist/11.1002/1000/5033">11.1002/1000/5033</a>   |
| 3.2     | ITU-T X.509 (1997) Technical Cor. 2 | 2001-02-02 | 7           | <a href="https://standards.iso.org/standards/catalog/standards/sist/11.1002/1000/5311">11.1002/1000/5311</a>   |
| 3.3     | ITU-T X.509 (1997) Technical Cor. 3 | 2001-10-29 | 7           | <a href="https://standards.iso.org/standards/catalog/standards/sist/11.1002/1000/5559">11.1002/1000/5559</a>   |
| 3.4     | ITU-T X.509 (1997) Technical Cor. 4 | 2002-04-13 | 17          | <a href="https://standards.iso.org/standards/catalog/standards/sist/11.1002/1000/6025">11.1002/1000/6025</a>   |
| 3.5     | ITU-T X.509 (1997) Technical Cor. 5 | 2003-02-13 | 17          | <a href="https://standards.iso.org/standards/catalog/standards/sist/11.1002/1000/6236">11.1002/1000/6236</a>   |
| 3.6     | ITU-T X.509 (1997) Technical Cor. 6 | 2004-04-29 | 17          | <a href="https://standards.iso.org/standards/catalog/standards/sist/11.1002/1000/7285">11.1002/1000/7285</a>   |
| 4.0     | ITU-T X.509                         | 2000-03-31 | 7           | <a href="https://standards.iso.org/standards/catalog/standards/sist/11.1002/1000/5034">11.1002/1000/5034</a>   |
| 4.1     | ITU-T X.509 (2000) Technical Cor. 1 | 2001-10-29 | 7           | <a href="https://standards.iso.org/standards/catalog/standards/sist/11.1002/1000/5560">11.1002/1000/5560</a>   |
| 4.2     | ITU-T X.509 (2000) Technical Cor. 2 | 2002-04-13 | 17          | <a href="https://standards.iso.org/standards/catalog/standards/sist/11.1002/1000/6026">11.1002/1000/6026</a>   |
| 4.3     | ITU-T X.509 (2000) Technical Cor. 3 | 2004-04-29 | 17          | <a href="https://standards.iso.org/standards/catalog/standards/sist/11.1002/1000/7284">11.1002/1000/7284</a>   |
| 4.4     | ITU-T X.509 (2000) Technical Cor. 4 | 2007-01-13 | 17          | <a href="https://standards.iso.org/standards/catalog/standards/sist/11.1002/1000/8637">11.1002/1000/8637</a>   |
| 5.0     | ITU-T X.509                         | 2005-08-29 | 17          | <a href="https://standards.iso.org/standards/catalog/standards/sist/11.1002/1000/8501">11.1002/1000/8501</a>   |
| 5.1     | ITU-T X.509 (2005) Cor. 1           | 2007-01-13 | 17          | <a href="https://standards.iso.org/standards/catalog/standards/sist/11.1002/1000/9051">11.1002/1000/9051</a>   |
| 5.2     | ITU-T X.509 (2005) Cor. 2           | 2008-11-13 | 17          | <a href="https://standards.iso.org/standards/catalog/standards/sist/11.1002/1000/9591">11.1002/1000/9591</a>   |
| 5.3     | ITU-T X.509 (2005) Cor. 3           | 2011-02-13 | 17          | <a href="https://standards.iso.org/standards/catalog/standards/sist/11.1002/1000/11042">11.1002/1000/11042</a> |
| 5.4     | ITU-T X.509 (2005) Cor. 4           | 2012-04-13 | 17          | <a href="https://standards.iso.org/standards/catalog/standards/sist/11.1002/1000/11577">11.1002/1000/11577</a> |
| 6.0     | ITU-T X.509                         | 2008-11-13 | 17          | <a href="https://standards.iso.org/standards/catalog/standards/sist/11.1002/1000/9590">11.1002/1000/9590</a>   |
| 6.1     | ITU-T X.509 (2008) Cor. 1           | 2011-02-13 | 17          | <a href="https://standards.iso.org/standards/catalog/standards/sist/11.1002/1000/11043">11.1002/1000/11043</a> |
| 6.2     | ITU-T X.509 (2008) Cor. 2           | 2012-04-13 | 17          | <a href="https://standards.iso.org/standards/catalog/standards/sist/11.1002/1000/11578">11.1002/1000/11578</a> |
| 6.3     | ITU-T X.509 (2008) Cor. 3           | 2012-10-14 | 17          | <a href="https://standards.iso.org/standards/catalog/standards/sist/11.1002/1000/11736">11.1002/1000/11736</a> |
| 7.0     | ITU-T X.509                         | 2012-10-14 | 17          | <a href="https://standards.iso.org/standards/catalog/standards/sist/11.1002/1000/11735">11.1002/1000/11735</a> |
| 7.1     | ITU-T X.509 (2012) Cor. 1           | 2015-05-29 | 17          | <a href="https://standards.iso.org/standards/catalog/standards/sist/11.1002/1000/12474">11.1002/1000/12474</a> |
| 7.2     | ITU-T X.509 (2012) Cor. 2           | 2016-04-29 | 17          | <a href="https://standards.iso.org/standards/catalog/standards/sist/11.1002/1000/12844">11.1002/1000/12844</a> |
| 7.3     | ITU-T X.509 (2012) Cor. 3           | 2016-10-14 | 17          | <a href="https://standards.iso.org/standards/catalog/standards/sist/11.1002/1000/13032">11.1002/1000/13032</a> |
| 8.0     | ITU-T X.509                         | 2016-10-14 | 17          | <a href="https://standards.iso.org/standards/catalog/standards/sist/11.1002/1000/13031">11.1002/1000/13031</a> |
| 9.0     | ITU-T X.509                         | 2019-10-14 | 17          | <a href="https://standards.iso.org/standards/catalog/standards/sist/11.1002/1000/14033">11.1002/1000/14033</a> |

**Keywords**

Attribute, attribute authority, certificate, certification authority, distinguished name, PKI, PMI, trust anchor, validation.

\* To access the Recommendation, type the URL <http://handle.itu.int/> in the address field of your web browser, followed by the Recommendation's unique ID. For example, <http://handle.itu.int/11.1002/1000/11830-en>.

## FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

## NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

## INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at <http://www.itu.int/ITU-T/ipr/>.

© ITU 2019

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

## CONTENTS

|                                                                                           | <i>Page</i> |
|-------------------------------------------------------------------------------------------|-------------|
| SECTION 1 – General .....                                                                 | 1           |
| 1 Scope .....                                                                             | 1           |
| 2 Normative references.....                                                               | 1           |
| 2.1 Identical Recommendations   International Standards .....                             | 1           |
| 2.2 Paired Recommendations   International Standards equivalent in technical content..... | 2           |
| 2.3 Recommendations .....                                                                 | 2           |
| 2.4 Other references .....                                                                | 2           |
| 3 Definitions .....                                                                       | 3           |
| 3.1 OSI Reference Model security architecture definitions.....                            | 3           |
| 3.2 Baseline identity management terms and definitions .....                              | 3           |
| 3.3 Directory model definitions .....                                                     | 3           |
| 3.4 Access control framework definitions.....                                             | 3           |
| 3.5 Public-key and attribute certificate definitions.....                                 | 3           |
| 4 Abbreviations .....                                                                     | 7           |
| 5 Conventions.....                                                                        | 8           |
| 6 Frameworks overview .....                                                               | 8           |
| 6.1 Digital signatures .....                                                              | 9           |
| 6.2 Public-key cryptography and cryptographic algorithms.....                             | 10          |
| 6.3 Distinguished encoding of basic encoding rules.....                                   | 12          |
| 6.4 Applying distinguished encoding.....                                                  | 12          |
| 6.5 Using repositories.....                                                               | 13          |
| SECTION 2 – PUBLIC-KEY CERTIFICATE FRAMEWORK.....                                         | 14          |
| 7 Public keys and public-key certificates .....                                           | 14          |
| 7.1 Introduction .....                                                                    | 14          |
| 7.2 Public-key certificate.....                                                           | 14          |
| 7.3 Public-key certificate extensions.....                                                | 17          |
| 7.4 Types of public-key certificates .....                                                | 18          |
| 7.5 Trust anchor .....                                                                    | 18          |
| 7.6 Entity relationship .....                                                             | 19          |
| 7.7 Certification path.....                                                               | 19          |
| 7.8 Generation of key pairs .....                                                         | 21          |
| 7.9 Public-key certificate creation.....                                                  | 21          |
| 7.10 Certificate revocation list .....                                                    | 22          |
| 7.11 Uniqueness of names.....                                                             | 25          |
| 7.12 Indirect CRLs .....                                                                  | 25          |
| 7.13 Repudiation of a digital signing .....                                               | 26          |
| 8 Trust models .....                                                                      | 27          |
| 8.1 Three-cornered trust model .....                                                      | 27          |
| 8.2 Four cornered trust model .....                                                       | 27          |
| 9 Public-key certificate and CRL extensions.....                                          | 28          |
| 9.1 Policy handling.....                                                                  | 29          |
| 9.2 Key and policy information extensions .....                                           | 31          |
| 9.3 Subject and issuer information extensions .....                                       | 38          |
| 9.4 Certification path constraint extensions .....                                        | 41          |
| 9.5 Basic CRL extensions .....                                                            | 45          |
| 9.6 CRL distribution points and delta CRL extensions .....                                | 52          |
| 9.7 Authorization and validation list extensions .....                                    | 57          |
| 9.8 Alternative cryptographic algorithms and digital signature extensions.....            | 58          |
| 10 Delta CRL relationship to base.....                                                    | 59          |
| 11 Authorization and validation lists.....                                                | 60          |
| 11.1 Authorization and validation list concept.....                                       | 60          |

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

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

## Introduction

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

## ISO/IEC DIS 9594-8:2020(E)

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)  
Full standard:  
<https://standards.iteh.ai/catalog/standards/sist/22f04b84-a5ca-41ae-ac62-2d2c137de238/iso-iec-dis-9594-8>

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

Full standard:  
<https://standards.iteh.ai/catalog/standards/sist/22f04b84-a5ca-41ae-ac62-2d2c137de238/iso-iec-dis-9594-8>

**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 lists** (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.