International Standard

ISO/IEC 9594-12

Information technology — Open systems interconnection —

Part 12:

The Directory: Key management and public-key infrastructure establishment and maintenance

First edition
2025-05

Reference number
ISO/IEC 9594-12:2025(en)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: 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.

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.

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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

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. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by ITU-T as ITU-T X.508 (10/2024) 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*.

A list of all parts in the ISO/IEC 9594 series can be found on the ISO and IEC websites.

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 and www.iec.ch/national-committees.

INTERNATIONAL STANDARD ISO/IEC 9594-12
RECOMMENDATION ITU-T X.508

Information technology – Open Systems Interconnection – The Directory: Key management and public-key infrastructure establishment and maintenance

Summary

Recommendation ITU-T X.508 | ISO/IEC 9594-12 is intended to fill the gap between Recommendation ITU-T X.509 | ISO/IEC 9594-8 and Recommendation ITU-T X.510 | ISO/IEC 9594-11 by giving a description of selected cryptographic algorithms with references to more detailed specifications. To establish the theory behind the cryptographic algorithm, an informative annex gives in introduction to the supporting mathematics. Also, some considerations on migration to post quantum algorithm are included.

Section 3 provides a best practice guideline for establishing and maintaining a public-key infrastructure (PKI) with emphasis on environments outside the traditional PKI environments, such as guidance for establishing a PKI for networks of Internet of things (IoT) and smart grid.

History [*]

Edition	Recommendation	Approval	Study Group	Unique ID
1.0	ITU-T X.508	2024-10-29	17	11.1002/1000/16196

Keywords

Authenticated encryption, authentication, block cipher, confidentiality, cryptography, encryption, information security, mode of operation.

[*] To access the Recommendation, type the URL https://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, and 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 not received notice of intellectual property, protected by patents/software copyrights, 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 appropriate ITU-T databases available via the ITU-T website at https://www.itu.int/ITU-T/ipr/.

CONTENTS

Page

1 Scope 1

2 Normative references 1
- 2.1 Identical Recommendations | International Standards 1
- 2.2 Paired Recommendations | International Standards equivalent in technical content 1
- 2.3 Recommendations 2
- 2.4 International Standards 2
- 2.4 Additional references 2

3 Definitions 2
- 3.1 Terms defined elsewhere 2
- 3.2 Terms defined in this Recommendation | International Standard 3

4 Abbreviations 4

5 Conventions 6

6 Cybersecurity considerations for communication networks 6
- 6.1 The challenge of large information and communication technology (ICT) networks 6
- 6.2 Connection-mode communication 7
  - 6.2.1 General 7
  - 6.2.2 Association establishment phase 8
  - 6.2.3 Data transfer phase 8
  - 6.2.4 Association termination phase 8
- 6.3 Security services 8

7 Overview of cryptographic algorithms 10
- 7.1 Introduction 10
- 7.2 Formal specification of cryptographic algorithms 10
- 7.3 Security properties of crypto graphic algorithms 11
- 7.4 Security strength 11
- 7.5 One-way functions 12
- 7.6 Random number generation and entropy 12

8 Symmetric-key algorithms 13
- 8.1 General 13
- 8.2 Symmetric key encryption 13
- 8.3 Authenticated encryption with associated data (AEAD) 13
- 8.4 Symmetric key requirements 14

9 Hash algorithms 14

10 Public key and asymmetric cipher 15
- 10.1 Public-key cryptography 15
- 10.2 Asymmetric cipher 15

11 Public key and digital signature algorithms 16
- 11.1 General 16

12 Key establishment algorithms 17

13 Integrity check value (ICV) algorithms 17

14 Post-quantum cryptography considerations 17
- 14.1 General considerations 17
- 14.2 Crypto agility 18
- 14.3 Quantum computers and cryptographic algorithm migration 18
- 14.4 Possible attacks by use of quantum computers 18
  - 14.4.1 Symmetric cryptographic algorithms 18
  - 14.4.2 Asymmetric cryptographic algorithms 18
- 14.5 Mathematic behind post-quantum cryptography 19

15 Hardware security modules 19

16 Public-key infrastructure establishment 21

17 Public-key certificates ... 21
17.1 General ... 21
17.2 The identity and role of the certification authority ... 21
17.3 Distinguished name considerations ... 21
17.4 Content of the basic structure of a public-key certificate ... 22
17.4.1 General ... 22
17.4.2 Version component ... 23
17.4.3 Serial number component ... 23
17.4.4 Signature component ... 23
17.4.5 Issuer component ... 23
17.4.6 Validity component ... 23
17.4.7 Subject component ... 24
17.4.8 Subject public-key information ... 24
17.4.9 Issuer unique ID and subject unique ID ... 25
17.5 Extensions for public-key certificates ... 25
17.5.1 Some considerations on extensions to public-key certificates and other data types ... 25
17.5.2 Basic constraints extension ... 25
17.5.3 Key usage extension ... 25
17.5.4 Subject alternative name extension ... 26
17.5.5 Authority information access extension ... 26
17.5.6 Authority key identifier extension ... 26
17.5.7 Subject key identifier extension ... 26
17.5.8 No revocation information available extension ... 26
17.5.9 Subject alternative public-key info extension ... 26
17.5.10 Alternative signature algorithm extension ... 27
17.5.11 Alternative signature value extension ... 27
17.5.12 Subject directory attribute extension type ... 27
17.7 Chaining of public-key certificates ... 27
17.7.1 Name chaining ... 27
17.7.2 Key identifier chaining ... 28
18 Certificate life-cycle management ... 29
18.1 General ... 29
18.2 Validity of certificates to be installed or reviewed ... 29
18.3 Local policy with respect to invalid certificates ... 29
19 Machine identity and machine-to-machine communication ... 30
20 Trust establishment ... 30
20.1 General ... 30
20.2 Single public-key infrastructure domain ... 30
20.3 Trust establishment between two public-key infrastructure domains ... 31
20.4 A worldwide federated public-key infrastructure ... 32
20.5 Trust anchor compromise ... 32
21 PKI configurations ... 33
21.1 Introduction ... 33
21.2 Public-key infrastructure (PKI) components ... 33
22 PKI establishment ... 34
22.1 Human resources ... 34
22.1.1 Public-key infrastructure knowledge ... 34
22.1.2 Cryptographic algorithm knowledge ... 34
22.2 IETF public-key infrastructure specifications ... 34
22.2.1 Enrolment over Secure Transport (EST) ... 34
22.2.2 Internet X.509 PKI Certificate Management Protocol (CMP) ... 34
22.2.3 Certificate Management over CMS (CMC) ... 35
23 Revocation of public-key certificates ... 35
23.1 Certificate revocation lists (CRLs) ... 35
23.2 Online certificate status protocol (OCSP) ... 35
Annex A Cryptographic primitives ... 36
A.1 Block cipher algorithms ... 36
A.1.1 Block cipher functions and block cipher operation modes ... 36

A.1.2 Feistel cipher structure 36
A.1.3 Advanced encryption standard 38
A.1.4 ShāngMi 4 (SM4) block cipher algorithm 43
A.1.5 Operation modes for block cipher symmetric-key algorithms 46
A.2 Authenticated encryption with associated data (AEAD) algorithms 51
A.2.1 General 51
A.2.2 Galois/counter mode (GCM) 51
A.2.3 Counter with CBC-MAC (CCM) 53
A.3 Cryptographic hash algorithms 55
A.3.1 General 55
A.3.2 Merkle-Damgaard construction 56
A.3.3 The SHA-2 series of hash algorithms 58
A.3.4 The Keccak (sponge) algorithms 59
A.3.5 SHA-3 series of hash algorithms 61
A.3.6 ShāngMi 3 (SM3) hash algorithm 62
A.4 The RSA crypto system 63
A.4.1 General about the RSA crypto system 63
A.4.2 Key generation 63
A.4.3 Security considerations 64
A.5 Asymmetric encryption 64
A.5.1 General 64
A.5.2 RSA asymmetric cipher 64
A.6 Public-key algorithms including digital signature algorithms 65
A.6.1 General 65
A.6.2 The RSA digital signature system 66
A.6.3 The DSA public-key algorithm 67
A.6.4 The elliptic curve digital signature algorithms (ECDSA) 67
A.6.5 SM2 algorithm 70
A.6.6 The Edwards-curve digital signature algorithms 70
A.7 Key establishment algorithms 72
A.7.1 Introduction 72
A.7.2 RSA symmetric key encapsulation 73
A.7.3 The Diffie-Hellman key agreement method 73
A.7.4 Key derivation function 75
A.8 Integrity check value (ICV) algorithms 76
A.8.1 Introduction 76
A.8.2 Keyed-hash message authentication code (HMAC) 76
A.8.3 Cipher-based message authentication code (CMAC) 76
A.8.4 Keccak message authentication code (KMAC) 77
A.8.5 Galois message authentication code (GMAC) algorithm 78

Annex B Basic mathematic concepts for cryptographic algorithms 80
B.1 Introduction to basic mathematic 80
B.1.1 Scope of annex 80
B.1.2 The prime number, the semiprime and the coprime number concepts 80
B.1.3 Greatest common divisor 80
B.1.4 The logarithm concept 80
B.1.5 Operations on matrices 80
B.1.6 Least common multiple 81
B.1.7 Bitwise logical operations 81
B.1.8 Bit masking 82
B.2 Modular arithmetic 82
B.3 Group theory 83
B.3.1 Introduction 83
B.3.2 Notation 84
B.3.3 Additive group of integers 84
B.3.4 Multiplicative group of integers 84
B.3.5 Cyclic groups 85
B.3.6 The discrete logarithm problem 85
B.3.7 Generalized discrete logarithm problem 86
B.3.8 Subgroup 86
B.3.9 Order of group and order of element 86

B.3.10 Ways to resolve or attack the discrete logarithm problem ... 86
B.4 Finite fields (Galois field) ... 87
B.4.1 General ... 87
B.4.2 Prime fields ... 87
B.4.3 Binary fields GF(2^m) ... 88
B.5 Overview of Elliptic curve cryptography ... 89
B.5.1 Reasons for using elliptic curve cryptography ... 89
B.5.2 Overview of polynomial forms for defining elliptic curves ... 90
B.5.3 Variants of the Weierstrass form ... 90
B.5.4 The Montgomery form ... 90
B.5.5 The twisted Edwards curves ... 90
B.6 Elliptic curve cryptography for short-Weierstrass form ... 90
B.6.1 Definition of curves based on the Weierstrass form ... 90
B.6.2 Defining group over elliptic curve ... 92
B.7 Montgomery elliptic curve cryptography ... 95
B.7.1 Introduction ... 95
B.7.2 Curve25519 and Ed25519 ... 95
B.7.3 Curve448 and Ed448 ... 95
B.7.4 The Montgomery curves ... 95
B.7.5 The Edwards curves ... 96
B.8 Conversion techniques ... 96
B.8.1 General ... 96
B.8.2 Bit string-to-integer conversion and binary length of integer ... 96
B.8.3 Integer-to-bit string conversion ... 96
B.8.4 Octet string to integer conversion ... 96
B.8.5 Integer-to-octet string conversion ... 96
B.8.6 Bitstring-to-octet string conversion ... 96
B.9 Miscellaneous formulae ... 97
B.9.1 Introductions ... 97
B.9.2 The Euclidean algorithm ... 97
B.9.3 The extended Euclidean algorithm ... 97
B.9.3 Fermat's little theorem ... 98
B.9.4 Lagrange's theorem ... 98
B.9.5 Euler's phi function ... 98
B.10 Endianness (big endian vs. little endian) ... 98
B.11 Selected attacks on cryptographic algorithms ... 98
B.11.1 Side-channel attack ... 98
B.11.2 Square root attack ... 99

Annex C Alphabetical list of cryptographic concepts and definitions ... 100

Bibliography ... 101

INTERNATIONAL STANDARD
ITU-T RECOMMENDATION

Information technology – Open Systems Interconnection – The Directory: Key management and public-key infrastructure establishment and maintenance

SECTION 1 – GENERAL

1 Scope

This Recommendation | International Standard supplements Rec. ITU-T X.509 | ISO/IEC 9594-8 and Rec. ITU-T X.510 | ISO/IEC 9594-11 by providing an extended description of cryptographic algorithms and guidance in establishment and maintenance of a public-key infrastructure (PKI).

It is outside the scope of this Recommendation | International Standard to define new cryptographic algorithms, but it is within scope to discuss already-defined cryptographic algorithms that provide optimal protection, including future protection against attacks using powerful quantum computers.

This Recommendation | International Standard specifies how public-key infrastructure (PKI) may be adapted to support machine-to-machine (M2M) communication, e.g., smart grid and Internet of things (IoT), to allow interworking.

This Recommendation | International Standard specifies the procedures for establishment and maintenance of a PKI supporting new areas, such as intelligent electricity network (smart grid) and industrial Internet of things.

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.501 (2019) | ISO/IEC 9594-2:2020, *Information technology – Open Systems Interconnection – The Directory: Models*.
- Recommendation ITU-T X.509 (2019) | ISO/IEC 9594-8:2020, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.
- Recommendation ITU-T X.510 (2020) | ISO/IEC 9594-11:2020, *Information technology – Open Systems Interconnection – The Directory: Protocol specifications for secure operations*.
- 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.680 (2021) | ISO/IEC 8824-1:2021, *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation*.
- Recommendation ITU-T X.681 (2021) | ISO/IEC 8824-2:2021, *Information technology – Abstract Syntax Notation One (ASN.1): Information object specification*.
- Recommendation ITU-T X.682 (2021) | ISO/IEC 8824-3:2021, *Information technology – Abstract Syntax Notation One (ASN.1): Constraint specification*.
- Recommendation ITU-T X.683 (2021) | ISO/IEC 8824-4:2021, *Information technology – Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications*.

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 (2021), *Baseline identity management terms and definitions*.

2.4 International Standards

- ISO/IEC 9797-2:2021, *Information security – Message authentication codes (MACs) – Part 2: Mechanisms using a dedicated hash-function*.
- ISO/IEC 10116:2017, *Information technology – Security techniques – Modes of operation for a n-bit block cipher*.
- ISO/IEC 10118-3:2018, *IT Security techniques – Hash-functions – Part 3: Dedicated hash-functions*.
- ISO/IEC 11770-6:2016, *Information technology – Security techniques – Key Management – Part 6: Key derivation*.
- ISO/IEC 14888-3:2018, *IT Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms*.
- ISO/IEC 18033-3:2010/Amd.1:2021, *Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers, Amendment 1: SM4*.
- ISO/IEC 19790:2012, *Information technology – Security techniques – Security requirements for cryptographic modules*.

2.4 Additional references

- IETF RFC 4210 (2005), *Internet X.509 Public Key Infrastructure, Certificate Management Protocol (CMP)*.
- IETF RFC 5280 (2008), *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*.
- IETF RFC 5905 (2010), *Network Time Protocol Version 4: Protocol and Algorithms Specification*.
- IETF RFC 6712 (2012), *Internet X.509 Public Key Infrastructure – HTTP Transfer for the Certificate Management Protocol (CMP)*.
- IETF RFC 6960 (2013), *X.509 Internet Public Key Infrastructure – Online Certificate Status Protocol – OCSP*.
- IETF RFC 7030 (2013), *Enrollment over Secure Transport*.
- IETF RFC 8017 (2016), *PKCS #1: RSA Cryptography Specifications Version 2.2*.
- IETF RFC 8032 (2017), *Edwards-Curve Digital Signature Algorithm (EdDSA)*.
- IETF RFC 8446 (2018), *The Transport Layer Security (TLS) Protocol Version 1.3*.
- NIST FIPS 186-5 (2023). *Digital Signature Standard (DSS)*.
- NIST PUB 202 (2015), *Permutation-Based Hash and Extendable-Output Functions*.
- NIST SP 800-38C (2004), *Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality*.
- NIST SP 800-38D (2007), *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC*.
- NIST SP 800-56A, Revision 3 (2018), *Recommendation for Pair-Wise Key, Establishment Schemes Using Discrete Logarithm Cryptography*.
- NIST SP 800-185 (2016), *SHA-3 Derived Functions: cSHAKE, KMAC, TupleHash and ParallelHash*.

3 Definitions

For the purposes of this Recommendation | International Standard, the following definitions apply:

3.1 Terms defined elsewhere

Terms defined in Rec. ITU-T X.800 | ISO 7498-2:

a) asymmetric (encipherment);

b) confidentiality;