International Standard

ISO/IEC 9594-11

Second edition
2025-08

Information technology — Open systems interconnection directory —

Part 11: Protocol specifications for secure operations

Reference number
ISO/IEC 9594-11:2025(en)

© ISO/IEC 2025



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2025

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
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.510 (10/2023) and drafted in accordance with its editorial rules, in collaboration with Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 6, *Telecommunications and information exchange between systems*.

This second edition cancels and replaces the first edition (ISO/IEC 9594-11:2020), which has been technically revised.

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.

© ISO 2025 – All rights reserved

CONTENTS

Page

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 ... 1
2.3 International Standards ... 2
2.4 Other references ... 2

3 Definitions ... 2
3.1 OSI reference model definitions ... 2
3.2 Directory model definitions ... 2
3.3 Public-key and attribute certificate definitions ... 2
3.4 Terms defined in this Recommendation | International Standard ... 3

4 Abbreviations ... 4

5 Conventions ... 5

6 Communication model ... 5

7 Common data types and special cryptographic algorithms ... 5
7.1 Introduction ... 5
7.2 ASN.1 information object class specification tool ... 5
7.3 Parameterized data types ... 7
7.4 Multiple cryptographic algorithm specifications ... 9
7.5 Parameterized data types for providing multiple-cryptographic algorithm-values ... 15
7.6 Formal specification of encipherment ... 16

8 Symmetric-key algorithms ... 17
8.1 Introduction to symmetric-key algorithms ... 17
8.2 Advance encryption standard (AES) – symmetric-key algorithms ... 18
8.3 Camellia symmetric-key algorithms ... 21
8.4 SEED – symmetric-key algorithms ... 24
8.5 SM4 – symmetric-key algorithms ... 26

9 Public-key and digital signature algorithms ... 28

10 Key establishment algorithms ... 28
10.1 General ... 28
10.2 Diffie-Hellman over prime field ... 28
10.3 Elliptic curve Diffie-Hellman ... 30
10.4 Key derivation ... 31

11 General concepts for securing protocols ... 32
11.1 Introduction ... 32
11.2 Protected protocol plug-in concept ... 32
11.3 Communication structure ... 32
11.4 Another view of the relationship between the wrapper protocol and the protected protocol ... 33
11.5 Structure of the application protocol data unit ... 33
11.6 Exception conditions ... 33

SECTION 2 – THE WRAPPER PROTOCOL ... 34

12 Wrapper protocol general concepts ... 34
12.1 Introduction ... 34
12.2 UTC time specification ... 34
12.3 Use of alternative cryptographic algorithms ... 34
12.4 Establishment of symmetric keys ... 34
12.5 Sequence numbers ... 35
12.6 Use of invocation identification in the wrapper protocol ... 35
12.7 Mapping to underlying services ... 35
12.8 Addressing of communicating entities ... 35

© ISO/IEC 2025 – All rights reserved

12.9 Definition of protected protocols ... 35
12.10 Overview of wrapper protocol data units ... 35

13 Association management ... 36
13.1 Introduction to association management ... 36
13.2 Association handshake request ... 36
13.3 Association handshake accept ... 37
13.4 Association reject due to security issues ... 38
13.5 Association reject by the protected protocol ... 39
13.6 Handshake security abort ... 40
13.7 Handshake abort by protected protocol ... 40
13.8 Data transfer security abort ... 41
13.9 Abort by protected protocol ... 41
13.10 Release request WrPDU ... 42
13.11 Release response WrPDU ... 42
13.12 Release collision ... 43

14 Data transfer phase ... 43
14.1 Symmetric keys renewal ... 43
14.2 Data transfer by the client ... 44
14.3 Data transfer by the server ... 45

15 Information flow ... 48
15.1 Purpose and general model ... 48
15.2 Protected protocol SAOC ... 49
15.3 Wrapper SAOC ... 49

16 Wrapper error handling ... 52
16.1 General ... 52
16.2 Checking of a wrapper handshake request ... 52
16.3 Checking of a wrapper handshake accept ... 53
16.4 Checking of data transfer WrPDUs ... 54
16.5 Wrapper diagnostic codes ... 56

17 End-to-end communications ... 57

SECTION 3 – PROTECTED PROTOCOLS ... 58

18 Authorization and validation list management ... 58
18.1 General on authorization and validation management ... 58
18.2 Defined protected protocol data unit types ... 58
18.3 Authorization and validation management protocol initialization request ... 59
18.4 Authorization and validation management protocol initialization accept ... 59
18.5 Authorization and validation management protocol initialization reject ... 59
18.6 Authorization and validation management protocol initialization abort ... 59
18.7 Add authorization and validation list request ... 60
18.8 Add authorization and validation list response ... 61
18.9 Replace authorization and validation list request ... 61
18.10 Replace authorization and validation list response ... 61
18.11 Delete authorization and validation list request ... 62
18.12 Delete authorization and validation list response ... 62
18.13 Authorization and validation list abort ... 63
18.14 Authorization and validation list error codes ... 63

19 Certification authority subscription protocol ... 64
19.1 Certification authority subscription introduction ... 64
19.2 Defined protected protocol data unit types ... 64
19.3 Certification authority subscription protocol initialization request ... 65
19.4 Certification authority subscription protocol initialization accept ... 65
19.5 Certification authority subscription protocol initialization reject ... 65
19.6 Certification authority subscription protocol initialization abort ... 65
19.7 Public-key certificate subscription request ... 66
19.8 Public-key certificate subscription response ... 66
19.9 Public-key certificate un-subscription request ... 67
19.10 Public-key certificate un-subscription response ... 68
19.11 Public-key certificate replacements request ... 69
19.12 Public-key certificate replacement response ... 69

© ISO/IEC 2025 – All rights reserved

19.13 End-entity public-key certificate updates request ... 70
19.14 End-entity public-key certificate updates response ... 71
19.15 Certification authority subscription abort ... 72
19.16 Certification authority subscription error codes ... 72

20 Trust broker protocol ... 72
20.1 Introduction ... 72
20.2 Defined protected protocol data unit types ... 73
20.3 Trust broker protocol initialization request ... 73
20.4 Trust broker protocol initialization accept ... 73
20.5 Trust broker protocol initialization reject ... 73
20.6 Trust broker protocol initialization abort ... 74
20.7 Trust broker request syntax ... 74
20.8 Trust broker response syntax ... 74
20.9 Trust broker error information ... 75

Annex A Crypto Tools in ASN.1 ... 76

Annex B General cryptographic algorithms ... 81

Annex C Wrapper protocol in ASN.1 ... 92

Annex D Protected protocol interface to the wrapper protocol ... 97

Annex E Authorization and validation list management in ASN.1 ... 99

Annex F Certification authority subscription in ASN.1 ... 102

Annex G Trust broker in ASN.1 ... 106

Annex H Migration of cryptographic algorithms ... 108
H.1 Migration of cryptographic algorithms ... 108
H.2 Migration tools or migration approaches ... 109
H.3 Migration of public-key certificates and other data types using the extension mechanism ... 110
H.4 General migration approach for communication protocols ... 110
H.5 Use of multiple and choice cryptographic algorithms ... 111

Annex I Auxiliary specifications ... 114

Annex J Amendments and corrigenda ... 119

Bibliography ... 120

© ISO/IEC 2025 – All rights reserved

Introduction

The Internet Engineering Task Force (IETF) maintains a substantial set of protocols for supporting public-key infrastructure (PKI). Recommendation ITU-T X.510 | ISO/IEC 9594-11 provides protocols to supplement those protocols developed by IETF, especially for:

a) supporting new functions specified by Rec. ITU-T X.509 | ISO/IEC 9594-8, for which IETF has not provided support, e.g., support for authorization and validation list (AVL) maintenance;

b) constraint environments, where lean protocols are required.

In addition, it specifies:

c) a wrapper protocol that provides security services for other protocols.

This Recommendation | International Standard consist of three sections as follows.

Section 1 gives general specifications for this Recommendation | International Standard.

Section 2 is the wrapper protocol specification.

Section 3 specifies some protocols to be protected by the wrapper protocol:

a) a protocol for maintaining authorization and validation lists (AVLs);

b) a protocol for subscribing public-key certificate status information from certification authorities (CAs); and

c) a protocol for accessing a trust broker.

The following annexes are included:

Annex A, which is an integral part of this Recommendation | International Standard, provides the ASN.1 module for specifications to be imported by protocols providing a migration path for cryptographic algorithms.

Annex B, which is an integral part of this Recommendation | International Standard, provides cryptographic algorithm specification.

Annex C, which is an integral part of this Recommendation | International Standard, provides the ASN.1 module for the wrapper protocol.

Annex D, which is an integral part of this Recommendation | International Standard, provides specifications for how a protected protocol is wrapped by the wrapper protocol.

Annex E, which is an integral part of this Recommendation | International Standard, provides the ASN.1 module for maintenance of the authorization and validation lists (AVLs) protocol.

Annex F, which is an integral part of this Recommendation | International Standard, provides the ASN.1 module for certification authority subscription protocol.

Annex G, which is an integral part of this Recommendation | International Standard, provides the ASN.1 module for the trust broker protocol.

Annex H, which is not an integral part of this Recommendation | International Standard, provides guidance for cryptographic algorithm migration.

Annex I, which is not an integral part of this Recommendation | International Standard, reproduces the ASN.1 specification from other Specifications in the Rec. ITU X.500 Series | ISO/IEC 9594-all parts.

Annex J, which is not an integral part of this Recommendation | International Standard, provides lists amendments and corrigenda included in this Specification.

© ISO/IEC 2025 – All rights reserved

INTERNATIONAL STANDARD
ITU-T RECOMMENDATION

Information Technology – Open systems Interconnection – The Directory – Protocol specifications for secure operations

SECTION 1 – GENERAL

1 Scope

This Recommendation | International Standard provides guidance on how to prepare new and old protocols for cryptographic algorithm migration and defines auxiliary cryptographic algorithms to be used for migration purposes.

This Recommendation | International Standard specifies a general wrapper protocol that provides authentication, integrity and confidentiality (encryption) protection for other protocols. This wrapper protocol includes a migration path for cryptographic algorithms allowing for smooth migration to stronger cryptographic algorithms as such requirements evolve. This will allow migration to quantum-safe cryptographic algorithms. Protected protocols can then be developed without taking security and cryptographic algorithms into consideration.

This Recommendation | International Standard also includes some protocols to be protected by the wrapper protocol primarily for support of public-key infrastructure (PKI). Other specifications, e.g., Recommendations or International Standards, may also develop protocols designed to be protected by the wrapper protocol.

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.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*.
- Recommendation ITU-T X.690 (2021) | ISO/IEC 8825-1:2021, *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 (2021) | ISO/IEC 8825-2:2021, *Information technology – ASN.1 encoding rules: Specification of Packed Encoding Rules (PER).*

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*.

© ISO/IEC 2025 – All rights reserved

2.3 International Standards

- ISO/IEC 10116:2017, *Information technology – Security techniques – Modes of operation for a n-bit block cipher*.
- ISO/IEC 18033-3:2010, *Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers*.
- ISO/IEC 18033-3:2010/Amd.1:2021, *Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers, Amendment 1: SM4*.

2.4 Other references

- IETF RFC 793 (1981), *Transmission Control Protocol*.
- IETF RFC 2104 (1997), *HMAC: Keyed-Hashing for Message Authentication*.
- IETF RFC 3526 (2003), *More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)*.
- IETF RFC 5084 (2007), *Using AES-CCM and AES-GCM Authenticated Encryption in the Cryptographic Message Syntax (CMS)*.
- IETF RFC 5114 (2008), *Additional Diffie-Hellman Groups for Use with IETF Standards*.
- IETF RFC 5869 (2010), *HMAC-based Extract-and-Expand Key Derivation Function (HKDF)*.
- IETF RFC 6932 (2013), *Brainpool Elliptic Curves for the Internet Key Exchange (IKE) Group Description Registry*.

3 Definitions

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

3.1 OSI reference model definitions

The following terms are defined in Rec. ITU-T X.800 | ISO 7498-2:

a) confidentiality;
b) cryptography;
c) digital signature.

3.2 Directory model definitions

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

a) attribute.

3.3 Public-key and attribute certificate definitions

The following terms are defined in Rec. ITU-T X.509 | ISO/IEC 9594-8:

a) attribute certificate;
b) authorization and validation list (AVL);
c) authorization and validation list entity (AVL entity);
d) authorizer;
e) certification authority (CA);
f) certification path;
g) end entity;
h) end-entity public-key certificate;
i) hash function;
j) key agreement;
k) private key;
l) public key;
m) public-key certificate;

© ISO/IEC 2025 – All rights reserved

n) public-key infrastructure (PKI);

o) relying party.

3.4 Terms defined in this Recommendation | International Standard

This Recommendation | International Standard defines the following terms:

3.4.1 abstract syntax: A specification of application-protocol-data-units by using notation rules that are independent of the encoding technique used to represent them.

NOTE – The term abstract syntax is originally an OSI term but is extended here to be general applicable.

3.4.2 alternative cryptographic algorithm: A cryptographic algorithm to which migration is wanted.

3.4.3 application entity: An active element embodying a set of capabilities which is pertinent to communication systems, and which is defined for the application layer.

NOTE – The term application entity is originally an open systems interconnection (OSI) term, but is extended here to be generally applicable.

3.4.4 application protocol data unit (APDU): Data that is transmitted as a single unit at the application layer between two application entities.

3.4.5 association: A cooperative relationship between two application entities, which enables the communication of information and the coordination of their joint operation for an instance of communication.

3.4.6 block: A string of bits of defined length.

3.4.7 block cipher: Symmetric encipherment system with the property that the encryption algorithm operates on a block of plain text, i.e., a string of bits of a defined length, to yield a block of ciphertext.

3.4.8 client: The entity that initiates an association.

3.4.9 cryptographic algorithm pluck-in concept: The ability to specify the use of a cryptographic algorithm in the base protocol, but the exact selection of the cryptographic algorithm is determined later for a particular instance of communication.

3.4.10 cryptographic check algorithm: Either an integrity check value (ICV) algorithm or a digital signature algorithm, i.e., an algorithm that takes as an input a message and a symmetric or private key and returns a string of bits that can be used to verify the origin and integrity of the message.

3.4.11 cryptographic check value: Output of a cryptographic check function invocation.

3.4.12 data transfer phase: The phase from the completion of the establishment of an association to the termination of the association.

3.4.13 digital signature: The result of a cryptographic transformation of data that, when properly implemented, provides a mechanism for origin authentication, data integrity and signatory non-repudiation.

3.4.14 inner cryptographic algorithm: A cryptographic algorithm that included as a parameter of an outer cryptographic algorithm.

3.4.15 native cryptographic algorithm: A cryptographic algorithm used prior to a migration period.

3.4.16 protected protocol data unit (PrPDU): Application protocol data unit defined by an application protocol to be protected by the wrapper protocol.

3.4.17 protected protocol pluck-in concept: The ability to specify the inclusion of a communications protocol to be protected in the base protocol, but the exact identification of a specific protocol is determined later for a particular instance of communication.

3.4.18 outer cryptographic algorithm: A cryptographic algorithm that has as parameters one or more other cryptographic algorithms, and in this way lets multiple inner cryptographic algorithms have the appearance of a single cryptographic algorithm.

3.4.19 server: The entity that accepts or rejects an association request.

3.4.20 symmetric key: A cryptographic key used for both encryption of plaintext and decryption of ciphertext.

3.4.21 wrapper protocol data unit (WrPDU): An application protocol data unit carrying security protocol control information and, when relevant, carrying a protected protocol data unit.

© ISO/IEC 2025 – All rights reserved