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)

COPYRIGHT PROTECTED DOCUMENT

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.

CONTENTS

Page

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.

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*.

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*.