DRAFT INTERNATIONAL STANDARD

ISO/IEC DIS 9594-11

ISO/IEC JTC **1**/SC **6**

Secretariat: **KATS**

Voting begins on:
2019-11-21

Voting terminates on:
2020-02-13

Information technology — Open systems interconnection — The directory —

Part 11:
Protocol specifications for secure operations

ICS: 35.100.70

This document is circulated as received from the committee secretariat.

Reference number
ISO/IEC DIS 9594-11:2019(E)

COPYRIGHT PROTECTED DOCUMENT

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
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword ..... **vi**

Introduction ..... **vii**

1 Scope **1**

2 Normative references **1**
2.1 Identical Recommendations | International Standards 1
2.2 Other references 2

3 Terms and 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 specified by this Recommendation | International Standard 3

4 Abbreviations **4**

5 Conventions **4**

6 Common data types and special cryptographic algorithms **5**
6.1 Introduction 5
6.2 Multiple cryptographic algorithm specifications 5
6.2.1 General 5
6.2.2 Multiple signatures algorithm 5
6.2.3 Multiple symmetric key algorithm 5
6.2.4 Multiple public-key algorithms 6
6.2.5 Multiple hash algorithm 6
6.2.6 Multiple authenticated encryption algorithm 6
6.2.7 Multiple integrity check value algorithm 6
6.3 Key establishment algorithms 7
6.3.1 General 7
6.3.2 Diffie-Hellman group 14 algorithm with HKDF-256 7
6.3.3 Diffie-Hellman group 23 algorithm with HKDF-256 7
6.3.4 Diffie-Hellman group 28 algorithm with HKDF-256 8
6.3.5 Key derivation 8
6.4 Multiple cryptographic algorithm-value pairs 9
6.4.1 Multiple digital signatures attached to data 9
6.4.2 Duplicate integrity check values attached to data 9
6.4.3 Formal specification of encryption 9
6.4.4 Formal specification of authenticated encryption 9

7 General concept for securing protocols **10**
7.1 Introduction 10
7.2 Protected protocol plug-in concept 10
7.3 Communications structure 10
7.4 Structure of application protocol data unit 11
7.5 Another view of the relationship between the wrapper protocol and the protected protocol 11
7.6 Information and control 12
7.7 Exception conditions 12

8 Wrapper protocol general concepts **14**
8.1 Introduction 14
8.2 UTC time specification 14
8.3 Use of the SIGNED parameterized data type 14
8.4 Use of alternative cryptographic algorithms 15
8.5 General on establishing shared keys 15
8.6 Sequence numbers 15
8.7 Use of invocation identification in the wrapper protocol 15

8.8 Mapping to underlying services ... 16
8.9 Definition of protected protocols ... 16
8.10 Overview of wrapper protocol data units ... 16

9 Association management ... 17
9.1 Introduction to association management ... 17
9.2 Association handshake request ... 17
9.2.1 Association handshake request syntax ... 17
9.3 Association accept ... 19
9.3.1 Association handshake accept syntax ... 19
9.4 Association reject due to security issues ... 20
9.5 Association reject by the protected protocol ... 21
9.6 Handshake security abort ... 22
9.7 Handshake abort by protected protocol ... 23
9.8 Data transfer security abort ... 23
9.9 Abort by protected protocol ... 24
9.10 Release request WrPDU ... 24
9.11 Release response WrPDU ... 25

10 Data transfer phase ... 25
10.1 Symmetric keys renewal ... 25
10.2 Data transfer by the requestor ... 25
10.3 Data transfer by the acceptor ... 27

11 Wrapper error handling ... 28
11.1 General ... 28
11.2 Checking of a wrapper handshake request ... 28
11.2.1 General ... 28
11.2.2 Digital signature checking ... 28
11.2.3 Checking of the to-be-signed part ... 29
11.3 Checking of a wrapper handshake accept ... 30
11.3.1 General ... 30
11.3.2 Digital signature checking ... 30
11.3.3 Checking of the to-be-signed part ... 30
11.4 Checking of data transfer WrPDUs ... 31
11.4.1 General ... 31
11.4.2 Mode checking ... 31
11.4.3 Integrity checking ... 32
11.4.4 Checking of common components for AadReq and AadAcc data values ... 32
11.4.5 AadReq data value specific checking ... 32
11.4.6 AadAcc data value specific checking ... 32
11.5 Wrapper error codes ... 32

12 Authorization and validation list management ... 34
12.1 General on authorization validation management ... 34
12.1.1 Introduction ... 34
12.1.2 Invocation identification ... 34
12.2 Defined protected protocol data unit (PrPDU) types ... 34
12.3 Authorization and validation management protocol initialization request ... 34
12.4 Authorization and validation management protocol initialization accept ... 35
12.5 Authorization and validation management protocol initialization reject ... 35
12.6 Authorization and validation management protocol initialization abort ... 35
12.7 Add authorization and validation list ... 36
12.8 Replace authorization and validation list ... 37
12.9 Delete authorization and validation list ... 38
12.10 Authorization and validation list reject ... 39
12.11 Authorization and validation list error codes ... 39

13 Certification authority subscription protocol ... 41
13.1 Certification authority subscription introduction ... 41
13.2 Overview of protocol data units ... 41

13.3 Certification authority subscription protocol initialization request 41
13.4 Certification authority subscription protocol initialization accept 42
13.5 Certification authority subscription protocol initialization reject 42
13.6 Certification authority subscription protocol initialization abort 42
13.7 Public-key certificate subscription 42
13.8 Public-key certificate un-subscription 44
13.9 Public-key certificate replacements 46
13.10 End-entity public-key certificate updates 47
13.11 Certification authority subscription reject 49
13.12 Certification authority subscription error codes 49

14 Trust broker protocol 50
14.1 Introduction 50
14.2 Defined protocol data unit (PDU) types 50
14.3 Trust broker request syntax 50
14.4 Trust broker response syntax 50
14.5 Trust broker error information 51

Annex A Crypto Tools in ASN.1 53

Annex B Wrapper protocol in ASN.1 56

Annex C Protected protocol interface to the wrapper protocol 61

Annex D Authorization and validation list management in ASN.1 63

Annex E Certification authority subscription in ASN.1 66

Annex F Trust broker in ASN.1 70

Annex G Migration of cryptographic algorithms 72

Bibliography 77

Foreword

Recommendation ITU-T X.509PROT | ISO/IEC 9594-11 specifies a general protocol, called the wrapper protocol, that provides cyber security for protocols designed for protection by the wrapper protocol. The wrapper protocol provides authentication, integrity and optionally confidentiality (encryption). The wrapper protocol allows cyber security to be provided independently of the protected protocols, which means that the security may enhanced without affecting protected protocol specifications.

The wrapper protocol is designed for easy migration of cryptographic algorithms, as stronger algorithms become necessary.

Recommendation ITU-T X.509PROT | ISO/IEC 9594-11 contains specifications for how other Recommendations and International Standards may include features for migration of cryptographic algorithms, and it includes ASN.1 specifications to be imported for that purpose.

Recommendation ITU-T X.509PROT | ISO/IEC 9594-11 also specifies three protocols that make use of the protection of the wrapper protocol. This includes a protocols provide for maintaining authorization and validation lists, a protocol for subscribing of public-key certificate status and a protocol for accessing a trust broker.

Keywords

Cryptography; cryptographic algorithm; digital signature; public-key certificate; certification authority: distinguished name; PKI, trust anchor; validation.

Introduction

The Internet Engineering Task Force (IETF) maintains a substantial set of protocols for supporting public-key infrastructure (PKI). This Specification 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; and

b) constrained 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:

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 CAs.

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 the ASN.1 module for the wrapper protocol.

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

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

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

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

Information technology — Open systems interconnection — The directory —

Part 11:
Protocol specifications for secure operations

SECTION 1 – GENERAL

1 Scope

The scope of this Recommendation | International Standard is threefold:

It provides guidance for how to prepare new and old protocols for cryptographic algorithm migration. It defines auxiliary cryptographic algorithms to be used for migration purposes

The scope includes 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. Protected protocols can then be developed without taking security and cryptographic algorithms into consideration.

The scope also includes some protocols to be protected by the wrapper protocol primarily for support of 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 509 (2019) | ISO/IEC 9594-8xx, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.

Recommendation ITU-T X 520 (2019) | ISO/IEC 9594-6xx, *Information technology – Open Systems Interconnection – The Directory: Selected attribute types*.

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 681 (2015) | ISO/IEC 8824-2:2015, *Information technology – Abstract Syntax Notation One (ASN.1): Information object specification*.

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 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)*.

3 Terms and 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.200 | ISO 7498-1:

a) abstract syntax;

b) confidentiality;

c) cryptography;

d) digital signature.

3.2 Directory model definitions

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

a) attribute;

b) distinguished name.

3.3 Public-key and attribute certificate definitions

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

a) authorization and validation list (AVL);

b) authorization and validation list entity (AVL entity);

c) authorizer;

d) certification authority (CA);

e) certification path;

f) end entity;

g) end-entity public-key certificate;

h) hash function;

i) key agreement;

j) private key;

k) public key;

l) public-key certificate;

m) public-key infrastructure (PKI);

n) relying party;

o) trust broker.

3.4 Terms specified by this Recommendation | International Standard

3.4.1 acceptor: The entity that accept or reject an association.

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.

3.4.4 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.

3.4.5 data transfer phase: The phase from the completion of the establishment of an association to the initiation of the association termination

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

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

3.4.8 protocol data unit: Data that is transmitted as single unit between two entities.

3.4.9 protected protocol data unit (PrPDU): Application protocol data unit (APDU) defined by a protected application protocol.

3.4.10 requestor: The entity that initiates an association.

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

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

4 Abbreviations

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

APDU	Application Protocol Data Unit
ASN.1	Abstract Syntax Notation One
AVL	Authorization and Validation List
AVMP	Authorization Validation Management Protocol
BER	Basic Encoding Rules
CA	Certification Authority
CASP	Certification Authority Subscription Protocol
DER	Distinguished Encoding Rules
DH	Diffie-Hellman
HKDF	HMAC-based Extract-and-Expand Key Derivation Function
HMAC	Keyed-hash Message Authentication Code
ICV	Integrity Check Value
IETF	Internet Engineering Task Force
MAC	Message Authentication Code
PDU	Protocol Data Unit
PKI	Public-Key Infrastructure
PMI	Privilege Management Infrastructure
PrPDU	Protected protocol Data Unit
TCP	Transmission Control Protocol
UTC	Coordinated Universal Time
WrPDU	Wrapper protocol Data Unit

5 Conventions

The term "Specification" (as in "this Specification") shall be taken to mean Rec. ITU-T X.510 | ISO/IEC 9594-11.

The term "The Directory Specifications" shall be taken to mean 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.

If an International Standard or ITU-T Recommendation is referenced within normal text without an indication of the edition, the edition shall be taken to be the latest one as specified in the normative references clause.

This Specification makes extensive use of the Abstract Syntax Notation One (ASN.1) for the formal specification of data types and values, as it is specified in Rec. ITU-T X.680 | ISO/IEC 8824-1, Rec. ITU-T X.681 | ISO/IEC 8824-2, Rec. ITU-T X.682 | ISO/IEC 8824-3, Rec. ITU-T X.683 | ISO/IEC 8824-4 and Rec. ITU-T X.690 | ISO/IEC 8825-1.

This Specification presents ASN.1 notation in the bold Courier New typeface. When ASN.1 types and values are referenced in normal text, they are differentiated from normal text by presenting them in the bold Courier New typeface

If the items in a list are numbered (as opposed to using "–" or letters), then the items shall be considered steps in a procedure.

6 Common data types and special cryptographic algorithms

6.1 Introduction

The intension here is not to define cryptographic algorithms as such, but the intention is to make specifications for how multiple cryptographic algorithms of a specific type may be specified by a single cryptographic algorithm specification. This is done by utilizing the flexibility provided by the **AlgorithmIdentifier** parameterized data type defined in clause 6.2 of Rec. ITU-T X.509 | ISO/IEC 9594-8. This is further described in clause 6.2 below.

It is the intention here is also to define data types that allow specification of multiple cryptographic algorithm and value pairs, where the value is generated using that algorithms or is a value that complies with that algorithm. Such data types are defined in clause 6.3.

6.2 Multiple cryptographic algorithm specifications

6.2.1 General

The **PARMS** field of the **ALGORITHM** object class allows any data type to be specified. This is utilized to define a data type that allows for multiple cryptographic algorithm specifications within an a single outer algorithm specification

6.2.2 Multiple signatures algorithm

The following is a specification of an **ALGORITHM** object that allows multiple digital signature algorithms to be specified.

```
multipleSignaturesAlgo ALGORITHM ::= {
  PARMS         MultipleSignaturesAlgo
  IDENTIFIED BY id-algo-multipleSignaturesAlgo }

MultipleSignaturesAlgo ::= SEQUENCE SIZE (1..MAX) OF
  algo  AlgorithmIdentifier{{SupportedSignatureAlgorithms}}

SupportedSignatureAlgorithms ALGORITHM ::= {...}
```

6.2.3 Multiple symmetric key algorithm

The following is a specification of an **ALGORITHM** object that allows multiple symmetric key algorithms to be specified.

```
multipleSymmetricKeyAlgo ALGORITHM ::= {
  PARMS         MultipleSymmetricKeyAlgo
  IDENTIFIED BY id-algo-multipleSymmetricKeyAlgo }

MultipleSymmetricKeyAlgo ::= SEQUENCE SIZE (1..MAX) OF
  algo  AlgorithmIdentifier{{SupportedSymmetricKeyAlgorithms}}
```