INTERNATIONAL STANDARD

ISO/IEC 9594-11

First edition
2020-12

Information technology — Open systems interconnection directory —

Part 11: Protocol specifications for secure operations

Reference number
ISO/IEC 9594-11:2020(E)

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

INTERNATIONAL STANDARD ISO/IEC 9594-11
RECOMMENDATION ITU-T X.510

Information technology – Open Systems Interconnection – The Directory: Protocol specifications for secure operations

Summary

Recommendation ITU-T X.510 | ISO/IEC 9594-11 specifies a general protocol, called the wrapper protocol, that provides cybersecurity for protocols designed for its protection. The wrapper protocol provides authentication, integrity and optionally confidentiality (encryption). The wrapper protocol allows cybersecurity to be provided independently of the protected protocols, which means that security may be enhanced without affecting protected protocol specifications.

The wrapper protocol is specified without specifying specific cryptographic algorithms, but is designed for plucking-in cryptographic algorithms as required.

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

Recommendation ITU-T X.510 | ISO/IEC 9594-11 contains recommendations for how other Recommendations and International Standards may include features for migration of cryptographic algorithms, and it includes ASN.1 specifications to be applied for that purpose.

Recommendation ITU-T X.510 | ISO/IEC 9594-11 also specifies three protocols that make use of the wrapper protocol protection. This includes a protocol for maintenance of authorization and validation lists (AVLs), a protocol for subscribing of public-key certificate status and a protocol for accessing a trust broker.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.510	2020-08-22	17	11.1002/1000/14320

Keywords

Certification authority, cryptography, cryptographic algorithm, digital signature, public-key certificate, PKI, quantum-safe, 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/.

CONTENTS

Page

SECTION 1 – GENERAL 1

1 Scope 1

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

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 specified by this Recommendation | International Standard 2

4 Abbreviations 3

5 Conventions 4

6 Common data types and special cryptographic algorithms 4
- 6.1 Introduction 4
- 6.2 ASN.1 information object class specification tool 4
- 6.3 Multiple-cryptographic algorithm specifications 6
- 6.4 Key establishment algorithms 7
- 6.5 Multiple-cryptographic algorithm-value pairs 9
- 6.6 Formal specification of encipherment 11

7 General concepts for securing protocols 11
- 7.1 Introduction 11
- 7.2 Protected protocol plug-in concept 12
- 7.3 Communications structure 12
- 7.4 Another view of the relationship between the wrapper protocol and the protected protocol 12
- 7.5 Structure of application protocol data unit 13
- 7.6 Exception conditions 13

SECTION 2 – THE WRAPPER PROTOCOL 14

8 Wrapper protocol general concepts 14
- 8.1 Introduction 14
- 8.2 UTC time specification 14
- 8.3 Use of alternative cryptographic algorithms 14
- 8.4 General on establishing shared keys 14
- 8.5 Sequence numbers 15
- 8.6 Use of invocation identification in the wrapper protocol 15
- 8.7 Mapping to underlying services 15
- 8.8 Definition of protected protocols 15
- 8.9 Overview of wrapper protocol data units 15

9 Association management 16
- 9.1 Introduction to association management 16
- 9.2 Association handshake request 16
- 9.3 Association accept 18
- 9.4 Association reject due to security issues 19
- 9.5 Association reject by the protected protocol 20
- 9.6 Handshake security abort 21
- 9.7 Handshake abort by protected protocol 21
- 9.8 Data transfer security abort 22
- 9.9 Abort by protected protocol 22
- 9.10 Release request WrPDU 23
- 9.11 Release response WrPDU 23
- 9.12 Release collision 24

Page

10 Data transfer phase ... 24
10.1 Symmetric keys renewal ... 24
10.2 Data transfer by the client ... 24
10.3 Data transfer by the server ... 26
11 Information flow ... 28
11.1 Purpose and general model ... 28
11.2 Protected protocol SAOC ... 29
11.3 Wrapper SAOC ... 29
12 Wrapper error handling ... 32
12.1 General ... 32
12.2 Checking of a wrapper handshake request ... 32
12.3 Checking of a wrapper handshake accept ... 33
12.4 Checking of data transfer WrPDUs ... 34
12.5 Wrapper diagnostic codes ... 36
SECTION 3 – PROTECTED PROTOCOLS ... 37
13 Authorization and validation list management ... 37
13.1 General on authorization and validation management ... 37
13.2 Defined protected protocol data unit (PrPDU) types ... 37
13.3 Authorization and validation management protocol initialization request ... 38
13.4 Authorization and validation management protocol initialization accept9 ... 38
13.5 Authorization and validation management protocol initialization reject ... 38
13.6 Authorization and validation management protocol initialization abort ... 38
13.7 Add authorization and validation list request ... 39
13.8 Add authorization and validation list response ... 40
13.9 Replace authorization and validation list request ... 40
13.10 Replace authorization and validation list response ... 40
13.11 Delete authorization and validation list request ... 41
13.12 Delete authorization and validation list response ... 41
13.13 Authorization and validation list abort ... 42
13.14 Authorization and validation list error codes ... 42
14 Certification authority subscription protocol ... 43
14.1 Certification authority subscription introduction ... 43
14.2 Defined protected protocol data unit (PrPDU) types ... 43
14.3 Certification authority subscription protocol initialization request ... 43
14.4 Certification authority subscription protocol initialization accept ... 44
14.5 Certification authority subscription protocol initialization reject ... 44
14.6 Certification authority subscription protocol initialization abort ... 44
14.7 Public-key certificate subscription request ... 44
14.8 Public-key certificate subscription response ... 45
14.9 Public-key certificate un-subscription request ... 46
14.10 Public-key certificate un-subscription response ... 46
14.11 Public-key certificate replacements request ... 47
14.12 Public-key certificate replacement response ... 48
14.13 End-entity public-key certificate updates request ... 49
14.14 End-entity public-key certificate updates response ... 49
14.15 Certification authority subscription abort ... 50
14.16 Certification authority subscription error codes ... 50
15 Trust broker protocol ... 51
15.1 Introduction ... 51
15.2 Defined protected protocol data unit (PrPDU) types ... 51
15.3 Trust broker protocol initialization request ... 51
15.4 Trust broker protocol initialization accept ... 52
15.5 Trust broker protocol initialization reject ... 52

Page

15.6 Trust broker protocol initialization abort 52
15.7 Trust broker request syntax 52
15.8 Trust broker response syntax 53
15.9 Trust broker error information 53
Annex A − Crypto Tools in ASN.1 55
Annex B − Wrapper protocol in ASN.1 58
Annex C − Protected protocol interface to the wrapper protocol 63
Annex D − Cryptographic algorithms 65
Annex E − Authorization and validation list management in ASN.1 67
Annex F − Certification authority subscription in ASN.1 70
Annex G −Trust broker in ASN.1 74
Annex H − Migration of cryptographic algorithms 76
H.1 Introduction 76
H.2 Negotiation of cryptographic algorithms 76
H.3 Non-negotiable digital signature algorithms 77
Annex I − Auxiliary specifications 80
Bibliography 85

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 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 cryptographic algorithm specification.

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.

The content of this Rec. ITU-T X.510 | ISO/IEC 9594-11 was moved to here from Rec. ITU-T X.509 (2016) | ISO/IEC 9594-8:2017 and subsequently updated.

INTERNATIONAL STANDARD ISO/IEC 9594-11
RECOMMENDATION ITU-T X.510

Information technology – Open Systems Interconnection – The Directory: Protocol specifications for secure operations

SECTION 1 – GENERAL

1 Scope

The scope of this Recommendation | International Standard is threefold.

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.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.509 (2019) | ISO/IEC 9594-8:2020, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.
- 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.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.691 (2015) | ISO/IEC 8825-2:2015, *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 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 terms are defined in Rec. ITU-T X.501 | ISO/IEC 9594-2:

a) attribute;

b) distinguished name (of an entry).

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 defined in this Recommendation | International Standard

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 original 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 OSI term (see Rec. ITU-T X.519 | ISO/IEC 9594-5), 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 client: The entity that initiates an association.

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

3.4.8 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.

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

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

3.4.11 server: The entity that accepts or rejects an association.

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

3.4.13 wrapper protocol data unit (WrPDU): An application protocol data unit 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:

AEAD	Authenticated Encryption with Associated Data
AES	Advanced Encryption Standard
AES-CBC	Advanced Encryption Standard-Cipher Block Chaining
APDU	Application Protocol Data Unit
ASN.1	Abstract Syntax Notation One

AVL	Authorization and Validation List
AVMP	Authorization and 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
ICT	Information and Communications Technology
ID	Identifier
LoA	Loss of Alignment
MODP	Modular exponential
OKM	Output Keying Material
OSI	Open Systems Interconnection
PDU	Protocol Data Unit
PKI	Public-Key Infrastructure
PMI	Privilege Management Infrastructure
PRK	Pseudorandom Key
PrPDU	Protected protocol Data Unit
RAOC	Receive Application Object Class
SAOC	Send Application Object Class
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 this Recommendation | International Standard.

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 one 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, Rec. ITU-T X.690 | ISO/IEC 8825-1 and Rec. ITU-T X.691 | ISO/IEC 8825-2.

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.

6 Common data types and special cryptographic algorithms

6.1 Introduction

This clause defines some auxiliary cryptographic specification as follows.

a) ASN.1 information object classes are heavily used for protocol design. The **`ALGORITHM`** information object class is important for this Specification. This is further expanded in clause 6.2.

b) Multiple cryptographic algorithms of a specific class may be specified by using a single containing cryptographic algorithm. This is done by utilizing the flexibility provided by the **`AlgorithmIdentifier`**

parameterized data type defined in clause 6.2.2 of Rec. ITU-T X.509 | ISO/IEC 9594-8. This is further described in clause 6.3.

c) There are advantages to the definition of cryptographic algorithms for key agreement procedures. This has been done for a few cases in clause 6.4.

d) Parameterized data types are defined in clause 6.5 for flexible protocol design.

e) Some formal specifications for encipherment are given in clause 6.6.

6.2 ASN.1 information object class specification tool

6.2.1 General information object class concept

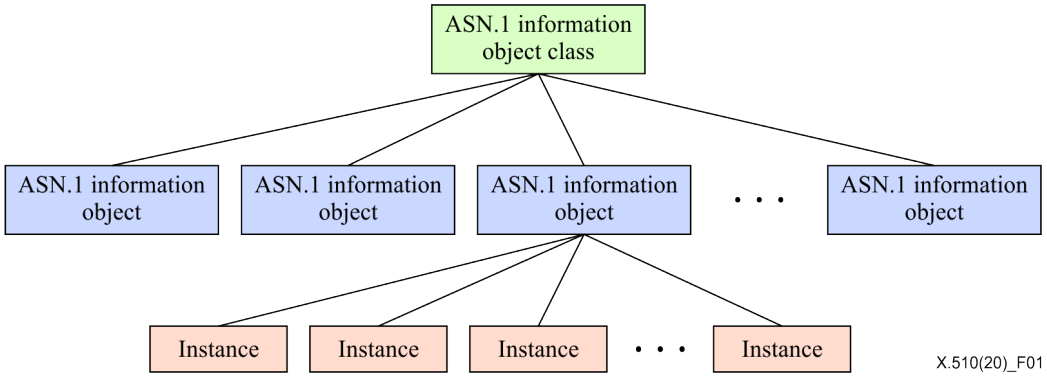

Figure 1 – ASN.1 information object class concept

The concept of ASN.1 information object class is specified in Rec. ITU-T X.681 | ISO/IEC 8824-2. It is vital for protocol design. For that reason, a short introduction is included here to encourage increased use of this facility. ASN.1 information object classes are widely used by the ITU-T X.500 series of Recommendations | ISO/IEC 9594-all parts for defining attributes, matching rules, extensions to public-key and attribute certificates, etc.

Figure 1 illustrates the general ASN.1 information object class concept. An ASN.1 information object class specifies the general syntax for a class of information objects, e.g., attribute types as defined by Rec. ITU-T X.501 | ISO/IEC 9594-2. From this general specification, specifications for specific attribute types are defined, e.g., an attribute type for e-mail addresses. From this specification, instances of e-mail address attributes may be generated. Instances may be transferred in the protocol or may be stored in a directory.

NOTE – The concept of object classes used in clause 11 is somewhat different from the concept of information object class defined in Rec. ITU-T X.681 | ISO/IEC 8824-2.

6.2.2 The ALGORITHM information object class

The information object class concept is also used to define cryptographic algorithms. The **ALGORITHM** information object class is defined in 6.2.2 of Rec. ITU-T X.509 | ISO/IEC 9594-8. The specification of this information is reproduced as follows for easy reference. The **ALGORITHM** information object class is different from most other information object classes in the sense that an instance of an information object is an invocation of the algorithm rather than specifying a value identifying something, like an e-mail address.

The following ASN.1 information object class is used to specify cryptographic algorithms.

```
ALGORITHM ::= CLASS {
  &Type           OPTIONAL,
  &DynParms       OPTIONAL,
  &id             OBJECT IDENTIFIER UNIQUE }
WITH SYNTAX {
  [PARMS          &Type]
  [DYN-PARMS      &DynParms ]
  IDENTIFIED BY   &id }
```

The **ALGORITHM** information object class has the following fields.

a) The **&Type** field is used to specify those fixed parameters that are necessary for specifying the exact procedure for deploying the cryptographic algorithm being defined. Not all cryptographic algorithms

require such parameters. The field is then absent or has the value **NULL**, as determined by the individual cryptographic algorithm specifications.

b) The **&DynParms** field is used to specify those dynamic parameters that determine the value(s) to be exchanged between two communicating entities when invoking the cryptographic algorithm. Not all cryptographic algorithms require dynamic parameters. In this case the **&DynParms** field shall be absent.

c) The **&id** field is used to uniquely identify the class of cryptographic algorithm being defined.

The **AlgorithmWithInvoke** parameterized data type defined as follows is used in situations where the type of cryptographic algorithm is signalled together with its invocation.

```
AlgorithmWithInvoke{ALGORITHM:SupportedAlgorithms} ::= SEQUENCE {
  algorithm       ALGORITHM.&id({SupportedAlgorithms}),
  parameters  [0] ALGORITHM.&Type({SupportedAlgorithms}{@algorithm}) OPTIONAL,
  dynamParms  [1] ALGORITHM.&DynParms({SupportedAlgorithms}{@algorithm}) OPTIONAL,
  ... }
```

The **AlgorithmWithInvoke** parameterized data type has the following components.

a) The **algorithm** component shall hold the object identifier that uniquely identify the cryptographic algorithm being defined.

b) The **parameters** component, when present, shall hold the values of the fixed parameters that further identify the cryptographic algorithm in question. This component shall be present when the **&Type** field is present in the information object for the cryptographic algorithm in question. Otherwise, it shall be absent.

c) The **dynamParms** component, when present, shall hold the value(s) required by the dynamic parameters for the cryptographic algorithm. This component shall be present when the **&DynParms** field is present in the information object for the cryptographic algorithm. Otherwise, it shall be absent.

The **AlgorithmIdentifier** parameterized data type defined as follows is used in situations where the type of cryptographic algorithm is signalled without a corresponding invocation.

```
AlgorithmIdentifier{ALGORITHM:SupportedAlgorithms} ::= SEQUENCE {
  algorithm       ALGORITHM.&id({SupportedAlgorithms}),
  parameters      ALGORITHM.&Type({SupportedAlgorithms}{@algorithm}) OPTIONAL,
  ... }
```


The components of **AlgorithmIdentifier** data type shall be as specified for the corresponding components of the **AlgorithmWithIvoke** parameterized data type.

The **AlgoInvoke** parameterized data type defined as follows is used when the cryptographic algorithm has previously been determined and where only invocation information is required.

```
AlgoInvoke{ALGORITHM:SupportedAlgorithms} ::=
    ALGORITHM.&DynParms({SupportedAlgorithms})
```

6.3 Multiple-cryptographic algorithm specifications

6.3.1 General

Multiple cryptographic algorithms of the same object class may be specified using a single outer algorithm and then used instead of a single algorithm as a tool for algorithm migration as discussed in Annex H.

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

6.3.2 Multiple signatures algorithm

The following is a specification of an **ALGORITHM** information 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}}
```