

INTERNATIONAL  
STANDARD

ISO/IEC  
24824-4

First edition  
2021-03

---

---

**Information technology — Generic  
applications of ASN.1 —**

Part 4:  
**Cryptographic message syntax**

**iTeh Standards**  
**(<https://standards.iteh.ai>)**  
**Document Preview**

[ISO/IEC 24824-4:2021](https://standards.iteh.ai/catalog/standards/iso/568c0045-fa47-4901-9dd0-a989cf6ac54e/iso-iec-24824-4-2021)

<https://standards.iteh.ai/catalog/standards/iso/568c0045-fa47-4901-9dd0-a989cf6ac54e/iso-iec-24824-4-2021>



Reference number  
ISO/IEC 24824-4:2021(E)

© ISO/IEC 2021

**iTeh Standards**  
**(<https://standards.iteh.ai>)**  
**Document Preview**

[ISO/IEC 24824-4:2021](https://standards.iteh.ai/catalog/standards/iso/568c0045-fa47-4901-9dd0-a989cf6ac54e/iso-iec-24824-4-2021)

<https://standards.iteh.ai/catalog/standards/iso/568c0045-fa47-4901-9dd0-a989cf6ac54e/iso-iec-24824-4-2021>



**COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2021

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](mailto:copyright@iso.org)  
Website: [www.iso.org](http://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. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see [www.iso.org/directives](http://www.iso.org/directives) or [www.iec.ch/members\\_experts/refdocs](http://www.iec.ch/members_experts/refdocs)).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see [www.iso.org/patents](http://www.iso.org/patents)) or the IEC list of patent declarations received (see [patents.iec.ch](http://patents.iec.ch)).

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](http://www.iso.org/iso/foreword.html). In the IEC, [www.iec.ch/understanding-standards](http://www.iec.ch/understanding-standards).

This document was prepared by ITU-T [Telecommunication Standardization Sector of ITU] (as ITU-T X.894 [10/2018]) 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 24824 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](http://www.iso.org/members.html) and [www.iec.ch/national-committees](http://www.iec.ch/national-committees).

CONTENTS

	<i>Page</i>
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 Additional References.....	1
3 Definitions.....	1
4 Abbreviations .....	2
5 Conventions.....	2
6 Cryptographic message syntax .....	2
7 Signcryption .....	3
7.1 The SigncryptedData type.....	4
7.2 The ContentInformation type.....	4
7.3 The Signcrypter type.....	10
8 Quantum safe SignedData signatures.....	11
8.1 Detached content consideration .....	12
8.2 Time stamp consideration .....	12
8.3 The tokenizedParts attribute.....	13
9 Other key management techniques.....	13
9.1 Constructive key management .....	13
9.2 Database encryption key management .....	14
Annex A – ASN.1 modules .....	17
A.1 Main CMS module (from IETF RFC 6268).....	17
A.2 Module CMSObjectIdentifiers.....	23
A.3 Module AlgorithmInformation-2009 (from IETF RFC 5912).....	25
A.4 Module CryptographicMessageSyntaxAlgorithms-2009 (from IETF RFC 5911).....	32
A.5 Module PKIX-Algs-2009 (from IETF RFC 5912).....	35
A.6 Module PKIXAttributeCertificate-2009 (from IETF RFC 5912).....	42
A.7 Module AttributeCertificateVersion1-2009 (from IETF RFC 5912).....	46
A.8 Module PKIX-CommonTypes-2009 (from IETF RFC 5912).....	47
A.9 Module PKIX-X400Address-2009 (from IETF RFC 5912).....	50
A.10 Module PKIX1Explicit-2009 (from IETF RFC 5912).....	54
A.11 Module PKIXImplicit-2009 (from IETF RFC 5912).....	60
A.12 Module PKIX1-PSS-OAEP-Algorithms-2009 (from IETF RFC 5912).....	67
A.13 Module SecureMimeMessageV3dot1-2009 (from IETF RFC 5911).....	71
A.14 Module CMSSigncryption .....	73
A.15 Module CMSSCKMKeyManagement .....	75
A.16 Module CMSDBKeyManagement.....	77
A.17 Module CMSProfileAttributes .....	79
A.18 Module TokenizationManifest .....	80
A.19 Module TransientKey .....	81
A.20 Module TrustedTimestamp .....	83
A.21 Module ANSI-X9-42 .....	88
A.22 Module ANSI-X9-62 .....	91
Annex B – Object identifiers defined in this Recommendation   International Standard .....	96
Bibliography.....	97

INTERNATIONAL STANDARD ISO/IEC 24824-4 RECOMMENDATION ITU-T X.894

# Information technology — Generic applications of ASN.1 —

## Part 4:

# Cryptographic message syntax

## 1 Scope

This Recommendation | International Standard enhances the existing cryptographic message syntax (CMS) protocol by adding signcryption techniques and providing a new Abstract Syntax Notation One (ASN.1) module which conforms to the latest edition of the ASN.1 standard which can be used with all standardized encoding rules of ASN.1.

## 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 (2016) | ISO/IEC 9594-8:2017, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.

### 2.2 Paired Recommendations | International Standards equivalent in technical content

None.

### 2.3 Additional References

- ISO 11568-1:2005, *Banking – Key management (retail) – Part 1: Principles*.
- ISO/IEC 11770-6:2016, *Information technology – Security techniques – Key management – Part 6: Key derivation*.
- ISO/IEC 18033-2:2006, *Information technology – Security techniques – Encryption algorithms – Part 2: Asymmetric ciphers*.
- ISO/IEC 29150:2011, *Information technology – Security techniques – Signcryption*.
- IETF RFC 5652 (2009), *Cryptographic message syntax (CMS)*.
- IETF RFC 6268 (2011), *Additional new ASN.1 modules for the cryptographic message syntax (CMS) and the public key infrastructure using X.509 (PKIX)*.

## 3 Definitions

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

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

- attribute certificate;
- CA certificate;
- certificate revocation list.

The following term is defined in ISO/IEC 29150:

- signcryption

## 4 Abbreviations

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

ASN.1	Abstract Syntax Notation One
CEK	Content Encryption Key
CKM	Constructive Key Management
CMS	Cryptographic Message Syntax
CRL	Certificate Revocation List
DBEKM	Database Encryption Key Management
DK	Data encryption Key
HK	HMAC Key
HMAC	Hashed Message Authentication
ID	Identifier
KDF	Key Derivation Function
MK	Master Key encryption key
PBKDF	Password-Based KDF
SCD	Secure Cryptographic Device
SHA	Secure Hash Algorithm
URI	Uniform Resource Identifier
XML	extensible Markup Language

## 5 Conventions

None. <https://standards.iteh.ai/catalog/standards/iso/568c0045-fa47-4901-9dd0-a989cf6ac54e/iso-iec-24824-4-2021>

## 6 Cryptographic message syntax

CMS is defined in the base text, IETF RFC 5652. ASN.1 modules have been revised to conform to the current ASN.1 standard in IETF RFC 6268.

CMS defines the following content types:

- data: used to transfer data defined string of octets;
- signed data: used to transfer data with zero or more signatures;
- enveloped data: used to transfer encrypted data with one or more content-encryption keys;
- digested data: used to transfer data with a message digest;
- encrypted data: used to transfer encrypted data;
- authenticated data: used to transfer data with a message authentication code and one or more encrypted authentication keys.

Each of these content types is uniquely identified by an object identifier:

- for data:  
`id-data OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs7(7) 1}`
- for signed data:  
`id-signedData OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs7(7) 2}`
- for enveloped data:

- ```

id-envelopedData OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
  rsadsi(113549) pkcs(1) pkcs7(7) 3}
- for digested data:
id-digestedData OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
  rsadsi(113549) pkcs(1) pkcs7(7) 5}
- for encrypted data:
id-encryptedData OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
  rsadsi(113549) pkcs(1) pkcs7(7) 6}
- for authenticated data:
id-ct-authData OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
  rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) ct(1) 2}

```

Data transferred with CMS use the following ASN.1 type:

```

ContentInfo ::= SEQUENCE {
  contentType      CONTENT-TYPE.&id({ContentSet}),
  content          [0] EXPLICIT CONTENT-
  TYPE.&Type({ContentSet}{@contentType})}

```

The **CONTENT-TYPE** information object class is defined as **TYPE-IDENTIFIER** and is used to assign one of the previous object identifiers to the corresponding ASN.1 type.

```
CONTENT-TYPE ::= TYPE-IDENTIFIER
```

```
ContentType ::= CONTENT-TYPE.&id
```

```

ContentSet CONTENT-TYPE ::= {
  -- Define the set of content types to be recognized
  ct-Data |
  ct-SignedData |
  ct-EnvelopedData |
  ct-DigestedData |
  ct-EncryptedData |
  ct-AuthenticatedData,
  ...}

```

|                             |                                                                          |
|-----------------------------|--------------------------------------------------------------------------|
| <b>ct-Data</b>              | <b>CONTENT-TYPE ::= {OCTET STRING IDENTIFIED BY id-data}</b>             |
| <b>ct-SignedData</b>        | <b>CONTENT-TYPE ::= {SignedData IDENTIFIED BY id-signedData}</b>         |
| <b>ct-EnvelopedData</b>     | <b>CONTENT-TYPE ::= {EnvelopedData IDENTIFIED BY id-envelopedData}</b>   |
| <b>ct-DigestedData</b>      | <b>CONTENT-TYPE ::= {DigestedData IDENTIFIED BY id-digestedData}</b>     |
| <b>ct-EncryptedData</b>     | <b>CONTENT-TYPE ::= {EncryptedData IDENTIFIED BY id-encryptedData}</b>   |
| <b>ct-AuthenticatedData</b> | <b>CONTENT-TYPE ::= {AuthenticatedData IDENTIFIED BY id-ct-authData}</b> |

Other content types can be defined by creation of new information objects of **CONTENT-TYPE** information object class using unique object identifiers.

The **ct-SignedCryptedData** defined in clause 7 is an example.

## 7 Signcryption

The **SigncryptData** uses the signcryption technique defined in ISO/IEC 29150. The signcryption technique simultaneously signs and encrypts the data to achieve origin authentication, data integrity and confidentiality. Signcryption can be used in CMS in four different modes:

- signcrypted-content**: content of any type or format is signcrypted using the signcryption algorithm;
- signcrypted-attributes**: content of any type or format and a collection of attributes of any type or format are together signcrypted;
- signcrypted-components**: elements of content of any type or format are signcrypted for one or more message recipients using the public-private keys of the sender and the public key of each recipient.