# ISO/IEC 24824-4:2021-03 (E)

## Information technology - Generic applications of ASN.1 - Part 4: Cryptographic message syntax

## Contents


Page

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 CMSCKMKeyManagement ... 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