ISO/IEC 9594-12:2025-05 (E)

Information technology - Open systems interconnection - Part 12: The Directory: Key management and public-key infrastructure establishment and maintenance

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 Recommendations 2
2.4 International Standards 2
2.4 Additional references 2

3 Definitions 2
3.1 Terms defined elsewhere 2
3.2 Terms defined in this Recommendation | International Standard 3

4 Abbreviations 4

5 Conventions 6

6 Cybersecurity considerations for communication networks 6
6.1 The challenge of large information and communication technology (ICT) networks 6
6.2 Connection-mode communication 7
6.2.1 General 7
6.2.2 Association establishment phase 8
6.2.3 Data transfer phase 8
6.2.4 Association termination phase 8
6.3 Security services 8

7 Overview of cryptographic algorithms 10
7.1 Introduction 10
7.2 Formal specification of cryptographic algorithms 10
7.3 Security properties of crypto graphic algorithms 11
7.4 Security strength 11
7.5 One-way functions 12
7.6 Random number generation and entropy 12

8 Symmetric-key algorithms 13
8.1 General 13
8.2 Symmetric key encryption 13
8.3 Authenticated encryption with associated data (AEAD) 13
8.4 Symmetric key requirements 14

9 Hash algorithms 14

10 Public key and asymmetric cipher 15
10.1 Public-key cryptography 15
10.2 Asymmetric cipher 15

11 Public key and digital signature algorithms 16
11.1 General 16

12 Key establishment algorithms 17

13 Integrity check value (ICV) algorithms 17

14 Post-quantum cryptography considerations 17
14.1 General considerations 17
14.2 Crypto agility 18
14.3 Quantum computers and cryptographic algorithm migration 18
14.4 Possible attacks by use of quantum computers 18

14.4.1 Symmetric cryptographic algorithms ... 18
14.4.2 Asymmetric cryptographic algorithms ... 18
14.5 Mathematic behind post-quantum cryptography ... 19
15 Hardware security modules ... 19
16 Public-key infrastructure establishment ... 21
17 Public-key certificates ... 21
17.1 General ... 21
17.2 The identity and role of the certification authority ... 21
17.3 Distinguished name considerations ... 21
17.4 Content of the basic structure of a public-key certificate ... 22
17.4.1 General ... 22
17.4.2 Version component ... 23
17.4.3 Serial number component ... 23
17.4.4 Signature component ... 23
17.4.5 Issuer component ... 23
17.4.6 Validity component ... 23
17.4.7 Subject component ... 24
17.4.8 Subject public-key information ... 24
17.4.9 Issuer unique ID and subject unique ID ... 25
17.5 Extensions for public-key certificates ... 25
17.5.1 Some considerations on extensions to public-key certificates and other data types ... 25
17.5.2 Basic constraints extension ... 25
17.5.3 Key usage extension ... 25
17.5.4 Subject alternative name extension ... 26
17.5.5 Authority information access extension ... 26
17.5.6 Authority key identifier extension ... 26
17.5.7 Subject key identifier extension ... 26
17.5.8 No revocation information available extension ... 26
17.5.9 Subject alternative public-key info extension ... 26
17.5.10 Alternative signature algorithm extension ... 27
17.5.11 Alternative signature value extension ... 27
17.5.12 Subject directory attribute extension type ... 27
17.7 Chaining of public-key certificates ... 27
17.7.1 Name chaining ... 27
17.7.2 Key identifier chaining ... 28
18 Certificate life-cycle management ... 29
18.1 General ... 29
18.2 Validity of certificates to be installed or reviewed ... 29
18.3 Local policy with respect to invalid certificates ... 29
19 Machine identity and machine-to-machine communication ... 30
20 Trust establishment ... 30
20.1 General ... 30
20.2 Single public-key infrastructure domain ... 30
20.3 Trust establishment between two public-key infrastructure domains ... 31
20.4 A worldwide federated public-key infrastructure ... 32
20.5 Trust anchor compromise ... 32
21 PKI configurations ... 33
21.1 Introduction ... 33
21.2 Public-key infrastructure (PKI) components ... 33
22 PKI establishment ... 34
22.1 Human resources ... 34
22.1.1 Public-key infrastructure knowledge ... 34
22.1.2 Cryptographic algorithm knowledge ... 34
22.2 IETF public-key infrastructure specifications ... 34
22.2.1 Enrolment over Secure Transport (EST) ... 34
22.2.2 Internet X.509 PKI Certificate Management Protocol (CMP) ... 34
22.2.3 Certificate Management over CMS (CMC) ... 35

23 Revocation of public-key certificates 35
23.1 Certificate revocation lists (CRLs) 35
23.2 Online certificate status protocol (OCSP) 35

Annex A Cryptographic primitives 36
A.1 Block cipher algorithms 36
A.1.1 Block cipher functions and block cipher operation modes 36
A.1.2 Feistel cipher structure 36
A.1.3 Advanced encryption standard 38
A.1.4 ShāngMi 4 (SM4) block cipher algorithm 43
A.1.5 Operation modes for block cipher symmetric-key algorithms 46
A.2 Authenticated encryption with associated data (AEAD) algorithms 51
A.2.1 General 51
A.2.2 Galois/counter mode (GCM) 51
A.2.3 Counter with CBC-MAC (CCM) 53
A.3 Cryptographic hash algorithms 55
A.3.1 General 55
A.3.2 Merkle-Damgaard construction 56
A.3.3 The SHA-2 series of hash algorithms 58
A.3.4 The Keccak (sponge) algorithms 59
A.3.5 SHA-3 series of hash algorithms 61
A.3.6 ShāngMi 3 (SM3) hash algorithm 62
A.4 The RSA crypto system 63
A.4.1 General about the RSA crypto system 63
A.4.2 Key generation 63
A.4.3 Security considerations 64
A.5 Asymmetric encryption 64
A.5.1 General 64
A.5.2 RSA asymmetric cipher 64
A.6 Public-key algorithms including digital signature algorithms 65
A.6.1 General 65
A.6.2 The RSA digital signature system 66
A.6.3 The DSA public-key algorithm 67
A.6.4 The elliptic curve digital signature algorithms (ECDSA) 67
A.6.5 SM2 algorithm 70
A.6.6 The Edwards-curve digital signature algorithms 70
A.7 Key establishment algorithms 72
A.7.1 Introduction 72
A.7.2 RSA symmetric key encapsulation 73
A.7.3 The Diffie-Hellman key agreement method 73
A.7.4 Key derivation function 75
A.8 Integrity check value (ICV) algorithms 76
A.8.1 Introduction 76
A.8.2 Keyed-hash message authentication code (HMAC) 76
A.8.3 Cipher-based message authentication code (CMAC) 76
A.8.4 Keccak message authentication code (KMAC) 77
A.8.5 Galois message authentication code (GMAC) algorithm 78

Annex B Basic mathematic concepts for cryptographic algorithms 80
B.1 Introduction to basic mathematic 80
B.1.1 Scope of annex 80
B.1.2 The prime number, the semiprime and the coprime number concepts 80
B.1.3 Greatest common divisor 80
B.1.4 The logarithm concept 80
B.1.5 Operations on matrices 80
B.1.6 Least common multiple 81
B.1.7 Bitwise logical operations 81
B.1.8 Bit masking 82
B.2 Modular arithmetic 82
B.3 Group theory 83
B.3.1 Introduction 83

B.3.2 Notation 84
B.3.3 Additive group of integers 84
B.3.4 Multiplicative group of integers 84
B.3.5 Cyclic groups 85
B.3.6 The discrete logarithm problem 85
B.3.7 Generalized discrete logarithm problem 86
B.3.8 Subgroup 86
B.3.9 Order of group and order of element 86
B.3.10 Ways to resolve or attack the discrete logarithm problem 86
B.4 Finite fields (Galois field) 87
B.4.1 General 87
B.4.2 Prime fields 87
B.4.3 Binary fields GF(2^m) 88
B.5 Overview of Elliptic curve cryptography 89
B.5.1 Reasons for using elliptic curve cryptography 89
B.5.2 Overview of polynomial forms for defining elliptic curves 90
B.5.3 Variants of the Weierstrass form 90
B.5.4 The Montgomery form 90
B.5.5 The twisted Edwards curves 90
B.6 Elliptic curve cryptography for short-Weierstrass form 90
B.6.1 Definition of curves based on the Weierstrass form 90
B.6.2 Defining group over elliptic curve 92
B.7 Montgomery elliptic curve cryptography 95
B.7.1 Introduction 95
B.7.2 Curve25519 and Ed25519 95
B.7.3 Curve448 and Ed448 95
B.7.4 The Montgomery curves 95
B.7.5 The Edwards curves 96
B.8 Conversion techniques 96
B.8.1 General 96
B.8.2 Bit string-to-integer conversion and binary length of integer 96
B.8.3 Integer-to-bit string conversion 96
B.8.4 Octet string to integer conversion 96
B.8.5 Integer-to-octet string conversion 96
B.8.6 Bitstring-to-octet string conversion 96
B.9 Miscellaneous formulae 97
B.9.1 Introductions 97
B.9.2 The Euclidean algorithm 97
B.9.3 The extended Euclidean algorithm 97
B.9.3 Fermat's little theorem 98
B.9.4 Lagrange's theorem 98
B.9.5 Euler's phi function 98
B.10 Endianness (big endian vs. little endian) 98
B.11 Selected attacks on cryptographic algorithms 98
B.11.1 Side-channel attack 98
B.11.2 Square root attack 99
Annex C Alphabetical list of cryptographic concepts and definitions 100
Bibliography 101