الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

National Cryptographic Standards

(NCS-2:2025)

Public Consultation

TLP: White

Document Classification: Public

Disclaimer: Please refer to the National Cybersecurity Authority's website (https://nca.gov.sa), to obtain the latest version of this document.

Public Consultation

Disclaimer: The following cryptographic standards document will be governed by and implemented in accordance with the laws of the Kingdom of Saudi Arabia, and must be subject to the exclusive jurisdiction of the courts of the Kingdom of Saudi Arabia. Therefore, the Arabic version will be the binding language for all matters relating to the meaning or interpretation of this document.

In the Name of Allah,
The Most Gracious,
The Most Merciful

Traffic Light Protocol (TLP):

This marking protocol is widely used around the world. It has four colors (traffic lights):

Red (Personal, Confidential, and for the Intended Recipient Only)

The recipient has no right to share the information with any person outside the defined range of recipients, either inside or outside the entity, beyond the scope specified for receipt.

Amber+ Strict

The recipient may share the information only within the entity.

Amber (Restricted Sharing)

The recipient may share the information within the entity only or with recipients who are required to take action related to the shared information outside the entity, based on a need-to-know basis.

Green – Sharing within the Same Community

The recipient may share information with other recipients inside the entity or outside it within the same sector or with a related entity. However, it is not allowed to exchange or publish this information on public channels.

Clear (No Restrictions)

The recipient may share information to the world.

Public Consultation

Update and Review

This version of the document (NCS-2:2025) supersede previous versions (NCS-1:2020). NCA periodically reviews and updates the NCS as per the evolving cryptographic requirements and related industry updates. The latest released version of the NCS supersedes all previous versions. NCA will communicate and publish the updated version of NCS.

Document Versions

Version	Year of Issuance	Updates
NCS - 1	2020	1st version
NCS - 2	2025	2nd version Appendix (G) illustrates the updates on the previous version.

Public Consultation

Table of Contents

Update and Review 5
Document Versions 5
Table of Contents 6
Executive Summary 8
1- **Introduction** 9
1-1 Scope 9
1-2 Levels of Cryptographic Standards 9
1-3 Structure of the Document 10
2- **Cryptographic Primitives** 12
2-2 Block Cipher Algorithms 12
2-3 Hash Functions 13
2-4 Classical Asymmetric Algorithms 13
2-5 Post-Quantum Algorithms 14
2-6 Lightweight Crypto Algorithms 15
3- **Cryptographic Schemes** 16
3-1 Block Cipher Modes of Operation 16
3-2 Authenticated Encryption with Associated Data (AEAD) 16
3-3 Message Authentication Codes (MACs) 17
3-4 Key Wrap Functions 17
3-5 Key Derivation Functions (KDFs) 18
3-6 Key Agreement and Key Transport 18
3-7 Integrated Encryption Schemes 19
3-8 Digital Signatures 19
3-9 End-to-End Encryption (E2EE) Schemes ٢٠
4- **Commonly Used Cryptographic Protocols** 21
4-1 IP Security (IPsec) 21
4-2 Transport Layer Security (TLS) 22
4-3 DNSSEC (Domain Name System Security) 22
4-4 Secure Shell (SSH) 23
4-5 Bluetooth 23
4-6 Universal Mobile Telecommunications Service (UMTS) / Long Term Evolution (LTE) / 5G 23
4-7 WPA (Wi-Fi Protected Access) 24
4-8 Kerberos Protocol 24
5- **Public Key Infrastructure (PKI)** 25
5-1 Algorithms for Certificates 25
5-2 Validity of the Certificates 25
6- **Key Lifecycle Management (KLM)** 26
6-1 Key Lifetime 26

Public Consultation

6-2 KLM Processes 26
6-2-1 Key Generation 26
6-2-2 Key Registration and Certification 26
6-2-3 Key Distribution and Installation 26
6-2-4 Key Use 27
6-2-5 Key Storage 27
6-2-6 Key Revocation and Validation 27
6-2-7 Key Archival 27
6-2-8 Key Destruction 28
6-2-9 Key Accounting 28
6-2-10 Key Recovery 28
7- Random Number Generators (RNGs) 29
8- Quantum Key Distribution (QKD) 30
9- Appendices 31
A Privacy Enhancing Cryptography 31
B. Side-Channel Attacks 32
C. Attribute-based Cryptography 33
D. Identity-based Cryptography 33
E. Terms and Definitions 34
F. Abbreviations 40
G. List of Changes 42

List of Tables

Table 1: Terms and Definitions 34
Table 2: List of Abbreviations 40
Table 3: List of Changes 42

List of Figures

Figure 1: NCS Subdomain 11

Public Consultation

Executive Summary

As per the mandate of the National Cybersecurity Authority (NCA) that was issued by the Royal Order number 6801, dated October 31, 2017, the NCA is mandated to draft the national cryptographic policies and standards, to ensure compliance with these standards and policies, and to review and update them periodically.

From this perspective, the NCA has reviewed and updated National Cryptographic Standards (NCS-1:2020). Therefore, this version of the document (NCS-2:2025) write off and supersede previous version.

(NCS-2:2025) prescribes the minimum acceptable cryptographic requirements for civilian and commercial purposes to protect national data, systems and networks. This document highlights the details of the national cryptographic standards, which are composed of two strength levels: MODERATE and ADVANCED.

This document includes the accepted symmetric and asymmetric primitives including Post-Quantum Cryptography, symmetric and asymmetric schemes, some of the accepted commonly used cryptographic protocols, Public Key Infrastructure (PKI), Key Lifecycle Management (KLM), Random Number Generators (RNGs) and Quantum Key Distribution (QKD). It further presents appendices that include some considerations regarding Privacy Enhancing Cryptography, Side-Channel Attacks, Identity and Attribute-based Cryptography.

Public Consultation

1- Introduction

1-1 Scope

The National Cryptographic Standards (NCS - 2: 2025) defines the minimum cryptography requirements to be met by national entities when using cryptography to protect data (in use, at rest and in transit), systems and networks for civilian or commercial purposes.

This cryptographic standards document is built with consideration of current and foreseeable advancements in the affordable computational power. The document encompasses cryptography primitives, schemes, commonly used cryptographic protocols, Public Key Infrastructure (PKI), Key Lifecycle Management (KLM), Random Number Generators (RNGs) and Quantum Key Distribution (QKD).

While this document prescribes the minimum acceptable cryptographic requirements, meticulous implementation of these requirements is crucial to avoid implementation-based vulnerabilities.

1-2 Levels of Cryptographic Standards

The NCS defines two strength levels for cryptographic standards: MODERATE level and ADVANCED levels. Having two strength levels provides more flexibility to choose the appropriate level of protection for different classes of data, systems and networks. Each national entity is required to choose and implement the appropriate cryptographic standard level based on the nature and sensitivity of the data, systems and networks to be protected. Furthermore, other cybersecurity regulations, issued by NCA, may mandate the use of a particular cryptographic standard level to protect data, systems and networks. The MODERATE and ADVANCED strength levels are designed to target 128-bit and 256-bit security levels, respectively. Specific requirements for each strength level are specified throughout this document. If the target security level is ADVANCED, all cryptosystems must satisfy the ADVANCED level, while If the target security level is MODERATE, all cryptosystems must either satisfy MODERATE or ADVANCED levels. Any requirement not specifically associated with one of these two strength levels applies equally to both. The security level of a cryptosystem is based on the lowest cryptographic security level of any cryptographic component.

Public Consultation

1-3 Structure of the Document

The rest of this document is organized as follows. Section 2 lists the accepted symmetric and asymmetric primitives with their key, block and initialization vector sizes, and includes the post-quantum key encapsulation mechanisms and signature algorithms. Section 3 provides the accepted symmetric and asymmetric schemes: block cipher modes of operation, MAC, AEAD, key wrap functions, key derivation functions, key agreement, key transport, integrated encryption , public key signatures and End-to-End Encryption (E2EE) Schemes. Section 4 provides requirements for the commonly used cryptographic protocols such as DNS Security (DNSSEC), IP Security (IPsec), Bluetooth, SSH, TLS, UMTS/LTE/5G, WPA and Kerberos. Section 5 provides a list of the accepted algorithms for certificates and the validity of the certificates. Section 6 provides the requirements for the key lifecycle to ensure that keys are managed properly from the moment they are generated until their destruction, and their usage is standardized across processes. Section 7 provides the minimum requirements that must be met when using Random Number Generators (RNGs). Section 8 provides requirements for Quantum Key Distribution (QKD). Finally, Section 9 provides appendices that present some information about privacy enhancing cryptography, side-channel attacks, attributes-based cryptography, definitions and abbreviations. **Error! Reference source not found.**) shows the main components and sub-components of the National Cryptographic Standards.

Public Consultation

2- Cryptographic Primitives	2-1	Stream Cipher Algorithms	2-2	Block Cipher Algorithms
	2-3	Hash Functions	2-4	Classical Asymmetric Algorithms
	2-5	Post-Quantum Algorithms	2-6	Lightweight crypto Algorithms
3. Cryptographic Schemes	3-1	BLOCK CIPHER MODES OF OPERATION	3-2	AUTHENTICATED ENCRYPTION WITH ASSOCIATED DATA (AEAD)
	3-3	MESSAGE AUTHENTICATION CODES (MACS)	3-4	KEY WRAP FUNCTIONS
	3-5	KEY DERIVATION FUNCTIONS (KDFs)	3-6	Key Agreement And Key Transport
	3-7	INTEGRATED ENCRYPTION SCHEME	3-8	Digital Signatures
	3-9	End-to-End Encryption (E2EE) Schemes		
4- Commonly Used Protocols	4-1	IP Security (IPsec)	4-2	TRANSPORT LAYER SECURITY (TLS)
	4-3	Domain Name System Security (DNSSEC)	4-4	Secure Shell (SSH) Bluetooth
	4-5	Bluetooth	4-6	Universal Mobile Telecommunications Service (UMTS) / Long Term Evolution (LTE) / 5G
	4-7	WPA (Wi-Fi Protected Access)	4-8	KERBEROS Protocol
5- Public Key Infrastructure (PKI)	5-1	Algorithms For Certificates	5-2	Validity Of The Certificates
6-Key Lifecycle Management	6-1	Key Protection and Lifetime	6-2	KLM Processes
7- Random Number Generators (RNGs)	7-1	Acceptable Random Number Generators (RNGs)	7-2	Pseudorandom Number Generators (PRNGs)
	7-3	RNGs Random Seed	7-4	Reseeding
	7-5	Random Number Generators (RNGs) Statistical Testing		
8- Quantum Key Distribution (QKD)	8-1	QKD Implementation	8-2	Quantum Bit-Error Rate (QBER)
	8-3	QKD Protection	8-4	Technical Limitations
	8-5	Compliance with Quantum Key Distribution (QKD) Standards		

FIGURE 1: NCS SUBDOMAIN

2- Cryptographic Primitives

2-1 Stream Cipher Algorithms

Accepted stream cipher algorithms:

2-1-1 SNOW 2.0 as in ISO/IEC 18033-4

2.1.1.1 128-bit key length for MODERATE.

2.1.1.2 256-bit key length for ADVANCED.

2-1-2 SOSEMANUK[1] as in eSTREAM project

2-1-2-1 128-bit and 256-bit key length for MODERATE.

2-1-2-2 Not accepted for ADVANCED.

2-1-3 The following requirements must be met for the above stream ciphers:

2-1-3-1 Initialization vector (IV) must be at least 128 bits.

2-1-3-2 IV must be unique for every encryption under the same key.

2-1-3-3 The key must not be used to encrypt more than 2^{64} bits.

2-1-3-4 Valid decryption must never be relied upon for message authentication.

2-2 Block Cipher Algorithms

Accepted block cipher algorithms:

2-2-1 Advanced Encryption Standards (AES) as in FIPS-197

2-2-1-1 128-bit and 192-bit key lengths for MODERATE.

2-2-1-2 256-bit key length for ADVANCED.

2-2-2 Camellia as in ISO/IEC 18033-3

2-2-2-1 128-bit and 192-bit key lengths for MODERATE.

2-2-2-2 256-bit key length for ADVANCED.

2-2-3 Serpent[2]

[1] C. Berbain et al. "Sosemanuk, a Fast Software-Oriented Stream Cipher." In: Robshaw M., Billet O. (eds.) New Stream Cipher Designs. LNCS 4986. Springer, 2008.

[2] E. Biham, R. Anderson, and L. Knudsen. SERPENT: A new block cipher proposal. In Fast Software Encryption - FSE'98, volume 1372 of Lecture Notes in Computer Science, pages 222–238. Springer-Verlag, 1998.

Public Consultation

2-2-3-1 128-bit and 192-bit key lengths for MODERATE.

2-2-3-2 256-bit key length for ADVANCED.

2-3 Hash Functions

Accepted hash functions are:

2-3-1 Secure Hash Algorithm-2 (SHA-2)[3]

2-3-1-1 SHA2-256, SHA2-384 and SHA2-512/256 for MODERATE, taking into consideration the risk of length extension attacks.

2-3-1-2 SHA2-512 for ADVANCED[4], taking into consideration the risk of length extension attacks.

2-3-2 Secure Hash Algorithm-3 (SHA-3)

2-3-2-1 SHA3-256, SHA3-384 and SHAKE128 for MODERATE.

2-3-2-2 SHA3-512 and SHAKE256 for ADVANCED.

2-3-3 The following requirements must be met

2-3-3-1 For SHAKE128, the output size "d" value must be ≥ 256 bits.

2-3-3-2 For SHAKE256, the output size "d" value must be ≥ 512 bits.

2-4 Classical Asymmetric Algorithms

Accepted Asymmetric Algorithms:

2-4-1 RSA

2-4-1-1 At least 3072 bits for the modulus "n" and "e" value > 65537 for MODERATE

2-4-1-2 Not accepted for ADVANCED

2-4-1-3 Strong Primes must be used, as defined in Appendix (E).

2-4-2 Diffie-Hellman and Finite Field

2-4-2-1 At least 3072 bits for the modulus "p" and 256 bits of entropy for the private keys for MODERATE.

2-4-2-2 Not accepted for ADVANCED.

2-4-2-3 Safe Primes must be used, as defined in Appendix (E).

[3] SHA2-256, SHA2-384, SHA2-512/256 and SHA2-512 are sometimes written as SHA-256, SHA-384, SHA-512/256 and SHA-512, respectively.

[4] SHA-384 is accepted whenever any other accepted hash function for ADVANCED cannot be implemented, taking into consideration the residual risk.

Public Consultation

2-4-3 Elliptic Curve

2-4-3-1 Curves NIST P-256, NIST P-384, BrainpoolP256r1, BrainpoolP384r1, Curve25519 for MODERATE.

2-4-3-2 Curves NIST P-521, Curve448[5] and BrainpoolP512r1 for ADVANCED.

2-5 Post-Quantum Algorithms

The accepted post quantum algorithms:

2-5-1 ML-KEM as in FIPS 203

2-5-1-1 ML-KEM-512 and ML-KEM-768 for MODERATE.

2-5-1-2 ML-KEM-1024 for ADVANCED.

2-5-2 Classic McEliece for KEM

2-5-2-1 mceliece348864, mceliece460896 for MODERATE

2-5-2-2 mceliece6688128, mceliece6960119 and mceliece8192128 for ADVANCED.

2-5-3 ML-DSA as in FIPS 204

2-5-3-1 ML-DSA-44 and ML-DSA-65 for MODERATE.

2-5-3-2 ML-DSA-87 for ADVANCED.

2-5-4 SLH-DSA as in FIPS 205

2-5-4-1 SLH-DSA-SHA2-128s, SLH-DSA-SHAKE[6]-128f, SLH-DSA-SHA2-192s and SLH-DSA-SHAKE-192f for MODERATE.

2-5-4-2 SLH-DSA-SHA2-256s AND SLH-DSA-SHAKE-256f for ADVANCED.

2-5-4-3 In all cases, key pairs should not be used to sign more than 2^{64} messages.

2-5-5 PQC cryptosystems must satisfy the following requirements:

2-5-5-1 A post-quantum cryptosystem must be used in hybrid with approved classical cryptosystems.

2-5-5-2 All cryptographic system or solutions must support PQC algorithms.

Public Consultation

[5] Curve448 is accepted for ADVANCED even though it operates at 224-bit security level because of its increased performance, resistance to a wide-range of side channel attacks and ease of implementation.

[6] Using SHAKE128 or SHAKE256 with output size less than what is specified in section 2.3 is accepted as an exception for PQC algorithms only and as specified in FIPS 203, FIPS 204 and FIPS 205.

2-6 Lightweight Crypto Algorithms

Accepted lightweight algorithms (on limited systems with constrained resources, where the use of conventional cryptographic standards is not acceptable):

2-6-1 Block ciphers as in ISO/IEC 29192-2

- 2-6-1-1 PRESENT, 80-bit or 128-bit key lengths.
- 2-6-1-2 CLEFIA, 128-bit, 192-bit or 256-bit key lengths.

2-6-2 Stream ciphers as in ISO/IEC 29192-3

- 2-6-2-1 Enocoro, 80-bit or 128-bit key lengths.
- 2-6-2-2 Trivium, 80-bit key length.

2-6-3 Asymmetric mechanisms as in ISO/IEC 29192-4

- 2-6-3-1 Unilateral authentication mechanisms.
- 2-6-3-2 ALIKE key exchange.
- 2-6-3-3 Identity-based signature.

2-6-4 Hash functions as in ISO/IEC 29192-5

- 2-6-4-1 PHOTON, 80-bit, 128-bit, 160-bit, 224-bit or 256-bit output sizes.
- 2-6-4-2 SPONGENT, 88-bit, 128-bit, 160-bit, 224-bit or 256-bit output sizes.
- 2-6-4-3 Lesamnta-LW, 256-bit output size.

2-6-5 Message Authentication Code (MAC) as in ISO/IEC 29192-6

- 2-6-5-1 Tsudik's keymode, hash-based.
- 2-6-5-2 Chaskey12, 128-bit key length.

2-6-6 Authenticated encryption with associated data (AEAD)

- 2-6-6-1 Ascon, 128-bit or 160-bit.

Public Consultation

3- Cryptographic Schemes

The cryptographic schemes must be used with the accepted cryptographic primitives as in Section 2.

3-1 Block Cipher Modes of Operation

The accepted block cipher modes of operation are:

3-1-1 Counter Mode (CTR), which could also be used as a stream cipher (refer to the requirements in 2.1.3), as in NIST SP 800-38A and RFC 3686.

3-1-2 Cipher Block Chaining (CBC) as in NIST SP800-38A for MODERATE only.

3-1-3 Output Feedback (OFB) as in NIST SP 800-38A.

3-1-4 Cipher Feedback (CFB) as in NIST SP 800-38A.

3-1-5 For the above modes of operation, a key must not be used for more than 2^{32} blocks of data, and IV/nonce must be random for every encryption under the same key.

3-1-6 XEX Tweakable Block Cipher with Ciphertext Stealing (XTS). XTS is limited to encrypt data at rest only (Disk Encryption), as in NIST SP 800-38E, with the maximum size of data unit encrypted with a single key must not exceed 2^{20} blocks.

3-2 Authenticated Encryption with Associated Data (AEAD)

The accepted AEAD are:

3-2-1 Galois Counter Mode (GCM) as in NIST SP 800-38D, with the following requirements:

3-2-1-1 At least 128-bit for Initialization Vector (IV)/nonce length.

3-2-1-2 IV/nonce must be unique for every encryption under the same key.

3-2-1-3 At least 128-bit for tag length.

3-2-1-4 A key must not be used for more than 2^{64} blocks of data.

3-2-2 Counter with CBC-MAC (CCM) as in NIST SP 800-38C.

3-2-2-1 IV/nonce must be unique for every encryption under the same key.

3-2-2-2 At least 128-bit for tag length.

3-2-2-3 A key must not be used for more than 2^{61} invocations[7] of the block cipher algorithm.

[7] Here, an invocation is a complete run of the underlying block cipher algorithm (e.g. AES).

Public Consultation

3-3 Message Authentication Codes (MACs)

The accepted message authentication codes are (considering that the length of the key should at least match the target security level):

3-3-1 Hash-based MAC (HMAC) as in FIPS PUB 198-1.

3-3-1-1 The tag and key lengths must at least match the target security level (for MODERATE or ADVANCED).

3-3-1-2 To be used with accepted hash functions as mentioned in Sub-Section 2-3.

3-3-2 Cipher-based MAC (CMAC) as in NIST SP 800-38B.

3-3-2-1 The key length must at least match the target security level (for MODERATE or ADVANCED).

3-3-2-2 A key must not be used for more than 2^{48} message blocks.

3-3-2-3 Used only in applications where no party learns all-0 string enciphering in the block cipher underlying the MAC.

3-3-2-4 At least 128-bit for tag length.

3-3-3 KECCAK Message Authentication Code (KMAC) as in NIST SP 800-185.

3-3-3-1 The tag and key lengths must at least match the target security level (for MODERATE or ADVANCED).

3-3-3-2 To be used with customizable Secure Hash Algorithm with KECCAK (cSHAKE128 and cSHAKE256) based on the target security level (for MODERATE or ADVANCED).

3-3-4 GMAC as in NIST SP 800-38D.

3-3-4-1 The key length must at least match the target security level (for MODERATE or ADVANCED).

3-3-4-2 At least 128-bit for Initialization Vector (IV)/nonce length.

3-3-4-3 At least 128-bit for tag length.

3-3-4-4 A key must not be used for more than 2^{64} blocks of data.

3-4 Key Wrap Functions

The accepted key wrap functions are:

3-4-1 Key Wrap (KW) as in NIST SP 800-38F.

3-4-2 Key Wrap with Padding (KWP) as in NIST SP 800-38F.

Public consultation

3-5 Key Derivation Functions (KDFs)

The accepted key derivation functions are:

3-5-1 RFC 5869 (HKDF)[8].

3-5-2 IKE-v2-KDF[8].

3-5-3 TLS-v1.2-KDF[8].

3-5-4 X9.63-KDF[8].

KDF must comply with one of the following:

3-5-5 NIST SP-800-56 A/B KDF (Single Step)[8].

3-5-6 NIST SP-800-56 C KDF (Extract-then-expand)[8].

3-5-7 NIST SP-800-108[8].

3-5-8 NIST SP-800-135.

3-6 Key Agreement and Key Transport

Accepted key exchange schemes:

3-6-1 RSA Key Establishment as in NIST 800-56B

- 3-6-1-1 At least 3072 bits for key length for MODERATE.
- 3-6-1-2 Not accepted for ADVANCED.

3-6-2 Diffie-Hellman (DH) as in RFC 3526:

- 3-6-2-1 At least 3072 bits for key length for MODERATE.
- 3-6-2-2 Not accepted for ADVANCED.

3-6-3 Elliptic Curve Diffie-Hellman (ECDH) as in NIST SP 800-56A:

- 3-6-3-1 Accepted Curves in section 2.4.3 must be used.
- 3-6-3-2 With forward secrecy and authenticated key establishment implementation.

3-6-4 Symmetric key exchange schemes:

- 3-6-4-1 Symmetric key agreement scheme must rely solely on shared long-term secrets.
- 3-6-4-2 All symmetric encryption schemes and primitives can be used as per Section 3 and Section 4.

Public Consultation

[8] European Commission, "eCrypt Algorithms, Key Size and Protocols Report," in eCrypt Algorithms, Key Size and Protocols Report, 2018.

3-6-4-3 Combination of an encryption scheme with a MAC in encrypt-then-MAC mode.

3-6-4-4 All keys must be wrapped using the accepted key wrapping functions in section 3.4.

3-7 Integrated Encryption Schemes

Accepted integrated encryption schemes:

3-7-1 Elliptic Curve Integrated Encryption Scheme (ECIES) For MODERATE and ADVANCED.

3-7-2 Discrete Logarithm Integrated Encryption Scheme (DLIES) for MODERATE only.

3-7-3 RSA with Optimal Asymmetric Encryption Padding (RSA-OAEP) as in PKCS #1 v2.1: RSA for MODERATE only.

3-8 Digital Signatures

Accepted digital signatures:

3-8-1 Digital Signature Algorithm (DSA) as in FIPS PUB 186-4

3-8-1-1 At least 3072 bits for modulus key for MODERATE.

3-8-1-2 Not accepted for ADVANCED.

3-8-2 Elliptic Curve Digital Signature Algorithm (ECDSA) and Edwards-curve Digital Signature Algorithm (EdDSA) as in FIPS PUB 186-5

3-8-2-1 Accepted Curves in section 2.4.3 must be used.

3-8-3 RSA signatures

3-8-3-1 RSA-PSS and RSA Digital Signature Scheme (RSA-DS2) are accepted[9,10].

3-8-3-2 Modulus lengths of 3072 bits for MODERATE.

3-8-3-3 Not accepted for ADVANCED.

Public consultation

[9] PKCS, "RSA Cryptographic Standard. Version 2.2," 2012.

[10] ISO, "ISO/IEC 9796-2-2010. Information technology - Security techniques - Digital Signature Schemes. Part 2: Integer Factorization based mechanisms.," 2010.

3-8-4 Merkle signatures

3-8-4-1 Accepted hash functions described in Section 2 must be used.

3-8-4-2 The required pseudo-random function family must be constructed with the HMAC construction based on the hash function used.

3-9 End-to-End Encryption (E2EE) Schemes

3-9-1 E2EE schemes must ensure that encryption and decryption occur exclusively within the authorized endpoints.

3-9-2 Plaintext and keying material must not be accessible to any intermediate system, relay, or server.

3-9-3 E2EE schemes must provide forward secrecy by means of ephemeral key exchange.

3-9-4 E2EE schemes must provide a way for endpoints to authenticate each other's identity, either through the use of certificates, authenticated public keys or pre-shared secrets.

3-9-5 E2EE schemes must allow the users to independently verify the established session keys, e.g., using out-of-band verification.

Public Consultation

4- Commonly Used Cryptographic Protocols

In the following, a list of commonly used cryptographic protocols is presented along with accepted requirements. Any protocols that are not listed here must follow the accepted primitives and/or schemes in Section 2 and Section 3. In addition, future versions of protocols listed below will be accepted if they follow the accepted primitives and/or schemes in Section 2 and Section 3.

4-1 IP Security (IPsec)

Accepted algorithms for IPsec:

To provide authentication only, can use one of the following suites[11]:

4-1-1 For MODERATE:

ENCR_NULL_AUTH_AES_GMAC_128,
AUTH_HMAC_SHA2_256_128,
AUTH_HMAC_SHA2_384_192,
AUTH_HMAC_SHA3_256_128 and
AUTH_HMAC_SHA3_384_192.

4-1-2 For ADVANCED:

ENCR_NULL_AUTH_AES_GMAC_256 ,
AUTH_HMAC_SHA2_512_256 and
AUTH_HMAC_SHA3_512_256.

To add confidentiality, Encapsulating Security Payload (ESP) is required by using one of the above MAC algorithms and one of the following encryption algorithms[12]:

4-1-3 ENCR_AES_CTR,
ENCR_CAMELLIA_CTR.

As an alternative, authenticated encryption can be used from the following modes[12]:

4-1-4 ENCR_AES_CCM_12,
ENCR_AES_CCM_16,
ENCR_CAMELLIA_CCM_12,
ENCR_CAMELLIA_CCM_16,
ENCR_AES_GCM_12,
ENCR_AES_GCM_16.

[11] Authentication Header (AH) should not be implemented or deployed.

[12] European Union Agency for Network and Information Security "Study on cryptographic protocols," 2014.

Public consultation

4-2 Transport Layer Security (TLS)

Accepted TLS versions:

4-2-1 It is acceptable to use TLS version 1.2 cipher suites with the strongest cryptographic primitives and schemes to ensure compatibility and implementing a configuration that does not allow downgrading[13].

4-2-2 While the transition to the new TLS 1.3 standard will take some additional time, it is recommended to be used.

Accepted cipher suites for TLS 1.2:

4-2-3 The following cipher suites accepted for MODERATE:

TLS_ ECDHE_ECDSA_WITH_AES_128_CBC[14]_ SHA2_256,

TLS_ ECDHE_ECDSA_WITH_AES_256_CBC[14]_SHA2_384,

TLS_ ECDHE_ECDSA_WITH_AES_128_GCM_SHA2_256,

TLS_ ECDHE_ECDSA_WITH_AES_128_CCM,

TLS_ ECDHE_ECDSA_WITH_AES_128_CCM_8,

TLS_ ECDHE_RSA_WITH_AES_128_ CBC[14]_SHA2_256,

TLS_ ECDHE_RSA_WITH_AES_256_ CBC[14]_SHA2_384,

TLS_ ECDHE_RSA_WITH_AES_128_GCM_ SHA2_256,

TLS_ ECDHE_RSA_WITH_AES_256_GCM_SHA2_384,

4-2-4 The following cipher suites accepted for ADVANCED:

TLS_ ECDHE_ECDSA_WITH_AES_256_GCM_SHA2_384,

TLS_ECDHE_ ECDSA _WITH_AES_256_CCM,

TLS_ECDHE_ ECDSA _WITH_AES_256_CCM_8.

Accepted cipher suites for TLS 1.3:

4-2-5 TLS_AES_128_GCM_SHA256 for MODERATE.

4-2-6 TLS_AES_256_GCM_SHA384 for ADVANCED.

4-3 DNSSEC (Domain Name System Security)

Accepted algorithms and schemes for zone data signing:

4-3-1 ECDSA_P256_SHA256 and ED25519 for MODERATE.

[13] E. Ronen, "The 9 Lives of Bleichenbacher's CAT. New Cache Attacks on TLS Implementations.," 2018.

[14] CBC must be used together with the Encrypt_then_MAC extension.

Public consultation

4-3-2 ECDSA_P384_SHA384[15] and ED488 for ADVANCED.

Accepted Message authentication algorithms:

4-3-3 HMAC-SHA384 for MODERATE.

4-3-4 HMAC-SHA512 for ADVANCED.

4-4 Secure Shell (SSH)

The accepted version of SSH is SSH-2 with the following encryption and MAC algorithms:

4-4-1 AEAD_AES_128_GCM for MODERATE.

4-4-2 AEAD_AES_256_GCM for ADVANCED.

4-5 Bluetooth

Accepted Bluetooth versions: 4.1 or higher as in NIST SP 800-121r2 with following requirements:

4-5-1 Use Security Mode 4, Level 4 (Authenticated link key using secure connection).

4-5-2 Use encryption algorithm AES-CCM.

4-5-3 Use secure connection feature with P-256 elliptic curve for link key generation.

4-5-4 Use encryption Mode 3 (all traffic is encrypted).

4-5-5 For low-energy feature of Bluetooth, use version 4.2 or higher with Low-Energy Security Mode 1 Level 4.

4-5-6 Organizations must use the strongest Bluetooth security mode that is available for their devices.

4-6 Universal Mobile Telecommunications Service (UMTS) / Long Term Evolution (LTE) / 5G

Accepted algorithms:

4-6-1 For UMTS, 128-UEA1 and 128-UIA1 must be used.

4-6-2 For LTE, 128-EEA2 and 128-EIA2 must be used.

4-6-3 For 5G, 128-NEA2 and 128-NIA2 or 256-NEA5 and 256-NIA5 must be used.

[15] As 512 bits is not implemented for ECC in this protocol, this is a special case for ADVANCED.

Public consultation

4-6-4 EIA0 and NIA0 can be used in the exceptional case of unauthenticated emergency calls in limited-service mode.

4-6-5 Only the cryptographic primitives and schemes listed in sections 2 and 3 must be used. However, KASUMI and both ECIES profiles are accepted, including the elliptic curves used in the profile, which are accepted as exceptions, solely for use under 3GPP systems.

4-7 WPA (Wi-Fi Protected Access)

Accepted versions:

4-7-1 WPA3-Enterprise

4-8 Kerberos Protocol

Accepted Kerberos encryption types:

4-8-1 CAMELLIA128-CTS-CMAC,
AES256-CTS-HMAC-SHA384 for MODERATE.

4-8-2 CAMELLIA256-CTS-CMAC for ADVANCED.

Public Consultation

5- Public Key Infrastructure (PKI)

5-1 Algorithms for Certificates

Accepted algorithms for Root CA certificates:

5-1-1 RSA

5-1-1-1 At least 4096 bits for key length.

5-1-2 Elliptic Curve Cryptography (ECC)

5-1-2-1 NIST P-384, NIST P-521, Curve448, BrainpoolP384r1 or BrainpoolP512r1

Accepted algorithms for Intermediate and End User certificates:

5-1-3 RSA

5-1-3-1 At least 3072 bits for key length.

5-1-4 ECC

5-1-4-1 NIST P-256, NIST P-384, NIST P-521, Curve25519, Curve448, BrainpoolP256r1, BrainpoolP384r1 or BrainpoolP512r1.

The following requirements must be met:

5-1-5 Certificates, Certificate Revocation Lists (CRLs) and Authority Revocation Lists (ARLs) must comply with X.509 PKI Certificate (RFC 5280).

5-1-6 Accepted hash functions described in Section 2 must be used.

5-1-7 Match the strength of the asymmetric key algorithms with the strength of the hash algorithm.

5-2 Validity of the Certificates

Accepted Root CA certificate validity life span:

5-2-1 At most 20 years[16].

Accepted Intermediate CA, Subordinate CA and Issuing CA certificate validity life span:

5-2-2 At most 10 years[16].

Accepted end user certificate validity life span:

5-2-3 At most 5 years for MODERATE[16].

[16] NIST, "X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework, Federal Public Key Infrastructure Policy Authority," NIST, 2015

Public consultation

5-2-4 At most 3 years for ADVANCED[16].

6- Key Lifecycle Management (KLM)

6-1 Key Lifetime

Accepted key lifetime:

6-1-1 Using Hardware cryptographic modules

6-1-1-1 Validity of private keys must not exceed 5 years (these do not limit CA certificates' lifetime) for MODERATE[17].

6-1-1-2 Validity of private keys must not exceed 3 years (these do not limit CA certificates' lifetime) for ADVANCED[17].

6-1-2 Using Software cryptographic modules

6-1-2-1 Private keys must not be valid longer than 2 years for MODERATE[17].

6-1-2-2 Not accepted for ADVANCED.

6-2 KLM Processes

The Key Lifecycle Management (KLM) requirements are:

6-2-1 Key Generation

6-2-1-1 Keys must be generated using a cryptographic RNG that meet the minimum requirements for RNGs (as described in section 7).

6-2-2 Key Registration and Certification

6-2-2-1 Public keys must be associated with their owners using certificates.

6-2-2-2 Root certificates must be distributed to relying parties and signatories in a secure manner.

6-2-2-3 A national CA that is trusted by the organization must be used based on the approval from the organization of an authorized official.

6-2-3 Key Distribution and Installation

6-2-3-1 Keys must be distributed to their users securely and must be under the users control.

17 NIST, "NIST Special Publication 800-57 Part 1 Revision 4. Recommendation for Key Management Part 1: General. Elaine Barker," 2016.

Public Consultation

6-2-3-2 Keys must be transported securely by protecting their confidentiality and authenticity

6-2-3-3 All copies of keys must be securely installed and stored.

6-2-3-4 Public keys must be transported in an authenticated way using certificates.

6-2-3-5 Private keys must be protected, and their usage must be authorized by the owner or the CA.

6-2-3-6 Keys must be protected, wrapped, authenticated or transported using cryptographic mechanisms that provide a security strength equal to or greater than the strength of the key being protected or the certificate owner's key pair.

6-2-4 Key Use

6-2-4-1 Keys must be protected against unauthorized use during their lifetimes.

6-2-4-2 Keys must be protected against misuse by their owners using secure hardware storage and applying appropriate authorization checks.

6-2-5 Key Storage

6-2-5-1 Organizations must require secure backups of keys (for internal or law enforcement use) when encryption is supported.

6-2-5-2 Keys used for authentication and non-repudiation must be under the sole control of their owners.

6-2-6 Key Revocation and Validation

6-2-6-1 Updated versions of the Certificate Revocation List (CRL) or the Online Certificate Status Protocol (OCSP) must be available to avoid the use of expired and revoked keys.

6-2-6-2 Key validation must be performed by checking the CRL or OCSP servers.

6-2-7 Key Archival

6-2-7-1 Expired or revoked keys must be archived to keep old data accessible when encryption is supported.

6-2-7-2 The archival process must be secured, and confidentiality of the archived keys must be maintained.

6-2-7-3 Archival systems must adhere to required retention periods as per relevant regulations.

Public consultation

6-2-8 Key Destruction

6-2-8-1 When a key expires and there is no need for it to be archived or stored, it must be removed from the hardware via a secure deletion process.

6-2-8-2 Media storage systems storing keys must be sanitized before disposal using a process that is compliant with the relevant regulations released by the National Cybersecurity Authority (NCA).

6-2-9 Key Accounting

6-2-9-1 An accountability mechanism must be defined for asymmetric keys during their lifecycle.

6-2-9-2 Key usage must be monitored.

6-2-9-3 Roles and responsibilities for key management must be documented and approved by the authorizing official.

6-2-10 Key Recovery

6-2-10-1 A recovery procedure for keys must be documented and approved by the authorizing official.

Public Consultation

7- Random Number Generators (RNGs)

The following requirements must be met:

7-1 All cryptographic solutions must use either True Random Number Generators (TRNGs), such as Quantum Random Number Generators (QRNGs), or Pseudo Random Number Generators (PRNGs) with nondeterministic/nonpredictable entropy sources (Hybrid-PRNGs).

7-2 PRNGs with deterministic/predictable entropy sources must never be used in cryptographic solutions.

7-3 The seed for a Hybrid-PRNG must be fresh and have an entropy of 128 bits for MODERATE and 256 bits for ADVANCED. The seed must be generated from a validated and nondeterministic/nonpredictable entropy source.

7-4 Hybrid-PRNGs must allow for reseeding at regular intervals and/or at the request of the component that consumes the random bit stream.

7-5 All RNGs must pass statistical testing that verifies the random properties of the generated bit stream using the most recent editions of standardized statistical test suites such as NIST SP 800-22 and Dieharder[18].

Public Consultation

[18] R. G. Brown "Dieharder: A Random Number Test Suite", Oct 2022. https://webhome.phy.duke.edu/~rgb/General/dieharder.php

8- Quantum Key Distribution (QKD)

Any Quantum Key Distribution (QKD) solution must adhere the following requirements:

8-1 QKD solutions must be implemented in a hybrid approach, integrating post-quantum and/or classical algorithms for authentication and key agreement.

8-2 Quantum Bit Error Rate (QBER) must be continuously monitored to detect any interference.

8-3 QKD solutions must be protected against Man-in-the-Middle (MITM) attacks such as physical MITM targeting network infrastructure.

8-4 Technical limitations and their associated cybersecurity risks, as well as the mechanisms for addressing them, must be taken into account when implementing QKD systems and solutions.

8-5 Any entity using a QKD solution must be compliant with at least one of the following standards:

8-5-1 ISO/IEC 23837

8-5-2 ETSI GS QKD 016 and ETSI GS QKD 008.

Public Consultation

9- Appendices

Appendix (A) Privacy Enhancing Cryptography

Recent advances in Privacy Enhancing Cryptography (PEC) involve specialized cryptography techniques that process or analyze data without exposing its content. These methods are used for outsourcing computations to the cloud, allowing data to remain secure even while it is actively being used. The following are core examples of PEC schemes:

1 Homomorphic Encryption (HE)

Homomorphic Encryption (HE) is used to enable secure computations on private data using the encrypted ciphertexts only. Fully Homomorphic Encryption (FHE), that supports arbitrary computation on ciphertexts, are yet to be standardized by international standardization bodies. It is expected that Lattice-based encryption schemes such as Brakerski-Gentry-Vaikuntanathan (BGV), Brakerski-Fan-Vercauteren (BFV) and Gentry-Sahai-Waters (GSW) to be standardized as FHE schemes. Partially Homomorphic Encryption (PHE) allows limited computations on encrypted data typically supporting either addition or multiplication. ISO/IEC 18033-6:2019 standardized two PHE schemes: Paillier encryption, and Exponantial Elgamal.

2 Multi-Party Computation (MPC)

Multi-Party Computation (MPC) is cryptographic field where schemes enable multiple parties to jointly compute a function on their collective inputs while keeping each individual collective input secret. This allows participants to learn the final output of the computation without revealing their private inputs to others. This field has multiple standardization efforts, such as the ISO/IEC 4922 series, where Part 1 establishes the general terminology and security models for interoperability, and Part 2 details specific secret-sharing mechanisms. Furthermore, NIST has initiated its "First Call for Multi-Party Threshold Schemes" through the IR 8214C public draft, seeking public submissions and reference to further develop this field.

3 Zero-knowledge proofs (ZKPs)

A zero-knowledge proof (ZKP) is a cryptographic scheme where one party can convince another party that a statement is true without revealing any information beyond the validity of the statement itself. This scheme is useful for authentication and validation.

The content of this section is not part of this standard and thus non-binding and contain no requirements.

Public Consultation

Major organizations such as NIST, the ISO, and ETSI are working to standardize ZKP schemes to enhance their security, interoperability, and adoption. NIST's efforts include the "First Call for Multi-Party Threshold Schemes" (NIST IR 8214C), are a key part of this process, as this document seeks submission for ZKPs in addition MPC schemes. ISO is developing standards like ISO/IEC 27565 to provide guidelines for using ZKPs, while ETSI is exploring their use for applications like digital identity wallets in technical reports such as ETSI TR 119 476.

Appendix (B) Side-Channel Attacks

Side-channel attacks on a cryptographic system make use of the results of the system's physical measurements, such as energy consumption, electromagnetic emanation and time consumption, in order to gain insight into sensitive data[20]. Attacks can be carried out by remote and passive adversaries which are difficult to be detected and may lead to a significant and unnoticed leakage of data. In order to prevent these attacks, the first step to minimize information leakage is to ensure that for the side channel signals, the signal-to-noise ratio is as low as possible. Further, it must also be ensured that the information leakages from side-channels are not useful for the adversaries[21]. For example, eliminate any correlation between the binary representation of secret key and side channel signals, i.e. use dummy operations to mask any potential correlation. In order to minimize the risk of side-channel attacks, it is important to satisfy the following requirements[22]:

- Cryptographic operations must be performed in certified hardware components, e.g. smart cards to protect the secret and/or private keys.
- Analyze thoroughly the effects of such side channels on certified hardware components in a specialized laboratory during the development process.
- Protect ciphertexts using MAC and verify ciphertexts before performing any other cryptographic operations.

Side-channel attacks cover a wide range of threat scenarios. Therefore, an extensive review of relevant threat scenarios should be carried out for the proper secure implementation.

Public Consultation

[20] P. C. Kocher, J. Jaffe and B. Jun, "Differential power analysis," in Differential power analysis, 2011.

[21] A. Vega, P. Bose and A. Buyuktosunoglu, "Rugged Embedded Systems: Computing in Harsh Environments", Morgan Kaufmann, 2017.

[22] BSI, "Cryptographic Mechanisms: Recommendations and Key Lengths", BSI - Technical Guideline, 2020.

Appendix (C) Attribute-based Cryptography

Attribute-based Cryptography (ABC) is a form of public-key cryptography where data is encrypted for anyone who possesses a specific set of attributes. This method provides fine-grained access control. For example, a file can be encrypted so that only users with the attributes "HR Department" and "Manager" can access it. These schemes are explored by standards bodies like NIST, for instance in NIST IR 8450 and NIST SP 800-162, which discusses the general concept of Attribute-based Access Control (ABAC). The ETSI also addresses this technology in ETSI TS 103 532, which specifies Attribute-based Encryption (ABE) for Attribute-based Access Control (ABAC), demonstrating its role in securing communications and data.

Appendix (D) Identity-based Cryptography

Identity-based Cryptography (IBC) is a type of asymmetric cryptography where a user's public key is a unique string related to their identity, such as an email address. This eliminates the need for a certificate authority to bind a public key to an identity. The private key is generated by a central authority known as the Private Key Generator (PKG). This cryptographic concept is formalized in ISO/IEC 18033-5:2015. The IETF, in RFC 5408, provides a specification for an identity-based signature (IBS) algorithm, highlighting the technology's application in digital signatures. NIST IR 8450 also examines the foundational principles and use cases of identity-based cryptography (IBC). Furthermore, the ETSI TR 103 719 offers a technical guide for the engineering and adoption of (IBC) systems.

Public Consultation

Appendix (E) Terms and Definitions

TABLE 1: TERMS AND DEFINITIONS

Term	Definition
Agility	The property of a system or an infrastructure that can be reconfigured, in which resources can be reallocated, and in which components can be reused or repurposed.
Asymmetric Algorithm	A cryptographic algorithm that uses one cryptographic key for encryption, and another key for decryption. The two keys are called private and public keys.
Authenticated Encryption	A transformation of data by cryptographic algorithm to produce ciphertext that cannot be altered by an unauthorized entity without detection. It provides data confidentiality, data integrity and data origin authentication.
Authentication	Verifying the identity of a user, process or device, often as a prerequisite to allowing access to resources in a system.
Authenticity	The property of being genuine and being able to be verified and trusted.
Block Cipher Algorithm	A symmetric key cipher method that segments data into groups or blocks, then encrypts each one separately.
Blocks of Data	The fixed-length input units supplied to the cryptographic algorithm during processing, such as plaintexts, IVs/nonces or associated data.
Certificate	A set of data that uniquely identifies an entity's public key and other information that is digitally signed by a Certification Authority (a trusted party), thereby binding the public key to the owner.
Certificate Revocation List (CRL)	A list of revoked certificates issued by a Certification Authority.
Certification Authority (CA)	A trusted entity that is responsible for issuing and revoking public key certificates.
Confidentiality	A property of preventing information from being available or disclosed to unauthorized individuals, entities or processes.
Cryptographic Primitive	A low-level cryptographic algorithm used as a basic building block for higher-level cryptographic algorithms.
Cryptographic Solution	The design, architectural, and implementation choices made by organizations in satisfying specified cryptographic requirements for systems or system components.

Public consultation

Term	Definition
Cryptography	Principles, means and methods of applying data transformation algorithms for security purposes including integrity, confidentiality, authentication, authenticity and non-repudiation.
Cryptosystem	A set of algorithms and schemes that performs cryptographic functions.
Cybersecurity	Cybersecurity is the protection of networks, IT systems, operational technologies systems and their components of hardware and software, their services and the data they contain, from any penetration, disruption, modification, access, use or unauthorized exploitation. The concept of cybersecurity also includes information security and digital security, etc.
Decryption	The process of transforming ciphertext into plaintext using a cryptographic algorithm and key.
Digital Signature	The result of a cryptographic transformation of data that, when properly implemented, provides origin authentication, data integrity and signatory non-repudiation.
Digital Signature Algorithm (DSA)	An asymmetric algorithm based on Discrete Logarithm problem that provides integrity, non-repudiation and message authentication.
Elliptic Curve Cryptography (ECC)	Asymmetric cryptographic methods using operations in an elliptic curve group.
Encryption	The process of transforming plaintext into ciphertext using a cryptographic algorithm and key.
End-to-End Encryption	E2EE is a cryptographic scheme in which data is encrypted by the originating endpoint and remains encrypted and unintelligible to all intermediate systems, networks, and service providers. It is decrypted exclusively by the intended receiving endpoint.
Entropy	A measure of the amount of uncertainty an attacker faces to determine the value of a secret. Entropy is usually stated in bits. A value having n bits of entropy has the same degree of uncertainty as a uniformly distributed n bits random value.
Hardware Security Module (HSM)	A physical computing device that safeguards and manages cryptographic keys and provides cryptographic processing. An HSM is or contains a cryptographic module.
Hash Function	A function that maps an input bit string of arbitrary length to a usually fixed-length output bit string. This output is often irreversible and serves as a condensed representation of the input.
Hash-based MAC (HMAC)	A message authentication code that uses an approved keyed-hash function.

Public Consultation

Term	Definition
Hybrid Encryption	An application of cryptography that combines two or more encryption algorithms, particularly a combination of symmetric and asymmetric encryption.
Hybrid PRNG	A PRNG that is seeded by nondeterministic entropy sources to be suitable for cryptographic applications.
Initialization Vector/ Nonce (IV/Nonce)	A known public vector used as an input to initialize an encryption algorithm to increase security and support synchronization.
Integrity	A property whereby data has not been altered in an unauthorized manner since it was created, transmitted or stored.
Invasive Attacks	Attacks that involve a physical alteration to the implementation that may also cause an operating aberration different from normal operation.
Integrity Check Value	Checksum capable of detecting modification of an information system.
KECCAK	The family of all sponge functions with a KECCAK-f permutation as the underlying function and multi-rate padding as the padding rule.
Key Agreement	A key-establishment procedure where resultant keying material is a function of information contributed by two or more participants, so that no party can predetermine the value of the keying material independently of any other party's contribution.
Key Archival	A function in the lifecycle of keying material; a repository for the long-term storage of keying material.
Key Derivation Functions (KDFs)	The process by which one or more keys are derived from either a pre-shared key or a shared secret and other information.
Key Destruction	Removing all traces of keying material so that it cannot be recovered by either physical or electronic means.
Key Exchange	The process of exchanging public keys to establish secure communications.
Key Generation	The process of generating keys for cryptography.
Key Lifecycle Management (KLM)	The activities involving the handling of cryptographic keys and other related security parameters (for example, initialization vectors) during the entire lifecycle of the keys, including their generation, storage, establishment, entry and output, use and destruction.

Public Consultation

Term	Definition
Key Registration / Certification	A function in the lifecycle of keying material; the process of officially recording the keying material by a registration authority.
Key Revocation	A function in the lifecycle of keying material; a process whereby a notice is made available to the affected entities that the keying material should be removed from operational use prior to the end of the established cryptoperiod of that keying material.
Key Transport/ Key Distribution	A key-establishment procedure whereby one entity distributes the key to another entity.
Key Wrap (KW)	A method of encrypting keys (along with associated integrity information) that provides both confidentiality and integrity protection using a symmetric key algorithm.
Lightweight Cryptography	A sub-category in the field of cryptography that intends to provide security solutions for resource-constrained devices.
Message Authentication Code (MAC)	A cryptographic checksum on data that uses a symmetric key to detect both accidental and intentional modifications of the data. MACs provide authenticity and integrity protection.
Message Blocks	The unit blocks formed by dividing the message binary string to 128-bit blocks.
Non-Invasive Attacks	Attacks enabled by leakage of information from a physical cryptographic solution. Characteristics that could be exploited in a non-invasive attack include timing, power consumption, and electromagnetic and acoustic emissions.
Non-Repudiation	A service using a digital signature that is used to support a determination of whether a message was actually signed by a given entity.
Online Certificate Status Protocol (OCSP)	An online protocol used to determine the status of a public key certificate.
Post-Quantum Cryptography (PQC)	A cryptosystem that would be secure against adversaries who have both quantum and classical computers and that can be deployed without drastic changes to existing communication networks and protocols.
Pre-Shared Key	A secret key that has been established between parties who are authorized to use it by means of some secure method (such as using a secure manual-distribution process or automated key-establishment scheme).
Private Key	In an asymmetric algorithm, the private key is used for digital signing and decrypting data, and it must remain secret.

Public Consultation

Term	Definition
Pseudo Random Number Generator (PRNG)	An RNG that has access to a randomness source to produce a sequence of bits from a secret initial value called a seed, along with other possible inputs.
Public Key	In an asymmetric algorithm, the public key is used for verifying digital signature and encrypting data, and it is publicly known.
Public Key Infrastructure (PKI)	A framework that is established to issue, maintain and revoke public key certificates.
Quantum Computing	A rapidly-emerging technology that harnesses the laws of quantum mechanics to solve problems too complex for classical computers.
Quantum Cryptography (QC)	Cryptographic solutions that take advantage of quantum physics to provide certain security services.
Quantum Key Distribution (QKD)	A secure key exchange method based on the quantum laws of physics rather than computational complexity.
Quantum Random Number Generation (QRNG)	Generation of truly random numbers based on the inherent unpredictability of quantum sources of entropy.
Random Number Generator (RNG)	A process that is invoked to generate a random sequence of values (usually a sequence of bits) or an individual random value.
Root Certificate	A self-signed certificate, as defined by IETF RFC 5280, issued by a root CA. A root certificate is typically securely installed on systems so they can verify end-entity certificates they receive.
RSA	An asymmetric algorithm that is used for key establishment and digital signature generation and verification.
Safe Primes	A prime p is safe prime if it satisfies $p = 2q + 1$, where q is also a prime. A generator of large order must be used.
Secret Key	A cryptographic key used by a secret-key (symmetric) cryptographic algorithm and that is not made public. A secret key is also called a symmetric key.

Public Consultation

Term	Definition
Security Level	A number characterizing the amount of work that is expected to suffice to "defeat" an implemented cryptographic mechanism (possibly by compromising its functionality and/or circumventing the protection that its use was intended to facilitate). The security strength is measured in bits. If the security strength of a particular implementation of a cryptographic mechanism is n bits, it is expected that the equivalent of (roughly) 2^n basic operations of some sort will be sufficient to defeat it in some way.
Seed	A secret initial input value to a pseudo random number generator. Different seeds along with other possible inputs generate different pseudo random sequences.
Stream Cipher Algorithm	A symmetric key cipher method where each plaintext bit/word is encrypted one at a time with a corresponding pseudorandom stream (keystream) using a time variant internal state to produce ciphertext bit/word.
Strong Primes	In cryptography, strong primes are primes whose products are hard to factor. More specifically, a prime p is a strong prime if: (a) $p-1$ has a large prime factor q, and (b) $q-1$ has a large prime factor, and (c) $p+1$ has a large prime factor.
Symmetric Algorithm	A cryptographic algorithm that uses a single secret key for both encryption and decryption.
True Random Number Generator (TRNG)	An RNG that always has access to an entropy source and (when working properly) produces outputs that have full entropy.

Public Consultation

Appendix (F) Abbreviations

TABLE 2: LIST OF ABBREVIATIONS

Abb.	Full Term
AEAD	Authenticated Encryption with Associated Data
AES	Advanced Encryption Standards
ALIKE	Authenticated Lightweight Key Exchange
ARLs	Authority Revocation Lists
CA	Certificate Authority
CBC	Cipher Block Chaining
CCM	Counter with CBC-MAC
CFB	Cipher Feedback
CMAC	Cipher-based Message Authentication Code
CRLs	Certificate Revocation Lists
cSHAKE	customizable Secure Hash Algorithm with KECCAK
CTR	Counter
DH	Diffie-Hellman
DLIES	Discrete Logarithm Integrated Encryption Scheme
DNSSEC	Domain Name System Security
DSA	Digital Signature Algorithm
ECC	Elliptic Curve Cryptography
ECDLP	Elliptic Curve Discrete Logarithm Problem
ECDSA	Elliptical Curve Digital Signature Algorithm
ECIES	Elliptic Curve Integrated Encryption Scheme
EEA	EPS Encryption Algorithm
EIA	EPS Integrity Algorithm
EPS	Evolved Packet System
ESP	Encapsulating Security Payload
E2EE	End-to-End Encryption
ETSI	European Telecommunications Standards Institute
FIPS	Federal Information Processing Standards
GCM	Galois Counter Mode
GMAC	Galois Message Authentication Code
GS QKD	Group Specification Quantum Key Distribution
HKDF	Hash-based Key Derivation Function
HMAC	Hash-based Message Authentication Code
HSM	Hardware Security Module
ICV	Integrity Check Value
IKE-v2	Internet Key Exchange version 2
IPsec	Internet Protocol Security
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission
IT	Information Technology

Public Consultation

Abb.	Full Term
IV	Initialization Vector
KDF	Key Derivation Functions
KLM	Key Lifecycle Management
KMAC	KECCAK Message Authentication Code
KW	Key Wrap
KWP	Key Wrap with Padding
LTE	Long-Term Evolution
MAC	Message Authentication Code
NIST	National Institution of Standard and Technology
NIST SP	National Institution of Standard and Technology Special Publication
OCSP	Online Certificate Status Protocol
OFB	Output Feedback
PKI	Public Key Infrastructure
PQC	Post-quantum Cryptography
PRNG	Pseudo Random Number Generator
QKD	Quantum Key Distribution
QRNG	Quantum Random Number Generator
RNG	Random Number Generator
RSA	Algorithm developed by Rivest, Shamir and Adelman
RSA-OAEP	RSA with Optimal Asymmetric Encryption Padding
SHA-2	Secure Hash Algorithm 2
SHA-3	Secure Hash Algorithm-3
SHAKE	Secure Hash Algorithm with KECCAK
SSH	Secure Shell
TLS	Transport Layer Security
TRNG	True Random Number Generator
UEA	UMTS Encryption Algorithm
UIA	UMTS Integrity Algorithm
UMTS	Universal Mobile Telecommunications System
WPA	Wi-Fi Protected Access

Public consultation

Appendix (G) List of Changes

Table 3: List of Changes

Version			Date
NCS-2			2025
Type	Section	Page	Description
Modification	Scope	9	Addressing the newly added sections.
Addition	Scope	9	Addressing the target security level of cryptosystems.
Modification	1-3	9	Addressing the newly added sections.
Deletion	2-1	11	Title removed.
Modification	2-1-3	11	Rewritten for accuracy.
Modification	2-3-1	12	Modified to add SHA2-256 and SHA2-512, Rewritten for accuracy.
Modification	2-3-2	12	Rewritten for accuracy.
Modification	2-3-3	12	Rewritten for accuracy.
Modification	2-4	12	Title change.
Modification	2-4-2	13	Rewritten for accuracy and addition of new requirements.
Addition	2-5	13	Addition of new standards for post-quantum algorithms.
Deletion	2-5-3	12	Moved to footnotes.
Addition	2-6-6	14	Addition of new standards for Ascon.
Modification	3	15	Common note removed as it is satisfied by 3-1-2.
Modification	3-1-1	15	Rewritten for accuracy.
Modification	3-1-2	15	Rewritten for accuracy.
Modification	3-1-3	15	Modified to limit XTS to encryption of data at rest.
Addition	3-1-6	15	Addition of new requirements for the modes of operation.
Modification	3-2-1	15	Rewritten for accuracy.
Modification	3-2-1-1	15	Modified to require 128-bit IV/nonce length.
Modification	3-2-1-2	15	Rewritten for accuracy.
Modification	3-2-1-3	15	Rewritten for accuracy.
Addition	3-2-1-4	15	Addition of new requirements.
Addition	3-2-2	15	Addition of new requirements.
Modification	3-3	16	Rewritten for accuracy.
Addition	3-3-1-1	16	Addition of a new requirement.
Addition	3-3-2-1	16	Addition of a new requirement.
Modification	3-3-2-4	16	Modified to require 128-bit tag length.
Addition	3-3-3	16	Addition of new standards for KMAC.
Addition	3-3-4	16	Addition of new standards for GMAC.
Modification	3-6-3	17	Rewritten for accuracy.
Modification	3-7	18	Title change
Modification	3-7-2	18	Rewritten for accuracy.
Modification	3-7-3	18	Rewritten for accuracy.
Modification	3-8	18	Title change
Modification	3-8-2	18	Rewritten for accuracy.
Addition	3-9	19	Addition of new requirements for End-to-End Encryption (EE2E).

Version		Date	
NCS-2		2025	
Type	Section	Page	Description
Modification	4-1	20	Rewritten for accuracy.
Modification	4-2-2	21	Rewritten for accuracy.
Modification	4-2-3	21	Rewritten for accuracy.
Modification	4-2-4	21	Rewritten for accuracy.
Modification	4-3	21	Modified to add ECDSA_P256_SHA256 , ED25519 and ED488.
Modification	4-7	23	Removed since it is satisfied by 4-7-1.
Modification	6-2-1	25	Rewritten for accuracy.
Modification	6-2-2-2	25	Rewritten for accuracy.
Modification	6-2-2-3	25	Rewritten for accuracy.
Addition	6-2-3-6	26	Addition of a new requirement.
Addition	6-2-5-1	26	Addition of a new requirement.
Modification	6-2-8-2	26	Reference document changed.
Modification	6-2-9-3	27	Rewritten for accuracy.
Addition	6-2-10-1	27	Addition of a new requirement.
Addition	7	28	Addition of new requirements on Random Number Generators (RNGs).
Addition	8	29	Addition of new requirements on Quantum Key Distribution (QKD).

Public Consultation


الهيئة الوطنية
للأمن السيبراني
National Cybersecurity Authority