वर्गीय आवश्यकताओं के लिए मानक

दस्तावेज़ सं: टी.ई.सी. 91010:2023

STANDARD FOR GENERIC REQUIREMENTS

No. TEC 91010:2023

क्वांटम सुरक्षित एवं क्लासिकल क्रिप्टोग्राफिक प्रणाली

QUANTUM-SAFE AND CLASSICAL CRYPTOGRAPHIC SYSTEMS

ISO 9001:2015

दूरसंचार अभियांत्रिकी केंद्र

खुर्शीदलाल भवन, जनपथ, नई दिल्ली-110001, भारत

TELECOMMUNICATION ENGINEERING CENTRE

KHURSHIDLAL BHAWAN, JANPATH, NEW DELHI–110001, INDIA

www.tec.gov.in

Release 1.0, March 2023

FOREWORD

Telecommunication Engineering Centre (TEC) functions under the Department of Telecommunications (DoT), Government of India. Its activities include:

- Issue of Generic Requirements (GR), Interface Requirements (IR), Service Requirements (SR) and Standards for Telecom Products and Services
- Field evaluation of products and Systems
- National Fundamental Plans
- Support to DoT on technology issues
- Testing & Certification of Telecom products

For testing, four Regional Telecom Engineering Centres (RTECs) have been established, which are located in New Delhi, Bangalore, Mumbai, and Kolkata.

ABSTRACT

Cryptographic systems are essential in securing communication and protecting sensitive data from unauthorized access. In recent years, the threat landscape has evolved rapidly, with quantum computers posing a significant threat to classical cryptographic systems. Classical and quantum-safe cryptographic systems are necessary in the present scenario for ensure secure communication and protect sensitive data. This document describes the generic requirements and specifications of classical and Quantum-safe Cryptographic systems.

This standard covers the requirements related to the secure implementation and operation of a cryptographic system, including functional capabilities, interfaces and interoperability requirements; roles, services, and authentication; software/firmware security; operating environment; quality requirements, safety requirements, Electro Magnetic Compatibility requirements, self-tests, etc. Guidelines to procurers for product procurement and operations have been specified.

Table of Contents

TABLE OF FIGURES

LIST OF TABLES

HISTORY SHEET

S.No.	GR No.	Title	Remarks
1.	TEC 91010 : 2023	Generic Requirements of Quantum-safe and Classical Cryptographic Systems	First issue

REFERENCES

The following referenced documents are necessary for the application of the present document.

Sr. No.	Document No.	Title/Document Name
1.	CISPR 32/ or IS/CISPR 32: 2015	Limits and methods of measurement of radio disturbance characteristics of Information Technology Equipment
2.	ETSI TR 103 619 V1.1.1 (2020-07)	Migration strategies and recommendations to Quantum-safe schemes
3.	ETSI GS QKD 014 V1.1.1 (2019-02)	Quantum Key Distribution (QKD); Protocol and data format of REST-based key delivery API
4.	FIPS 140-3	Security Requirements for Cryptographic Modules
5.	FIPS PUB 197	Advanced Encryption Standard (AES) 2001
6.	FIPS PUB 198	The Keyed-Hash Message Authentication Code (HMAC) 2002
7.	IEC 60825-2/ IS 14624-2	Safety of laser products Part 2 safety of optical fibre communication systems OFCS (First Revision)
8.	IEC 61000-4-11/ IS 14700 (Part 4/Sec 11) : 2020	Testing & measurement technique- voltage dips, short interruptions, and voltage variations immunity tests.
9.	IEC 61000-4-2 / IS 14700 (Part 4/Sec 2) : 2018	Testing and measurement techniques of Electrostatic discharge immunity test
10.	IEC 61000-4-29	Testing and measurement techniques- Voltage dips, short interruptions, and voltage variations on D.C input power port immunity test.

11.	IEC 61000-4-3/. IS 14700 (Part 4/Sec 3) : 2010	Radiated RF electromagnetic field immunity test
12.	IEC 61000-4-4/ IS 14700 (Part 4/Sec 4) : 2018	Testing and measurement techniques of electrical fast transients/burst immunity test
13.	IEC 61000-4-5(2017)/ IS 14700 (Part 4/Sec 5) : 2019	Testing & Measurement techniques for surge immunity test.
14.	IEC 61000-4-6 / IS 14700 (Part 4/Sec 6) : 2016	Testing & Measurement techniques for surge immunity test and Immunity to conducted disturbances
15.	IEEE 802.1AE	Media Access Control (MAC) Security
16.	IEEESTD.2018.8585421	IEEE Standard for Local and metropolitan area networks–Media Access Control (MAC) Security. IEEE. December 2018.
17.	IEC 60215/ IS 10437(1986)	Safety requirements for radio transmitting equipment
18.	IEC 60950-1(2005)/ IS 13252 (2010)	Safety of information technology equipment
19.	ISO/IEC 10116:2006 / IS 15116 : 2018	Information technology – Security techniques – Modes of operation for an n-bit block cipher
20.	ISO/IEC 18033-3:2010/	Information Technology Security Techniques Encryption algorithms
21.	ISO/IEC 19790:2012	Information technology — Security techniques — Security requirements for cryptographic modules
22.	ISO/IEC 24759:2017	Information technology - Security techniques - Test requirements for cryptographic modules
23.	ITU-T X.1710	Security framework for quantum key distribution networks Series X: Data Networks, Open System Communications And Security
24.	ITU-T X.1811	Security guidelines for applying quantum-safe algorithms in IMT-2020 systems

25.	ITU-T X.800	Security architecture for Open Systems Interconnection for CCITT applications
26.	ITU-T Y.3802	Quantum key distribution networks - Functional architecture
27.	ITU-T Y.3803	Quantum key distribution networks - Key management
28.	ITU-T Y.3804	Quantum key distribution networks - Control and management
29.	NISTIR 8105	Report on Post-Quantum Cryptography
30.	QM-333	Specification for environmental testing of electronic equipment for transmission and switching use
31.	RFC 3602	The AES-CBC Cipher Algorithm and Its Use with IPsec
32.	RFC 3686	Using Advanced Encryption Standard (AES) Counter Mode with IPsec Encapsulating Security Payload (ESP)
33.	RFC 4106	The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating
34.	RFC 4301	Security Architecture for the Internet Protocol
35.	RFC 4302	IP Authentication Header
36.	RFC 4303	IP Encapsulating Security Payload
37.	RFC 4307	Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)
38.	RFC 4308	Cryptographic Suites for IPsec
39.	RFC 4868	Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec
40.	RFC 5282	Using Authenticated Encryption Algorithms with the Encrypted Payload of the Internet Key Exchange Protocol Version 2 (IKEv2)
41.	RFC 7296	Internet Key Exchange Protocol Version 2 (IKEv2)
42.	RFC 7321	Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)

43.	TEC/SD/DD/EMC-221/05/OCT-16	Electromagnetic Compatibility Standard for Telecommunication Equipment

Note: Unless otherwise explicitly stated, the latest approved issue of the standards/documents referred to above, with all amendments in force, on the issuance date of this GR shall be applicable.

CHAPTER-1

Cryptographic Systems

1.1. Introduction to Cryptographic systems

Cryptography is the practice of securing communication and protecting data from unauthorized access by converting plaintext into ciphertext using mathematical algorithms, making it unintelligible to anyone without the proper key. It plays a critical role in securing our digital infrastructure.

The typical cryptographic system is shown in Figure 1. The original message is usually termed as plaintext and the scrambled mesage is called the ciphertext. The encryption algorithm converts the plaintext to the ciphertext and the decryption algorithm performs a reverse process to get back the original message.

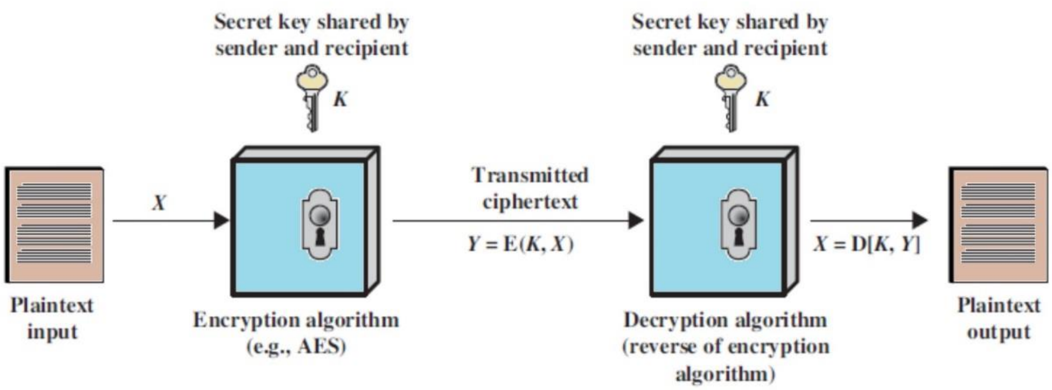

Figure 1: Block Diagram of a typical Cryptographic System

Our most crucial communication protocols rely on three core cryptographic primitives: public key encryption, digital signatures and key exchange. These primitives are implemented using state-of-the-art of cryptographic algorithms, e.g., AES, Diffie-Hellman Key Exchange(DHKE), the RSA (Rivest-Shamir-Adleman) algorithm, and elliptic curve cryptography(ECC).

Quantum-safe cryptographic systems, also known as post-quantum cryptography, are designed to be resistant to attacks from both classical and quantum computers. These systems use algorithms that are believed to be secure even against quantum computers. Quantum-safe cryptography is becoming increasingly important as quantum computers continue to evolve and become more powerful.

Quantum-safe and classical cryptographic systems are both used to secure communication and protect sensitive data from unauthorized access. Classical cryptographic systems use mathematical algorithms that are currently secure against attacks from classical computers. However, with the emergence of quantum computers, classical cryptographic systems are at risk of being broken, as quantum computers have the potential to solve certain mathematical problems much faster than classical computers.

Table 1: Impact of Quantum Computing on common cryptographic algorithms

Sl. No.	Cryptographic Algorithms	Type	Purpose	Impact of the large scale quantum computer
1	AES	Symmetric Key	Encryption	Larger key sizes needed
2	SHA-2, SHA-3	--------------	Hash functions	Larger output needed
3	RSA	Public key	Signatures, key establishment	No longer secure
4	ECDSA, ECDH	Public key	Signatures, key exchange	No longer secure

Classical and quantum-safe cryptographic systems provide confidentiality, integrity, authentication, and non-repudiation to ensure secure communication and protect sensitive data.

The security of the public key cryptographic primitives depends on the difficulty of a number of theoretical problems, such as integer Factorisation and the

Discrete Log Problem. In 1994, Peter Shor showed that quantum computers, a new technology leveraging the physical properties of matter and energy to perform calculations, can efficiently solve factorisation and discrete log problems, thereby rendering all public key cryptosystems based on such assumptions insecure. Thus, a sufficiently powerful quantum computer will peril many forms of modern communication, from Key exchange to encryption to digital authentication. As a result, RSA and DHKE are no longer secure in a post-quantum era.

Today’s most important uses of public key cryptography are for digital signatures and Key establishment. Grover’s algorithm provides a quadratic speed-up for quantum search algorithms compared to search algorithms on classical computers. We don’t know that Grover’s algorithm will ever be practically relevant, but if it is, doubling the Key size will be sufficient to preserve security in a symmetric cryptographic system. Furthermore, it has been shown that an exponential speed-up for search algorithms is impossible, suggesting that symmetric algorithms and hash functions should be usable in a quantum era. Consequently, the search algorithms believed to resist attacks from classical and quantum computers have focused on public key algorithms. Thus, Quantum-safe (post-quantum) cryptography is needed. In the last two decades, cryptographers have proposed a few families of computationally hard problems for Quantum-safe cryptography in Mathematics, which are also believed to be hard for quantum computers. These families come from lattice theory, coding theory, multivariate polynomials, isogeny and a handful of others (not yet confirmed quantum computer resistant).

It is critical to begin planning for the replacement of hardware, software, and services that can interoperate with existing communications protocols and networks. Consequently, the search algorithms believed to resist attacks from classical and quantum computers have focused on public key algorithms. Most quantum-resistant algorithms have larger Key sizes than the ones they will substitute, which is a big challenge. Quantum-safe algorithms may change various Internet protocols, such as the Transport Layer Security (TLS) protocol or the Internet Key Exchange (IKE). Implementing quantum-safe algorithms requires identifying hardware and software modules, operating systems, communication protocols, cryptographic libraries, and applications employed in data centres on-premises or in the cloud and distributed computing, storage, and network infrastructures.

1.2. Classification of cryptographic algorithms

Cryptographic algorithms are broadly classified into two categories, i.e., traditional and modern, based on the type used during the encryption and decryption process (refer to figure 2).

1.2.1. Traditional cryptography

Traditional cryptography refers to cryptographic methods and techniques developed before the advent of computers. Examples of traditional cryptography techniques include:

- Substitution ciphers (Caesar ciphers, etc.).
- Transposition ciphers (Rail Fence cipher, etc.).
- Polyalphabetic ciphers (such as the Vigenère cipher).

These techniques relied on the secrecy of the encryption key and sometimes also on the algorithm to secure communication.

1.2.2. Modern Cryptography

Modern cryptography is based on publicly known mathematical algorithms that operate on binary bit sequences and utilise secret keys. There are three types of modern cryptography:

i Symmetric (Secret Key)cryptography
ii Asymmetric (Public Key) cryptography
iii Cryptographic Hash Functions

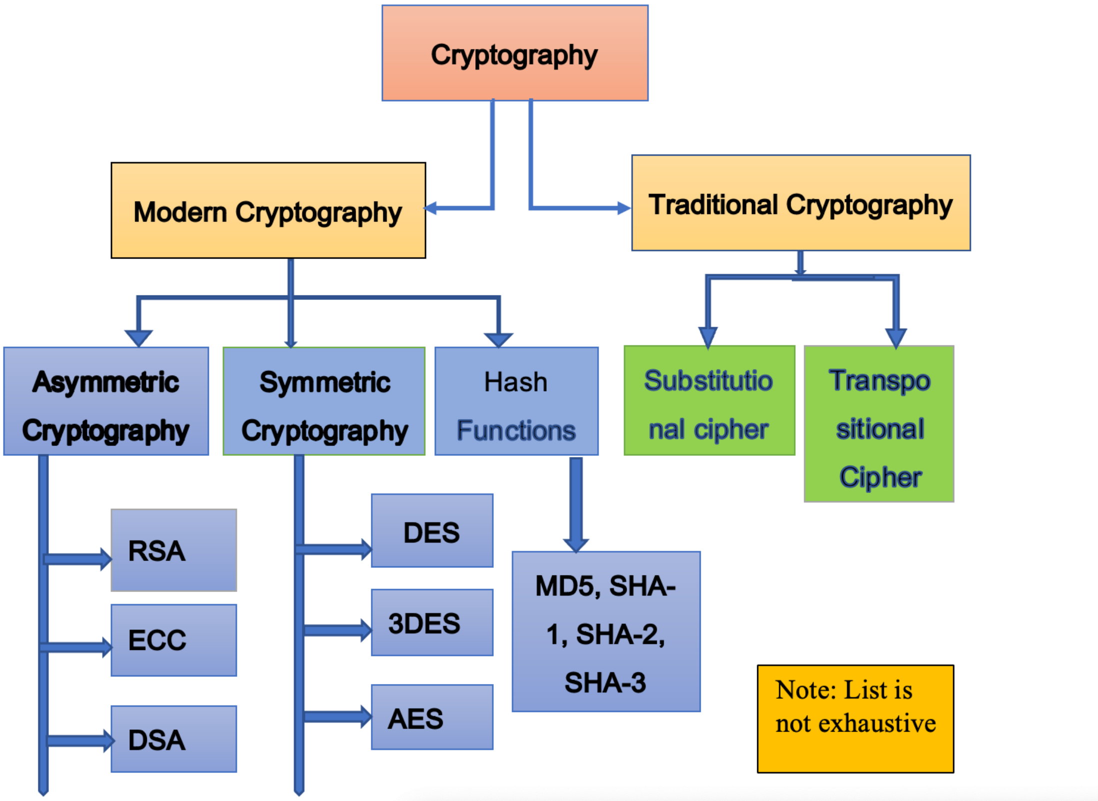

Figure 2: Block Diagram of classification of classical cryptography

1.2.2.1 Symmetric key cryptography

Encryption and decryption keys are identical in this scheme and should be known only to the communicating parties. Symmetric key cryptography is much faster than Asymmetric key cryptography, is far less resource-intensive than asymmetric encryption and is an incredibly efficient way to protect large volumes of data. Examples are Advanced Triple-Data Encryption Standard (DES), i.e., 3DES, Advanced Encryption System (AES), etc.

1.2.2.2 Asymmetric key cryptography

In this scheme, two keys are used, i.e., public key (for encryption) and private key (for decryption). The private key is kept secret as it is used for decryption, while the public key is not. For a secure public key cryptosystem, it is impossible to determine the private key's value by knowing the corresponding public key.

Most public communication networks use a combination of asymmetric and symmetric key cryptography schemes. An asymmetric/ Public Key

Cryptography scheme is used for key distribution. At the same time, the data flow is secured using a symmetric technique because of its better performance in the encryption/decryption process.

1.2.2.3 Hash Function

A Hash function is a cryptographic algorithm that takes an input message of any size and outputs a short fingerprint of fixed length. Typically, it does not require any key along with the input message, and the output is usually called hash-value or hash-digest. These algorithms are typically used to ensure the authenticity or integrity of data. Hash functions can also use keys, referred to as Keyed-hash functions, under such usage. Many operating systems/applications store passwords using hash functions.

1.2.3. Types of configuration of cryptographic system

A cryptographic module shall be a set of hardware, software, firmware or some combination thereof that at a minimum, implements a defined cryptographic service employing an approved cryptographic algorithm, security function or process and contained within a defined cryptographic boundary.The cryptographic systems can be classified based on the hardware, software and or firmware used in modular form within the cryptogpraphic boundary. These modules may be part of any interdependent or standalone system.

The cryptographic module/system can be defined as one of the following types:

i. **Hardware module**: It is a module whose cryptographic boundary is specified at a hardware perimeter. Firmware and/or software, which may also include an operating system, may be included within the hardware cryptographic boundary.

ii. **Software module**: It is a module whose cryptographic boundary delimits the exclusive software component(s) (may be one or multiple software components) that execute(s) in an adjustable operational environment. The computing platform and operating system of the working environment in which the software performs are external to the defined software module boundary.

iii. **Firmware module**: It is a module whose cryptographic boundary delimits the exclusive firmware component(s) that execute(s) in a limited or non-modifiable operational environment. The computing platform and operating system of the operational environment in which the firmware executes in are external to the defined firmware module boundary but explicitly bound to the firmware module.

iv. **Hybrid Software module**: It is a module whose cryptographic boundary delimits the composite of a software component and a disjoint hardware component (i.e. the software component is not contained within the hardware module boundary). The computing platform and operating system of the operational environment in which the software executes are external to the defined hybrid software module boundary.

v. **Hybrid Firmware module**: It is a module whose cryptographic boundary delimits the composite of a firmware component and a disjoint hardware component (i.e. the firmware component is not contained within the hardware module boundary). The computing platform and operating system of the operational environment in which the firmware executes in are external to the defined hybrid firmware module boundary but explicitly bound to the hybrid firmware module.

1.2.3.1 Classification of Quantum-safe cryptography configuration

The Quantum-safe cryptography module can be classified in a similar manner to classical cryptography modules. However, the algorithms will be different, especially for public key infrastructure like public key encryption schemes, key exchange mechanisms, digital signature schemes and hash functions. These algorithms need to resist attacks by quantum computers, and at the same time, they should still be secure against classical computer attacks.

For symmetric key cryptography, doubling the key size can provide some protection against quantum computing attacks, but this is not a complete solution. New search algorithms are being developed for asymmetric key cryptography to resist quantum computing attacks. NIST has been developing

Quantum-safe cryptographic standards in four phases, and the final set of standards is expected to be released in 2024.

1.2.3.2 Quantum-safe symmetric cryptography

Symmetric key cryptography is vulnerable to quantum attacks. It is mostrly threatened by Grover's algorithm.. Unlike the asymmetric encryption alogorithms (eg. RSA, etc) which could be completely breaken by the Quantum computer; for symmetric algorithms like AES, the best known Gorver's algorithm for attacking these encryption algorithms only weakens them. Grover's algorithm decreases the effective key length of a symmetric encryption algorithm by half, so AES-128 has an effective key space of 2^64 and AES-256 has an effective key space of 2^128. . However, increasing the cipher's key length can address an attack from the Quantum computer

1.2.3.3 Quantum-safe asymmetric cryptography

Today's most important uses of public key cryptography are for digital signatures and key establishment. Constructing a large-scale quantum computer would render many of these public key cryptosystems insecure. In particular, this includes those based on the difficulty of integer factorisation, such as RSA and those based on the hardness of the discrete logarithm problems. Quantum-safe Cryptography mainly refers to developing new asymmetric cryptography techniques that use a different class of hard mathematical problems. There are a few popular Quantum-safe cryptographic approaches that have emerged, such as Lattice-based, Code-based, multivariate-based and hash based cryptography. These mathematically hard problems are believed to be secure against classical as well as quantum computers.

1.2.3.4 Quantum-safe Hash functions

Hash-based cryptography offers one-time signature schemes based on hash functions such as Lamport-Diffie or Winternitz signature. Since Winternitz and Lamport-Diffie signatures can use securely once, they combine with structures like binary trees. Instead of using a signing key for a single, one-time use signature, a key may use for several signatures limited and bounded by the size of the binary tree.

SHA512 is sufficient to meet the requirements of any of our five security strength categories and performs well in software, especially for 64-bit architectures. TupleHash256 (specified in SP 800-185.), etc., is under consideration in NIST.

Extended Merkle signature scheme (XMSS) is a stateful signature scheme, and stateful hash based signature methods need extra care to implement safely. XMSS is a more current scheme that NIST includes in the standardisation process. It builds on Merkle Trees.

1.3. Elements or Subsystems and Applications of a cryptographic systems

A cryptographic system relies upon two basic components, i.e., an algorithm (or cryptographic methodology) and a cryptography key. Cryptographic subsystems in classical cryptography are the same as in Quantum-safe cryptographic systems except that different algorithms are implemented on hardware (Key sharing methods are different in Quantum Key Distribution (QKD) and Quantum-safe Cryptography). It also consists of software/firmware modules, operating systems, communication protocols, cryptography libraries, and applications deployed in data centres on-premises or in cloud, distributed computing, storage and network infrastructure.

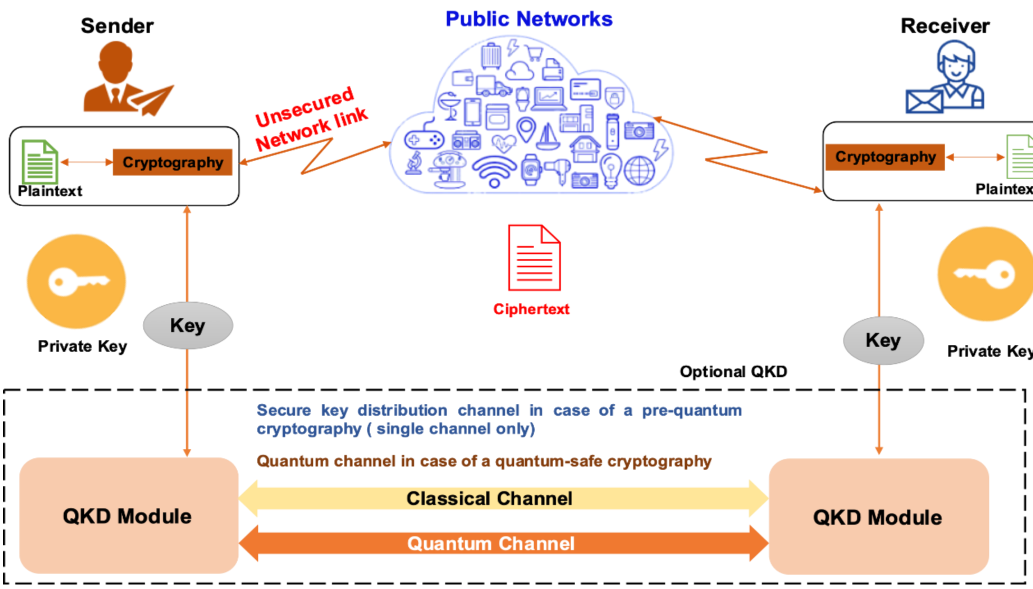

Figure 3: Block Diagram of a Symmetric cryptographic system

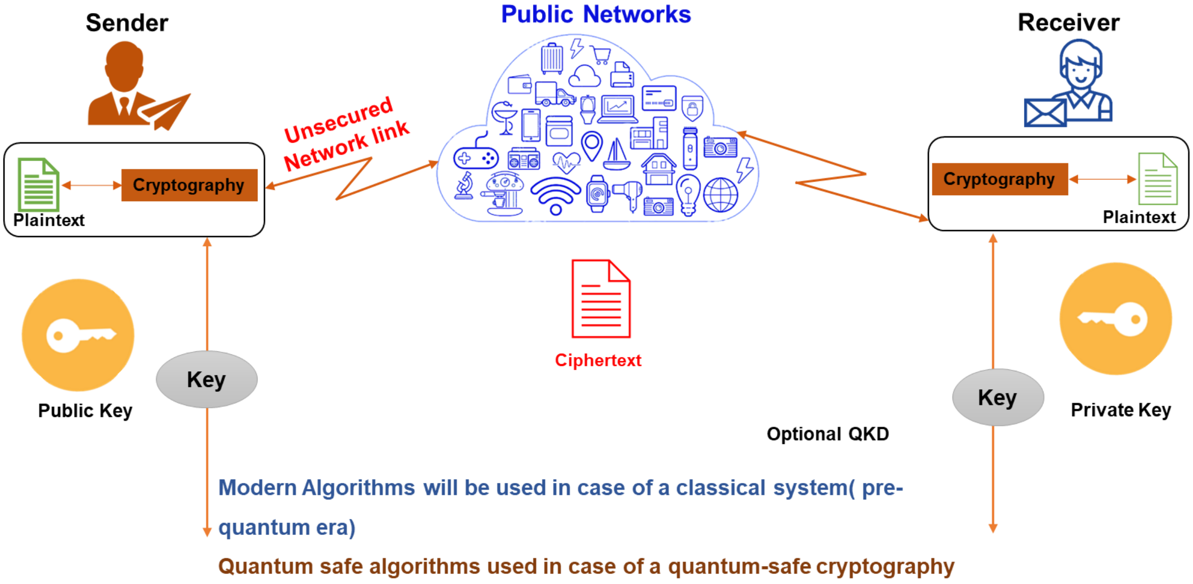

Figure 4: Block Diagram of Asymmetric cryptographic system

Note: Encryption algorithms are the same, but in symmetric cryptographic systems, the key is transported through quantum modules over the QKD channel, whereas in the case of Asymmetric cryptography systems, the key is shared using Quantum-safe Cryptography key sharing algorithms. QKD is one of the key sources, as shown in Figure 3 .

1.3.1 Encryptor

Communicates Data over an unsecured network by changing it from plain text to cipher text using an encryption algorithm driven by Key.

1.3.2 Decryptor

The receiver, who holds the same key and decryption algorithm, turns the cipher text into plain text. In this way, data transmit securely over an unsecured communication channel.

1.3.3 Hash Functions

Hashing is a method used to verify data integrity (already referred to in para 1.2.2.3). This technique is referred to as collision resistance, refer to figure 5.

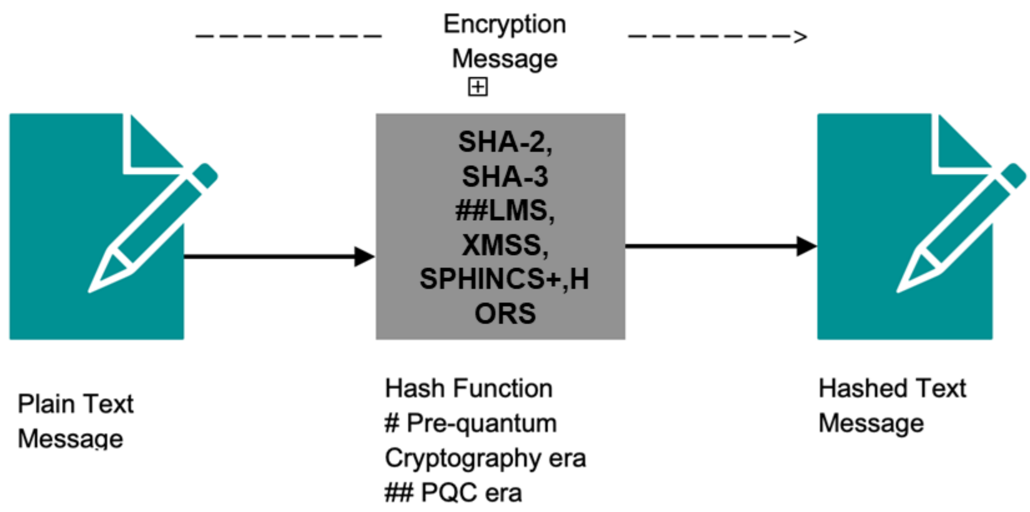

Figure 5: Block Diagram of Hash functions

i) A Message Digest 5 algorithm [MD5]: This creates a 128-bit digest used in the hash function. (Not recommended for use).

ii) Secure Hash Algorithm 1 (SHA-1): This creates a 160-bit digest (Not recommended for use).

iii) Secure Hash Algorithm 2 (SHA-2): Options include a digest between 224 and 512 bits.

iv) Secure Hash Algorithm 3 (SHA-3): Options include a digest between 224 and 512 bits.

v) SPHINCS+: For Quantum safe cryptography hash functions

1.3.4 Hashed Message Authentication Code (HMAC)

It uses the hashing mechanism but kicks it up a notch. Instead of using a hash that anyone can calculate, it includes a secret key. Currently, there are three approved general purpose MAC algorithms: HMAC, KMAC and CMAC.

1.3.5 Random Number Generator

In cryptography, randomness is found everywhere, from the generation of keys to encryption systems, even how cryptosystems are attacked. Without randomness, all crypto operations would be predictable and hence, insecure. A good random number generator consists of two parts: a source of entropy and a cryptographic algorithm. Cryptographic algorithms require Keys. A Random Number Generator (RNG), also called a Random Bit Generator (RBG), is needed in the key generation process to create a random (strong) key as well as for other cryptographic purposes such as initialisation vectors and nonces. Typically, a True Random Number Generator (TRNG) provides a source of randomness or "entropy" to seed a Pseudo-Random Number Generation (PRNG), also called a Deterministic Random Bit Generator (DRBG).

1.3.6 Digital Signatures

Offers Authentication, Data Integrity, and Non-repudiation. Digital signatures involve public and private key pairs, hashing, and encryption.

1.3.7 Key Management

Deals with generating keys, verifying keys, exchanging keys, storing keys, and at the end of their lifetime, destroying keys. The bigger the key, the more secure the algorithm will be. The only negative of having an extremely long key is that the longer the key, the more the CPU is used to decrypt and encrypt data.

1.3.8 Key Management Interoperability Protocol (KMIP)

Deals with generating keys, KMIP protocol allows communication between key management systems and cryptographically enabled applications, such as email, databases, and storage devices. KMIP is an extensible communication protocol for manipulating cryptographic keys on a key management server that defines message formats. Clients can also ask a server to encrypt or decrypt data without directly accessing the key using KMIP. The key management interoperability standard can support legacy systems and quantum-safe cryptographic applications.

1.3.9 Cryptography Interfaces and APIs

i. **Cryptography API:** Next Generation (CNG) is the long-term replacement for CryptoAPI. CNG is designed to be extensible at many levels and cryptography agnostic in behaviour. CNG is intended for use by developers of applications that will enable users to create and exchange documents and other data in a secure environment, especially over nonsecure media such as the Internet. At the CNG level, it was necessary to provide substitution and discoverability for all the algorithm types (symmetric, asymmetric, hash functions), random number generation, and other utility functions. The protocol-level changes are more significant because, in many cases, the protocol APIs needed to add algorithm selection and other flexibility options that did not previously exist.

ii. **Web Cryptography API:** This specification describes a JavaScript API for performing basic cryptographic operations in web applications, such as hashing, signature generation and verification, and encryption and decryption. Additionally, it describes an API for applications to generate and/or manage the keying material necessary to perform these operations. Uses for this API range from user or service authentication, document or code signing, and communications' confidentiality and integrity.

iii. **PKCS #11**: This refers to the programming interface to create and manipulate cryptographic tokens (a token where the secret is a cryptographic key). The API defines the most commonly used cryptographic object types (RSA keys, X.509 certificates, DES/Triple DES keys, etc.) and all the functions needed to use, create/generate, modify and delete those objects. Most commercial certificate authority (CA) software uses PKCS #11 to access the CA signing key or to enrol user certificates.

iv. **Java Cryptography Extension (JCE):** The Java Cryptography Extension (JCE) is an officially released Standard Extension to the Java Platform and part of Java Cryptography Architecture (JCA). JCE provides a framework and implementation for encryption, key generation/management and Message Authentication Code (MAC) algorithms. JCE supplements the Java platform, which already includes interfaces and implementations of message digests and digital signatures.

1.3.10 QKD Key delivery interface

The communication protocol is an Application Program Interface (API) that allows authentication and communication between the Cryptographic system by Secure Application Entity (SAE) and the Quantum Key Distribution Entity(QKDE) by Key Management Entity (KME). REST-based APIs are predominantly used due to their simplicity and ease for developers to understand. They are common in many applications; libraries, implementations, and guidance documents are available to the community. Each KME shall have one or multiple QKDEs to connect with other KMEs via QKD links. KMEs shall be able to distribute keys to other KMEs. In each Trusted Node, there shall be at least one KME. One or multiple SAEs may connect with a KME within a Trusted Node, as mentioned in figure 6. It is assumed that each Trusted node is securely operated and managed. Each trusted node shall be located on its site. SAEs shall be located with their connected KMEs on their site. The API between SAE and KME shall be used within a security boundary on each site. KMEs shall provide Web API server functionality to deliver keys to SAEs via HTTPS protocols. Each KME shall have a unique ID (KME ID). A KME ID shall be unique in a QKD network. SAEs make HTTPS requests to KMEs to get keys and status information. Each SAE shall have a unique ID (SAE ID). SAE ID shall be unique in a QKD network.

All communications between SAE and KME shall use the HTTPS protocols (with TLS version 1.3 or higher) (IETF RFC 7230, IETF RFC 7231, IETF RFC 7235, IETF RFC 5246, IETF RFC 8446). KMEs shall authenticate each request and identify the unique SAE ID of the calling SAE. Data in the message body of HTTPS requests from SAE to KME and HTTPS responses from KME to SAE shall be encoded in JSON format as per IETF RFC 8259.

This key delivery API is a REST-based API, a simple request and response style API between a SAE and a KME. Figure 6 shows how the key delivery API can be used for Multiple SAEs connected to a single KME. KME A and KME B exchange and store keys; each key delivered is assigned a universally unique ID.

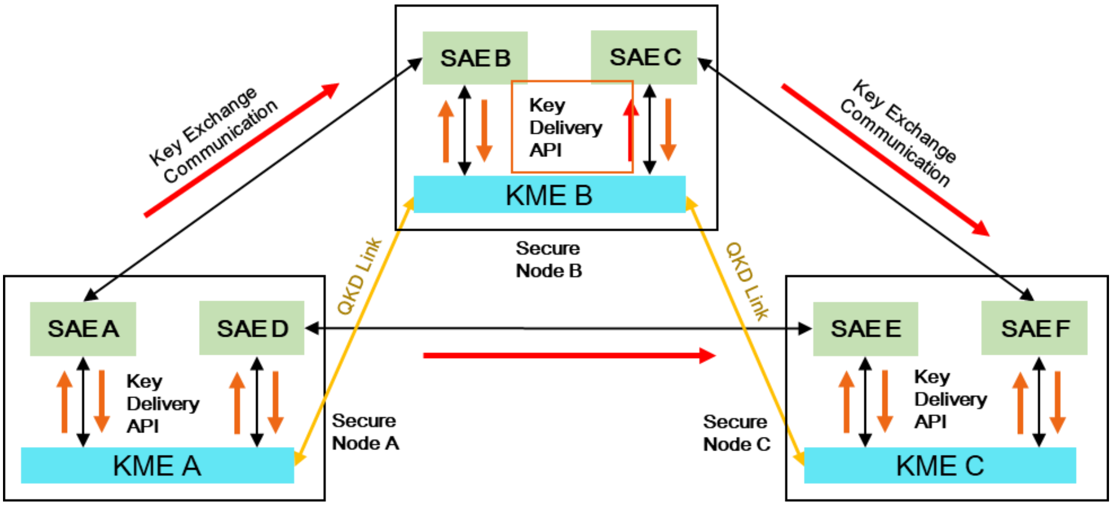

Figure 6: Block Diagram of communication flow of Key delivery management

1.3.11 Encryption Protocols

Encryption is done through encryption algorithms. These algorithms do all the cryptographic operations, using the encryption key, on the plaintext data. These algorithms are then utilised within encryption protocols to protect data for different purposes. The point of an encryption protocol is to fulfil a specific function. The functions of encryption protocols can vary, from communications with TSL to remote connections to computers with SSH.

1.3.12 Public and Private key pairs

A key pair is a set of two keys that work together as a team. In a typical key pair, you have one public and one private key.

1.3.13 Key Encapsulation Mechanisms (KEM)

In cryptographic protocols, a Key Encapsulation Mechanism (KEM) is used to secure symmetric key material for transmission using asymmetric (public key) algorithms. KEM makes this possible through a collection of three algorithms:

i. A key generation algorithm, Generate, generates a public key and a private key (a key pair).

ii. An encapsulation algorithm, Encapsulate, takes as input a public key and outputs a shared secret value and an "encapsulation" (a ciphertext) of this secret value.

iii. A decapsulation algorithm, Decapsulate, takes as input the encapsulation and the private key and outputs the shared secret value.

1.3.14 Post-quantum or Quantum-safe Algorithms

i. Code-based cryptosystems: The notion of code-based cryptography was first introduced by an encryption scheme published by McEliece in 1978. The McEliece cryptosystem builds on (binary) Goppa codes and their security based on the syndrome decoding problem. It is known to be extremely fast in encryption and reasonably quick in decryption.

ii. Lattice-based cryptosystems: Shortest Vector Problem (SVP) is to find the shortest non-zero vector within the lattice. SVP is known to be an NP-hard problem. The running time of solving a specific SVP instance remains to be discovered, i.e., it is still hard to estimate the exact computation of attacking a lattice-based cryptosystem. The security of the schemes is based on a lattice problem which is NP-hard under randomised reduction. And unlike the factorisation problem nor the discrete log problem, there is no known quantum-safe algorithm to solve SVP with the help of a quantum computer. Among all the candidates, the two algorithms are Learning With Error (LWE) based algorithms such as CRYSTALS-KYBER and CRYSTALS-Dilithium. LWE is a mathematical problem widely used in lattice-based cryptography to create secure encryption algorithms to deliver the best performance and security. In practice, the Ring Learning With Error (R-LWE) variant is usually used to boost the efficiency of LWE-based systems. The security of the R-LWE problem reduces to the same lattice problem as SVP.

iii. Multivariate cryptosystems: The simplest Matrix (or ABC) encryption is currently the most promising multivariate encryption scheme. Multivariate cryptosystems are public key based systems used for digital signatures. The most promising signature schemes include Unbalanced Oil and Vinegar (UOV) and Rainbow. There also exist BigField methods such as Hidden Field Equations (HFE) and pFLASH.

iv. **Lattice-based signature Scheme**: Lattice-based algorithms are faster and are considered quantum-safe. The security of lattice-based signature schemes is based on a short integer solution(SIS) problem. TLS has two protocols, handshake and record. The first protocol establishes the shared secret keying material and takes place with NewHope. Then, certificate-based mutual authentication is performed with CRYSTALS-Dilithium.

1.3.15 Hash based cryptosystems

Hash-based cryptography offers a one-time signature based on hash functions such as Lamport-Diffie or Winternitz signatures. The security of such one-time signature schemes relies solely on the collision resistance of the chosen cryptographic hash function.

1.3.16 Hybdrid X.509 certificates

X.509 defines public key certificates used to authenticate entities via signatures from publicly trusted authorities. These certificates are used in IETF's Public Key Infrastructure (PKI) X.509 (PKIX) standards and are widely deployed online for authentication. This describes a method of embedding alternative sets of cryptographic materials into X.509v3 digital certificates, X.509v2 Certificate Revocation Lists (CRLs), and PKCS #10 Certificate Signing Requests (CSRs). The embedded alternative cryptographic materials allow a Public Key Infrastructure (PKI) to use multiple cryptographic algorithms in a single object and transition to the new cryptographic algorithms while maintaining backward compatibility with systems using the existing algorithms. Thus, to use new Quantum-safe signatures in X.509, changes would be required in the X.509 algorithms. To authenticate the service channel required by a QKD system during the key distillation phase of the QKD protocol.

1.3.17 Internet Key Exchange version 2 (IKEv2)

Internet Key Exchange (IKEv2) is a protocol used to establish keys and Security Associations (SAs) to set up a secure Virtual Private Network (VPN) connection that protects network packets from being read or intercepted over a public Internet connection. The IKE protocol standard is rigid and does not permit VPN designers to choose beyond a small set of cryptographic algorithms. At present, the allowed algorithms are only partially quantum-safe. IKE provides authenticated connections using RSA, DSS or MAC with a pre-shared secret. IKE security associations are built on Perfect Forward Secrecy (PFS); in conventional security terms, ephemeral, one-time-use keys are created for every new secure connection. This ensures that the compromise of a long-term key only affects the confidentially of sessions established before the compromise. A replacement algorithm for the first and third exchanges, for instance, a quantum-safe alternative to replace the Diffie-Hellman key agreement to establish the shared secret for an IKE SA with perfect forward security. Together with a quantum-resistant authentication algorithm, this would enable IKE to negotiate quantum-safe symmetric keys. QKDs or any quantum sourced/TRNG shared secrets may be used with conventional encryption ciphers or for one-time pad encryption in high-security applications. QKD or any quantum sourced/TRNG may also be used for the second pass to solve the key management problem of distributing shared secret keys for message authentication.

1.3.18 Transport Layer Security (TLS)

TLS is used to secure a variety of applications, including web traffic (the HTTP protocol), file transfer (FTP application) and mail transport (SMTP application). The design of TLS is mainly independent of cryptographic algorithms and allows parties to negotiate cipher suites (combinations of cryptographic algorithms to use). As of TLSv1.3, all cryptographic components (public key authentication, key exchange, hash functions, bulk encryption) can be negotiated, although generally, all must be arranged simultaneously in a single cipher suite rather than independently. Currently, most servers are authenticated using X.509

certificates containing RSA public keys and thus can not be considered quantum safe.

A quantum-safe key exchange mechanism with perfect forward secrecy replaces existing key exchange mechanisms. To ease adoption, non-quantum-safe digital signatures, such as RSA, can continue to provide authentication. Quantum-safe cipher suites should match the security estimates of their symmetric primitives to the security estimates of their public key primitives. For example, a cipher suite utilising a quantum-safe public key algorithm at the 128-bit security level should use symmetric primitives at the 256-bit level to account for the impact of quantum search attacks.

Quantum-safe digital signatures are deployed in certificates to authenticate the purely quantum-safe key exchange mechanism introduced in stage 1 above. A suitable mechanism for incorporating key material established from a quantum key distribution channel into TLS would allow parties to achieve high computational security from a relatively short QKD key.

1.3.19 Secure/Multipurpose Internet Mail Extention (S/MIME)

It is a standard for digital signatures and public key encryption to send email messages securely. It offers origin authentication, non-repudiation, data integrity, and confidentiality through digital signatures and message encryption. This Standard is widely adopted throughout government and enterprise. S/MIME, and a similar scheme called OpenPGP, allow email to remain encrypted during the entire path from the sender to the receiver. The most potent alternative to S/MIME for preserving end-to-end security is OpenPGP. Content encryption in S/MIME relies upon symmetric ciphers like AES that are believed to be quantum-safe. The above mentioned key establishment algorithms for these symmetric keys and the algorithms used for digital signatures are insecure in a Quantum-safe environment.

1.3.20 Secure Shell (SSH)

It is a secure remote-login protocol. It has pervasive and diverse applications and can be used for various purposes, including constructing cost-effective secure Wide Local Area Networks (WLAN), secure connectivity for cloud-based services, and essentially any other enterprise process requiring secure server access from a remote client. The SSH protocol involves three major sub-protocols: the Transport Layer Protocol, the User Authentication Protocol, and the Connection Protocol. Each uses its algorithms to perform specific functions at different network layers. Within this protocol, several parameters are negotiated between server and client, including symmetric encryption algorithms, message authentication algorithms, and hash algorithms – all of which are quantum-safe. However, much like S/MIME, Key exchange and public key authentication methods rely upon insecure algorithms in the presence of quantum advantage. The following recommendations are suggested at the level of the Transport Layer Protocol:

i) Use of the Diffie-Hellman (DH) key exchange must be replaced by a quantum-safe algorithm that offers fast key-pair generation and perfect forward secrecy.

ii) The use of the Digital Signature Algorithm (DSA), the Elliptic Curve Digital Signature Algorithm (ECDSA) and the RSA Signature Scheme Algorithm (RSA-SSA) for host authentication must be replaced by the use of quantum-safe authentication mechanisms such as quantum-safe digital signatures or message authentication codes based on a pre-shared symmetric key.

iii) Quantum Key Distribution is one of the viable methods for secret key generation within the SSH protocol. Using QKD would bypass issues related to the presently unsafe practices of private key exchange and could replace the current key-establishment methods for symmetric (AES) keys.

1.3.21 Endpoint devices

Endpoint devices include any piece of hardware that a user utilises to interact with a distributed computing system or network. These can include canonical examples such as personal computers and mobile phones, kiosks/terminals in banks, stores, and airports, and any embedded technology connected to a broader network. Encryption and authentication of endpoint devices refer to making the contents of the device unreadable to unauthorised parties through cryptography and security protocols. This mechanism is a critical practice to prevent unauthorised data transfer and access, to ensure that only approved devices are allowed access to the system, and to deal appropriately with rogue or compromised devices that threaten system security through intrusions such as malware, key loggers, or viruses.

1.3.22 Lightweight Cryptography

Storage servers and data must be secure throughout their entire transfer through a network from one location. The security of resource-constrained devices is critical in the IoT field, given that everything is interconnected. The concern is that the limited resources on these devices may cause performance issues when the standard cryptographic algorithms are running on them. Therefore, in recent years, researchers have been working on developing lightweight cryptography and various efficient cryptographic technologies. Its requirements are constrained by security, low cost and high performance.

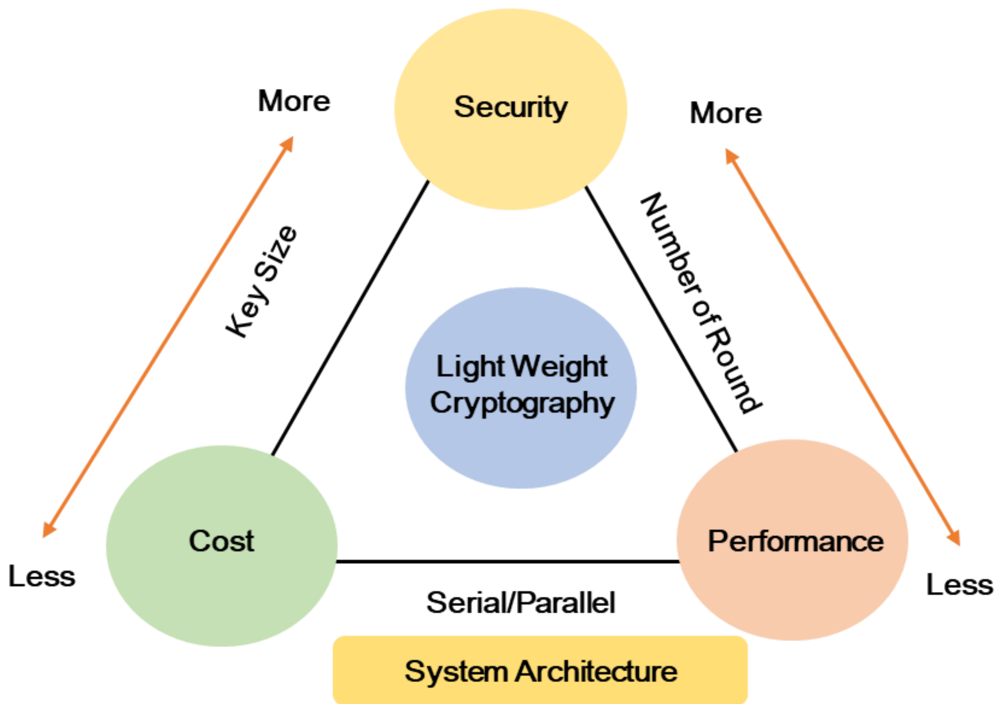

Figure 7: Block Diagram of Lightweight cryptography design trade-offs.

These requirements are balanced accordingly by adjusting the key size, the number of encryption rounds and the system architecture. Thus, the target of lightweight cryptography is to find a better balance between performance and security within cost constraints (refer Figure 7). The chosen algorithms are designed to protect information created and transmitted by the Internet of Things (IoT), including its myriad of tiny sensors and actuators. They are also designed for other miniature technologies, such as implanted medical devices, stress detectors inside roads and bridges, and keyless entry fobs for vehicles.

Devices like these need "lightweight cryptography" protection that uses the limited amount of electronic resources they possess.

The most important in lightweight cryptography: authenticated encryption with associated data (AEAD) and hashing.

AEAD protects the confidentiality of a message, but it also allows extra information, such as the header of a message, or a device's IP address, to be included without being encrypted. The algorithm ensures that all of the protected data is authentic and has not changed in transit. AEAD can be used in vehicle-to-vehicle communications, and it also can help prevent the counterfeiting of messages exchanged with the Radio Frequency IDentification (RFID) tags that often help track packages in warehouses. They need to compliant NIST protocols as listed from time to time as per the user requirements.

1.3.23 Network infrastructure encryption

Storage servers and data must be secure throughout their entire transfer through a network from one location to another. Network infrastructure encryption refers to the idea that as data moves throughout a network, the reliant network infrastructure must use cryptography in a way impervious to an adversary's attempt to undermine data integrity, confidentiality or authenticity. Areas of concern include the Internet backbone over which much of the principal internet traffic travels between the Internet's many networks, the encryption between linked enterprise data centres and the encryption used to secure a wide-area network.

1.3.24 Quantum Computing

Quantum computing utilises the properties of quantum states, such as superposition and entanglement, to perform computation. It is a new branch of computing in which the fundamental computational unit is a qubit rather than bits, as in conventional computing. A Qubit can exist both in the logical 0 state and logical 1 state at the same time. In short, Quantum computers can perform very rapid parallel computations compared to classical computers for a particular class of problems.

1.3.25 Cloud Storage and Computing

Cloud storage allows users to access centralised shared resources (hardware and software) over a network. Cloud services have become ubiquitous due to the rise of high-capacity networks, the decreased cost of computers and data storage devices, and trends toward hardware virtualisation and infrastructure, platform, and software-as-a-service models. Cloud computing has numerous benefits. However, a significant issue with the help of cloud computing is that since these services are shared by many users and often not offered over a private network but rather to large organisations on an opt-in basis, encryption is essential. A quantum-safe server, endpoint, and network infrastructure security subsume options for quantum-safe cloud computing. Key exchange parameters for protocols such as Hypertext Transfer Protocol Secure (HTTPS) should no longer use RSA, DSA, or ECDSA. Fortunately, cloud computing offers the distinct advantage of having a centralised IT security management system across many applications and businesses, reducing security overhead for individual enterprises and consequently offering an easier transition to quantum-safe protocols. This transition is essential in particular because cloud storage is, by definition, remotely accessed, requiring data to traverse a public network between the user and the cloud. The need for strong encryption is further amplified by the multitude of distinct and untrusted users sharing the infrastructure.

1.3.26 Cryptography-as-a-Service

Deploying cryptographic keys to endpoints such as smartphones, virtual machines in the public cloud and smart grid equipment is risky. Therefore, this proposes a Cryptography as a Service (CaaS) model, which allows cryptographic operations to be performed without exposing cryptographic keys and recommends overcoming the pitfalls associated with this technology. Keyed cryptographic operations, such as encryption and decryption, are performed by a CaaS provider on behalf of a device via web services APIs. Cryptography as a service has been defined as being "Keyed cryptographic operations, such as encryption and decryption that are performed by a CaaS provider on behalf of a device via web service APIs". The way that the "as a service" architecture works is through the implementation of HTTP and systems such as REST and SOAP. The overall architecture is extremely similar to Public Key Authorities (PKA) and Certificate Authorities (CA). The cryptographic keys used to perform these operations are stored within the CaaS provider, so devices do not possess these keys at any time (refer figure 8).

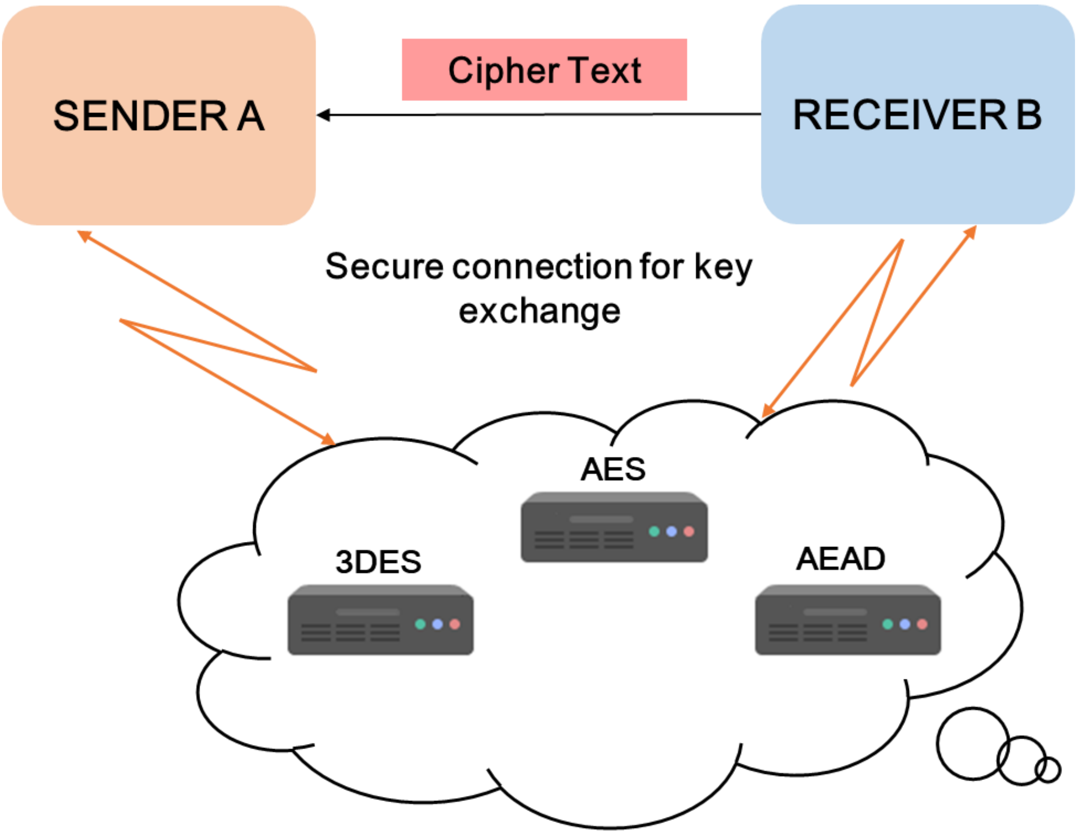

Figure 8: Block Diagram - Cryptography-as-a-Service

1.3.27 Cryptography Service Provider (CSP)

As organisations continue to test and integrate cloud computing into their IT environments, Cryptography-as-a-service and Entropy-as-a-service are into service to safeguard cryptographic keys with the same dynamic and virtualised attributes of cloud computing environments. Additionally, when storing data in multi-clouds, using native encryption from cloud service providers creates silos of data and the risk of not having full control over your keys and data. On-premises Hardware-Secure-Module(HSM) diminish those silos and enable users to know the whereabouts of their keys at all times.

BYOE (bring your encryption), or BYOK (bring your keys), is a security model tailored explicitly to cloud computing. It allows cloud service customers to use their encryption tools and manage their encryption keys. A cryptographic Service Provider (CSP) allows Cryptographic applications and services to access secure cryptographic operations and Key management. This provider uses the standard REST API, JCE (Java Cryptographic Extension) programming interface. PKCS#11, Cryptography API: Next Generation (CNG), HTTPS, Web API (W3C), Microsoft CAPI, and OpenSSL.

1.3.28 Security Services

Encryption is vital in protecting sensitive data transmitted over an unsecured network or stored at rest in computer systems. During the transfer of data over an unsecured network, a cryptographic system should ensure the following security services to ensure the security of the system or data transmission.

i) Approved Confidentiality Technique:
The data in network traffic must be available only to the intended recipient. In other words, the data in network traffic must not be available to anyone other than the intended recipient.

ii) Approved Integrity Technique:
The data in network traffic must not be altered while in a network. In other words, the recipient's data must be the same as the data sent by the Sender.

iii) Approved Authentication Technique:
The Sender and the Recipient must prove their identity to each other.

iv) Access Control:
The principle of access control decides who should be capable of accessing information or a system through a communication link. It supports the avoidance of unauthorised use of a resource.

v) Non-repudiation:
Non-repudiation prevents either sender or receiver from adverse a transmitted message. Therefore, when a message is sent, the receiver can validate that the asserted sender sent the message. Similarly, when a

message is received, the sender can validate that the asserted receiver received the message.

1.4. Functional requirements of a cryptographic system

Based on network deployment topologies, the cryptographic system should work in point-to-point/ point-to-multipoint / multipoint-to-multipoint mode. The cryptographic system shall provide Ethernet payload encryption over a point-to-point network. Encryption of standard Ethernet frame payload and Ethernet frames with multiple VLAN tags (Q-in-Q) using operator-selected symmetric key encryption scheme (optional for defence/user requirements for customisation, in case required) foolproof and fully reprogrammable (preferably FPGA based or equivalent on any programmable device on H/W and or stack over S/W).

It must be possible for an operator to select a particular encryption scheme for payload encryption system wise.

i. It shall provide confidentiality and protection from firmware upgrades.

ii. It shall support Policy based encryption.

iii. It shall provide data protection against unauthorised access by users and processes in physical, virtual, and cloud environments so that implementation is seamless and transparent to application/presentation of layer of system and its storage. So it can work across an enterprise's entire environment.

iv. Regardless of performance level, the cryptographic system shall be interoperable with the appropriate Application interface.

v. It shall provide confidentiality using standard encryption algorithms in a Quantum-safe cryptosystem and applicable algorithms in asymmetric and hash functions as per the product's specification sheet.

vi. It shall support encryption through a proprietary encryption algorithm also.

Table 2: Functional requirements of a cryptographic system

Sl. No	Parameter Type	Description and range of the Parameters	Reference Standard(s)	Remarks
1	Traffic type	Unicast/Multicast/Broadcast	TCP/IP (Ipv4/Ipv6)	Confirmation as per the RFCs
2	No of Concurrent connection	User to server mode		Atleast upto 100/500 connections
3	Direction of data transmission	Full duplex		Low overhead bits
4	Separation of data/control plane	Separation of Control plane and data plane		Physical and logical separation of data and control plane
5	Latency@ specific rate@ server/client	Latency at node (Non-aggregation state)	Not more than 10 μsec on data@10 GB maximum	independently of the packet/Ethernet frame size
6	Support of Jumbo frames	More than the standard ethernet frame size of any size		Beyond standard ethernet frame size
7	Mode of secure key uploading	Manual/Automatic		As applicable according to secure level 1/2/3/4
8	Encryption Modes	Block ciphers (ECB, CBC)	ISO/IEC 18033-3 Encryption Algorithms-Part 3:	NIST listed : CMAC, XTS-AES,CCM,KW/KWP /TKW, GCM/GMAC/XPN
9	Encryption Modes	Stream ciphers (CFB, OFB)	ISO/IEC 18033-4 Encryption Algorithms-Part 4	

Sl. No	Parameter Type	Description and range of the Parameters	Reference Standard(s)	Remarks
10	Asymmetric algorithms and techniques	Integer factorisation based techniques	ISO/IEC 9796-2 Information technology– Security	techniques — Digital signatures with message recovery – Part 2
11	Asymmetric algorithms and techniques	Discrete logarithm based techniques	ISO/IEC 9796-3 Information technology– Security techniques	Digital signature with message recovery – Part 3
12	Asymmetric algorithms and techniques	Digital signatures	ISO/IEC 14888 (all parts) Information technology–	Security techniques – Digital Signatures
13	Asymmetric algorithms and techniques	Cryptographic techniques based on elliptic curves	ISO/IEC 15946 (all parts) Information technology–	Security techniques
14	Asymmetric algorithms and techniques	Asymmetric cryptographic algorithms	ISO/IEC 18033-2: Information technology–	Security techniques — Encryption Algorithms Part 2:
15	Message Authentication Codes (MAC)	Mechanisms using a dedicated hash-function	ISO/IEC 9797-2 Information technology– Security techniques also Message Authentication Codes (MACs) - Part 2	FIPS-198, RFC 4868 for IPsec

Sl. No	Parameter Type	Description and range of the Parameters	Reference Standard(s)	Remarks
16	Hash functions	Hash functions using an n-bit block cipher.	ISO/IEC 10118-2 Information technology –	Security techniques – Hash functions – Part 2
17	Hash functions	Dedicated hash functions	ISO/IEC 10118-3 Information technology –	Security techniques – Hash functions – Part 3
18	Hash functions	Hash functions using modular arithmetic.	ISO/IEC 10118-4 Information technology –	Security techniques – Hash functions – Part 4
19	Authentication	Mechanisms using symmetric encipherment algorithms.	ISO/IEC 9798-2 Information technology –	Security techniques – Entity authentication – Part 2
20	Authentication	Mechanisms using digital signature techniques.	ISO/IEC 9798-3 Information technology – Security techniques –	Entity authentication – Part 3
21	Authentication	Mechanisms using a cryptographic check function.	ISO/IEC 9798-4 Information technology –	Security techniques – Entity authentication – Part 4
22	Authentication	Mechanisms using zero-knowledge techniques.	/IEC 9798-5 Information technology –	Security techniques – Entity authentication – Part 5
23	Authentication	Mechanisms using manual data transfer	ISO/IEC 9798-6 Information technology –	Security techniques – Entity authentication – Part 6

Sl. No	Parameter Type	Description and range of the Parameters	Reference Standard(s)	Remarks
24	Authentication	Mechanisms using symmetric techniques	ISO/IEC 11770-2 Information technology	Security techniques Key Management Part 2
25	Authentication	Mechanisms using asymmetric techniques	ISO/IEC 11770-3 Information technology –	Security techniques – Key Management – Part 3
26	KEM based on weak secrets.	Key Establishment Mechanisms (KEM) for all types	ISO/IEC 11770-4 Information technology – Security techniques –	Key Management – Part 4
27	Random bit generation	Truly Random Number Generation (TRNG) Pseudo-Random Number Generation (PRNG). Quantum Random Number Generation (QRNG). RNGs require entropy, and entropy originates from a noise source. Noise sources can be divided into two categories: Physical noise sources use dedicated hardware to generate randomness.	ISO/IEC 18031 Information technology	Developers must demonstrate that their entropy source is sufficiently random through a combination of design and/or test processes and continuous checks during operation. Any fault could have catastrophic consequences for generating secure cryptographic keys.
28	Software/ Firmware loading	The cryptographic module can load	ISO/IEC 19790:2012/Cor.1: 2015(E) 7.4.3.4	A validation authority shall validate the loaded

Sl. No	Parameter Type	Description and range of the Parameters	Reference Standard(s)	Remarks
		software or firmware from an external source.		software or firmware before loading.
29	Self-test for the integrity of H/W and S/W modules	Cryptographic module pre-operational and conditional self-tests provide the operator assurance that faults have not been introduced that would prevent the module's correct operation.	ISO/IEC 19790:2012/Cor.1: 2015(E) 7.10.1	Conditional self-tests shall be performed when an applicable security function or process is invoked.
30	Lightweight Cryptography	NIST-approved technique for AEAD and hashing protect against side-channel attacks, fault attacks,etc.	FIPS 197, SP 800-38D, FIPS 180-4	For security and privacy requirements, small devices, such as IoT devices, RFID tags, industrial controllers, sensor nodes, smart cards, etc.

Note: These parameters are applicable based on the product and which algorithms and Key sources are implemented in Quantum-safe(or Post-quantum) or Classical (pre quantum-era) cryptographic systems. Appropriate parameters are only to be confirmed with relevant products. Similarly applicable to all the tables for meeting conformity assessment of any parameters in this document.

1.5. Operational requirements of a cryptographic system

1.5.1 The equipment should be able to work without any degradation in the saline atmosphere near coastal areas and should be protected against corrosion.

1.5.2 Visual indication to show power ON/OFF status shall be provided.

1.5.3 It shall provide the requisite alarms.

1.5.4 Transactions logs and their period to be maintained per user requirements.

Table 3: Operational requirements of a cryptographic system

Sl. No	Name of the Sub parameter	Types of Parameters range	Reference Standard(s)	Remarks
1	Module's version	The cryptographic module shall output the name or module identifier and the versioning information	ISO/IEC 19790:2012 (E)7.4.3.1 (a)	Hardware, software and/or firmware versioning information
2	Status	The cryptographic module shall output the current status	ISO/IEC 19790:2012 (E) 7.4.3.1 (b)	Visual indicators in response to a service request/ normal state
3	Self-tests	pre-operational self-tests before loaded code can be executed	ISO/IEC 19790:2012 (E) 7.4.3.1 (c)	Pre-operational to confirm reflects the status
4	Approved Security function test	approved security functions	ISO/IEC 19790:2012 (E) 7.4.3.1 (d)	at least one test in the approved

				mode of operation
5	Zeroisation	Perform zeroisation (zeroise all unprotected SSPs and key components within the module at all security levels)	ISO/IEC 19790:2012 (E) 7.4.3.1 (e)	Zeroisation is immediate and uninterruptable in Seurity Level 4
6	Mode of operation	Normal/degraded	ISO/IEC 19790:2012(E) 7.2.4	Provided all pre-operational self-tests pass.
7	Bypass test	Indicate whether the Bypass capability is activated or not	ISO/IEC 19790:2012(E) 7.4.3.2	Bypass capability only if the capability to prevent the inadvertent bypass of plaintext data due to a single error.
8	Self-Initiated cryptographic output Test	Indicate the capability of a crypto module without being configured by the Crypto Officer. The status will be indicated in case activated	ISO/IEC 19790:2012(E) 7.4.3.3	this configuration may be preserved over resetting, rebooting, or power cycling of the module

9	Operational environment	i. A non-modifiable operational environment ii. A limited operational environment iii. A modifiable operational environment	ISO/IEC 19790:2012/Cor.1:2015 (E) 7.6	Functions may be added or modified within the operational environment.
10	Life-cycle assurance	Confirm the best practices by the vendor of a cryptographic module during the design, development, operation and end of life of a cryptographic module.	ISO/IEC 19790:2012 (E) 7.11	The vendor needs to confirm the following stages
11	Power	AC supply	During DUT	110-230V +10% 50/60 Hz AC
12	DC power	DC Power supply Range from -40 V to -60 V (from renewable sources also)	During DUT	AC or DC supply or both as optional
13	Size	Dimensions in mm or inches in length, width and height	Dimensions indicate multiple 1U size	Desirable is 1U size or optional able to place in the rack
14	Cooling	a) Requirement of Ingress or Egress fans (suck and exhaust kind of setup).		Depending on the environmental conditions a fan is not mandatory, but maintaining temperature is a prime concern.

15	Min Altitude without any degradation	Equipment without any degradation at an altitude of upto 3,000 meters.		The manufacturer shall guarantee satisfactory performance
16	Power Supply Alarm	Any visual indicator(G/R)		Indicate the status of power AC/DC.
17	Encryption/Decryption Alarm	Any visual indicator(G/R or any other colour)		To indicate status
18	Fault Indicator Alarm	Any visual indicator(G/R)	Log message and visual indicator	To indicate status
19	Capable of functioning in a saline environment	Without any degradation system able to function		Self certificate to be submitted if no test environment is available.

1.6. Interface requirements of a cryptographic system

The cryptographic system shall support 10/100/1000/2500/10000 BASE-TX electrical or optical interface or any open standard port for management as per the user requirement. Hardware/Software of Plaintext Interface shall be physically separate from Hardware/Software of Cipher interface.

Table 4: Interface requirements of a cryptographic system

Sl. No	Name of the Sub parameter	Types of Parameters range	Reference Standard(s)	Remarks
1	Management Interface	Optical//Ethernet (RJ45) Ethernet data input through the command line interface also.SNMP v3 or above, or XML/JSON shall be supported for EMS/NMS/NOC.	ISO/IEC, 19790 para 7.10.2	i. Hardware module Interface (HMI) Data port Management port. ii. Software or Firmware Module (SFM) Interface Support of SFP/SFP+. iii. Hybrid Software or Hybrid Firmware Interface(HSMI or HFMI) Plain Text/ Cipher Interface.
2	Data input interface	Interface (plain text, cipher text and SSP)	ISO/IEC, 19790 Cor.1:2015 (E) para 7.3.3 (a)	
3	Data output interface	Interface (plain text, cipher text and SSP)	ISO/IEC, 19790 Cor.1:2015 (E) para 7.3.3 (b)	
4	Control input interface	All input commands, signals, and control data	ISO/IEC, 19790 Cor.1:2015 (E) para 7.3.3 (c)	Clock input, function calls and manual controls such as switches, buttons, and keyboards
5	Control output interface	All output commands, signals, and control data	ISO/IEC, 19790 Cor.1:2015 (E) para 7.3.3 (d)	Inhibited when the cryptographic module is in an error state unless exceptions are specified
6	Entropy Source input	Dependent on external triggers to generate random numbers. Non-		Most operating systems have built-in crypto PRNGs. Most of

		deterministic inputs in the form of physical measurements of temperature or phase noise or clock signals, generate unpredictable numbers as their output. (There are, however, some concerns about the security of this type of random number generator, mainly since RNGs are a very good target for cryptographic backdoors.)		them are software based but some can also be pure hardware. In Linux, the device files /dev/random and /dev/urandom are the user and interfaces to the crypto RNG, which can reliably generate random bits.
7	Power interface	(All external electrical power that is input to a cryptographic module) Except for the software/firmware cryptographic modules	ISO/IEC, 19790 Cor.1:2015 (E) para 7.10.3 (f)	Except in the software module, power is provided internally by the source of the battery.
8	Status output	All output signals, indicators, and status data and physical indicators such as visual, audio	ISO/IEC, 19790 Cor.1:2015 (E) para 7.10.3 (e)	Error indicator, including return codes, display, indicator lamps, buzzer, tone, ring, vibration
9	Trusted channel (Security Level 3 and above)	Link for the transmission of unprotected plaintext CSPs, key components and authentication data between the cryptographic module and the sender or receiver endpoint of the cryptographic module	ISO/IEC, 19790 Cor.1:2015 (E) para 7.3.4	For Security Level 4, multi-factor identity-based authentication shall be employed for all services utilising the trusted channel

1.7. Interoperable requirements of a cryptographic system

Interoperability is one of the essentials to making seamless internetwork function in a heterogeneous network environment. The application service layer in the cryptographic system communicates with the key management controller. Communication protocol and data format for a quantum key distribution (QKD) network or any Key source network to supply cryptographic keys to an application, i.e., a Cryptographic system.

Table 5: Interoperable requirements of a cryptographic system

Sl. No	Name of the Sub parameter	Types of Parameters range	Reference Standard(s)	Remarks
1	IP Layer	Internet Protocol (IP) IPV4/IP6, Internet Control Message Protocol (ICMP), Internet Group Management Protocol (IGMP), IPSec	IETF RFC	Confirmation of interworking on IPv4 and IPv6 interworking
2	Authentication	CA or other agency		RADIUS server
3	Encryption	Various encryption methods as listed	NIST standards	Devices
4	Key exchange (KMIP)	During a key exchange with other systems	OASIS standard	NIST standard documents also
5	API with QKD interface	REST-based API Code for middleware function	API using the HTTPS protocol and data encoded in the JSON format *as per IETF RFC 8259*	The standard REST API, JCE (Java Cryptographic Extension) programming interface, is used.

				PKCS#11, Cryptography API: Next Generation (CNG), HTTPS, Web API (W3C), Microsoft CAPI, and OpenSSL.
6	Inter Secure Application Entity (SAE)	Master SAE to Slave SAE communication	QKD link as per the NIST/ETSI standards	SAE of cryptography is connected to the KME of QKD.
7	SSH	user authentication layer, transport layer, connection layer	RFC 4252, RFC 4253, RFC 4254	SSH may be used in several methodologies
8	TLS	TLS v1.3 or above	IETF RFC 8446	
9	Entropy source	Proven randomness	NIST standards	e.g. Clock, CPU, special circuitry, external dongle
10	Clock	Internal circuit or External I/O		For control functions and timing/ticks management
11	Link layer protocols	Tunnels, PPP, MAC	IETFs relevant RFCs	Layer 2 protocol communications

1.8. Quality requirements of a cryptographic system

1.8.1 The manufacturer shall furnish the MTBF values. A minimum value of MTBF shall be 10,000 hours. The calculations shall be based on the guidelines specified in the standard.

1.8.2 The product/systems shall be manufactured by the international quality management system ISO 9001:2000, for which the manufacturer should be duly accredited. A quality plan describing the manufacturer's quality assurance system must be submitted.

1.8.3 The product/systems shall conform to the requirements for the environment specified in document QM 333 {Latest issue: March 2010}: " Standard for environmental testing of Telecommunication Equipment" The applicable tests shall be for environmental category B2, including vibration test.

Table 6: Quality requirements of a cryptographic system

Sl.No	Name of the Sub parameter	Description of Parameters and its range	Reference Standard (s)	Remarks
1	Operating Temperature	0°C to +60°C and defence and space requirements shall work in the range -100°C to 200°C	IEC/ISO	For defence and space requirements to be met as per user specs.
2	Humidity	10 to 90% RH	IEC/ISO	
3	Reliability	(Indicate percentage in operational status)		Updated based on the operational status
4	Basic environmental Test	BIS adopted ISO standards	IEC 60068-2-27/ IS 9000	User can define specific requirements
5	MTBF	Metric		To be stated
6	MTTR	Metric		To be stated
7	Manufactured process compliance	International quality management	ISO 9001:2000	

1.9. EMI/EMC Requirements of a cryptographic system

The equipment shall conform to the EMC requirements as per the following standards and limits indicated therein. An accredited test agency shall furnish a test certificate and test report.

a) Conducted and radiated emission:

Name of EMC Standard: “CISPR 32 (2015) - Limits and methods of measurement of radio disturbance characteristics of Information Technology Equipment".

Limits: -

i. To comply with Class B limits of CISPR 32

ii. For Radiated Emission tests, limits below 1 GHz shall be as per relevant limits for measuring the distance of 10m OR as per relevant limits for measuring the distance of 3m.

b) Immunity to Electrostatic discharge:

Name of EMC Standard: IEC 61000-4-2 {2008) "Testing and measurement techniques of Electrostatic discharge immunity test".

Limits: -

i. Contact discharge level 2 {± 4 kV} or higher voltage;
ii. Air discharge level 3 {± 8 kV} or higher voltage;

c) Immunity to radiated RF:

Name of EMC Standard: IEC 61000-4-3 (2010) "Testing and measurement techniques-Radiated RF Electromagnetic Field Immunity test".

Limits: -

For Telecom Equipment and Telecom Terminal Equipment with Voice interface (s)

i. Under Test level 2 {Test field strength of 3 V/m} for general purposes in the frequency range 80 MHz to 1000 MHz and
ii. Under test level 3 (10 V/m) for protection against digital radio telephones and other RF devices in the frequency ranges 800 MHz to 960 MHz and 1.4 GHz to 6.0 GHz.
iii. For Telecom Terminal Equipment without Voice interface (s)
iv. Under Test level 2 {Test field strength of 3 V/m} for general purposes in the frequency range 80 MHz to 1000 MHz and for protection against digital radio telephones and other RF devices in frequency ranges 800 MHz to 960 MHz and 1.4 GHz to 6.0 GHz.

d) Immunity to fast transients (burst):

Name of EMC Standard: IEC 61000- 4- 4 {2012) "Testing and measurement techniques of electrical fast transients/burst immunity test".

Limits: -

Test Level 2, i.e., a) 1 kV for AC/DC power lines; b) 0. 5 kV for signal/control/ data/telecom lines;

e) Immunity to surges:

Name of EMC Standard: IEC 61000-4-5 (2014) "Testing & Measurement techniques for Surge immunity test".

Limits: -

i. For mains power input ports: (a)2 kV peak open circuit voltage for line-to-ground coupling (b) 1 kV peak open circuit voltage for a line-to-line coupling
ii. For telecom ports: (a) 2 kV peak open circuit voltage for a line to ground
iii. (b)2 kV peak open circuit voltage for a line-to-line coupling.

f) Immunity to conducted disturbance induced by Radiofrequency fields:

Name of EMC Standard: IEC 61000-4-6 (2013) "Testing & measurement techniques-Immunity to conducted disturbances induced by radio- frequency fields".

Limits: -

i. Under the test level 2 {3 V r.m.s.} in the frequency range 150 kHz-80 MHz for AC / DC lines and Signal /Control/telecom lines.

g) Immunity to voltage dips & short interruptions (applicable to only ac mains power input ports, if any):

Name of EMC Standard: IEC 61000-4-11 (2004) "Testing & measurement techniques- voltage dips, short interruptions and voltage variations immunity tests".

Limits: -

i. A voltage dip corresponding to a reduction of the supply voltage of 30% for 500ms (i.e., 70 % supply voltage for 500ms)

ii. A voltage dip corresponding to a reduction of the supply voltage of 60% for 200ms; (i.e., 40% supply voltage for 200ms)
iii. A voltage interruption corresponds to a reduction of a supply voltage of > 95% for 5s.
iv. A voltage interruption corresponds to a reduction of a supply voltage of >95% for 10ms.

Note 1: Classification of the equipment:

Class B: Class B is a category of apparatus that satisfies the class B disturbance Limits. Class B is intended primarily for use in the domestic environment and may include the following :

- Equipment with no fixed place of use; for example, portable equipment powered by built-in batteries;
- Telecommunication terminal equipment powered by the telecommunication networks
- Personal computers and auxiliary connected equipment

Please note that the domestic environment is an environment where the use of broadcast radio and television receivers may be expected within a distance of 10 m of the apparatus connected.

Class A: Class A is a category of all other equipment that satisfies the class A limits but not the class B limits.

Note 2: The testing agency for EMC tests shall be an accredited agency and details of accreditation shall be submitted.

Note 3: For checking compliance with the above EMC requirements, the method of measurements shall follow TEC Standard No. TEC/SD/DD/EMC-221/05/OCT-16 and the references mentioned therein unless otherwise specified. Alternatively, corresponding relevant Euro Norms of the above IEC/CISPR standards are also acceptable subject to the condition that frequency range and test level are met as per the above mentioned sub clauses (a) to (g) and TEC Standard No. TEC/SD/DD/EMC-221/05/OCT-16.

Table 7: EMI/EMC requirements of a cryptographic system

Sl. No	Name of the Sub parameter	Types of Parameters range	Reference Standard(s)	Remarks
1	Conducted and radiated emission:		IEC CISPR 32 (2015) AMD1:2019	AC or DC supply voltage not exceeding 600 V
2	Immunity to Electrostatic discharge		IEC 61000-4-2 {2008)	static electricity discharges from operators directly and from personnel to adjacent objects
3	Immunity to radiated RF		IEC 61000-4-3 (2020)	
4	Immunity to fast transients (burst):		IEC 61000-4- 4 {2012)	
5	Immunity to surges:		IEC 61000-4-5 (2014)	
6	Immunity to conducted disturbance induced by Radio frequency fields:		IEC 61000-4-6 (2013)	Radiofrequency (RF) transmitters in the frequency range of 150 kHz up to 80 MHz
7	Immunity to voltage dips & short interruptions		IEC 61000-4-11 (2020)	equipment with input current up to 16 A per phase

1.10. Safety Requirements of a cryptographic system

1.10.1 Electrical safety

IEC 62368-1 [replaced IS 13252-1/IEC 60950-1] is a primary reference for the safety of telecommunications equipment. Active electronics must comply with locally applicable electrical safety requirements in all cases. These safety parameters may include electrical insulation, grounding, fuses, current loss switches, etc. In case remote line powering is applied, it should comply with [ITU-T K.50], [ITU-T K.51] and [IEC 60950-21]. The safe working practices described in [ITU-T K.64] should be followed when work is carried out outside plant electronic equipment.

1.10.2 Laser safety

Since the box house active optical devices, it should comply with IEC 60825- 1 and IS 14624-2/IEC 60825-2 for optical safety requirements.

Note: This test shall be applicable if laser components are directly mounted in the box.

Table 8: Safety requirements of a cryptographic system

Sl. No	Name of the parameter	Description of Parameters and its range, if any	Reference Standard(s)	Remarks
1	Hazard-based product-safety standards for ICT and AV equipment	Audio/video, information and communication technology equipment - Part 1	IEC 62368-1: 2018 and COR1: 2020	Electrical safety for Hardware or S/W and or F/W over H/W
2	Safe limits for operating voltages and currents	telecommunication systems powered over the network	ITU-T K.50	Electrical safety for Hardware

3	safety criteria for telecommunication network equipment	requirements intended to reduce risks of fire, electric shock or injury	ITU-T K.51	persons who may come into contact with the equipment
4	Safe working practices for outside equipment installed in particular environments	working practices for service personnel to help them work safely in telecommunication installations	ITU-T K.64	The specific environments covered are characterized by wet conditions or close proximity to exposed metallic parts.
5	Information Technology Equipment – SAFETY	Remote power feeding	IEC 60950-21	Part 21 of IEC 60950
6	Safety of laser products emitting laser radiation	wavelength range 180 nm to 1 mm	IEC 60825- 1	Laser safety
7	safe of optical fibre communication systems (OFCSs)		IS 14624-2/IEC 60825-2	does not address safety issues associated with explosion or fire
8	Public safety: RoHS compliance	Safety from Hazardous material	EU 2015/863 directive	restricts chemicals and heavy metals in electronic products

1.11. Security services requirements of a cryptographic system

The following security services are required for the enhancement of security;

(i) Authentication mechanisms may be needed within a cryptographic module to authenticate an operator accessing the module and to verify that the operator is authorised to assume the requested role and perform services within that role. The cryptographic system shall support lossless data encryption/ decryption key change.

(ii) It should implement a key integrity check and authentication mechanism through a suitable hashing algorithm.

(iii) Encryption keys should be encrypted, stored in a secure device and only accessible to the user, regardless of data and key storage methods.

1.11.1 Security service level classification

The cryptographic techniques are identical over the four security levels. The security requirements cover areas relative to the design and implementation of a cryptographic module. The selection of a cryptographic module is based on an overall security rating of a to provide a level of security appropriate for the security requirements of the application and environment in which the module is to be utilised and for the security services that the module is to provide.

(i) Security Level 1: Provides a baseline level of security. Basic security requirements are specified for a cryptographic module (e.g. at least one approved security function or approved sensitive security parameter establishment method shall be used). Ideally appropriate for security applications where controls, such as physical security, network security, and administrative procedures, are provided outside the module but within the deployable environment.

(ii) Security Level 2: Enhances the physical security mechanisms of Security Level 1 by adding the requirement for tamper evidence, including tamper-evident coatings or seals or pick-resistant locks on removable covers or doors. Security Level 2 allows a cryptographic software module to be executed in an adaptable environment that implements role-based access controls or, at the minimum, a discretionary access control with the robust mechanism of defining new groups and assigning restrictive permissions through access control lists (e.g. ACLs), and with the capability of setting each user to more than one group, and that protects against unauthorised execution, modification, and reading of cryptographic software.

(iii) Security Level 3: Provides additional requirements to mitigate unauthorised access to SSPs held within the cryptographic module. Physical security mechanisms required at Security Level 3 are intended to have a high probability of detecting and responding to attempts at direct physical access, use or modification of the cryptographic module and probing through ventilation holes or slits. The physical security mechanisms may include solid enclosures and tamper detection/response circuitry that zeroise all CSPs when the removable covers/doors of the cryptographic module are opened. Security Level 3 requires identity-based authentication mechanisms, enhancing the security provided by the role-based authentication mechanisms specified for Security Level 2. A cryptographic module authenticates the identity of an operator and verifies that the identified operator is authorised to assume a specific role and perform a corresponding set of services. Security Level 3 requires manually established plaintext CSPs to be encrypted, utilise a trusted channel or use a split knowledge procedure for entry or output.

(iv) Security Level 4:The physical security mechanisms provide a complete envelope of protection around the cryptographic module to detect and respond to all unauthorised attempts at physical access when SSPs are contained in the module, whether external power is applied or not. Penetration of the cryptographic module enclosure from any direction is highly likely to be detected, resulting in the immediate zeroisation of all unprotected SSPs. Security Level 4 introduces the multi-factor authentication requirement for operator authentication. At a minimum, this requires two of the following three attributes. At Security Level 4, a cryptographic module is required to include special environmental protection features designed to detect voltage and temperature boundaries and zeroise all unprotected SSPs to provide a reasonable assurance that the module will not be affected when outside of the normal operating range in a manner that can compromise the security of the module.

Table 9: Security services requirements of a cryptographic system

Sl. No.	Parameter	Security Level-1	Security Level-2	Security Level-3	Security Level-4	Reference standards
1	Cryptographic Module Interfaces	Required and optional interfaces. Specification of all interfaces and all input and output data paths.		Trusted channel.		
2	Roles, Services, and Authentication	Logical separation of required and optional roles and services.	Role-based or identity-based operator authentication.	Identity-based operator authentication.	Multi-factor authentication.	ISO/IEC 19790:2012 / Cor.1:2015(E) 7.4.4.
3	Software/Firmware Security	Approved integrity technique, or EDC-based integrity test. Defined SFMI, HFMI and HSMI.	An approved digital signature or keyed message authentication code-based integrity test.	Approved digital signature-based integrity test.		ISO/IEC 19790:2012 /
		Executable code.				Cor.1:2015(E) 7.5

<table>
<tr><td rowspan="2">4</td><td rowspan="2">Operational Environment</td><td>Non-Modifiable, Limited or Modifiable.</td><td>Modifiable.</td><td colspan="2" rowspan="2">Non-modifiable</td><td rowspan="2"></td></tr>
<tr><td>Control of SSPs.</td><td>Role-based or discretionary access control. Audit mechanism</td></tr>
<tr><td rowspan="2">5</td><td rowspan="2">Physical Security</td><td rowspan="2">Production-grade components.</td><td>Tamper evidence.</td><td rowspan="2">Tamper detection and response for covers and doors. Strong enclosure or coating. Protection from direct probing. EFP or EFT.</td><td rowspan="2">Tamper detection and response envelope. EFP. Fault injection mitigation.</td><td rowspan="2">ISO/IEC 19790:2012 / Cor.1:2015 (E) 7.7.</td></tr>
<tr><td>Opaque covering or enclosure.</td></tr>
<tr><td>6</td><td>Non-Invasive Security</td><td colspan="4">The Module is designed to mitigate against non-invasive attacks. Documentation and effectiveness of mitigation techniques specified for security classes 1&2. Mitigation testing is essential in security classes 3&4.</td><td>ISO/IEC 19790:2012 / Cor.1:2015(E) 7.8</td></tr>
<tr><td>7</td><td>Sensitive security parameter generation</td><td colspan="4">Random bit generators, SSP generation, establishment, entry and output, storage, and zeroization. Automated SSP transport and SSP agreement using approved methods.</td><td>ISO/IEC 19790:2012 / Cor.1:2015 (E) 7.9.7</td></tr>
</table>

<table>
<tr><td></td><td></td><td colspan="2">Manually established SSPs may be entered or output in plain text</td><td colspan="2">Manually established SSPs may be entered, or output in encrypted form via trusted channel or split knowledge procedures</td><td></td></tr>
<tr><td rowspan="2">8</td><td rowspan="2">Self-Tests</td><td colspan="4">Pre-operational: Software/firmware integrity, bypass and critical functional test.</td><td rowspan="2">ISO/IEC 19790:2012 / Cor.1:2015(E) 7.9.2</td></tr>
<tr><td colspan="4">Conditional: Cryptographic algorithm, pair-wise consistency, Software/firmware loading, manual entry, bypass and critical functional test.</td></tr>
<tr><td rowspan="2">9</td><td rowspan="2">Mitigation of other attacks</td><td colspan="3" rowspan="2">Specification of Mitigation of attacks for which no testable requirements are available currently</td><td rowspan="2">Specification of Mitigation of attacks with testable requirements</td><td>ISO/IEC 19790:2012 / Cor.1:2015(E)</td></tr>
<tr><td>7.12</td></tr>
<tr><td>10</td><td>Replay attacks</td><td></td><td></td><td></td><td></td><td>To be verified</td></tr>
<tr><td>11</td><td>Fault injection attacks</td><td></td><td></td><td></td><td></td><td>To be verified</td></tr>
<tr><td>12</td><td>timing-based side-channel attacks</td><td></td><td></td><td></td><td></td><td>To be verified</td></tr>
<tr><td>13</td><td>Man-in-the-middle attack</td><td></td><td></td><td></td><td></td><td>To be verified</td></tr>
</table>

14	Documentation and validation					ISO/IEC 19790:2012 / Cor.1: 2015(E) Annex-A

1.12. Information for the procurer of the product for maintenance and operation

1.12.1 It shall support In-field firmware upgrades from time to time for a continuation of functionality with the advancement of technology and interoperable and supporting systems to make it compatible.

1.12.2 It shall support remote system Software/Firmware upgrades.

1.12.3 Purchaser may specify the functional requirement as per the parameters mentioned in Table 2 and the range of values from table number 10/11 to suit his requirements.

1.12.4 OEM has to comply with the mandatory parameters as envisaged in the product specification table.

1.12.5 The discretion of the Purchaser allows them to include the latest technical Specification as per their requirements in addition to mandatory parameters.

1.12.6 As and when software bugs are found/ determined, the Manufacturer shall provide patches/firmware replacement, if involved, as mutually agreed between the Purchaser of the instrument and supplier. Modified documentation, wherever applicable, shall also be supplied.

1.12.7 The manufacturer/supplier shall furnish the list of recommended spares.

1.12.8 The supplier shall have a maintenance/repair facility in India. The supplier shall furnish MTBF and MTTR values.

1.12.9 The Purchaser would like to stock the spares as and when the supplier decides to close down the production of the offered product. In such an event, the supplier shall give three years' notice to the Purchaser to stock the spares or agreed between them, whichever is applicable.

1.12.10 The accessories cables shall have a low attenuation cable link, either optical or ethernet cable of the latest. The vendor will submit the Specification for the same.

1.12.11 Purchaser would like to procure additional spares/sub-systems which comply with standards; the onus on OEM is to ensure the product shall work.

1.12.12 It shall support encryption through a proprietary encryption algorithm (optional for defence/space application users, wherever desired).

1.12.13 It must be possible for an operator to select a particular encryption scheme for payload encryption system wide.

1.12.14 It shall automatically exchange a new session key on a pre-set interval of 1-60 minutes.

1.12.15 The new session key shall be generated automatically by a True Random Number Generator (TRNG) or a Pseudo Random Number Generator (PRNG). QRNGs are preferred over other TRNGs and PRNGs.

1.12.16 These devices should support high entropy throughput with very high randomness (entropy)

1.12.17 It shall provide confidentiality-protected firmware/software upgrades.

1.12.18 The encryption devices should be future-proof and fully reprogrammable (preferably FPGA based) for an upgrade to new algorithms based on the user requirements or availability of technology from time to time.

1.12.19 Cryptographic system can also support Quantum-safe key exchange algorithms under the standardisation process of NIST, along with classical algorithms in a hybrid manner.

1.12.20 Remote management should be possible only through secure Management software with minimum 2-factor authentication with hardware binding.

1.12.21 Cryptographic system shall support SNMPv3 or the latest and shall provide multiple manager support.

1.12.22 Cryptographic system shall support audit and event logging with Syslog support.

1.12.23 Cryptographic system shall be able to work with the NTP server for time synchronisation.

1.12.24 Cryptographic system shall be able to work with RADIUS or TACAS+ server for authentication.

1.12.25 Repair procedure;

(i) List of replaceable parts used to include their sources and the approving authority.

(ii) Detailed ordering information for all the replaceable parts shall be listed in the manual to facilitate the reordering of spares as and when required.

(iii) A systematic procedure for troubleshooting and sub-assembly replacement shall be provided. Test fixtures and accessories required for repair shall also be indicated. Systematic troubleshooting procedures shall be given for the probable faults with their remedial actions.

Note: The Purchaser may mention the repair manual requirement at the time of ordering.

1.12.26 Technical literature in Hindi or English of the instrument with block schematic diagrams shall be provided. The complete layout and circuit diagrams of various assemblies with test voltages and waveforms at different test points of the units shall be provided, wherever required. All aspects of installation, operation, maintenance and repair shall be covered in the manuals. The soft copy/hard copy of the manuals shall also be provided. The manual shall include the following two parts:

(i) Installation, operation and maintenance manual.

(ii) Safety measures to be observed in handling the equipment.

(iii) Precautions for setting up, measurements and maintenance

(iv) Product/equipment required for routine maintenance and calibration, including their procedures.

(v) Illustration of internal and external mechanical parts.

(vi) A detailed description of the operation of the software used in the equipment, including its installation, loading and debugging etc.

1.12.27 Identification of Equipment

i) Equipment shall be marked with the supplier's or Manufacturer's logo/name.

ii) The Model No., serial No., The month and year of manufacture shall be indicated by screen printing on the body of the equipment or by a tamper-proof sticker pasted on the body of the equipment.

iii) Power Supply requirements shall be indicated on the body.

iv) The above markings shall be legible, indelible and easily visible.

CHAPTER-2

Specifications and Certification

2.1 Specification requirements of the configuration of the product for Testing, Validation and Certification.

Classical cryptosystems are detailed in the chapter-1, and conformity assessment is based on the standards mentioned in the tables against standards for each parameter in Classical and Quantum-safe cryptographic systems. There are four types of cryptosystems, as envisaged in chapter -1 and four levels of security level against security services. Specifications are given for each category across all security levels. The user will have a choice to take as per the specifications of optional parameters in the list, not exhaust, and a user may seek more capabilities/proprietary algorithms as per the need basis within its capabilities.

2.1.1 Specification requirements of a Classical (pre-quantum era) cryptographic systems

Table 10: Specification requirements of a Classical cryptographic systems

Sl. No	Name of the parameter	Security Level 1/2/3/4				Remarks
		HCM	SCM	FCM	HyCM	
1	Interface for data	Ethernet /optical	API	API	Ethernet/ Optical/API	Support 10/100/1000 BASE-TX with option SFP/SFP+ capable transceivers
2	Interface for management	Ethernet/API and CLI compatibility.				Support 10/100/1000 BASE-TX with option SFP/SFP+ capable transceivers

<table>
<tr><td>3</td><td>Throughput/Information pay load at client/Spoke</td><td colspan="4">10Mbps/ 100Mbps/1Gbps/10 Gbps</td><td>Concatenation of data in case more than one port</td></tr>
<tr><td>4</td><td>Throughput/Information pay load at Server/Hub</td><td colspan="4">100Mbps/1Gbps/10Gbps/100 Gbps</td><td>10 times the client requirements atleast</td></tr>
<tr><td>5</td><td>Latency at client/Spoke</td><td colspan="4">1/5/10 microseconds</td><td>User Option</td></tr>
<tr><td>6</td><td>Latency at Server/Hub</td><td colspan="4">1/5/10 microseconds</td><td>User Option</td></tr>
<tr><td>7</td><td>No Concurrent connections</td><td colspan="4">100/500 @server to handle simultaneous connections</td><td>User Option</td></tr>
<tr><td>8</td><td>Level of trustworthiness (Risk of compromise)</td><td>Very Low</td><td>Low</td><td>Medium</td><td>High</td><td>Digital Signature Services (DSS) uses PKI to verify the trustworthines of electronic signatures.</td></tr>
<tr><td>9</td><td>Error Correction Code Rate over the channel</td><td colspan="4">The ECC structure should have sufficient weight words to resist attack in polynomial time. Achieves self-synchronisation without degradation of error correcting capability. Error detection is commonly realised using a suitable hash function (specifically, a checksum, cyclic redundancy check or other algorithms). A hash function adds a fixed-length tag to a message, which enables receivers to verify the delivered message by recomputing the tag and comparing it with the one provided.</td><td>Various message/key encoding or reconciliation techniques that usually encode one payload bit into several coefficients have been proposed.</td></tr>
</table>

10	Symmetric Key encryption	AES-128, AES-192, AES-256 and above, AEAD (authenticated encryption protocol for smart and lightweight devices)	Any proprietary algorithms as per the needs of the user.
11	Asymmetric Key Encryption	RSA-2048 and above, Elgamal, Elliptic Curve	Capable of perform any proprietary algorithms, if any
12	Key Exchange algorithms	Diffie-Hellman-2048 and above and ECDH	Any proprietary algorithms as per the needs of the user, if any
13	Key encapsulation mechanism	Satisfy use cases of KEM by higher level security protocols such as TLS and cryptographic schemes such as HPKE (Hybrid Public Key Encryption). Allow service providers to plug in Java or native implementations of KEM algorithms.	It uses asymmetric (public key) algorithms. It is commonly used in hybrid cryptosystems.
14	Digital Signature	RSA-2048 and above/ECDSA 224-255, 256 and above/RSA-2048 and above or Elgamal	Also, proprietary algorithms as per the user requirements, if any desired.
15	Hash Functions	SHA-2, SHA-3	User option, if any.
16	n-bit block cipher	Electronic codebook (ECB), Cipher block chaining (CBC), Cipher Feedback (CFB), Output feedback (OFB), Counter (CTR) Galois/Counter Mode(GCM)	User option
17	N/W Topology	Hub and spoke or Mesh network or Point -to -Point or Point-to-Multipoint or Star	User option

18	Protocol communication between Key Managers and the Cryptographic module	Seamless Interoperable	Protocols shall function as per the user's requirements within their capabilities.

2.1.2 Specifications requirements of a Quantum-safe cryptographic systems

Table 11: Specification requirements of Quantum-safe cryptographic systems

Sl. No	Name of the parameter	Security Level 1/2/3/4				Remarks
		HCM	SCM	FCM	HyCM	
1	Interface for data	Ethernet /optical	API	API	Ethernet/ Optical/ API	Support 10/100/1000 BASE-TX with option SFP/SFP+ capable transceivers.
2	Interface for management	Ethernet/API and CLI compatibility				Support 10/100/1000 BASE-TX with option SFP/SFP+ capable transceivers.
3	Throughput/Information pay load at client/Spoke	10Mbps/ 100Mbps/1Gbps/10 Gbps				Concatenation of data in case more than one port.
4	Throughput/Information pay load at Server/Hub	100Mbps/1Gbps/10Gbps/100 Gbps				10 times the client requirements atleast, User option.

<table>
<tr><td>5</td><td>Latency at client/Spoke</td><td colspan="4">1/5/10 microseconds</td><td>User Option</td></tr>
<tr><td>6</td><td>Latency at Server/Hub</td><td colspan="4">1/5/10 microseconds</td><td>User Option</td></tr>
<tr><td>7</td><td>No Concurrent connections</td><td colspan="4">100/500 @server to handle simultaneous connections</td><td>User Option</td></tr>
<tr><td>8</td><td>Level of trustworthiness (Risk of compromise)</td><td>Very Low</td><td>Low</td><td>Medium</td><td>High</td><td>Digital Signature Services (DSS) uses PKI to verify the trustworthiness of electronic signatures.</td></tr>
<tr><td>9</td><td>Error Correction Code Rate over the channel</td><td colspan="4">PQC lattice-based cryptography can profit from classical and modern codes by combining BCH and LDPC codes.
(Achieve quasi-error-free communication and an increase of the estimated Quantum-safe bit-security level and a decrease of the communication overhead)</td><td>Various message/key encoding or reconciliation techniques that usually encode one payload bit into several coefficients have been proposed .</td></tr>
<tr><td>10</td><td>Symmetric Key encryption</td><td colspan="4">Symmetric ciphers (like AES-256, Twofish-256, SHA-512). Use 256 bits or more as the key length, AEAD</td><td>NIST qualified cases, AEAD encryption for smart devices.</td></tr>
<tr><td>11</td><td>Asymmetric Key Encryption</td><td colspan="4">BIKE, Classic McEliece, HQC</td><td>For NIST qualified cases</td></tr>
<tr><td>12</td><td>Key Exchange algorithms</td><td colspan="4">Diffie–Hellman key exchange (DHKE) and Elliptic-curve Diffie–Hellman (ECDH), RSA-OAEP and RSA-KEM (RSA key transport), PSK (pre-shared key),</td><td>For NIST qualified cases</td></tr>
</table>

		SRP (Secure Remote Password protocol), FHMQV (Fully Hashed Menezes-Qu-Vanstone), ECMQV (Ellictic-Curve Menezes-Qu-Vanstone) and CECPQ1 (quantum-safe key agreement).	
13	Key Encapsulation Mechanism (KEM)	CRYSTALS-KYBER Kyber-512, Kyber-768, and Kyber-1024	For NIST qualified cases
14	Digital Signature	CRYSTALS-Dilithium, FALCON, and SPHINCS+, Rainbow, GeMSS	For NIST qualified cases
15	Hash Function	LMS, XMSS, SPHINCS+, HORS, Cryptographic hashes (like SHA2, SHA3, BLAKE2), SHA384, SHA512 and SHA3-384, SHA3-512, AEAD along with hashing	Hashing along AEAD for smart devices
16	n-bit block cipher	Electronic codebook (ECB), Cipher block chaining (CBC), Cipher Feedback (CFB),Output feedback (OFB), Counter (CTR), Galois/Counter Mode(GCM)	List of codes as per the NIST
17	N/W Topology	Hub and spoke or Mesh network or Point -to -Point or Point-to-Multipoint or Star	
18	Protocol communication between Key Managers and the Cryptographic module/system	Seamless Interoperable with NIST recommended and or Govt of India/FIPS approved protocols/algorithms.	Protocols shall function as per the user's requirements within their capabilities.

Note:

i. All the specifications applicable for commercial products and as per the user requirements, environment parameters can be modified to comply the products for industrial/defence/Space requirements.
ii. Proprietary/private algorithms are to be implemented by OEMs as per the user requirements. Aaccordingly, those parameters will be reflected as optional parameters in the user certificate unless data maintain under confidentiality.

2.2 TEC Certification

TEC offers a number of voluntary certification schemes based on its product and interface related technical standards. These schemes certify the product/equipment based on the Testing against the various parameters and conditions in the respective TEC technical standards. The Testing is generally carried out on-site at the OEMs premises or in a lab environment. TEC designated labs' test reports related to EMC, Safety, Environmental Testing, etc., are also accepted for these certifications. For more details, refer to the TEC portal (https://www.tec.gov.in). The different schemes under the Voluntary Certification Regime are as below;

2.2.1 Classification of Voluntary Certificates

(i) Type Approval (TA): Type Approval is the process of Testing and certification of telecom & related ICT product by the TEC Test Guide for conformance with the Standard for Generic Requirements for a Product/Equipment issued by TEC. Optional parameters per the user choice will be shown in the Certificate against a type of product/service if any deviation in the mandatory parameters in all respects from the procedure will be reflected in the Certificate.

(ii) Interface Approval (IA): Interface Approval is the process of Testing and certification of telecom and related ICT product, by the TEC Test Guide, for conformance with the Standard for Interface Requirements for a Product/Equipment issued by TEC. Optional parameters per the user choice will be shown in the Certificate against a type of product/service if any deviation in the mandatory parameters in all respects from the procedure will be reflected in the Certificate.

(iii) Certificate of Approval (CoA): Certificate of Approval is the process of Testing and certification of telecom & related ICT product (including integrated/innovative products & software in emerging technology like 5G adv/AI/ML/Metaverse/FSOC/Quantum tech etc.) as per Manufacturer's specifications. This Certificate is granted only when TEC does not have a Standard/Specifications for the Generic/ Interface Requirements of the Product. The Test Guide approved by TEC shall conduct the Testing. The objective should be to complete the certification process as early as possible to encourage innovators/entrepreneurs/startups to seekcertification.

(iv) **Technology Approval:** Technology Approval is a process of testing and Certification of a prototype of a telecom and related ICT product developed by C-DoT, both public and private. Academic Institutions/ Research Organisations / Startups in the field of the sector. Optional parameters per the user choice will be shown in the certificate against a type of product/service if any deviation in the mandatory parameters in all respects from the procedure will be reflected in the Certificate.

2.2.2 Specific remarks to be mentioned in the Certificate

The following information shall be mentioned in the Certificate:

i. Parameter name, description of message and range of value, reference standards, remarks on conformity assessment, details of lab, remarks.

ii. Similarly, other parameters are given in Section 2.1 above.

2.2.3 Mandatory Certification

The Indian Telegraph (Amendment) Rules, 2017, provides that every telecom equipment must undergo mandatory Testing and certification before selling, importing, or using in India. Under these rules, the final detailed procedure for Mandatory Testing and Certification of Telecom Equipments(MTCTE) has been notified separately. The Testing is to be carried out for conformance to Essential Requirements for the equipment by Indian Accredited Labs designated by TEC. Based on their test reports, TEC shall issue a certificate.

Note: The eligible applicant shall offer the product to the RC Division, TEC-HQ (the nodal division for coordination), along with requisite documents. The RC Division will acknowledge the same and forward it to the concerned Core Division for further processing.

DEFINITIONS AND TERMINOLOGY

Algorithm:

A specified mathematical process for computation; is a set of rules that, if followed, will give a prescribed result.

Application link:

A communication link is used to provide cryptographic applications in the user network.

Asymmetric key:

A cryptographic key is used with an asymmetric key (public key) algorithm. The Key may be a private key or a public key.

Authentication:

It is a property of an entity or party whose identity establish with a required assurance. The authenticated party could be a user, subscriber, home environment or serving network.

Approved:

Any authorised agency of Govt of India/FIPS approved and/or NIST-recommended.

Authentication protocol:

A defined sequence of messages between an entity and a verifier enables the verifier to perform authentication of an entity.

Authorisation:

The granting of rights, which includes granting access based on access rights.

Availability:

The property of an entity is accessible and useable upon demand by an authorised entity.

Credential:

A set of data presented as evidence of a claimed identity and/or entitlements.

Confidentiality:

The property that information is not made available or disclosed to unauthorised individuals, entities, or processes.

Communication channel:

Two communicating parties use that for exchanging data encoded in a form that may be non-destructively read and fully reproduced.

Certificate Revocation List (CRL):

A list of certificates revoked without expiry by a Certification Authority.

Certification Authority (CA):

The entity in a public key infrastructure (PKI) is responsible for issuing certificates to certificate subjects and exacting compliance with a PKI policy.

Ciphertext:

Data in its encrypted form.

Compromise:

The unauthorised disclosure, modification, substitution, or use of sensitive data (e.g., a secret key, private key, or secret metadata).

Confidentiality:

The property that sensitive information is not disclosed to unauthorised entities (i.e., the secrecy of key information is maintained).

Cross-certify:

Establishing a trust relationship between two Certification Authorities (CAs) by signing each other's public key in certificates is called a "cross-certificate."

Cryptographic algorithm:

A well-defined computational procedure that takes variable inputs, including a cryptographic key (if applicable), and produces an output.

Cryptographic boundary:

An explicitly defined continuous perimeter that establishes the physical bounds of a cryptographic module and contains all the hardware, software, and or firmware components of a cryptographic module.

Cryptographic checksum:

A mathematical value is created using a cryptographic algorithm assigned to data and later used to test the data to verify that the data has not changed.

Cryptographic hash function:

A function that maps a bit of arbitrary string length to a fixed-bit string length.

Approved hash functions satisfy the following properties:

1. One-way – Finding any input that maps to any pre-specified output is computationally infeasible.
2. Collision resistant – Finding two distinct inputs that map to the same output is computationally infeasible.

Cryptographic key:

A parameter used with a cryptographic algorithm determines its operation so that an entity with knowledge of the key can reproduce or reverse the process while an entity without knowledge of the key cannot. Examples include

1. The transformation of plaintext data into ciphertext data,
2. The transformation of ciphertext data into plaintext data,
3. The computation of a digital signature from data,
4. The verification of a digital signature,
5. The computation of a message authentication code (MAC) from data,
6. The verification of a MAC received with data,
7. The computation of a shared secret used to derive keying material.

Cryptographic primitive:

A low-level cryptographic algorithm is a fundamental building block for higher-level cryptographic algorithms. Cryptography is the discipline that embodies the principles, means, and methods for providing information security, including confidentiality, data integrity, source authentication, and non-repudiation.

Cryptoperiod:

When a specific key is authorised for use or in which the keys for a given system may remain in effect.

Data integrity:

A property whereby data has not been altered unauthorised since it was created, transmitted, or stored. Data integrity authentication: The process of determining the integrity of the data, also called integrity authentication or integrity verification.

Decryption:

The process of changing ciphertext into plaintext using a cryptographic algorithm and key.

Discrete Log Problem:

A mathematical problem is considered hard for a conventional computer to solve but is easily solved by a quantum computer. The problem requires an understanding of the concept of an algebraic group. Solve for k, where b^k=g and b and g are elements in the same algebraic group.

Digital signature:

The result of a cryptographic transformation of data that, when properly implemented, provides the services of NIST SP 800-175B

1. Source authentication,
2. Data integrity, and
3. Support for signer non-repudiation.

Digital Signature Algorithm (DSA):

A public key algorithm is used to generate and verify digital signatures.

Domain parameters:

The parameters used with a cryptographic algorithm are common to a domain of users.

Elliptic Curve Cryptography(ECC):

It is a type of public key cryptography; this acronym refers to a group of ciphers based on their security on the discrete logarithm problem over an elliptic curve cyclic group, i.e., a family of ciphers like ECDH, ECDSA and others.

Elliptic Curve Digital Signature Algorithm (ECDSA):

A digital signature algorithm that is an analogue of DSA using elliptic curves.

Encryption:

The process of changing plaintext into ciphertext using a cryptographic algorithm for security or privacy.

Entity:

An individual (person), organisation, device, or process. Ephemeral key pair A short-term key pair is used with a public key(asymmetric-key) algorithm that is generated when needed; the public key of a short key pair is not provided in a public key certificate, unlike static public keys, which are often included in a certificate.

Hash Function:

Used interchangeably with an algorithm in this document. Hash function See cryptographic hash function. Hash value results from applying a hash function to information, also called a message digest.

Identity authentication:

The process of assuring the identity of an entity interacting with a system; also see Source authentication.

Initialisation Vector (IV):

A vector is used in defining the starting point of a cryptographic process.

Integrity:

The property that Data has not been modified or deleted in an unauthorised and undetected manner.

Integrity authentication (integrity verification):

The process of determining the integrity of the data; is also called data integrity authentication.

Interoperability:

The ability of one entity to communicate with another entity. Key agreement A (pair-wise) key-establishment procedure where secret keying material is generated from information contributed by two participants so that no party can predetermine the value of the private keying material independently from the other party's contributions. Contrast with key-transport.

Key Confirmation:

A procedure assures one party that another possesses the same keying material and/or shared secret.

Key Derivation:

The process of keying material is derived from either a pre-shared key or a shared secret produced during a key-agreement scheme along with other information.

Key Establishment:

The procedure results in keying material that is shared among different entities.

Key Hierarchy:

A tree structure represents the relationship of different keys. In a key hierarchy, a node represents a key used to derive the keys the descendent nodes represent. A key can only have one precedent but may have multiple descendent nodes.

Keying material:

A cryptographic key and other parameters (e.g., IVs or domain parameters) are used with a cryptographic algorithm. When keying, the material is derived as specified in SP 800-56C4 and SP 800-108:5. Data is represented as a bit string such that any non-overlapping segments of the string with the required lengths can be used as secret keys, secret initialisation vectors, and other secret parameters.

Keying relationship, cryptographic:

The state exists between two entities, sharing at least one cryptographic Key.

Key Information:

Information related to a key includes the keying material and associated

metadata linking to that key.

Key Life Cycle:

A sequence of steps that a key undergoes from its reception by a key manager (KM) through its use in a cryptographic application and until deletion or preservation depending on the key management policy.

Key Management:

All activities performed on keys during their life cycle, starting from their reception from the quantum layer, storage, formatting, relay, synchronisation, authentication and supply to a cryptographic application and deletion or preservation, depending on the key management policy.

Key Manager (KM):

A functional module is located in a quantum key distribution (QKD) node to perform key management in the Key management layer.

Key Manager Link:

A communication link connecting key managers (KMs) to perform key management.

Key pair:
A public key and its corresponding private key; a key pair is used with a public key (asymmetric-key) algorithm

Key Relay: A method to share keys between arbitrary quantum key distribution (QKD) nodes via intermediate QKD node(s).

Key Symmetry: The key symmetry means that bit '0' and bit '1' probability detection should be nearly equal. NIST randomness test has to be performed on the raw key (bits detected by SPD) to validate the symmetry.

Key Supply: A function providing keys to cryptographic applications.

Key transport:
A key-establishment procedure whereby one party (the sender) selects a value for the secret keying material and then securely distributes that value to another party (the receiver). Contrast with a key agreement.

Key wrapping:
A method of cryptographically protecting the confidentiality and integrity of keys using a symmetric-key algorithm. Key-wrapping key A symmetric key provides confidentiality and integrity protection for other keys.

Merkle Tree:
A quantum-safe public key cryptography system based on a tree of message digests where each child leaf is computed using a cryptographic hash function that is keyed with a key derived from its parent.

Message Authentication Code (MAC):
A cryptographic checksum on data that uses an approved security function and a symmetric key to detect accidental and intentional modifications of data.

Message digest Metadata:
The information associated with a key describes its specific characteristics, constraints, acceptable uses, ownership, etc., sometimes called the key's attributes.

Mode of operation:
An algorithm that uses a block cipher algorithm as a cryptographic primitive to provide a cryptographic service, such as confidentiality or authentication.

Non-repudiation:

A service uses a digital signature that is used to support a determination of whether a given entity signed a message.

NP:

Class of computational decision problems for which any given yes-solution can be verified as a solution in polynomial time by a deterministic Turing machine (or solvable by a non-deterministic Turing machine in polynomial time).

NP-hard problem:

The problem X that we considered earlier should be as hard as every NP problem so that an easy solution for X will give an easy solution for every NP problem is called the NP-hard problem.

Network Function Virtualisation NFV:

Technology that enables the creation of logically isolated network partitions over shared physical networks so that heterogeneous collections of multiple virtual networks can simultaneously coexist over the shared networks.

One-time pad:

An unconditionally secure encryption method, where plaintext is encrypted with a random secret key(or pad) of the same length as the message. The Private Key must be known by the sender and receiver and used only once.

Owner of a certificate:

The entity that is responsible for managing the certificate, including requesting, replacing, and revoking the certificate if and when required. The certificate owner is not necessarily the subject entity associated with the public key in the certificate (i.e., the key pair owner).

Owner of a key or key pair:

One or more entities are authorised to use a symmetric key or the private key of a key pair.

Perfect Forward Secrecy:

An attribute of a security protocol that means that temporary/ephemeral cryptographic keys are used in the protocol so that if an adversary breaks the keys and can listen to traffic in the session, they can only listen for the current session and need to break the keys again in any future secure session.

Plaintext:

Data that has not been encrypted; intelligible data that has meaning and can be understood without decryption.

Pre-Shared Key:

A secret key that has previously been established between the parties who are authorised to use it by means of some secure method (e.g., using a secure manual distribution process or automated key-establishment scheme).

Polynomial Time:

A term used by computer scientists to describe the amount of computing time required to solve a mathematical problem as the problem scales upwards in size. A polynomial time algorithm means that the algorithm solves a problem very fast.

Privacy:

The right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

Private key:

A cryptographic key is used with a public key cryptographic algorithm uniquely associated with an entity and not made public. In an asymmetric (public) key cryptosystem, the Private key is associated with a public key. Depending on the algorithm, the private key may be used to: -

i) Compute the corresponding public key,
ii) Compute a digital signature that the corresponding public key may verify.
iii) Decrypt data that was encrypted by the corresponding public key, or
iv) Compute a shared secret during a key-agreement process.

Protocol:

A set of rules used by two or more communicating entities that describe the message order and data structures for information exchanged between the entities.

Public key:

A cryptographic key is used with a public key (asymmetric key) algorithm uniquely associated with an entity that may be made public. In an asymmetric (public) key cryptosystem, the public key is associated with a private key. Anyone may know the public key and, depending on the algorithm may be used to -

1. Verify a digital signature signed by the corresponding private key.
2. Encrypt data that can be decrypted by the corresponding private key, or
3. Compute a shared secret during a key-agreement process.

Public key (Asymmetric-key) Cryptographic Algorithm:

A cryptographic algorithm that uses two related keys: a public key and a private key. The two keys have the property that determining the private key from the public key is computationally infeasible.

Public Key Infrastructure (PKI):

A framework is established to issue, maintain, and revoke public key certificates.

Quantum Channel: Communication channel for transmitting quantum signals.

Quantum-Safe Algorithm :

A step-by-step procedure that could run on a working quantum computer.

Quantum computing:

A computing device based on Qubits that can run the quantum computer.

Random Bit Generator (RBG):

A device or algorithm that outputs a sequence of bits that appears to be statistically independent and unbiased.

Relying party:

An entity that relies on the Certificate and the CA that issued the Certificate to verify the identity of the certificate owner, the validity of the public key, associated algorithms, and any relevant parameters in the Certificate, as well as the owner's possession of the corresponding private key.

RFC:

Request For Comment, which is a type of standard that the Internet Engineering Task Force publishes.

RSA:

A public key algorithm is used for key establishment and the generation and verification of digital signatures.

Scheme:

A set of unambiguously specified transformations that provide a (cryptographic) service (e.g., key establishment) when properly implemented and maintained. A scheme is a higher-level construct than a primitive and a lower-level construct than a protocol.

Secret key:

A single cryptographic key is used with a symmetric (secret key) cryptographic algorithm and is not made public (i.e., the key is kept secret). A private key is also called a symmetric key.

Sensitive (information):

Sensitive but unclassified information.

Security Association:

An instance of an encipherment key that temporarily protects network communications in an IPSec based VPN. An SA is a setup using the IKE protocol.

Security function: Cryptographic algorithms, together with modes of operation (if appropriate); for example, block cipher algorithms, digital signature algorithms, asymmetric key-establishment algorithms, message authentication codes, hash functions, or random bit generators.

Security strength:

A number is associated with the amount of work (i.e., the number of operations) required to break a cryptographic algorithm or system.

Sender/ Receiver:

This document defines the sender/transmitter and the receiver.

Shor's algorithm:

A method intended to run on a quantum computer that solves an instance of the Integer Factorization Problem and Discrete Log Problem in polynomial.

Signature Generation:

A digital signature algorithm and a private key generate a digital signature on data.

Signature Verification:

Using a digital signature and a public key to verify a digital signature on data.

Source Authentication:

The process of assuring the source of information is sometimes called data-origin authentication. Compare with Identity authentication.

SSL:

Secure Sockets Layer is an internet RFC that is a predecessor

Static Key Pair:

A long-term key pair for which the public key is often provided in a public key certificate.

Symmetric Key:

A single cryptographic key used with a symmetric (secret key) algorithm is uniquely associated with one or more entities and is not made public (i.e., the key is kept secret); a symmetric key is often called a secret key.

Symmetric-Key (Secret-Key) Algorithm:

A cryptographic algorithm that uses the same secret key for an operation and its complement (e.g., encryption and decryption).

TLS :

Transport Layer Security is an Internet RFC specifying a security protocol to encrypt and authenticate network communications for software applications. TLS v1.0 is the subsequent version of SSL v3.

Trusted Channel:

A channel where the endpoints are known and data integrity is protected in transit. Data privacy may be protected in transit depending on the communications protocol used. Examples include Transport Layer Security (TLS), IP security (IPSec), and secure physical connection.

User Network:

A network in which cryptographic applications consume keys supplied by a quantum key distribution (QKD) network or classical Key distribution network.

ACRONYMS

For this document the following abbreviations apply:

AC	Alternating Current
ACL	Access Control List
AEAD	Authenticated Encryption with Associated Data
AES	Advanced Encryption Standard
AH	Authentication Header
ANS	American National Standard
ANSI	American National Standard Institute
CA	Certificate Authority
CBC	Cipher-Block Chaining
CFB	Cipher FeedBack mode
CLI	Command Line Interface
CMAC	Cipher-based Message Authentication Code
CNG	Cryptography API: Next Generation
CSR	Certificate Signing Requests
CTR	Counter
DC	Direct Current
DH	Diffie-Hellmen
DHKE	Diffie-Hellman Key Exchange
DSA	Digital Signature Algorithm
ECB	Electronic Code Book
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EMI	electromagnetic Interference
EMC	Electromagnetic compatibility
ESP	Encapsulating Security Payload
FPGA	Field Programmable Gate Array
FTP	File Transfer Protocol
GCM	Galois/Counter Mode
HFE	Hidden Field Equations

HMAC	Hash-based Message Authentication Code
HTTPS	Hypertext Transfer Protocol Secure
IEC	International Electrotechnical Commission
IP	Internet Protocol
IPsec	IP security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IKE	Internet Key Exchange
IKEv2	Internet Key Exchange version 2
ITU	International Telecommunication Union
IV	Initialisation Vector
KMAC	Keccak Message Authentication Code
KME	Key Management Entity
KMF	Key Management Framework
KMIE	Key Management Interoperability Protocol
LWE	Learning With Error
MAC	Message Authentication Code
NIST	National Institute of Standards and Technology
OASIS	Organization for the Advancement of Structured Information Standards
OFB	Output FeedBack mode
OID	Object Identifier
OSI	Open Systems Interconnection
PFS	Perfect Forward Secrecy
PKI	Public Key Infrastructure
PQC	Post-Quantum Cryptography
PRNG	Pseudo Random Number Generator
QKD	Quantum Key Distribution
QKDE	Quantum Key Distribution Entity
RADIUS	Remote Authentication Dial-In User Service
REST	REpresentational State Transfer
RH	Relative Humidity
RFC	Request For Comment

RSA	Rivest, Shamir and Adleman
SA	Security Associations
SAE	Secure Application Entity
SIS	Short Integer Solution
SFP	Small Form-factor Pluggable
S/MIME	Secure/Multipurpose Internet Mail Extention
SNMP	Simple Network Management Protocol
SP	Special Publication
SSH	Secure Shell
SSL	Secure Sockets Layer
SVP	Shortest Vector Problem
TLS	Transport Layer Security
TRNG	True Random Number Generator
TACAS	Terminal Access Controller Access Control System
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide Area Network
XMSS	eXtended Merkle Signature Scheme

======End of the document ======