□□□□□□ □□□□□□□□□□□ □□ □□□ □□□□

□□□□□□□□□□ □□: □□.□.□□. 91010:2023

STANDARD FOR GENERIC REQUIREMENTS
No. TEC 91010:2023

CRYPTOGRAPHY SYSTEM

ISO 9001:2015

□□□□□□□□ □□□□□□□□□□□□□ □□□□□□

□□□□□□□□□□□ □□□, □□□□, □□ □□□□□□–110001, □□□□

TELECOMMUNICATION ENGINEERING CENTRE
KHURSHIDLAL BHAWAN, JANPATH, NEW DELHI–110001, INDIA
www.tec.gov.in

© □□.□.□□., 2023
© TEC, 2023

All rights reserved and no part of this publication may be reproduced, stored in a retrieval system or transmitted, in any form and by any means - electronic, mechanical, photocopying, recording, scanning or otherwise, without written permission from the Telecommunication Engineering Centre, New Delhi.

Release1.0, March 2023

Draft document TEC No. 91010:2023 After SubDCC and Mr

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

This document describes the generic requirements and specifications of the Cryptography system for classical as well as Post-Quantum requirements as per the recommendations of ITU-T Y.3802 to Y.3804 for QKD system, ISO/IEC 19790 on information security, security techniques, security requirements for cryptography modules and National Institute of Standards and Technology (NIST) documents on cyber security for use in the Indian public/private networks for safeguarding data integrity, confidentially and authentication for information (primarily personal and commercial/strategic data) against cyber-attacks. The document fulfils users' requirements and developers' interests to have fair market access and guiding documents for ease of business and safeguarding the country's security.

Table of Content

Draft document TEC, No. 91010:2023 After SubDCC and MF

TABLE OF FIGURES

Draft document TEC No. 910 10.2023 After SubDCC and MF

List of tables

Draft document TEC No. 91010:2023 After SubDCC and MF

HISTORY SHEET

Sl.No.	GR No.	Title	Remarks
1.	TEC No : 91010 : 2023	Generic Requirements Standard document for Cryptography System (Post-Quantum/Classical).	First release

Draft document TEC No. 91010:2023 After SubDCC and MF

173

REFERENCES

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.	FIPS 140-3	Security Requirements for Cryptographic Modules
4.	FIPS PUB 197	Advanced Encryption Standard (AES) 2001
5.	FIPS PUB 198	The Keyed-Hash Message Authentication Code (HMAC) 2002
6.	IEC 60825-2/ IS 14624-2	Safety of laser products Part 2 safety of optical fibre communication systems OFCS (First Revision)
7.	IEC 61000-4-11/ IS 14700 (Part 4/Sec 11) : 2020	Testing & measurement technique- voltage dips, short interruptions, and voltage variations immunity tests.
8.	IEC 61000-4-2 / IS 14700 (Part 4/Sec 2) : 2018	Testing and measurement techniques of Electrostatic discharge immunity test
9.	IEC 61000-4-29	Testing and measurement techniques- Voltage dips, short interruptions, and voltage variations on D.C input power port immunity test.
10.	IEC 61000-4-3/. IS 14700 (Part 4/Sec 3) : 2010	Radiated RF electromagnetic field immunity test
11.	IEC 61000-4-4/ IS 14700 (Part 4/Sec 4) : 2018	Testing and measurement techniques of electrical fast transients/burst immunity test
12.	IEC 61000-4-5(2017)/ IS 14700 (Part 4/Sec 5) : 2019	Testing & Measurement techniques for surge immunity test.
13.	IEC 61000-4-6 / IS 14700 (Part 4/Sec 6) : 2016	Testing & Measurement techniques for surge immunity test and Immunity to conducted disturbances
14.	IEEE 802.1AE	Media Access Control (MAC) Security
15.	IEEESTD.2018.8585421	IEEE Standard for Local and metropolitan area networks–Media Access Control (MAC) Security. IEEE. December 2018.
16.	IEC 60215/ IS 10437(1986)	Safety requirements for radio transmitting equipment
17.	IEC 60950-1(2005)/ IS 13252 (2010)	Safety of information technology equipment
18.	ISO/IEC 10116:2006 / IS 15116 : 2018	Information technology – Security techniques – Modes of operation for an n-bit block cipher
19.	ISO/IEC 18033-3:2010/	Information Technology Security Techniques Encryption algorithms

20.	ISO/IEC 19790:2012	Information technology — Security techniques — Security requirements for cryptographic modules
21.	ISO/IEC 24759:2017	Information technology - Security techniques - Test requirements for cryptographic modules
22.	ITU-T X.1811	Security guidelines for applying quantum-safe algorithms in IMT-2020 systems
23.	ITU-T X.800	Security architecture for Open Systems Interconnection for CCITT applications
24.	ITU-T Y.3802	Quantum key distribution networks - Functional architecture
25.	ITU-T Y.3803	Quantum key distribution networks - Key management
26.	ITU-T Y.3804	Quantum key distribution networks - Control and management
27.	NIST standard document	Post-Quantum Cryptography
28.	QM-333	Specification for environmental testing of electronic equipment for transmission and switching use
29.	RFC 3602	The AES-CBC Cipher Algorithm and Its Use with IPsec
30.	RFC 3686	Using Advanced Encryption Standard (AES) Counter Mode with IPsec Encapsulating Security Payload (ESP)
31.	RFC 4106	The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)
32.	RFC 4301	Security Architecture for the Internet Protocol
33.	RFC 4302	IP Authentication Header
34.	RFC 4303	IP Encapsulating Security Payload
35.	RFC 4307	Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)
36.	RFC 4308	Cryptographic Suites for IPsec
37.	RFC 4868	Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec
38.	RFC 5282	Using Authenticated Encryption Algorithms with the Encrypted Payload of the Internet Key Exchange version 2 (IKEv2) Protocol
39.	RFC 7296	Internet Key Exchange Protocol Version 2 (IKEv2)
40.	RFC 7321	Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)
41.	TEC/SD/DD/EMC-221/05/OCT-16	Electromagnetic Compatibility Standard for Telecommunication Equipment

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

CHAPTER-1

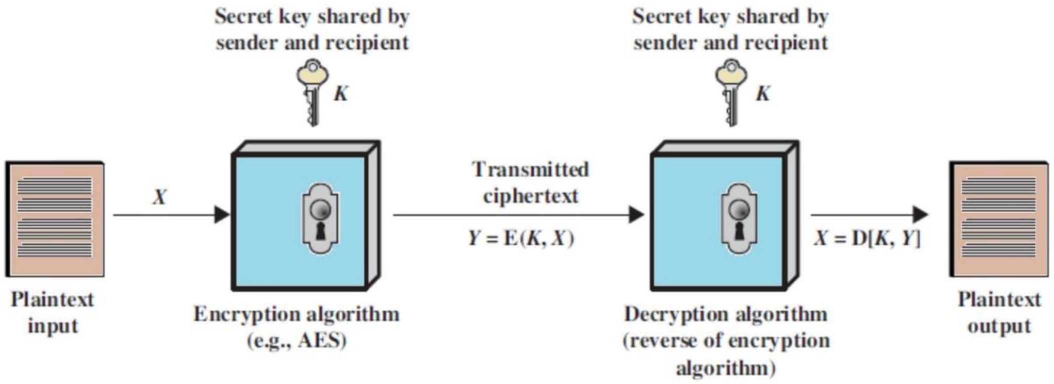
Cryptography System

1.1. Introduction to Classical /Post-quantum(Quantum-safe) Cryptography System

Cryptography is the practice of creating a secure communication channel and protecting data from unauthorised access and modification. It secures communication by protecting the confidentiality and integrity of messages and sensitive data that security practitioners use to safeguard anything that relies on electronic communication and data storage; refer to Figure-1 for a basic cryptographic flow. Cryptography uses computational hardness as a means to protect sensitive data(X). There are cryptographic problems that are difficult or impossible to solve using conventional computing. Public key cryptography has become indispensable to our global communication digital infrastructure. These networks support many applications that are important to our economy, security, and way of life, such as mobile phones, internet commerce, social networks, and cloud computing.

Figure 1: Diagram of the basic flow of a Classical Cryptography

Our most crucial communication protocols rely principally on three core cryptographic functionalities: public key encryption, digital signatures, and key exchange. They implement using Diffie-Hellman key exchange, the RSA (Rivest-Shamir-Adleman) cryptosystem, and elliptic curve cryptosystems. The



security of these depends on the difficulty of specific number theoretical problems such as Integer Factorization or the Discrete Log Problem over various groups.

In 1994, Peter Shor of Bell Laboratories showed that quantum computers, a new technology leveraging the physical properties of matter and energy to perform calculations, can efficiently solve each problem, thereby rendering all public key cryptosystems based on such assumptions impotent. Thus, a sufficiently powerful quantum computer will put many forms of modern communication from key exchange to encryption to digital authentication in peril. In particular, this includes those based on the difficulty of integer factorization, such as RSA and those based on the hardness of the discrete log problem.

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

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 cryptography 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. These families include those based on lattices, codes, multivariate polynomials, 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 so that public-key algorithms protect information on digital infrastructure from future attacks. Consequently, the search algorithms believed to resist attacks from classical and quantum computers have focused on public key algorithms. These are substitutes for what is in use today in classical cryptography systems. The most quantum-resistant algorithms have larger key sizes than the ones they will substitute, which is a big challenge. Quantum 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 a cryptography system

Cryptographic algorithms are broadly classified into two categories i.e., classical and Modern based on the type used during the encryption and decryption process.

1.2.1. Classification of a classical cryptography

Classical cryptography, also known as traditional cryptography, refers to cryptographic methods and techniques developed before the advent of computers. Examples of classical cryptography techniques include substitution ciphers (Caesar ciphers, etc.), transposition ciphers (rail fence cipher,etc), and polyalphabetic ciphers (such as the Vigenère cipher). These techniques rely on the secrecy of the encryption key to secure communication.

1.2.2. Classification of Modern Cryptography

Modern cryptography is based on publicly known mathematical algorithms that operate on binary bit sequences (qubits in the case of quantum technology) and utilise secret keys. There are three types of modern cryptography:

i Symmetric key cryptography
ii Asymmetric key cryptography
iii Hash Function

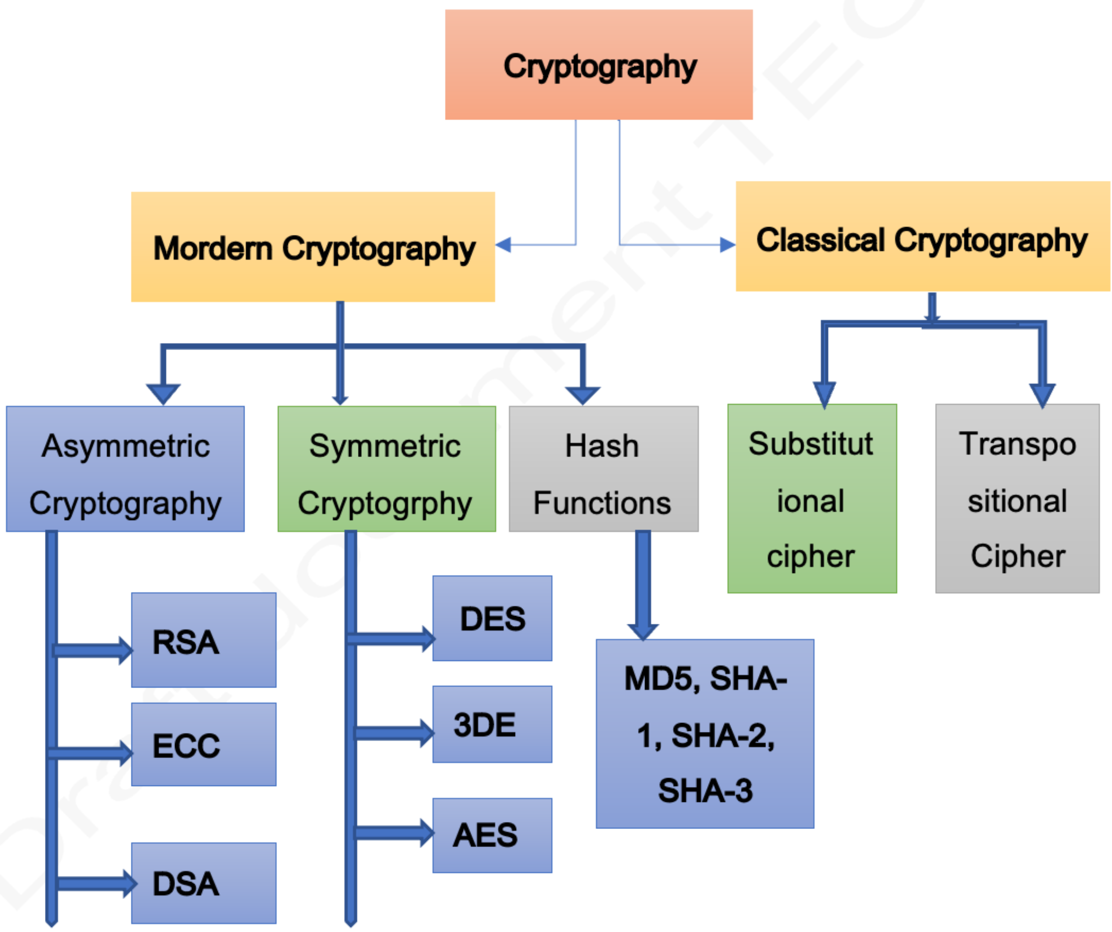


Figure 2 : Diagram of classification of cryptographic techniques/algorithms

1.2.2.1 Symmetric/Secret Key of a Cryptography

In this scheme, encryption and decryption keys are identical, and they 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 Encryption System (AES) and Triple-Data Encryption Standard (DES), i.e., 3DES.

1.2.2.2 Asymmetric/Public 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. It is impossible to determine the private key's value by knowing the corresponding public key. Examples are RSA (Rivest-Shamir-Adleman public-key cryptosystem), DSA (Digital Signature Algorithm), ECC (Elliptic Curve Cryptography), and the Diffie-Hellman algorithm. A combination of asymmetric and symmetric key cryptography schemes is used in most public communication networks. 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 Functions

This algorithm makes no use of any keys. A hash value with a fixed length. There are cryptographic protocols, that do not use keys such as algorithms that require authentication of the integrity of data. Hash functions can also use keys which are called keyed-hash functions. Many operating systems/applications encrypt passwords using hash functions.

1.2.3. Types of a configuration of a cryptographic system

These levels are intended to cover the wide range of potential applications and environments in which cryptographic modules may be employed. Classification of cryptography into modules based on the hardware, software and firmware used within the security boundary. This is applicable to any interdependent or standalone system.

The cryptographic module is defined as one of the following module 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 this 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 working environment's computing platform and operating system in which the firmware runs 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 are external to the defined hybrid firmware module boundary but explicitly bound to the hybrid firmware module.

1.2.3.1 Classification of a Post-quantum (Quantum-safe) Cryptography configuration

Cryptographic modules for post-quantum cryptography systems will need to be updated or replaced with new modules specifically designed for post-quantum cryptography. The classification of post-quantum cryptography modules is like classical cryptography modules, but the algorithms used will be different, especially for public key infrastructure, encryption, key exchange, and hash functions. These algorithms will need to be resistant to quantum computing attacks such as Shor's algorithm. For symmetric key cryptography, doubling the key size can provide some protection against quantum computing attacks, but this is not a complete solution. For asymmetric key cryptography, new search algorithms will need to be developed to be resistant to quantum computing attacks. NIST has been developing post-quantum cryptographic standards in four phases, and the final set of standards is expected to be released in 2024.

1.2.3.2 Post-quantum (Quantum-safe) Symmetric cryptography

Cryptography is vulnerable to quantum attacks. Still, they can correct, including symmetric key algorithms like AES that can be broken faster by a quantum computer running Grover’s algorithm than by a classical computer. However, doubling the cipher’s key length can make a quantum computer work as hard as a conventional computer. The symmetric algorithm AES-128 is as difficult for a classical computer to break as AES-256 would be for a quantum computer. AES considers quantum-safe because the cipher can adapt to a quantum attack by increasing its key size to contain a vulnerability introduced by quantum computing.

1.2.3.3 Post-quantum Asymmetric cryptography

Today's most important uses of public key cryptography are for digital signatures and key establishment. As mentioned in Section 1, 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 factorization, such as RSA and those based on the hardness of the discrete log problem. Post-Quantum Cryptography (PQC) mainly refers to developing new asymmetric cryptography techniques that use a different class of underlying, such as Lattice-based, Code-based, multivariate-based and hash-based mathematically hard problems, which are believed to be secure against both classical and quantum computers.

1.2.3.4 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.) is under consideration in NIST.

XMSS is a more current scheme and is in the process of becoming standardised. It builds on Merkle Trees.

1.3. Elements/subsystems and applications of a cryptography system

Cryptography system Subsystems in classical cryptography systems are the same as in post-quantum cryptography systems except for the implementation of quantum-safe algorithms requires different algorithms on hardware (Key sharing elements like QKD, etc., differ in PQC based on quantum mechanics principle) and software/firmware 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.

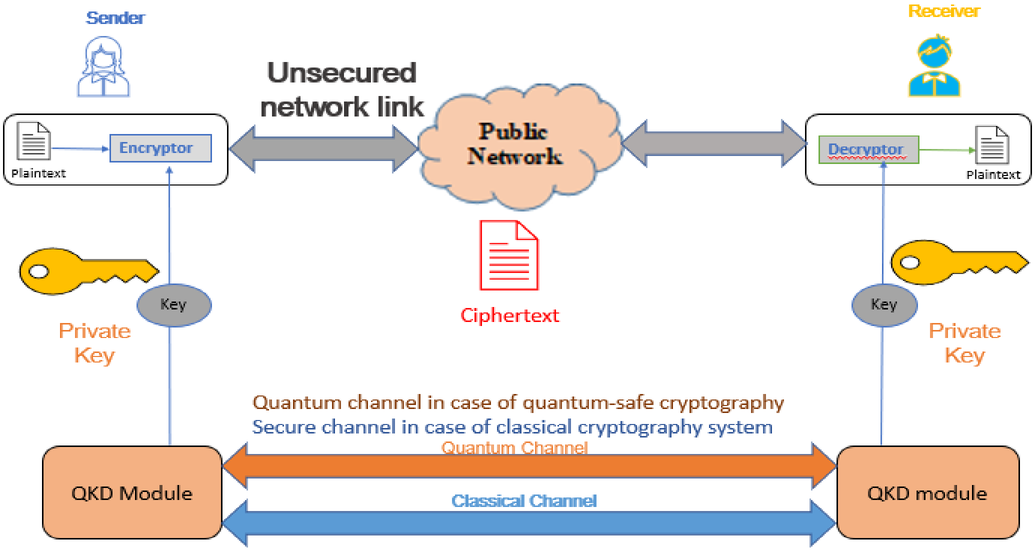


Figure 3 : Block diagram of a Symmetric cryptography system

Note: Encryption algorithms are the same, but the key is from quantum technology basis. Cryptography Key is being shared through QKD and assuming the physical network is secured to ensure theoretically information is secure in quantum key infrastructure.

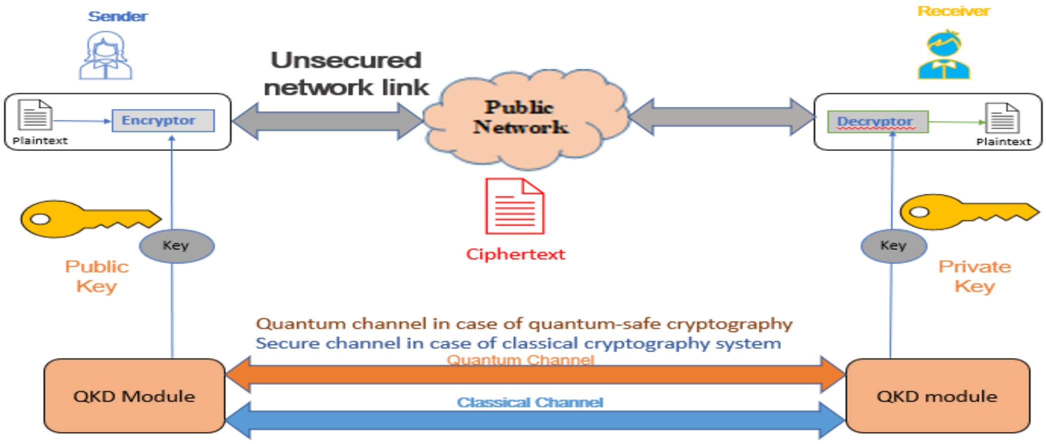


Figure 4 : Block diagram of Asymmetric cryptography system

Note: Encryption algorithms are different, but the Key is from quantum technology basis. In the case of Post-quantum cryptography, the Key is being shared through QKD and assuming the physical network is secured to ensure, theoretically, information is secure in Quantum Key infrastructure.

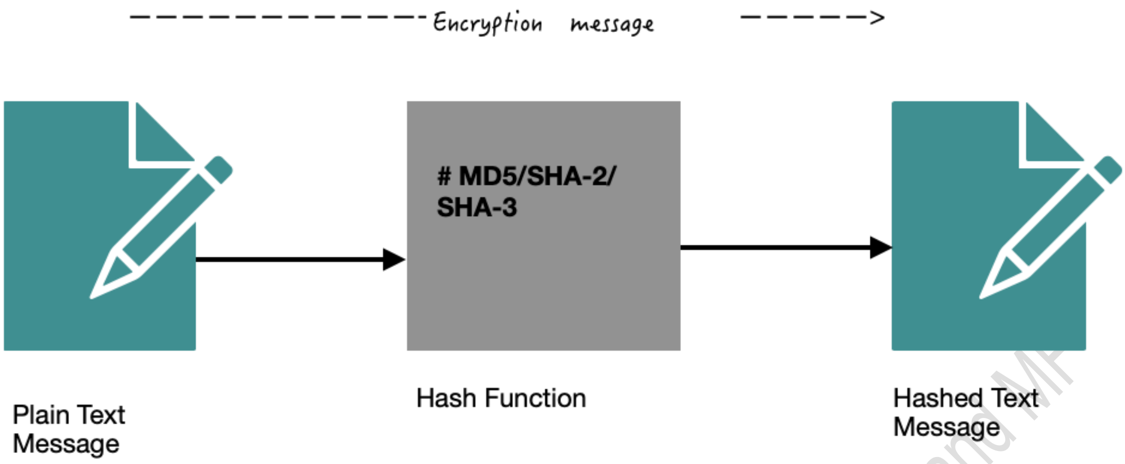


Figure 5 : Block diagram of a Hash functions

Note: Hash function algorithms differ in classical and Post-quantum protocols/algorithms.

1.3.1 Encryptor

Communicate over an unsecured network. Data encryption is changing data from plain text to cipher text using an encryption algorithm and key.

1.3.2 Decryptor

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

1.3.3 Hash Function

Hashing is a method used to verify data integrity. A cryptographic hash function is a process that takes a block of data and creates a small fixed-sized hash value. It is impossible (at least not realistically) to generate the same hash from a different data block. This technique is referred to as collision resistance, refer to figure 5.

i) A Message digest 5 algorithm [MD5]: This creates a 128-bit digest used in the hash function.
ii) Secure Hash Algorithm 1 (SHA-1): This creates a 160-bit digest.
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.

1.3.4 Hashed Message Authentication Code (HMAC)

It uses the mechanism of hashing, but it kicks it up a notch. Instead of using a hash that anyone can calculate, it includes a secret key of some type in its calculation.

1.3.5 Digital Signatures

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

1.3.6 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.

1.3.7 Encryption Protocols

i) Asymmetric key signature and key establishment protocols : DSA (for AES), RSA (for Triple-DES),etc.
ii) Symmetric protocols : DES, 3DES, AES,etc.
iii) Hash algorithms/protocols: MD5, SHA-1, SHA-2 and SHA-3, etc.

1.3.8 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.

1.3.9 Quantum Computing

Quantum computing is the exploitation of collective properties of quantum states, such as superposition and entanglement, to perform computation. It is a new branch of computing in which the fundamental storage unit is Qubits rather than bits in the conventional computer. A Qubit can store both 0 and 1 at the same time. Quantum computers perform calculations based on the probability of an object's state before it is measured - instead of just 1s or 0s - which means they have the potential to process more data exponentially compared to classical computers. In short, Quantum computers can perform very rapid parallel computations compared to classical computers.

1.3.10 QKDN Controller

It Controls Key distribution between QKD and Cryptosystem for key sharing over a quantum channel.

1.3.11 QKD channel

It uses a small amount of random secret data initially shared between the sender and receiver.

1.3.12 Post-quantum (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. This problem is NP-hard. And unlike the factorization problem nor the discrete log problem, there is no known quantum algorithm to solve SVP with the help of a quantum computer. Among all the candidates, the two **algorithms** NTRU (enhanced version SS-NTRU, which had a reduction to problems over ideal lattice) and Learning With Error (LWE) is a mathematical problem that is widely used in cryptography to create secure encryption algorithms, deliver the best performance and security. In practice, the Ring Learning With Error (R-LWE) variant is usually used to boost efficiency. The R-LWE and SS-NTRU are reducible to the same lattice problem.

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 UOV and Rainbow. There also exist BigField methods such as HFE (Hidden Field Equations) and pFLASH.

iv. **Lattice-based signature Scheme**: Lattice-based algorithms are faster and are considered quantum-safe. The parameter for lattice problems is named lattice-based signature schemes based on short integer solution(SIS). The latest outcome, BLISS (Bimodal Lattice Signature Scheme), is currently popular. The signature scheme has approximately 0.6 KB public-key size and 0.25 KB private key size comparable in strength to AES-128.

1.3.13 Hash based cryptosystems

Hash-based 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. XMSS is a more current scheme and is in the process of becoming standardised likely.

1.3.14 X.509 certificates

To authenticate the service channel required by a QKD system during the key distillation phase of the QKD protocol.

1.3.15 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 Diffie- Hellman key agreement that maintains QKD, may be used 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. QKD's shared secrets may be used with conventional encryption ciphers or for one-time pad encryption in high-security applications. QKD may also be used for the second pass to solve the key management problem of distributing shared secret keys for message authentication.

1.3.16 Transport layer security (TLS)

TLS is used to secure a variety of applications, including web traffic (the HTTP protocol), file transfer (FTP), and mail transport (SMTP). 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 TLSv1.2, all cryptographic components (public key authentication, key exchange, hash functions, bulk encryption) can be negotiated, although generally, all must be arranged at once 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 utilizing 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.

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

It is a standard for digital signatures and public-key encryption used 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 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. Unfortunately, the aforementioned key establishment algorithms for these symmetric keys and the algorithms used for digital signatures are insecure in a post-quantum environment.

1.3.18 Secure Shell (SSH)

It is a secure remote-login protocol. It has pervasive and diverse applications and can be used for various purposes, including the construction of 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 algorithms that are insecure 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 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 a viable method 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.

1.3.19 Encryption and authentication of endpoint devices

Endpoint devices include any piece of hardware that a user utilizes 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 of endpoint devices refers to the practice of making the contents of the device unreadable to unauthorized parties through the use of cryptography and security protocols. This mechanism is a critical practice to prevent unauthorized 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.

1.3.20 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.

1.3.21 Cloud Storage and computing

Cloud storage allows users to utilise centralised, shared resources (both 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, including accessibility from multiple devices/locations, a reduction in a business's need for in-house IT solutions, and optimised use of computing power distributed across many users and businesses. 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 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.

1.3.22 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, an encryptor 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) **Non-repudiation**:
Nonrepudiation prevents either sender or receiver from adverse a transmitted message. Therefore, when a message is sent, the receiver can validate that the asserted sender actually sent the message. Similarly, when a message is received, the sender can validate that the asserted receiver actually received the message.

1.4. Functional requirements of a cryptography system

Cryptographic System should work in point-to-point/ point-to-multipoint / multipoint-to-multipoint mode based on network deployment topologies (Refer Figure 6).

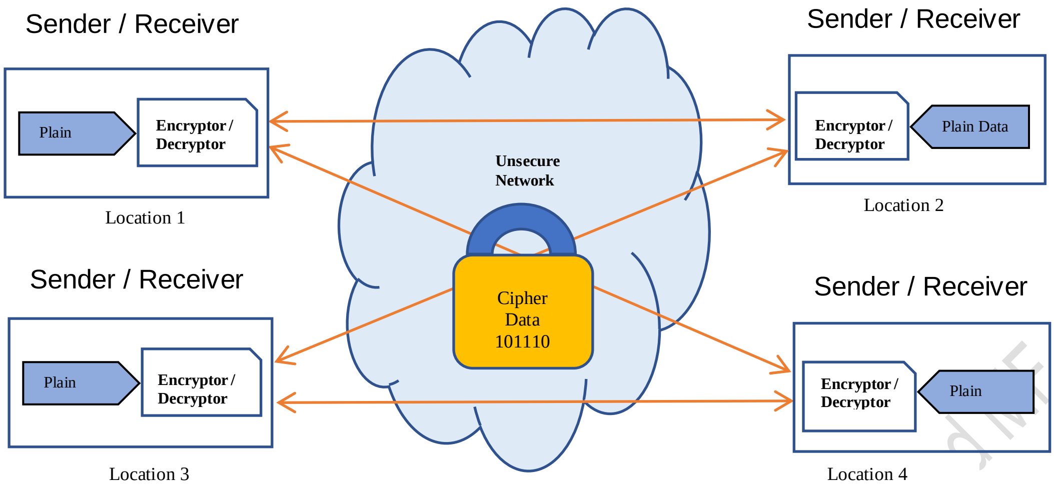


Figure 6 : Deployment of PQC/Classical Network

i. Point to Point: Sender ‘A’ can transmit encrypted data to a single Receiver. ‘A’ can transmit encrypted data to “C” and vice versa.

ii. Point to Multipoint: Sender ‘A’ can transmit encrypted data to two or more Receivers. ‘A’ can transmit encrypted data to both ‘C’ and ‘D’ and vice-versa.

iii. Multipoint to Multipoint: Multiple Senders can transmit encrypted data to Multiple Receivers. ‘A’ and ‘B’ can transmit encrypted data to both ‘C’ and ‘D’ and vice-versa.

1.4.1 Functional requirements of classical Cryptography System

The Cryptographic System shall provide Ethernet payload encryption over a point-to-point network. Encryption of payload of normal Ethernet frame and Ethernet frames with multiple VLAN tags (Q-in-Q) using operator selected symmetric key encryption scheme. (optional for defence/user requirements for custom use in case user required) future-proof and fully reprogrammable (preferably FPGA based or equivalent on any programmable device on H/w or stack over S/W.

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

ii. It shall provide confidentiality protected firmware upgrades.

iii. It shall support Policy based encryption.

iv. It shall be protocol and application transparent Encryption provides continuous file-level encryption that protects against unauthorized access by users and processes in physical, virtual, and cloud environments so that implementation is seamless and transparent to your applications/databases and storage, and so it can work across an enterprise’s entire environment.

v. The Encryptor, regardless of performance level, shall be interoperable with each other with the appropriate Application interface.

vi. It shall provide confidentiality using standard encryption algorithms in a post-quantum cryptosystem and applicable algorithms in asymmetric and hash functions.

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

Table 2 : Functional requirements of a cryptography system

S. 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 RFC
2	No of Concurrent connection	User to server mode		Atleast 500 connections
3	Direction of data transmission	Full duplex line-rate encryption		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	Latency at node	Not more than 10 µsec on data@10 GB maximum	independently of the packet/Ethernet frame size (Non-aggregation state)
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:	
9		Stream ciphers (CFB, OFB)	ISO/IEC 18033-4 Encryption Algorithms-Part 4	
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		Discrete logarithm based techniques	ISO/IEC 9796-3 Information	Digital signature with message recovery – Part 3

Draft document TEC No. 91010:2023 After SubDCC and MF

S. No	Parameter Type	Description and range of the Parameters	Reference Standard(s)	Remarks
			technology–Security techniques	
12		Digital signatures	ISO/IEC 14888 (all parts) Information technology–	Security techniques – Digital Signatures
13		Cryptographic techniques based on elliptic curves	ISO/IEC 15946 (all parts) Information technology–	Security techniques
14		Asymmetric cryptographic algorithms	ISO/IEC 18033-2: Information technology–	Security techniques — Encryption Algorithms Part 2:
15	Message Authentication Codes	Mechanisms using a dedicated hash-function	ISO/IEC 9797-2 Information technology–Security techniques —	Message Authentication Codes (MACs) - Part 2
16	Hash functions	Hash functions using an n-bit block cipher.	ISO/IEC 10118-2 Information technology –	Security techniques – Hash functions – Part 2
17		Dedicated hash functions	ISO/IEC 10118-3 Information technology –	Security techniques – Hash functions – Part 3
18		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		Mechanisms using digital signature techniques.	ISO/IEC 9798-3 Information technology – Security techniques –	Entity authentication – Part 3
21		Mechanisms using a cryptographic check function.	ISO/IEC 9798-4 Information technology –	Security techniques – Entity authentication – Part 4

Draft document TEC No. 91010:2023 After SubDCC and MF

S. No	Parameter Type	Description and range of the Parameters	Reference Standard(s)	Remarks
22		Mechanisms using zero-knowledge techniques.	/IEC 9798-5 Information technology –	Security techniques – Entity authentication – Part 5
23		Mechanisms using manual data transfer	ISO/IEC 9798-6 Information technology –	Security techniques – Entity authentication – Part 6
24		Mechanisms using symmetric techniques	ISO/IEC 11770-2 Information technology	Security techniques Key Management Part 2
25		Mechanisms using asymmetric techniques	ISO/IEC 11770-3 Information technology –	Security techniques – Key Management – Part 3
26	Key establishment mechanisms based on weak secrets.		ISO/IEC 11770-4 Information technology – Security techniques –	Key Management – Part 4
27	Random bit generation	Truly Random bit generation	ISO/IEC 18031 Information technology	Security techniques
28	Software/ Firmware loading	The cryptographic module has the capability of loading software or firmware from an external source	ISO/IEC 19790:2012/Cor.1:2015(E) 7.4.3.4	the loaded software or firmware shall be validated by a validation authority prior to loading
29	Self-test for 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

Draft document TEC No. 91010:2023 After SubDCC and MF

1.5. Operational requirements of a cryptography 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.

Table 3 : Operational requirements of a cryptography system

S.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 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 to reflect 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)	Zeroization 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 passes
7	Bypass test	Indicate whether 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

Draft document TEC No. 9110:2023 After SubCC and MF

				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 50/60 Hz AC
12	DC power	DC Power supply Range from -40 V to -60 V	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
14	Cooling	a) Requirement of Ingress or Egress fans (suck and exhaust kind of setup).		
15	Min Altitude without any degradation	equipment without any degradation at an altitude upto 3,000 meters.		The manufacturer shall guarantee the 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)	Visual observation	

1.6. Interface requirements of a cryptography system

Cryptographic System shall support 10/100/1000 BASE-TX 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 the Cryptography system

S	Name of the Sub parameter	Types of Parameters range	Reference Standard(s)	Remarks
1	Management Interface	Optical//Ethernet (RJ45) Ethernet data input (plain text, cipher text, SSP, and status information from other module) through command line interface also.	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	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 software module, power is provided internally by the source of battery
7	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
8	Trusted channel (Secuirty Level 3 and above)	Link for the transmission of unprotected plaintext CSPs, key components and authentication data between the	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

		cryptographic module and the sender or receivers endpoint of the cryptographic module		

1.7. Interoperable requirements of a cryptography system

Interoperability is one of the essentials to assessing internetwork function in a heterogenous network.

Table 5 : Interoperable requirements of a cryptography system

Sl. No	**Name of the Sub parameter**	**Types of Parameters range**	**Reference Standard(s)**	**Remarks**
1	IP packet IPv4/6	IPV4/IP6 stack	IP network type	Confirmation of interworking on IPv4/6
2	Authentication	CA or other agency	RADIUS server	
3	Encryption		Devices	
4	Key exchange	During key exchange with other system	System	
5	API	Code for middleware function		
6	SSH			
7	TLS			
	Clock			

1.8. Quality requirements of a cryptography 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 in accordance with the international quality management system ISO 9001:2000 for which the manufacturer should be duly accredited. A quality plan describing the quality assurance system followed by the manufacturer would be required to 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 cryptography systems

Draft document TEC No. 91010:2025 After SubDCC and MF

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	Shock			
5	Vibration			
6				

1.9. EMI/EMC Requirements

The equipment shall conform to the EMC requirements as per the following standards and limits indicated therein. A test certificate and test report shall be furnished by an accredited test agency.

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 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 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.

Draft document TEC No. 91010:2023 After SubDCC and MF

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 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 corresponding to a reduction of supply voltage of > 95% for 5s.

iv. A voltage interruption corresponding to a reduction of 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 specifically. 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 the cryptography system

S	**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)	

Draft document TEC No. 91010:2023 After Sub DCC and MF

6	**Im**munity to conducted disturbance induced by Radio frequency fields:		IEC 61000-4-6 (2013)	radio-frequency (RF) transmitters in the frequency range 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

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 should 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 the cryptography system

S	**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 telecommunicat	requirements intended to reduce risks of fire, electric	ITU-T K.51	persons who may come into contact

	ion network equipment	shock or injury		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

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

Draft TEC No. 91010:2023 After SubDCC and MF

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 cryptography system

Draft document TEC No. 91010:2023 After SubDCC and MF

	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 of 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. Executable code.	An approved digital signature or keyed message authentication code-based integrity test.	Approved digital signature based integrity test.		ISO/IEC 19790:2012/ Cor.1:2015(E) 7.5
4	Operational Environment	Non-Modifiable, Limited or Modifiable. Control of SSPs.	Modifiable. Role-based or discretionary access control. Audit mechanism.	Non modifiable		

Draft document TEC No. 91010:2023 After SubDCC and MF

5	Physical Security	Production-grade components.	Tamper evidence. Opaque covering or enclosure.	Tamper detection and response for covers and doors. Strong enclosure or coating. Protection from direct probing. EFP or EFT.	Tamper detection and response envelope. EFP. Fault injection mitigation.	ISO/IEC 19790:2012 / Cor.1:2015(E) 7.7.
6	**Non-Invasive Security**	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.				ISO/IEC 19790:2012 / Cor.1:2015(E) 7.8
7	**Sensitive security parameter generation**	Random bit generators, SSP generation, establishment , entry and output , storage, and zeroization. Automated SSP transport and SSP agreement using approved methods.				ISO/IEC 19790:2012 / Cor.1:2015 (E) 7.9.7
		Manually established SSPs may be entered or output in plain text		Manually established SSPs may be entered or output in encrypted form via trusted channel or split knowledge procedures		
8	Self Tests	Pre-operational :Software/firmware integrity , bypass and critical functional test. Conditional: Cryptographic algorithm, pair-wise consistency, Software/firmware loading, manual entry, bypass and critical functional test.				ISO/IEC 19790:2012/ Cor.1:2015(E) 7.9.2
9	Mitigation of other attacks	Specification of Mitigation of attacks for which no testable requirements are available currently			Specification of Mitigation of attacks with testable requirements	ISO/IEC 19790:2012/ Cor.1:2015(E) 7.12
1	Replay attacks					
1	Fault injection attacks					
1	timing-based side-channel attacks					

Draft document TEC No. 9010:2025 After SubCC and MF

1	Other unknown attacks					
1	Documentation and validation					

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 As per clause 2.1, Purchaser may specify the functional requirement as per the requirements under optional parameters.

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

1.12.5 The discretion of the Purchaser allows them to include the latest technical Specification as per their own 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 so as 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 Specification for the same will be submitted by the vendor.

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 exchange a new session key automatically 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 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 Encryptors can also provide support for Post-quantum key exchange algorithms that are 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 Encryptor shall support SNMPv3 or the latest and shall provide multiple manager support.

1.12.22 Encryptor shall support audit and event logging with Syslog support.

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

1.12.24 Encryptor 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 requirement of the repair Manual may be clearly mentioned by the Purchaser 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.

Draft document TEC No. 91010:2023 After SubDCC and MF

CHAPTER-2

Specifications and Certification

2.1 Specification requirements of the category/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/post-quantum Cryptography 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 but no change in compliance.

2.1.1 Specification requirements of the category/configuration of a Classical cryptography systems

Table 10 :Specification* requirements of the category/configuration *of a Classical cryptography systems

S 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 for applicable capacity
2	Interface for management	Ethernet/API				support 10/100/1000 BASE-TX with option SFP/SFP+ capable transceivers for applicable capacity and CLI compatibility.
3	Throughput/Information pay load at client/Spoke	10Mbps/ 100Mbps/1Gbps				Concatenation of data in case more than one port
4	Throughput/Information pay	100Mbps/1Gbps/10Gbps				

Draft document TEC No. 91010:2023 After SubDC

	load at Server/Hub		
5	Latency at client/Spoke	1/5/10 micro seconds	
6	Latency at Server/Hub	1/5/10 micro seconds	
7	No Concurrent connections	500 @server to handle simultaneous connections	
8	Level of trustyworthiness		
9	Symmetric Key encryption and decryption	AES-128, AES-192, AES-256 and above	Any proprietary algorithms as per the needs of the user
10	Asymmetric Key encryption and decryption	RSA-2048 and above	Any proprietary algorithms as per the needs of the user
11	Key Exchange	Diffie-Hellman-2048 and above/ RSA-2048 and above	Any proprietary algorithms as per the needs of the user , if any
12	Digital Signature	DSA-2048 and above/ECDSA 224-255 , 256 and above/RSA-2048 and above	Any proprietary algorithms as per the needs of the user, if any
13	n-bit block cipher	Electronic codebook (ECB), Cipher block chaining (CBC), Cipher Feedback (CFB),Output feedback (OFB) Counter (CTR)	
14	N/W Topology	Hub and spoke or Mesh network or Point -to -Point or Point-to-Multipoint	

2.1.2 Specifications *requirements of the category/configuration* of Post-quantum cryptography systems

Table 11 : Specification* requirements of the category/configuration *of a post-quantum cryptography systems

S	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 for

Draft document TEC No. 9100:2023 After SubDC

			applicable capacity
2	Interface for management	Ethernet/API	support 10/100/1000 BASE-TX with option SFP/SFP+ capable transceivers for applicable capacity and CLI compatibility.
3	Throughput/Information pay load at client/Spoke	10Mbps/ 100Mbps/1Gbps	Concatenation of data in case more than one port
4	Throughput/Information pay load at Server/Hub	100Mbps/1Gbps/10Gbps	100Mbps/1Gbps/ 10Gbps
5	Latency at client/Spoke	1/5/10 micro seconds	1/5/10 micro seconds
6	Latency at Server/Hub	1/5/10 micro seconds	
7	Level of trustyworthiness		
8	Symmetric Key encryption and decryption	256 and above	PQC safe algorithms
9	Asymmetric Key encryption and decryption	NTRU, Classic McEliece	
10	Key Exchange algorithms/Key encapsulation mechanism	CRYSTALS-KYBER Kyber-512, Kyber-768, and Kyber-1024	
11	Digital Signature	CRYSTALS-KYBER,CRYSTALS-Dilithium, FALCON, and SPHINCS+	
12	Hash Function	LMS, XMSS, SPHINCS+, HORS	
13	n-bit block cipher	Electronic codebook (ECB), Cipher block chaining (CBC), Cipher feedback (CFB),Output feedback (OFB) Counter (CTR)	
14	N/W Topology	Hub and spoke or Mesh network or Point -to -Point or Point-to-Multipoint	

Note:

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

Draft document TEC No. 91010:2023 After SubDCC and MF

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 laid down in the respective TEC technical standards. The testing is generally carried out on-site at the OEMs premises or in a lab environment. For these certifications, test reports related to EMC, Safety, Environmental Testing etc., from TEC designated labs are also accepted. 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 List of Voluntary Certificates

(i) Type Approval (TA): Type Approval is the process of testing and certification of telecom & related ICT product in accordance with TEC Test Guide for conformance with the Standard for Generic Requirements for a Product/Equipment issued by TEC. Optional parameters as 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, in accordance with TEC Test Guide, for conformance with the Standard for Interface Requirements for a Product/Equipment issued by TEC. Optional parameters as 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 testing shall be conducted in accordance with the Test Guide approved by TEC. The objective should be to complete the certification process as early as possible in order to encourage innovators/entrepreneurs/startups to seek certification.

(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 as 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 / information 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 table 2.1 above.

2.2.3 Mandatory Testing and Certification of Telecom Equipment (MTCTE)

The Indian Telegraph (Amendment) Rules, 2017, provides that every telecom equipment must undergo mandatory testing and certification prior to sale, import, or use in India. The final detailed procedure for Mandatory Testing and Certification of Telecom Equipments(MTCTE) under these rules 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 and based upon their test reports, a certificate shall be issued by TEC.

Note 1. The eligible applicant shall offer the product to the RC Division, TEC-HQ (being the nodal division for coordination) along with requisite documents (No. TEC 05019:2021 15 mentioned in para 7.2.1). The RC Division will acknowledge the same and forward it to the concerned Core Division for further processing. In case any clarification/information is required, the Core division shall directly communicate with the applicant.

Draft document TEC No. 91010:2023 After SubCC and MF

DEFINITIONS AND TERMINOLOGY

Application link:

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

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.

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.

Classical channel: A 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:

Draft document TEC No. 91010:2023 After SubDCC and MF

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 module:
The hardware, software, and/or firmware that implements approved security functions (including cryptographic algorithms and key generation) is contained within a cryptographic boundary.

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.

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 the purpose of 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.

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.

Initialization 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.

Draft document TEC No 9106:2023 After SubDCC and MF

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

Key Supply: A function providing keys to cryptographic applications.

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 Confirmation:
A procedure is used to assure 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.

Key information:
Information related to a key includes the keying material and associated metadata linking to that key.

Key management:
The activities involve handling cryptographic keys and related security parameters (e.g., IVs and counters) during the entire life cycle of the keys, including their generation, storage, establishment, entry, output, use, and destruction.

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

Key transport:

Draft Document TEC No 91010:2023 After SubDCC and MF

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 is used to provide confidentiality and integrity protection for other keys.

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 such that they share at least one cryptographic key.

Message Authentication Code (MAC):
A cryptographic checksum on data that uses an approved security function and a symmetric key to detect both 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 message was actually signed by a given entity.

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.

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 that 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.

Draft Document TEC No. 9010:2023 Att: SubDCC and MT

Plaintext:
Data that has not been encrypted; intelligible data that has meaning and can be understood without the application of 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).

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 that is uniquely associated with an entity and is 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: -

1. Compute the corresponding public key,
2. Compute a digital signature that may be verified by the corresponding public key.
3. Decrypt data that was encrypted by the corresponding public key, or
4. 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 that is uniquely associated with an entity, and that may be made public. In an asymmetric (public) key cryptosystem, the public key is associated with a private key. The public key may be known by anyone and, depending on the algorithm, may be used to -

1. Verify a digital signature that is 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 is determining the private key from the public key is computationally infeasible.

Public Key Infrastructure (PKI):
A framework that is established to issue, maintain, and revoke public key certificates.
Quantum Channel: Communication channel for transmitting quantum signals.

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 and 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 is published by the Internet Engineering Task Force.

RSA:
A public-key algorithm that 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 secret key is also called a symmetric key. The use of the term "secret" in this context does not imply a classification level but rather implies the need to protect the key from disclosure. Compared with a private key, which is used with a public-key (asymmetric key) algorithm.

Sensitive (information):
Sensitive but unclassified information.
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) that is required to break a cryptographic algorithm or system.

Server:

A computer or device on a network that manages network resources. Examples include file servers (to store files), print servers (to manage one or more printers), network servers (to manage network traffic), and database servers (to process database queries).

Sender/ Receiver:
This document defines the sender/transmitter as Alice and the receiver as Bob.
Signature Generation:
The use of a digital signature algorithm and a private key to generate a digital signature on data.

Signature Verification:
The use of a digital signature and a public key to verify a digital signature on data.

Source Authentication:
The process of providing assurance about 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

Draft document TEC No. 91010:2023 After Sub/CC and MF

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 that is 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 that specifies a security protocol that is used to encrypt and authenticate network communications for software applications. TLS v1.0 is the subsequent version of SSL v3.

User Network:

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

Draft document TEC No. 91010:2023 After SubDCC and MF

ACRONYMS:

For this document the following abbreviations apply:

AC	Alternating Current
ACL	Access Control List
AES	Advanced Encryption Standard
AH	Authentication Header
ANS	American National Standard
ANSI	American National Standard Institute
CA	Certificate Authority
CBC	cipher-block chaining
CTR	Counter
CLI	Command Line Interface
DC	Direct Current
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 Arrays
GCM	Galois/Counter Mode
HMAC	Hash-based Message Authentication Code
IEC	International Electrotechnical Commission
IP	Internet Protocol
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	Initialization Vector
LAN	Local Area Network
MAC	Message Authentication Code
NIST	National Institute of Standards and Technology
OFB	Output Feedback Mode
OID	Object Identifier
OSI	Open Systems Interconnection
PFS	Perfect Forward Secrecy
PKI	Public Key Infrastructure
PRNG	Pseudo Random Number Generator
QKD	Quantum Key Distribution
RADIUS	Remote Authentication Dial-In User Service
RH	Relative Humidity
RFC	Request For Comments
RSA	Rivest, Shamir, Adleman
SFP	Small Form Factor Pluggable
SNMP	Simple Network Management Protocol
SSL	Secure Sockets layer
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
WAN	Wide Area Network

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

Draft document TEC No. 91010:2023 After SubDCC and MF