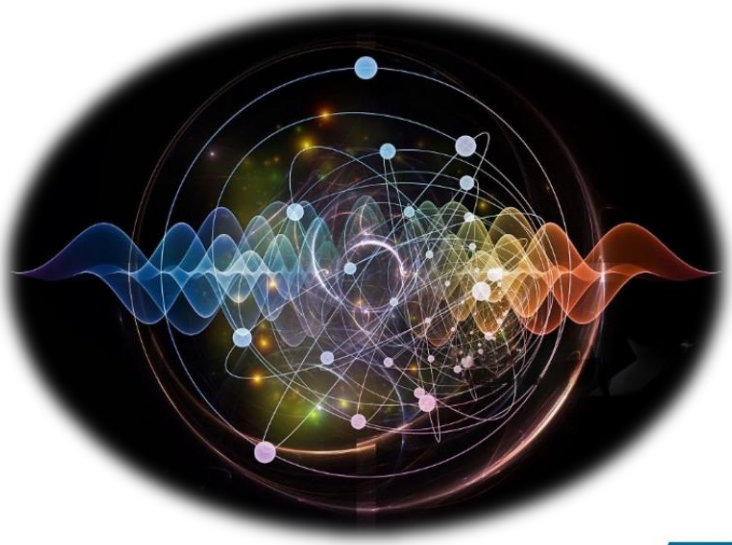
सत्यमेव जयते

TECHNICAL REPORT
on
Quantum Secure 5G / beyond 5G Core using Post-Quantum Cryptography

TEC 910028:2025



ISO 9001:2015

दूरसंचार अभियांत्रिकी केंद्र
खुर्शीदलाल भवन, जनपथ, नई दिल्ली – ११०००१, भारत
TELECOMMUNICATION ENGINEERING CENTRE
KHURSHIDLAL BHAWAN, JANPATH, NEW DELHI–110001, INDIA
https://www.tec.gov.in

RELEASE 1.0 JANUARY 2025

Important Notice

Individual copies of the present document can be downloaded from **http://www.tec.gov.in**
Users of the present document should be aware that the document may be subject to revision or change of status.

Any comment/suggestions may please be sent to: ddgqt.tec-dot@gov.in

Disclaimer

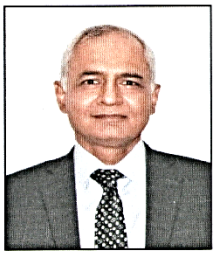
The information contained in the report is compiled based on the contributions received from the members of the committee formed for this purpose. The report is based on the consensus built upon the contributions of the members deliberated on the subject in the multiple rounds of meeting.

डॉ. नीरज मित्तल, भा.प्र.से.
सचिव
DR. NEERAJ MITTAL, IAS
Secretary

सत्यमेव जयते

आज़ादी का अमृत महोत्सव

भारत सरकार
संचार मंत्रालय
दूरसंचार विभाग
Government of India
Ministry of Communications
Department of Telecommunications



MESSAGE

I am delighted that Telecommunication Engineering Centre (TEC), in collaboration with the subject matter expert from the Academia, Industry and Start-ups, has prepared technical report on ***Quantum Secure 5G / beyond 5G Core using Post-Quantum Cryptography.*** This report will be useful to the telecom service providers and captive non-public network (CNPN) users.

The purpose of the report is to sensitize the organizations about securing different interfaces of the 5G Core system by using PQC algorithms which are designed to resist quantum attacks. By securing the interfaces within the 5G Core with PQC, either through a full transition or a hybrid approach combining classical and quantum-safe encryption, we can ensure long-term data protection and network integrity. This proactive step will safeguard telecom infrastructure, prevent potential cyber threats, and ensure that India's digital ecosystem remains secure and future-ready.

Since, 5G Core systems rely on interconnected subsystems that communicate using classical cryptographic techniques, the emergence of quantum computers could expose these interfaces to cyber risks, making it crucial to enhance security measures now. Therefore, there is an immediate need for organizations to prepare for dealing with the quantum threat by securing the interfaces of the 5G Core system.

I appreciate the efforts of Telecommunication Engineering Centre in bringing out the report.

New Delhi
Dated: 26th March, 2025

(Dr. Neeraj Mittal)

कमरा नं. 210, संचार भवन, 20, अशोक रोड, नई दिल्ली-110001 / Room No. 210, Sanchar Bhawan, 20, Ashoka Road, New Delhi - 110001
Ph. : +91-11-23719898, Fax : +91-11-23711514, E-mail : secy-telecom@gov.in

तृप्ति सक्सेना,
TRIPTI SAXENA
वरिष्ठ उप महानिदेशक एवं प्रमुख
Sr. Deputy Director General & Head

सत्यमेव जयते

भारत सरकार
दूरसंचार विभाग
दूरसंचार अभियांत्रिकी केन्द्र
खुर्शीद लाल भवन, जनपथ, नई दिल्ली 110001
Govt. of India
Department of Telecommunications
Telecom Engineering Centre
Khurshid Lal Bhawan, Janpath, New Delhi-110001

Foreword

TEC has played a crucial role in the development of telecom ecosystem of India as the technical arm of Department of Telecommunications. TEC is committed to develop standards for the telecommunication sector in India, to ensure development of world class telecom network and smooth interconnection of individual networks.

TEC provides technical support to DOT and other government departments by formulating technical standards for telecom equipment, networks, systems and services to be deployed in Indian Telecom Network. TEC actively participates in the meetings of standards development organizations, viz., ITU, ETSI, APT, WRC, etc. These standards are made after wide stakeholder consultations. During formulation of above mentioned documents, 'Test Schedule Test Procedure' (TSTP) is also prepared to carry out testing and certification of the equipment.

To disseminate information and awareness about the latest developments in Telecom and IT domain, TEC regularly organise Webinars and release Study Papers. In this endeavour, Quantum technology division under TEC, DoT has prepared a technical report on Quantum Secure 5G / beyond 5G Core using Post-Quantum Cryptography with active participation and contribution of subject matter experts from Academia, Industry and start-ups of National Working Group on Quantum Technology (NWG-QT) and members of Manufacturer's Forum of Mobile Technology (MT) and Quantum Technology (QT) division.

The report will be very useful to telecom service providers and captive non-public network (CNPN) users to sensitize the organizations about securing interfaces of the 5G Core system by using post-quantum cryptographic algorithms.

I wish all the best to the officers involved in releasing the report on the important subject.

(Ms. Tripti Saxena)

ISO 9001:2015

दूरभाषा/Tel.:+91-11-23320252
ई-मेल/E-mail: srddg.tec@gov.in वेबसाइट/Website : www.tec.gov.in

List of Contributors

A. Approving Authority

Name	Designation	Organization
Ms. Tripti Saxena	Sr DDG & Head	TEC, DoT

B. Authors / Drafting Committee

S.No.	Name	Organization
1.	Sh. Kamal Kr Agarwal, DDG (QT)	TEC, DoT
2.	Sh. Vipin Rathi, Assistant Professor	University of Delhi
3.	Sh. Aditya Koranga	Coran Labs
4.	Sh. Shubham Kumar	Coran Labs
5.	Sh. Lakshya Chopra	Coran Labs
6.	Sh. Jaswinder S. Oberai	Synergy Quantum India Pvt Ltd.
7.	Sh. Vipin Gupta	Ericsson
8.	Sh. Ajay Nijwahan	Intel
9.	Sh. Sabyasachi Mandal	C-DoT
10.	Smt. Vibha Mehra	Nokia
11.	Col Suhail Zaidi (Retd) Director General	MAIT
12.	Professor Prasanta K. Panigrahi	IISER Kolkata
13.	Smt. Arpita Maitra	TCG Crest
14.	Sh. Anuj Mehrotra	IOTAONEIQ Solutions Pvt. Ltd.
15.	Sh. Neelesh Singh Katoch	Quantum Al Global

C. Editorial Committee

S.No.	Name	Organization
1.	Ms. Poonam Kumari, ADET (QT)	TEC
2.	Sh. Aryan Joshi, RA (QT)	TEC
3.	Sh. Adil Shaharyar, RA (QT)	TEC

Table of Contents

Executive Summary

With the advancement in Quantum technologies, there is a looming threat to the existing classical cryptography. It is paramount to safeguard the critical telecom infrastructure by using the post quantum cryptography algorithm announced by NIST in the recent past or by applying Quantum key distribution approaches.

India has rolled out 5G in mobile communication in the shortest span of time. Now, the 5G system is the backbone of communication at present. The Core of the 5G system is having multiple sub systems. These sub systems are interfaced with each other by using the existing classical cryptography techniques. Now, it is imperative to secure the interfaces using the post quantum cryptography algorithms to start with as the quantum computers may be available in the telecom network any time.

This technical report defines one of the possible solutions to secure different interfaces of the 5G Core system. This technical report emphasizes flexibility, offering both homogeneous and hybrid cryptographic approaches to telecom operators to safeguard their network against the emerging quantum threats.

1.0 Introduction

The field of Quantum computing has seen notable advancements in the last few years. With the development of Quantum computers looming around the corner which have the computational capabilities that their classical counterparts fail to match, the modern digital security systems may soon collapse. These systems are based on public-key cryptosystems which would be rendered moot once we have the computational power of quantum computers. This poses a serious threat to the integrity of digital communications, especially in sectors like telecommunications where security is of utmost importance.

Post-Quantum Cryptography (PQC), also known as quantum-resistant cryptography, is a nascent field, evolving on a daily basis that focuses on developing cryptographic algorithms that are secure against the advanced capabilities of quantum as well as classical computers and can integrate efficaciously with the existing communication protocols and networks.

In 2015, NIST initiated the selection and standardization of quantum-resistant algorithms to counter potential threats from quantum computers. After assessing 82 algorithms from 25 countries, the top 15 were identified with global cryptographers' assistance. These were categorized into finalists and alternative algorithms, with draft standards released in 2023. From the original 82 submissions, eight made it into the final third round. From those eight, NIST chose one key agreement scheme and three signature schemes.

In August 2024, NIST officially released standards for three post-quantum cryptographic algorithms — Module-Lattice-Based Key Encapsulation (ML-KEM) under FIPS 203, Module-Lattice-Based Digital Signature Algorithm (ML-DSA) under FIPS 204, and Stateless Hash-Based Digital Signature Algorithm (SLH-DSA) under FIPS 205. These algorithms were selected as part of NIST's 2022 post-quantum cryptography standardization initiative, which also included CRYSTALS-Kyber, CRYSTALS-Dilithium, Sphincs+, and FALCON. With these new standards, global organizations can now begin integrating them into their encryption infrastructures to enhance security against quantum threats.

Given the importance of security in the telecom industry, there are pressing questions about the encryption methods being used today and, more importantly, how PQC can tackle the challenges posed by quantum computing. This technical report along with raising these pertinent questions also provides a comprehensive framework for considering and verifying the implementation of PQC in the 5G/B5G core network architecture. The main objective is to incorporate quantum-safe cryptography (PQC algorithm) into the emerging next-generation network (NGN) whenever applicable, and at the same time, to establish a means to compare and assess the reference scale.

The technical report is in line with NIST standards and meets the security requirements outlined in the 3rd Generation Partnership Project (3GPP) and IETF (Internet Engineering Task Force) standard. This alignment makes it evident that the telecom industry is well-prepared for the shift from the existing cryptography to quantum-resistant cryptography. Such

preparation is crucial for ensuring security and maintaining the integrity of digital communications.

The objective of this technical report is to enable the industry's transition to PQC in a 5G core network. This technical report helps in the implementation approach for PQC in the 5G system, this will substantiate the telecom operator's commitment to PQC.

Understanding that attacks can occur at any stage of data encryption, decryption, or key distribution, the industry must assess its cryptographic posture, identify which data needs protection, and determine how long that protection is required. This cryptographic posture will guide the industry in deciding on an appropriate migration strategy, allowing for the use of new algorithms as necessary. While the PQC algorithms continue to mature, it is recommended to combine the PQC algorithm process with the classical algorithm approach for hyper-secure systems.

This technical report is structured into three key sections. Section 4 explores the conventional cryptographic systems used in the 5G core network. Section 5 discusses the post-quantum cryptographic methods that can be adopted within the 5G system. Finally, Section 6 provides a roadmap for migrating to a quantum-secure 5G system, detailing the implementation strategies at different component and area levels within the network.

2.0 Terminology

2.1 NF Definitions

The primary Network Functions (NFs) and their associated capabilities, as defined in the current technical reports, are as follows:

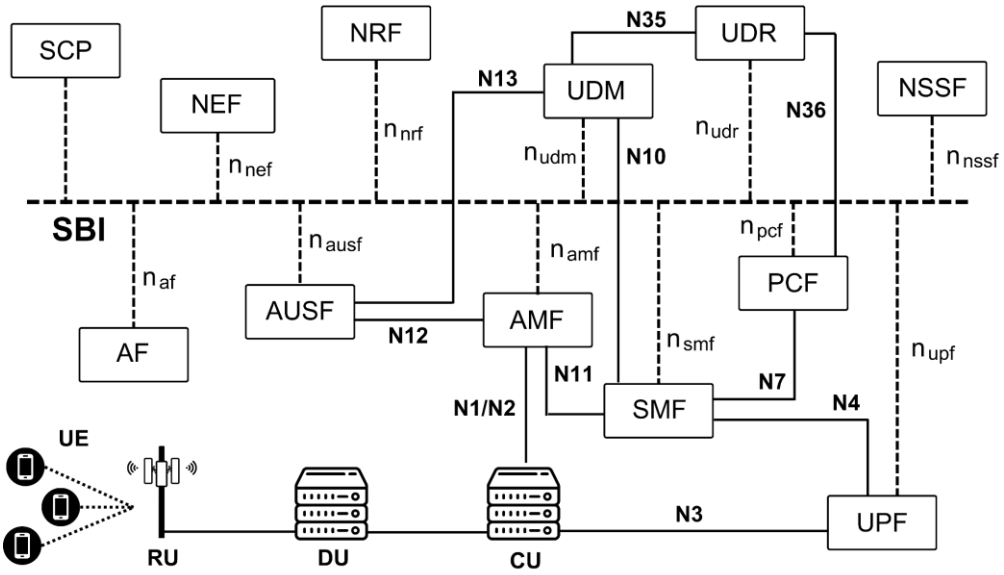


***Figure 1**: 5G Core Network Architecture*

i. **Access and Mobility Management Function (AMF)** - It is responsible for managing the termination of NAS signaling, including NAS ciphering and integrity protection. It also oversees registration management, connection management, mobility management, access authentication and authorization, and security context management. Additionally, the AMF serves as the termination point for the RAN control plane (CP) interface i.e. N2.

   a) **Security Anchor Function (SEAF)** - This NF operates within the serving network, closely integrated with the AMF, acting as an intermediary during the authentication process between the User Equipment (UE) and its home network.

ii. **Authentication Server Function (AUSF)** - It performs authentication and authorization for subscribers accessing the 5G network. It functions as the authentication server, securely storing authentication information such as user identities, passwords, and cryptographic keys, and validating user requests for network access.

iii. **Session Management Function (SMF)** - It is responsible for session management, including the establishment, modification, and release of sessions. It manages UE IP address allocation and management, DHCP functions, termination of NAS signaling related to session management, Downlink (DL) data notifications, and the configuration of traffic steering for the UPF to ensure proper traffic routing.

iv. **User Plane Function (UPF) -** The UPF supports several key tasks, including packet routing and forwarding, packet inspection, and QoS handling. It also acts as an external PDU session point that connects to the Data Network (DN) and serves as an anchor point for intra- and inter-RAT mobility.

v. **Network Repository Function (NRF) -** The NRF is essential for service discovery within the network, maintaining profiles of NF instances and their supported services. It supports:

   a) Maintaining NF profiles and available NF instances.

   b) Managing SBI, and facilitating management and maintenance.

vi. **Unified Data Management (UDM) -** It stores subscriber data and profiles, manages the generation of Authentication and Key Agreement (AKA) credentials, handles user identification, access authorization, and oversees subscription management. The UDM has two key components:

   a) **Subscription Identifier De-concealing Function (SIDF)**: A component of the UDM responsible for decrypting the SUCI to reveal the subscriber's SUPI.

   b) **Authentication Credential Repository and Processing Function (ARPF)**: Another component of the UDM, tasked with generating 5G Home Environment Authentication Vectors (5G HE AV) based on the subscriber's shared secret key.

vii. **Policy Control Function (PCF) -** It provides a unified policy framework that delivers policy rules to CP functions and accesses subscription information from the UDR for policy decisions. It supports policy management for network slicing, roaming, and mobility management.

viii. **Unified Data Repository (UDR) -** The UDR is a centralized database that stores and manages subscriber data, Subscriber Identity Module (SIM) identities, and network service configurations. It serves as the data repository for NFs like UDM, PCF, NEF, and others.

ix. **Network Slice Selection Function (NSSF) -** The NSSF is responsible for selecting the appropriate Network Slice instances to serve the UE, determining the allowed Network Slice Selection Assistance Information (NSSAI), and selecting the AMF set to serve the UE.

x. **Application Function (AF) -** It acts as an application server that can interact with other control-plane NFs. AFs can support various application services and may be operated by the network operator or trusted third parties. The AF enables application influence on traffic routing and interacts with the policy framework for policy control. For trusted services, the AF can directly access NFs, while untrusted or third-party AFs interact via the NEF.

xi. **Network Exposure Function (NEF) -** The NEF supports the exposure of network capabilities and events, securely provisioning information from external applications to the 3GPP network, and translating internal/external data. It functions as an API gateway, allowing external entities, such as enterprises or partner operators, to monitor, provision, and enforce application policies for users within the operator's network. It also:

a) Provides security when services or AFs access 5G Core nodes.

b) Acts as a proxy, or API aggregation point, or translator into the Core Network.

xii. **Service Communication Proxy (SCP) -** The SCP is a new HTTP/2-based NF that enables dynamic scaling and management of communication and services within the 5G network.

2.2 Key Concepts

1. **National Institute of Standards and Technology (NIST)** - The leading organization globally for standardizing PQC, responsible for developing and promoting encryption standards through an open, collaborative process involving industry, government, and academia.

2. **Federal Information Processing Standards (FIPS)** - A set of standards developed by NIST to ensure the security and protection of government data, mandating compliance for entities handling such data.

3. **3rd Generation Partnership Project (3GPP)** - 3GPP is a global collaboration between telecommunications organizations that creates and maintains specifications for mobile networks.

4. **Non-Access Stratum (NAS)** - It is a protocol in 5G that's responsible for communication between the UE and the Core Network (CN).

5. **Control Plane (CP)** - It manages signaling and control functions in the network, including authentication, mobility management, and session management, typically centralized to handle network management decisions.

6. **User Plane (UP)** - Also known as the data plane, handles user data traffic, focusing on data forwarding and packet processing, often positioned closer to the network edge to enhance efficiency and reduce latency.

7. **Quality of Service (QoS)** - A set of parameters that define the performance of a network service as experienced by users, with each QoS flow uniquely identified by a QoS Flow ID (QFI) within a PDU session.

8. **5G Home Environment Authentication Vector (AV)**: Authentication data consisting of RAND, AUTN, XRES, and Kausf to authenticate the UE using 5G AKA. This vector is received by the AUSF from the UDM/ARPF in the Nudm_UEAuthentication_Get Response.

9. **Packet Data Unit Session (PDU Session)** - A logical connection between user UE and a DN in 5G, providing end-to-end user plane connectivity through the UPF and supporting one or more QoS flows, each identified by a unique 5G Quality of Service Identifier (5QI).

10. **Data Network (DN)** - In 5G architecture, it refers to networks providing service provider services, Internet access, or third-party services.

11. **Service Based Interface (SBI)** - In the 5G core network's Service Based Architecture (SBA), SBIs facilitate communication between NFs using a common protocol based on OpenAPI v3 with JSON over HTTP/2, where each interface consists of one or more specific services provided by NFs. Each service consists of a service producer

(server) and a service consumer (client). Each service is typically oriented at executing a very specific function.

12. **Single Network Slice Selection Assistance Information (S-NSSAI)** - A 5G identifier for Network Slices, consisting of SST (Slice/Service Type) and optionally SD (Service Differentiator), used to uniquely identify and differentiate network slices based on their specific features and services.

13. **Radio Access Technology (RAT)** - A technology that defines the air interface for wireless communication, with 5G NR (New Radio) being the global standard developed by 3GPP for 5G networks.

14. **Universal Subscriber Identity Module (USIM)** - A secure element in UE that stores and manages sensitive subscriber data, controlled by the home network operator and managed via Over-The-Air (OTA) mechanisms.

15. **Server Name Indication (SNI)** - An extension of the TLS protocol allowing a client to specify the hostname during the TLS handshake, enabling the server to select the appropriate certificate and key for the connection.

16. **Certificate Authority (CA)** - A trusted third party that issues digital certificates to authenticate the identity of online entities.

17. **Open Authentication (OAuth)** - An open-standard authorization framework that allows users to grant websites or applications access to their information without sharing their passwords.

18. **IMSI Catching Attack** - A privacy threat where a device mimics a cell tower to collect the International Mobile Subscriber Identity (IMSI) from nearby phones, allowing tracking and potential interception of communications.

19. **Null-Scheme** - A dummy scheme in 5G that enables 5G UE to calculate the SUCI without hiding the SUPI.

20. **Subscription Permanent Identifier (SUPI)** - A globally unique identifier assigned to each subscriber in the 5G system, typically consisting of a string of 15 decimal digits, and provisioned in the UDM/UDR.

21. **Subscription Concealed Identifier (SUCI)** - A privacy-preserving identifier that contains the concealed SUPI, used to protect subscriber identity.

22. **SNOW3G** - A stream cipher that forms the basis of the ciphering and integrity protection algorithms that have been mandated by 3GPP for the protection of data over the air interface.

23. **ZUC** - A word-oriented stream cipher that uses a 128-bit secret key and a 128-bit initialization vector (IV) to generate a keystream of 32-bit words for encryption or decryption.

24. **Counter (CTR) mode** - It is a block cipher implementation that converts a block cipher into a stream cipher by using a counter to generate unique keystream blocks for encryption or decryption.

25. **Internet Protocol Security (IPSec)** - A suite of open standards used to ensure private communications over public networks, typically providing encryption and integrity for IP traffic and creating VPNs.

26. **Encapsulating Security Payload (ESP)** - The protocol within IPsec that transports encrypted and integrity-protected network communications, with the option to use NULL encryption when only integrity protection is required.

27. **Internet Key Exchange (IKE)** - The protocol used by IPsec to negotiate connection settings, authenticate endpoints, define security parameters, and manage session keys and communication channels.

28. **Lattice** - Lattice is a regular arrangement of points in multi-dimensional space, generated by integer linear combinations of a set of basis vectors. It can be visualized as infinite grids formed by points in space, where each point corresponds to a vector. These vectors can be manipulated through mathematical operations, such as addition and scalar multiplication, to create new vectors that define the lattice structure.

29. **Lattice Based Cryptography (LBC)** - It is a branch of post-quantum cryptography that relies on the hardness of mathematical problems associated with lattice structures in multi-dimensional spaces.

30. **Learning with Errors (LWE)** - It is a mathematical problem widely used in lattice-based cryptography. Its security relies on the difficulty of solving systems of linear equations that have been slightly "noisy" or distorted, making them hard to decode.

31. **Module Learning with Errors (MLWE)** - It is a variation of the LWE problem, used in LBC. It involves solving noisy linear equations over a module, which is like a more structured lattice.

32. **Harvest Now, Decrypt Later (HNDL)** - It is a cybersecurity threat model wherein attackers collect encrypted data today with the intention of decrypting it in the future, particularly when advancements in decryption technology, such as quantum computing, make it feasible. This strategy is also referred to as "store now, decrypt later" or "retrospective decryption."

33. **Elliptic Curve Discrete Logarithm Problem (ECDLP)** - It is a mathematical problem that forms the basis of the security of ECC. It involves finding the integer k such that, given an elliptic curve point P and another point $Q=kP$, it is computationally infeasible to determine k (the discrete logarithm) from P and Q.

34. **Hash-based Cryptography (HBC)** - It refers to a family of cryptographic techniques that use hash functions as the primary building blocks for security. These methods are

designed to leverage the inherent properties of hash functions—such as collision resistance and one-wayness—to provide secure digital signatures, key exchange, and other cryptographic operations.

3.0 Application of the Technical Report

3.1 Scope

The technical report addresses 3 key areas:

i. Identifying conventional cryptographic systems currently in use within the 5G core network.

ii. Establishing PQC methods suitable for integration in the 5G network infrastructure.

iii. Developing a migration strategy for transitioning from traditional cryptographic techniques to quantum-secure solutions within the 5G system.

The principal objective of this report is to create a comprehensive framework, which can be used for the evaluation and implementation of PQC in 5G as well as the next-generation networks. This will secure the present and future telecommunications infrastructure against emerging quantum threats.

This report will serve as a guiding framework for telecom operators, enabling them to assess and transition their current security practices to quantum-resistant counterparts. This technical report aims to provide a flexible framework that can be adapted to meet the specific needs of different network components and use cases.

Even though it provides a structured approach to transition to PQC, it does not intend to forge a strict regulatory agreement. One of the approaches it takes to be more flexible is by encouraging both homogeneous and hybrid approaches, allowing developers and network operators to choose between complete adoption of quantum-resistant cryptography or combining it with classical cryptography, depending on their specific network requirements, thereby enabling them, hence permitting them to evaluate their requirements and only then implement the necessary security measures.

This technical report can also act as a reference for independent audits, providing a basis for third parties to assess and verify the security of 5G networks in a post-quantum era. As the telecom industry is moving towards quantum-safe technologies, this technical report will help the industry toward a future with secure and reliable network operations.

3.2 Intended Users of the technical Report

3.2.1 Telecom Service Providers and Network Service Providers

The cardinal users of this report are telecom operators and network service providers who have the responsibility for maintaining and securing 5G networks. When these organizations need to assess their cryptographic infrastructure and implement PQC wherever applicable, this report will serve as a guiding framework. By following the guidelines and procedures outlined in the framework, they can ensure their networks are well prepared to resist future quantum threats while maintaining compliance with security standards.

3.2.2 Network Equipment Manufacturers

Manufacturers of network equipment that integrate into the 5G core network are another important user group of this technical report. When PQC requirements and guidelines in the technical reports are implemented, these organizations will need to revise their products to ensure that their equipment maintains compatibility with the emerging security protocols. This will call for adapting or updating hardware and software to meet the standards for quantum-resistant cryptography.

3.2.3 Third-Party Security Auditors

Independent security auditors, who are accredited by relevant certifying bodies, may use this technical report to conduct thorough audits of 5G networks. The audit may lead to issuing compliance certificates, which assure the network providers and other concerned parties that the security protocols are in place. These auditors will do this by verifying the proper implementation of PQC measures and evaluating adherence to the technical report's guidelines.

3.2.4 Government and Regulatory Bodies

This technical report can also be referred to when policies and regulations are being formulated related to network security by various government agencies and regulatory bodies that are responsible for maintaining telecommunications infrastructure. These bodies might make it mandatory for the adoption of PQC measures in critical infrastructure and use the technical report as a benchmark for ensuring compliance. Additionally, they may require third-party auditors to ensure that network operators are adhering to the recommended security guidelines.

3.2.5 Network Infrastructure Developers and Integrators

Organizations involved in the development and integration of 5G and next-generation network components, including software developers and system integrators, will use this technical report to guide the consolidation of quantum-resistant cryptography into their projects. These entities will apply the technical report's framework to develop secure, reliable networks, capable of resisting quantum computing threats.

3.2.6 Startups and Industry

Start-ups and industry operating in the telecom sector may adopt this technical report to ensure their innovations and products meet the security requirements needed for integration

into 5G & Beyond networks. By ensuring compliance with these technical reports, these companies can gain broader acceptance and market trust, particularly if they seek to partner with larger telecom operators or equipment manufacturers.

3.2.7 Cybersecurity Researchers

Cybersecurity researchers play a critical role in advancing the field of network security and quantum-resistant cryptography. This technical report will serve as a valuable resource for researchers working on the development, analysis, and evaluation of new security protocols and algorithms. By referring to this report, researchers can gain insights into current cryptographic practices, identify potential vulnerabilities, and contribute to the evolution of quantum-secure solutions. This report will support their efforts in advancing the security of telecom networks, ensuring they are resilient against the emerging threats posed by quantum computing.

4.0 Conventional Cryptographic System in 5G Core

Conventional cryptographic systems play a vital role in protecting data and communications throughout the 5G Core. Different types of cryptographic algorithms and techniques are being used to make sure that the information sent and received between different network functions is safe and secure. This is how classical cryptographic systems help in the security of 5G Core:

i. **TLS** and **IPSec** are used to secure communication channels, ensuring that data transmitted over the network remains confidential. The AE**S** is employed to encrypt sensitive data, making it unreadable to unauthorized parties.

ii. **ECC** enables efficient key exchange, allowing network entities to securely share the encryption keys.

iii. **Deterministic Cryptographic Keys** are generated using specific cryptographic algorithms known as KDFs. They ensure consistent & reproducible key generation for secure operations while preserving the entropy of the input. They are one way in nature.

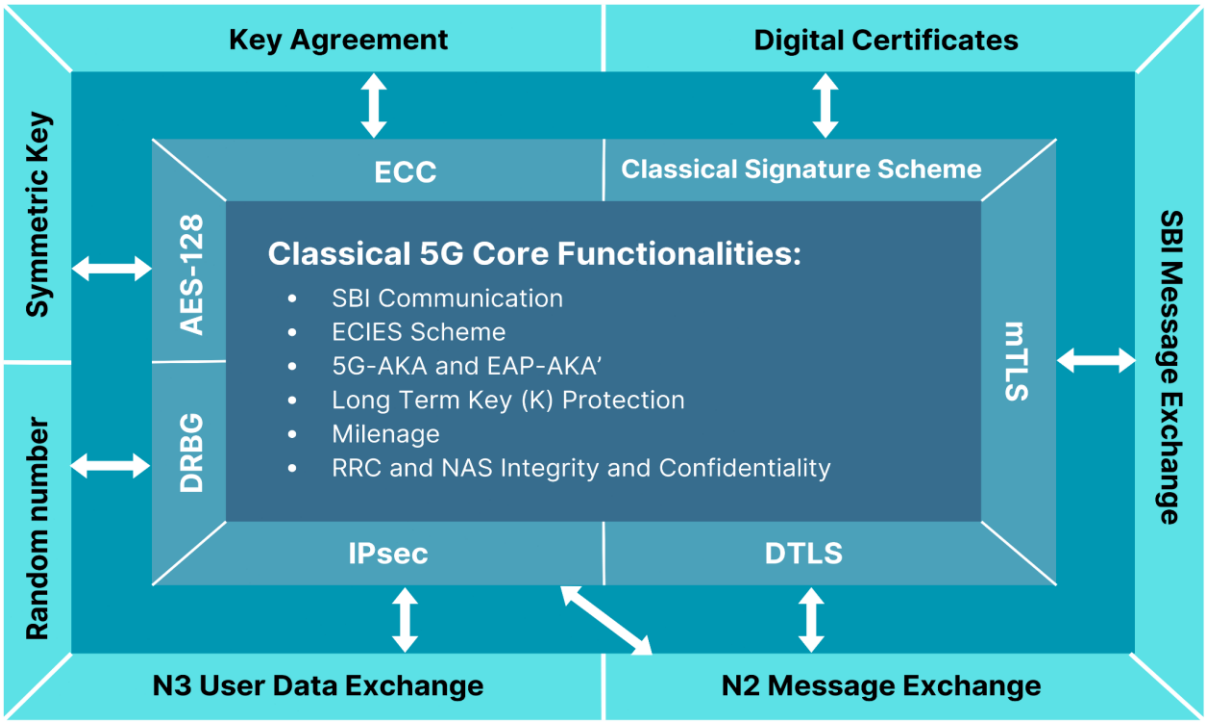


***Figure 2**: Classical Cryptographic System in 5G Core*

By combining these techniques of Figure 2, classical cryptographic systems create a strong security framework within the 5G Core. These techniques are effective in securing both user data and network operations from potential threats.

4.1 Random Number Generation

The random number generator is used to generate [50] seeds and keys randomly in many cryptographic systems. For this reason, it is essential to use keys to encrypt and decrypt the

transferring information, and the security of these keys is closely related to the security of the 5G network.

Random numbers are fundamental to most use of cryptography (e.g., to securely generate keys). A common pattern for doing this is to mix together input from one or more entropy sources and then process the output through a deterministic function called a DRGB (Deterministic Random Bit Generator, sometimes also called PRNG – Pseudo Random Number Generator). This is the way it is done in the Linux RNG (Random Number Generator) shown in Figure 3.

Deterministic and pseudorandom numbers generated for cryptographic applications will be unpredictable if the seed and generation algorithm are unknown [33]. Since, in many cases the generation algorithm is publicly available, the seed must be kept secret and should not be derivable from the pseudorandom sequence that it produces.

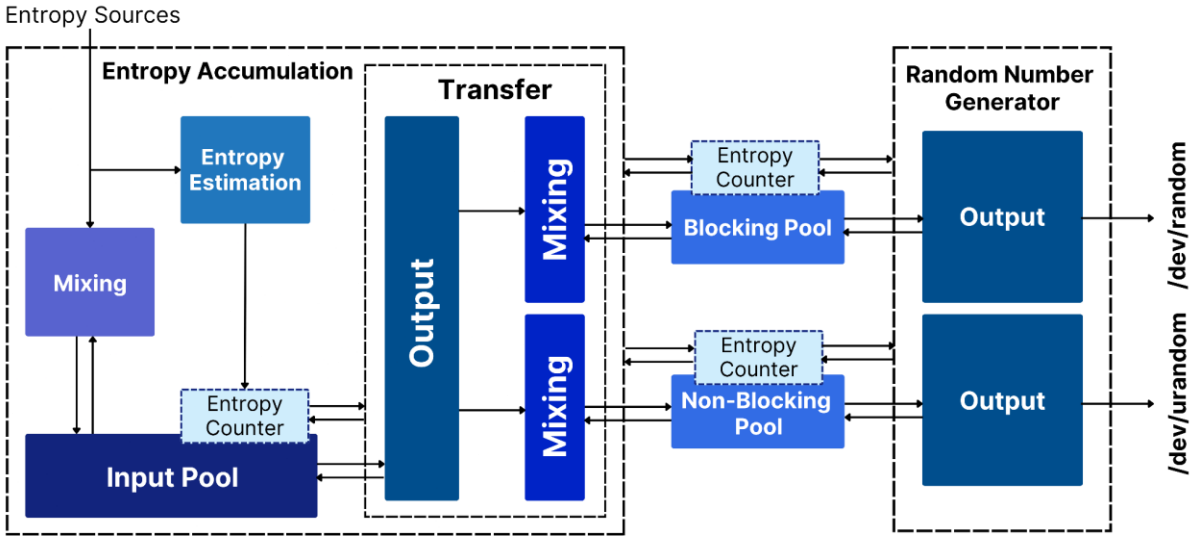


***Figure 3**: General Structure of Linux PRNG*

4.1.1 Long Term Key

The long-term key, denoted as K, is a 128-bit key and acts as the root of the key derivation hierarchy. All other keys used for ciphering and integrity are derived from K. These unique long-term keys are stored in the UDM and on the UE and do not change over time. They are used in multiple places during security transactions. These long-term keys act as the base of authentication, authorization, and security management processes in the core network. These keys have specific applications within the 3GPP framework:

i. Authenticating the connection between the Core Network and the UE.

ii. Authorizing services that are provided to the UE.

The long-term keys are securely stored in the USIM of the UE as well as in the core network. As mandated in clause 5.2.4 in 3GPP TS 33.501 [1], the long-term key(s) of the subscription credential(s) (i.e., K) shall be confidentiality protected within the UE using a tamper-resistant secure hardware component.

A key aspect of the security and effectiveness of long-term keys lies in their generation process. The long-term key (K), is generated through a PRNG/DRBG which when supplied with sufficient entropy, produces a key K with a high degree of unpredictability and randomness, making it resistant to classical cryptographic attacks.

The long-term key K serves as a 128-bit secret key, which plays a very important role in the Milenage function – a widely utilized algorithm within the 5G system as per 3GPP TS 35.205 [2] for authenticating and establishing secure communications. The 5G-AKA procedure heavily relies on K to perform various cryptographic operations. Consequently, it becomes imperative for this key to be accessible on both ends: within the core network and the UE. This dual availability ensures that both parties – the network and the UE – can securely authenticate each other and establish a trusted communication channel.

4.1.2 Authentication Parameter RAND

The authentication parameter RAND (Random Challenge) is a 128-bit random number generated by a PRNG/DRBG within the core network and is sent to the UE in the NAS Authentication Response message during the 5G-AKA procedure as per 3GPP TS 33.501 [1]. As the name suggests, it acts as a challenge that UE must respond to, in order to prove its identity and establish secure communication with the network.

The UE uses the received RAND and other parameters such as Authentication Token (AUTN) and Sequence Number (SQN) along with its stored authentication credentials (e.g. shared secrets) to generate Response (RES) and Ciphering Key (CK) using UE milenage algorithm as specified in 3GPP TS 35.206 [3]. UE then sends a NAS Authentication Request message to the network, which includes the RES and CK.

The network verifies the UE's response (RES) calculated using RAND and other authentication parameters and generates a Session Key (Ks_nas) and an Integrity Key (Ik_nas) based on the AKA algorithm, as mentioned in Figure 4. The network sends a NAS Authentication Response message to the UE, which includes these keys, indicating a successful authentication and key agreement.

In case of an authentication failure, the stored RAND and RES in the UE are deleted, and the process is restarted to ensure synchronization between the network and the UE during the authentication process, preventing any potential security issues.

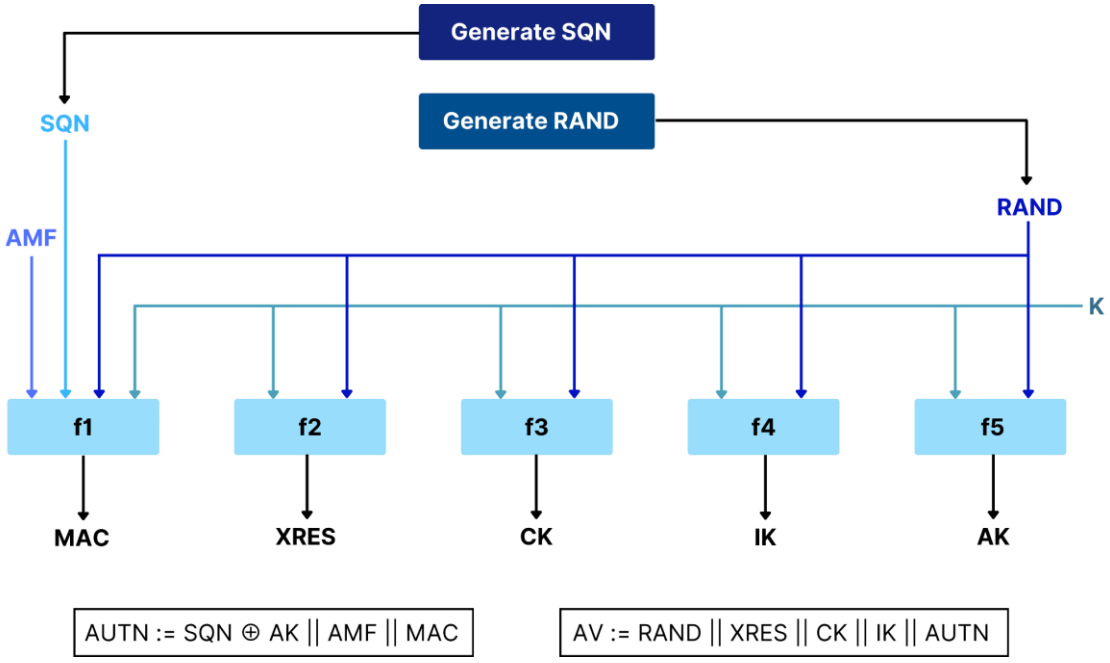


***Figure 4**: Generation of Authentication Vector*

4.1.3 Seed for Home Network Key Pair Generation

Home Network (HN) key pairs play an important role in the concealment, de-concealment, and protection of the SUPI within 5G networks. The key pairs are securely stored in the UDM (SIDF) of the 5G Core while only the HN Public Key is stored in the UE. As shown in Figure 5, The HN Public Key is involved in the encryption process of SUPI on the UE side, and the HN Private Key is involved in the decryption process of SUCI to re-obtain SUPI on the core side for UE authentication.

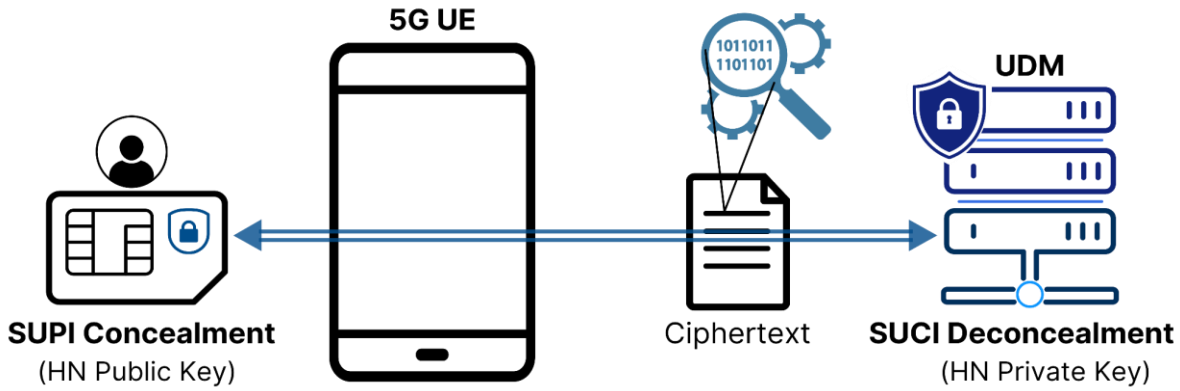


***Figure 5**: User Identity Concealment*

The HN Public Key Identifier must be securely stored within the USIM. As highlighted in clause 5.2.5 of 3GPP TS 33.501 [1], it is important to ensure that the HN key pair is both highly random and secure to prevent unauthorized access or decryption. The randomness and security of these keys depend on both the entropy source and the performance of the PRNG/DRBG.

4.1.4 Seed for ephemeral Key pair

Ephemeral key pairs are short-term or temporary keys that are only used for one time which means for each session, a new pair of ephemeral keys will be generated. The key pair relies on PRNG/DRBG to obtain seeds for their key generation processes. These keys are also used in various security protocols within the core network for ensuring the security and confidentiality of short-term communications, such as mTLS for securing SBI communication, ECIES for encrypting data, Digital certificates for identity verifications, etc.

4.2 Symmetric Encryption

In symmetric cryptography as shown in Figure 6, the same key is used for both encryption and decryption, making it an efficient and secure method for the protection of sensitive information being sent between two parties. One of the most widely used symmetric encryption algorithms in 5G is AES, especially in its 128-bit key version called AES-128.

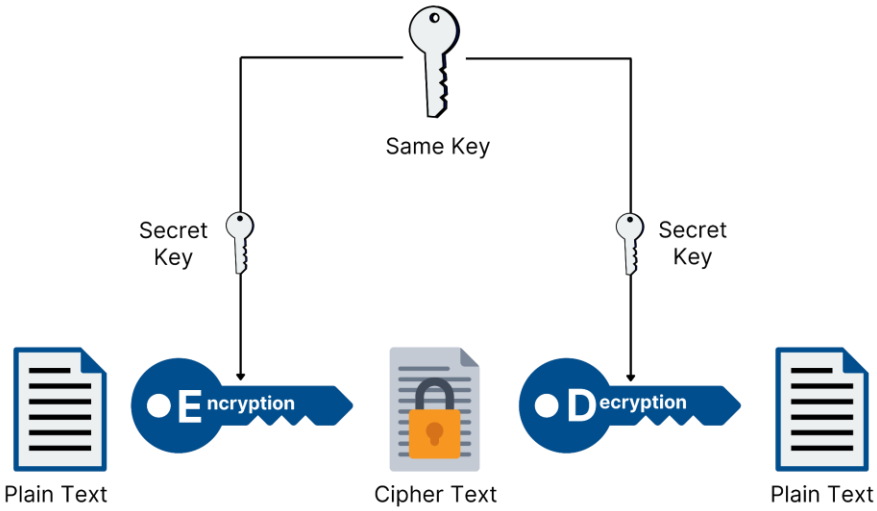


***Figure 6**: Symmetric Encryption*

4.2.1 NAS Integrity and Ciphering Algorithm

In 5G, NAS security algorithms play an important role in ensuring data confidentiality and integrity between UE and AMF. These algorithms are implemented at the NAS layers of both the UE and AMF.

Ciphering (also known as encryption), encrypts the plaintext into ciphertext to prevent unauthorized access. It cannot be deciphered without the appropriate key, even if the ciphertext is intercepted. For NAS security, signaling messages are encrypted using the following algorithms:

i. **NEA0**: Null ciphering algorithm where the keystream is all zeros, meaning plaintext is not encrypted, offering no security.

ii. **128-NEA1**: A 128-bit cipher based on the SNOW 3G algorithm

iii. **128-NEA2**: A 128-bit AES-based algorithm operating in Counter (CTR) mode.

iv. **128-NEA3**: A 128-bit cipher based on the ZUC stream cipher.

The main goal of Integrity protection is to ensure that the contents of a message have not been altered. A Message Authentication Code (MAC) is calculated and added to each message, and the receiving party calculates its own MAC to compare with the transmitted one. If the validation fails, the message is rejected, otherwise, proceed further. The NAS integrity protection algorithms [1] include:

i. **NIA0**: Null integrity protection algorithm where the generated MAC consists entirely of zeros, and no validation is performed by the receiver.

ii. **128-NIA1**: A 128-bit algorithm based on SNOW 3G.

iii. **128-NIA2**: A 128-bit AES-based algorithm that uses Cipher-based Message Authentication Code (CMAC) mode for integrity protection.

iv. **128-NIA3**: A 128-bit algorithm based on the ZUC stream cipher.

4.2.2 Milenage

The Milenage algorithm is a set of cryptographic functions defined in 3GPP TS 35.205 [2] used in the Authentication and Key Agreement (AKA) protocol for authentication and session establishment in the 5G network. As per the part of the 5G AKA procedure, it is used in the calculations of different key parameters that are necessary for the authentication between the UE and the network.

As per 3GPP TS 35.206 [3], the overall Milenage algorithm (shown in Figure 7) set consist of five cryptographic functions, denoted as f1, f2, f3, f4, and f5, each of which generates specific values necessary for the AKA procedure. It also includes resynchronization functions (f1* and f5*) to handle scenarios where the sequence number between the network and the UE is misaligned.

Input Parameters	Size (bits)	Functions (Input to)
RAND	128	f1, f1*, f2, f3, f4, f5, f5*
K	128	f1, f1*, f2, f3, f4, f5, f5*
SQN	48	f1, f1*
AMF	16	f1, f1*

Output Parameters	Size (bits)	Functions (generate Output)
MAC-A	64	f1
MAC-S	64	f1*
RES	64	f2
CK	128	f3
IK	128	f4
AK	48	f5, f5*

Both f5 and f5* outputs are called AK according to the reference [44]. In practice, only one of them will be calculated in each instance of the 5G-AKA procedure.

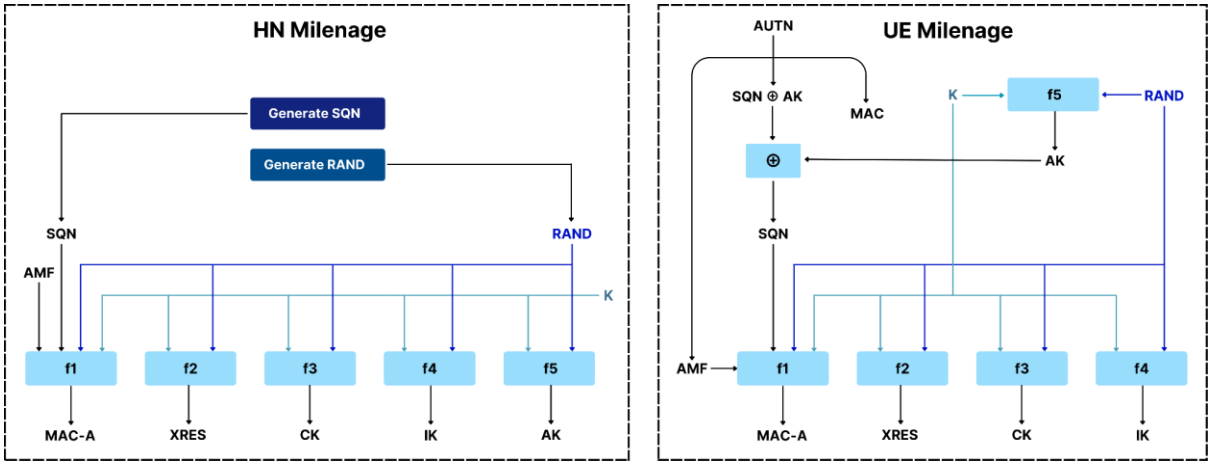


***Figure 7**: HN and UE Milenage*

The Milenage algorithm set is based on the AES (Rijndael) algorithm. Using AES the confidentiality is provided by the derived CK and IK keys that are used in the encryption and verification of the integrity of messages whereas the f1 function uses AES for the calculation of the MAC for network authentication that enhances both the security and integrity of the authentication process.

4.2.3 5G Authentication Framework

Authentication and key management are fundamental [8] to the security of cellular networks because they provide mutual authentication between users and the network and derive cryptographic keys to protect both signaling and user plane data. In 5G, a unified authentication framework has been defined to ensure the authentication is both open (e.g., with the support of EAP) and access-network agnostic (e.g., supporting both 3GPP and non-3GPP access networks such as Wi-Fi and cable networks).

When EAP is used (e.g., EAP-AKA' or EAP-TLS), authentication occurs between the UE and AUSF through the SEAF (acts as an EAP pass-through authenticator). When authentication is over untrusted, non-3GPP access networks, a new function, Non-3GPP Interworking Function (N3IWF) serves as a VPN server, allowing UE to access the 5G core through IPsec tunnels over the untrusted, non-3GPP networks.

5G-AKA (Authentication and Key Agreement): AKA is a technique for mutual authentication between a network and a subscriber, and key agreement for protecting traffic. 5G-AKA is similar to 4G EAP-AKA, but with improvements for roaming security. As described in Figure 8, the SEAF [40] initiates the authentication procedure after receiving any signaling message from the UE, which sends either a temporary identifier (5G-GUTI) or a SUCI. The SEAF forwards the request to the AUSF, which verifies the serving network's authorization and then sends an authentication request to the ARPF. If an SUCI is provided, the SIDF decrypts it to obtain the SUPI, and the ARPF selects and executes 5G-AKA.

The ARPF sends an AV to the AUSF, which includes an AUTH token, an XRES token, and a key (Kausf) as specified in 3GPP TS 33.501 [1]. The AUSF computes a hash of the HXRES and forwards the AUTH token and HXRES to the SEAF. The SEAF sends the AUTH token to the UE, which validates it using its shared key with the home network. The UE then sends a response (RES token) to the SEAF, which forwards it to the AUSF for final validation. If successful, the AUSF generates an anchor key (Kseaf) and sends it to the SEAF, along with the SUPI if applicable.

The SEAF derives the AMF key (Kamf) and forwards it to the AMF, which further derives (a) confidentiality and integrity keys for protecting signaling messages and (b) another key (Kgnb) for the gNB to derive the keys used to protect subsequent communication between the UE and the gNB. The UE, with its long-term key, can derive all necessary keys, ensuring secure communication with the network.

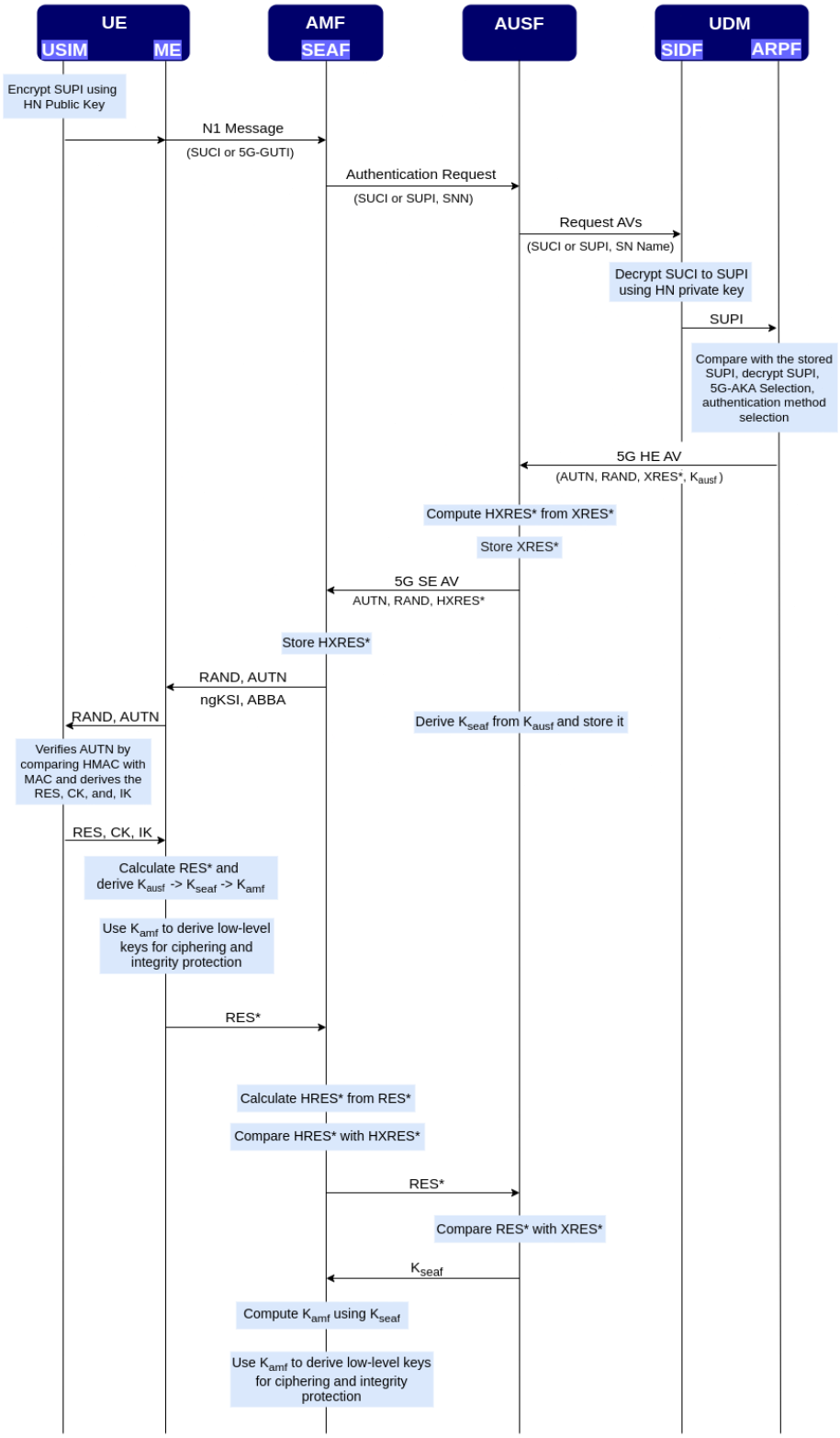


Figure 8: *5G-AKA Procedure*

EAP-AKA' (Extensible Authentication Protocol-AKA') - EAP-AKA' [15] is another authentication method supported in 5G, functioning as a challenge-and-response protocol based on a cryptographic key shared between a UE and its home network. It provides the same level of security properties as 5G-AKA, such as mutual authentication between the UE

and the network. Because it is based on EAP, its message flows differ from those of 5G-AKA [8]. Note that EAP messages are encapsulated within NAS messages between the UE and SEAF and within 5G authentication messages between the SEAF and the AUSF. Other differences between 5G-AKA and EAP-AKA' are:

i. In EAP-AKA', the EAP message exchanges occur between the UE and AUSF through the UDM (SEAF), which forwards the message without being involved in any authentication decision. In 5G-AKA, the SEAF verifies the UE's authentication response and may act on failed verification, though no specific actions are defined in 3GPP TS 33.501 [1].

ii. In 5G-AKA, the Kausf key is computed by UDM (ARPF) and sent to the AUSF, while in EAP-AKA', the AUSF derives the Kausf key based on keying materials received from the ARPF.

4.3 SBI Protection

The Service Based Architecture (SBA) in the 5G Core as shown in Figure 9 is designed to make the Core Network more scalable, functional, reliable, and secure. The SBA allows the Core Network Functions to communicate with each other through standardized SBIs.

The communication provided by the SBI must be authenticated and encrypted so that they are safe against security threats and no unauthorized NF can access the 5G system.

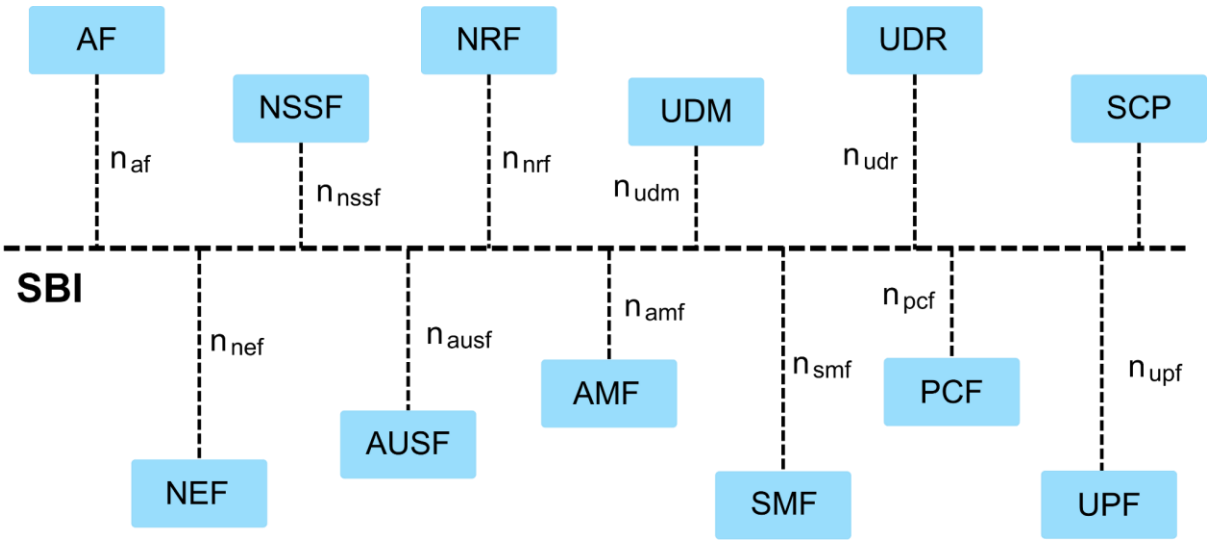


***Figure 9**: 5G Service-Based Architecture*

4.3.1 mTLS in 5G Core Network

TLS [49] is a cryptographic protocol that provides data integrity, confidentiality & authenticity between communication applications. It is widely used in email, and VoIP, but its use in securing HTTPS remains the most prominent.

In 5G Core, a slightly modified version of TLS known as mTLS (Mutual TLS) is used to secure the communication over the standardized SBIs between NFs such as AMF, SMF, and UPF, protecting against potential threats such as interception, tampering, and impersonation attacks. Unlike standard TLS, mTLS provides mutual authentication and verifies the identities of both the parties involved in the communication through digital certificates which are typically issued by an organization's Private CA. mTLS also supports Zero Trust Architecture [7] in various networks, including 5G SBA. Zero Trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location.

According to clause 13.1.0 of TS 33.501 [1], all NFs shall support mutually authenticated TLS and HTTPS as described in RFC 9113 [4] and RFC 9110 [5]. The identities in the end entity certificates shall be used for authentication and policy checks. The NFs shall support both server-side and client-side TLS certificates that must comply with the SBA certificate profile specified in clause 6.1.3c of TS 33.310 [6]. The TLS profile shall follow the profile given in clause 6.2 of TS 33.210 [11] with the restriction that it shall be compliant with the profile given by HTTP/2 as defined in IETF RFC 9113 [4]. TLS clients shall include the SNI extension.

4.3.2 Role of NRF and SCP in Mutual Authentication

NF service-based discovery and registration must ensure confidentiality, integrity, and replay protection. The NRF is responsible for authorizing these NF Discovery and registration requests. It also ensures that the topology of available or supported NFs is hidden from entities in different administrative or trust domains (e.g., between visited and home networks).

According to 3GPP TS 33.501 [1], The NF Service Request and Response procedures support mutual authentication between the NF Service Consumer and the NF Service Producer. Each network function must validate all incoming messages, rejecting or discarding any that do not conform to protocol specifications or network state.

The NRF gets NF Discovery Requests straight from NF instances. It gives info about NF instances it finds and keeps NF profiles up to date. When it logs or updates NF profiles, the NRF checks if the details in the NF profile match those in the public key certificate of the NF instance. This check makes sure approved network functions can get in. As shown in Figure 10, SCP handles all the service requests from each network function by dealing with access token requests from NF Service Consumers and giving out authorization tokens when needed by handling with NRF. As an authorization server, the NRF makes sure both it and the NFs asking for services through SCP prove who they are to each other. This keeps the service-based setup safe and reliable.

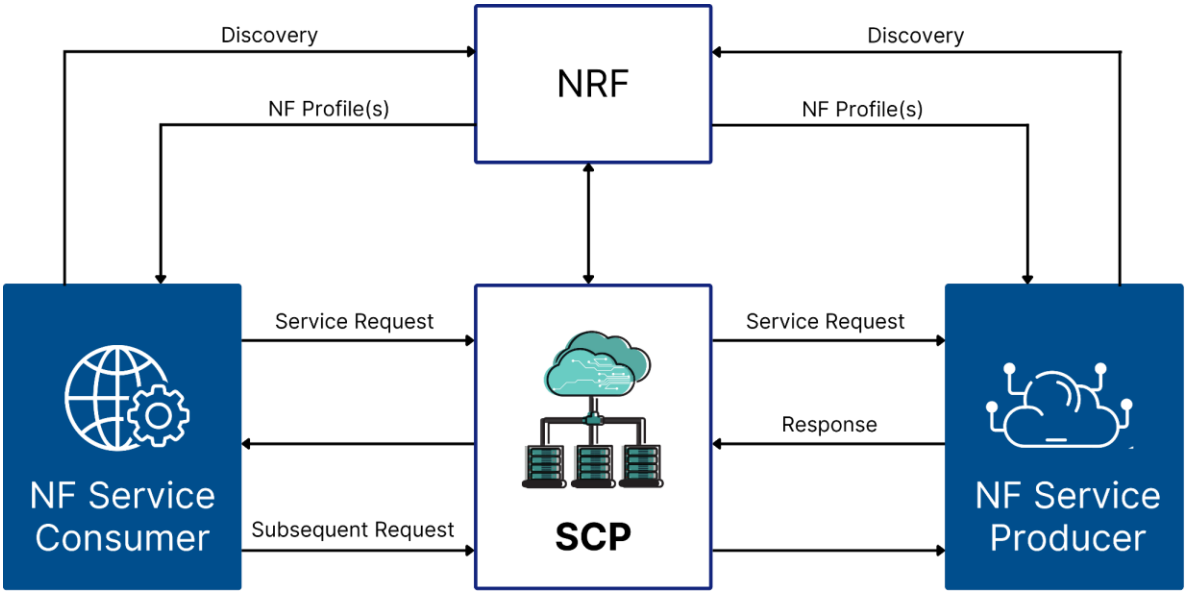


***Figure 10**: NF-NF Service Interaction*

The NRF manages digital certificates for mTLS authentication in the 5G Core network. It receives and handles the distribution of these certificates. This process makes sure approved network functions can communicate to each other keeping the network safe and intact.

When two network functions need to connect, they exchange certificates to check each other's identity through mTLS. After they confirm who they are, they encrypt the data they share, which keeps it private and unchanged. The NRF plays a key part in this. It makes sure the certificates are real and trusted NFs can join in secure communication.

4.4 Protection of the NEF – AF Interface

In the 5G system, the NFs securely expose capabilities and events to 3rd party AF via NEF. As shown in Figure 11, The NEF also enables secure provision of information in the 3GPP network by authenticated and authorized AFs.

As specified in TS 33.501 [1] in clause 12.2, for authentication between an NEF and an AF that resides outside the 3GPP operator domain, mutual authentication based on client and server certificates shall be performed between the NEF and AF using TLS. Certificate-based authentication shall follow the profiles given in 3GPP TS 33.310 [6], clause 6.1.3a. The identities in the end entity certificates shall be used for authentication and policy checks. TLS shall be used to provide integrity protection, replay protection, and confidentiality protection for the interface between the NEF and the AF. The support of TLS is mandatory. Security profiles for TLS implementation and usage shall follow the provisions given in clause 6.2 of TS 33.310 [6].

After the authentication, NEF determines whether the AF is authorized to send requests for the 3GPP Network Entity. The NEF shall authorize the requests from AF using an OAuth-based authorization mechanism; the specific authorization mechanisms shall follow the provisions given in IETF RFC 6749 [36].

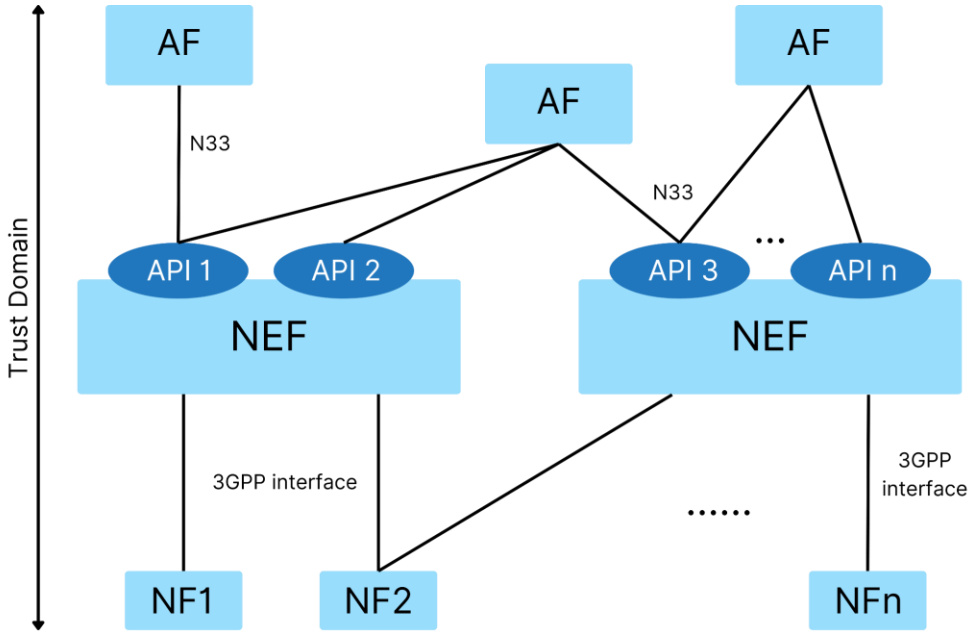


***Figure 11**: NEF-AF Interaction*

4.5 Token Based Authentication

The authorization framework uses the OAuth 2.0 framework as specified in IETF RFC 6749 [36] to allow NF Service Producers to authorize the requests from NF Service Consumers. Grants shall be of the type Client Credentials Grant, as described in clause 4.4 of RFC 6749 [40]. Access tokens shall be JSON Web Tokens as described in RFC 7519 [41] and are secured with digital signatures or Message Authentication Codes (MAC) based on JSON Web Signature (JWS) as described in RFC 7515 [42].

As suggested in clause 13.4.1.1.1 of TS 33.501 [1], the OAuth 2.0 roles as defined in clause 1.1 of RFC 6749 [36], are defined as follows:

i. The NRF shall be the OAuth 2.0 authorization server.

ii. The NF Service Consumer shall be the OAuth 2.0 client.

iii. The NF Service Producer shall be the OAuth 2.0 resource server.

The service request process includes requesting an access token by the NF Service Consumer, and then verification of the access token by the NF Service Producer.

i. The NF Service Consumer shall request an access token from the NRF in the same PLMN using the Nnrf_AccessToken_Get request operation. The message shall include the NF Instance ID(s), scope including the expected NF Service name(s), and optionally additional scope information (i.e. requested resources and requested actions (service operations) on the resources).

ii. The NRF shall verify that the input parameters such as NF Instance ID, NF type as well as PLMN ID(s) and if the authorization is successful, the NRF shall generate and digitally sign the generated access token based on a shared secret or private key as

described in RFC 7515 [42]. Then, NRF sends an access token to the NF Service Consumer in the Nnrf_AccessToken_Get response operation.

iii. Once the NF Service Consumer receives the token, it requests service from the NF Service Producer including the access token in the message. The NF Service Producer validates the token by verifying the signature using NRF's public key or checking the MAC value using the shared secret to ensure that the NF Service Consumer is authorized to access the requested service.

iv. Stored tokens may be re-used for accessing service(s) from NF Service Producer during their validity time.

When there is no mutual authentication between the NF Service Consumer and NRF at the transport layer, the NF Service Consumer performs the following procedure as shown in Figure 12 to obtain the access token from NRF and use it for service access at the NF Service Producer.

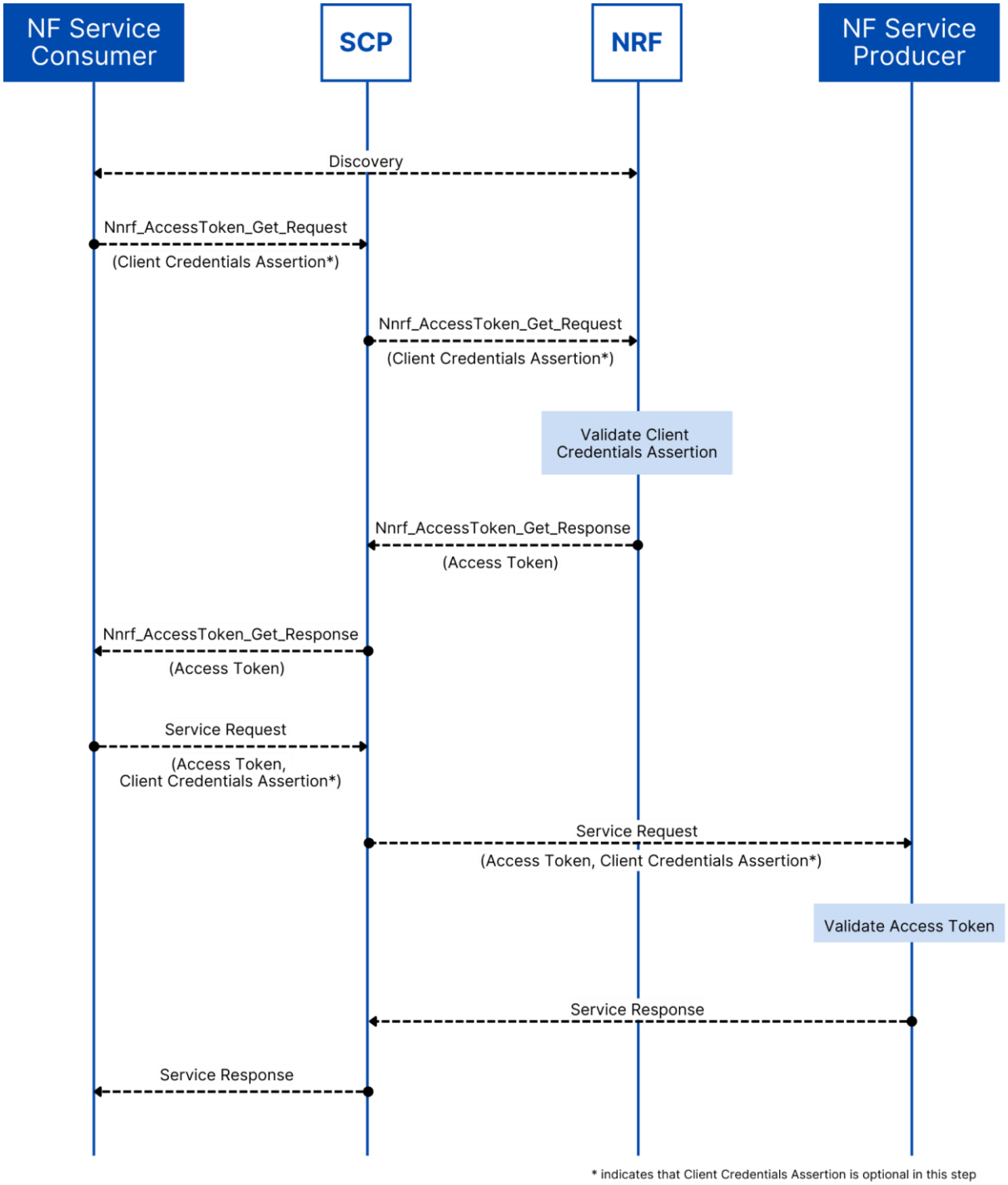


***Figure 12**: Access Token Based Authentication without mutual authentication between NF and NRF at the transport layer*

4.6 ECIES Scheme

In 5G networks, 3GPP improves subscribers' identities by no longer sending the IMSIs as plain text by adding a layer of encryption over it. To improve privacy even more, the system uses the SUCI (mentioned in Figure 14), an encrypted form of the SUPI (mentioned in Figure 13). This saves the SUPI from IMSI catchers which keeps the subscriber's information protected.

3GPP defines more than one type of SUPI, with the IMSI-based SUPI being the most common, equivalent to the traditional IMSI. This identifier [9] is a numeric string of up to 15 digits: the first 3 digits represent the Mobile Country Code (MCC), the next 2-3 digits denote the Mobile Network Code (MNC) identifying the network operator, and the remaining digits form the Mobile Subscriber Identification Number (MSIN).

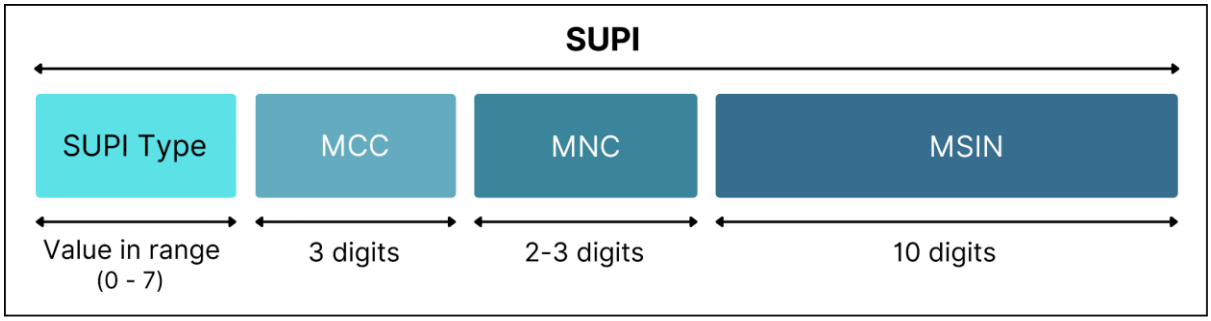


***Figure 13**: SUPI*

During the authentication process, a subscriber sends their SUCI to the network. The SUCI, derived from the SUPI, comprises [9] six components: the type of SUPI, the Home Network Identifier (which includes the MCC and MNC for IMSI-based SUPIs), and the Routing Indicator for internal network routing. Additionally, it includes the Protection Scheme ID, which indicates the encryption method used, the Home Network Public Key ID, identifying the operator's public key, and the encrypted output of the selected Protection Scheme.

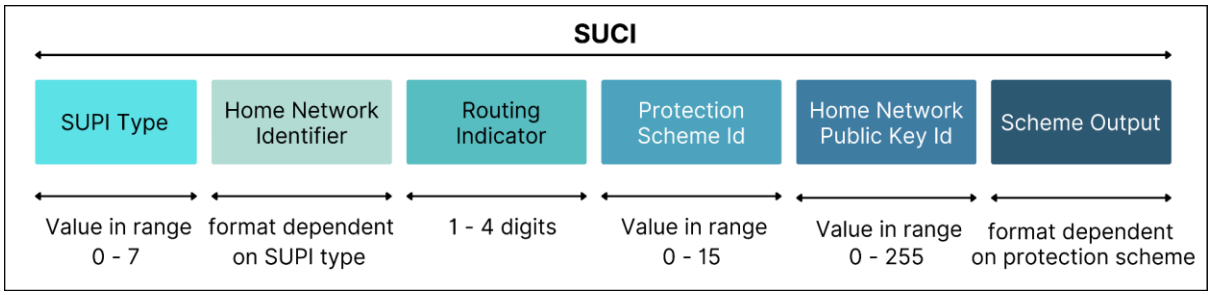


***Figure 14**: SUCI*

In the SUCI, the MNC and MCC are transmitted directly, with only the MSIN being encrypted. While subscribers can still authenticate by sending their MSIN in plaintext using the null-scheme, 5G introduces encrypted transmission for enhanced security. This encryption employs one of two predefined ECIES profiles, Profile A and Profile B, mentioned in the table below, which primarily differ in their elliptic curve parameters.

ECIES Parameters	Profile A	Profile B
EC domain parameters	Curve25519	secp256r1

EC Diffie-Hellman primitive	X25519	Elliptic Curve Cofactor Diffie- Hellman Primitive
Point Compression	N/A	true
KDF	ANSI-X9.63-KDF	ANSI-X9.63-KDF
Hash	SHA-256	SHA-256
SharedInfo1	R (the ephemeral public key octet string)	R (the ephemeral public key octet string)
MAC	HMAC-SHA-256	HMAC-SHA-256
mackeylen	32 octets (256 bits)	32 octets (256 bits)
maclen	8 octets (64 bits)	8 octets (64 bits)
SharedInfo2	the empty string	the empty string
ENC	AES-128 in CTR mode	AES-128 in CTR mode
enckeylen	16 octets (128 bits)	16 octets (128 bits)
icblen	16 octets (128 bits)	16 octets (128 bits)

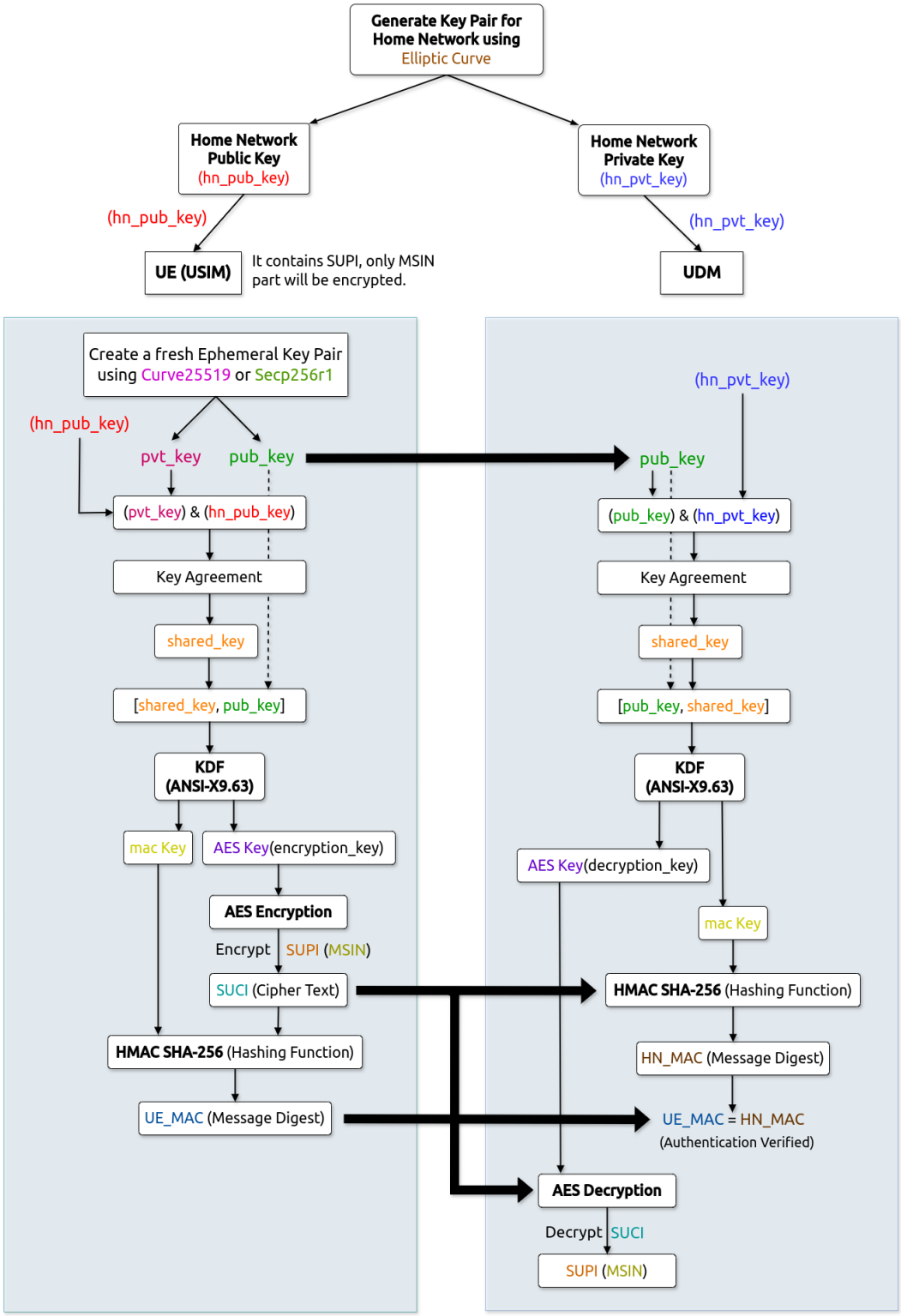


***Figure 15**: ECIES Scheme*

ECIES as shown in Figure 15, is a public key encryption method that combines ECC with symmetric encryption and MAC, and it is the standard approach [35] used for concealing the SUPI in every 3GPP-compliant 5G Core.

4.7 Security Mechanism on N2 Interface

N2 is the reference point between the AMF and the 5G-AN. It is used to carry NAS signaling traffic between the UE and the AMF over 3GPP and non-3GPP networks. The transport of control plane data over N2 shall be integrity, confidentiality and replay-protected.

Additionally, mutual authentication shall be supported over the N2 interface between the AMF and the 5G-AN using DTLS and/or IPSec/IKEv2 [21] as per 3GPP TS 33.501 [1] to verify their identity and build a secure communication channel to protect from potential security breaches. The use of cryptographic solutions to protect the N2 interface is completely an operator's decision. In case the RAN node has been placed in a physically secured environment, this environment must also secure other nodes and links that are connected to the RAN node.

4.7.1 IPSec on N2

As per 3GPP TS 33.501 [1], to protect the N2 reference point, it is required to implement IPsec ESP and IKEv2 [21] certificates-based authentication with confidentiality, integrity, and replay protection. IPsec is mandatory to implement on the gNB whereas on the core network side, a SEG (Security Gateway) may be used to terminate the IPsec tunnel.

IPsec ESP transports encrypted and integrity-protected data while IKEv2 certificates-based authentication provides [34] the secure exchange of cryptographic keys by selecting the appropriate cryptographic algorithm, which establishes a secure connection for IPSec ESP.

4.7.2 DTLS on N2

The N2 interface uses DTLS over SCTP to ensure communication privacy in the network that uses SCTP as their transport protocol and allows AMF and RAN to communicate in a way that is designed to prevent eavesdropping and detect tampering or message forgery.

In addition to IPsec, DTLS shall be supported as specified in 3GPP TS 33.501 [1] to provide mutual authentication, integrity protection, replay protection, and confidentiality protection. Security profiles for DTLS implementation and usage shall follow the TLS profile given in clause 6.2 of TS 33.210 [11] and the certificate profile given in clause 6.1.3a of TS 33.310 [6]. The identities in the end entity certificates shall be used for authentication and policy checks.

4.8 Security Mechanism on N3 Interface

N3 is the reference point between the 5G-AN and UPF. It is used to carry user plane data from the UE to the UPF. The transport of user data over N3 shall be integrity, confidentiality, and replay-protected.

4.8.1 IPSec on N3

According to 3GPP TS 33.501 [1], to protect the traffic on the N3 interface, it is required to implement IPsec ESP and IKEv2 certificate-based authentication with confidentiality, integrity, and replay protection. IPsec is mandatory to implement on the gNB whereas on the core network side, a SEG may be used to terminate the IPsec tunnel.

4.9 Vulnerabilities to Quantum Attacks

The advent of quantum computing poses a significant threat to the cryptographic systems currently used in the 5G Core network. While traditional public-key algorithms such as RSA and ECC offer robust protection against conventional computational threats, these algorithms are vulnerable to quantum-based attacks.

ECC is widely used in 5G networks for securing communications, but it is vulnerable to quantum attacks, particularly from Shor's Algorithm, which can efficiently solve the ECDLP. This allows attackers to derive private keys from public keys, thereby compromising ECC-based security.

Given these vulnerabilities, transitioning to quantum-resistant cryptographic solutions is critical to ensuring the long-term security and integrity of 5G networks. This shift is necessary to protect against emerging threats, including Harvest Now, Decrypt Later (HNDL) attacks, where encrypted data intercepted today could be decrypted in a quantum-enabled future. Some areas of the 5G Core have already begun transitioning to quantum-resistant methods, as discussed in Chapter 5, with further upgrades planned to address additional vulnerabilities in the near future.

5.0 Post Quantum Cryptography Techniques

PQC holds cryptographic algorithms that are secure against the threats of quantum computers. Algorithms such as Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM) and Module-Lattice-Based Digital Signature Algorithm (ML-DSA), Stateless Hash-Based Digital Signature Algorithm (SLH-DSA) are quantum-proof algorithms.

The Internet is heavily reliant on Public Key Encryption (PKE) and the digital signature standard [37] to provide confidentiality, authenticity & privacy to all of its digital communications. These schemes form the basis of Internet security and are sometimes referred to as Public Key Infrastructure (PKI) when combined with Certificate Authorities (CAs). The current security standards make use of classical cryptographic algorithms, including RSA, ECC, DH, and DSA. These classical cryptosystems, however, are vulnerable to quantum attacks, if a large-scale fault-tolerant Quantum Computer is built in the future. Thus, the main goal of PQC is to develop quantum-safe cryptographic algorithms that can be easily integrated into the current security standards. These algorithms are based on differential computations that appear to be hard for even quantum computers and typically involve high dimensional lattices, error-correcting codes, isogenies between elliptic curves, collisions in hash functions, multivariate quadratic equations over finite fields, etc [25].

i. Traditional public key cryptosystems like RSA and ECC will be insecure by quantum computers. For instance, Shor's algorithm, which is a quantum algorithm, is capable of factoring large integers and computing discrete logarithms in Abelian groups in polynomial time [31]. Since these problems form the security basis of RSA & ECC, information encrypted using these schemes could be compromised when a Cryptographically Relevant Quantum Computer (CRQC) becomes a reality [46].
ii. Keys used in the current classical cryptography are often not truly random.
iii. Key sizes in symmetric encryption can be larger to improve the security [46].

To address the threat of quantum attacks, it is essential to adopt Post-Quantum Cryptographic algorithms and additionally for truly random numbers QRNG/TRNGs can also be utilised.

5.1 QRNG/TRNG

Unlike traditional deterministic random number generators, quantum mechanics being inherently non-deterministic, can serve as an ideal source to generate truly random numbers [58] [59]. The laws of quantum mechanics can be used to measure the quality of these random numbers. With advancements in quantum technology, it is now possible to generate high-quality random numbers that can be used in unconditionally secure cryptography applications [42]. The random number generators that use quantum sources to produce a certifiable source of randomness are known as quantum random number generators (QRNGs), mentioned in Figure 16.

Quantum systems have unique properties [43] such as the existence of superposition states, collapse on the measurement, entangled but space-like separated particles, the existence of nonlocal correlations, and the existence of indistinguishable particles, which are non-intuitive

from a classical perspective. These features play a pivotal role in making the quantum systems intrinsically random and, hence, provide the sources for a new class of randomness for cryptographic security.

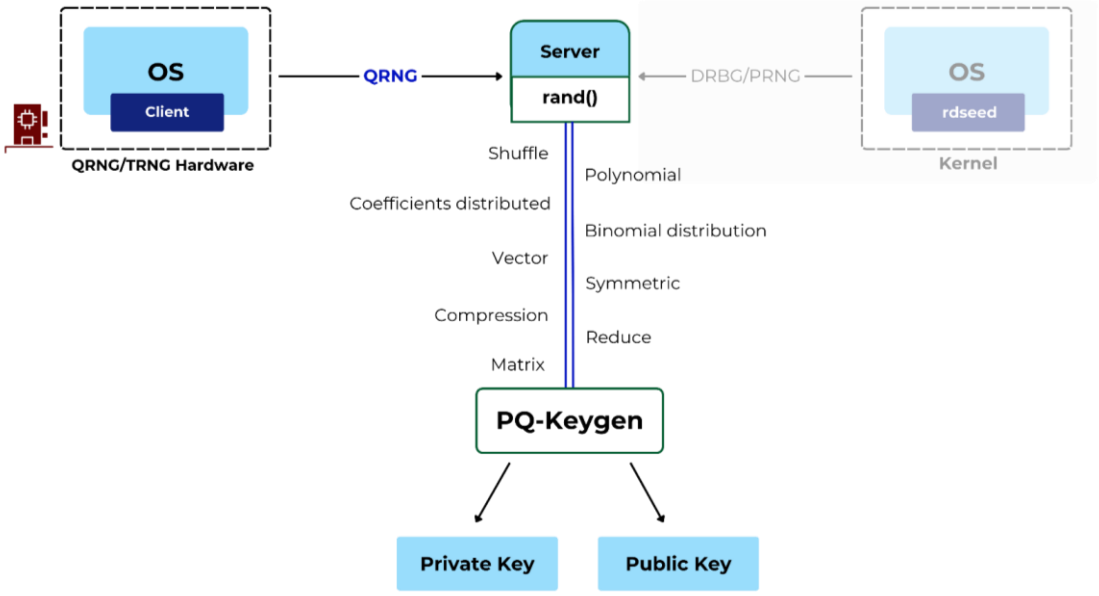


***Figure 16**: QRNG/TRNG*

5.2 AES-256

AES is a symmetric block cipher that processes data blocks of length 128 bits using cipher keys of length 128, 192, or 256 bits [48]. It repeatedly performs four transformations, which are (in order) SubBytes, ShiftRows, MixColumns, and AddRoundKey, and these constitute one full round. When working under different key lengths, the required numbers of rounds are different: 10 rounds for AES-128, 12 rounds for AES-192, and 14 rounds for AES-256.

Even though the quantum computer doesn't seem to have such major effects on symmetric keys, still in order to achieve the highest level of security it is recommended to use AES-256 [51] [54] [56] [57]. AES-256 employs a larger key size (32 bytes), which provides a much stronger defense against quantum-based threats [28]. In digital networks, AES-256 is highly valuable and improves all the symmetric encryption done for the concealment of data.

5.3 ML-KEM

According to FIPS-203 [14], a key-encapsulation mechanism (KEM) is a set of algorithms that, under certain conditions, can be used by two parties to establish a shared secret key over a public channel. A shared secret key that is securely established using a KEM can then be used with symmetric-key cryptographic algorithms to perform basic tasks in secure communications, such as encryption and authentication.

NIST has specified a key encapsulation mechanism known as the Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM), which is based on the computational difficulty of the Module Learning with Errors (MLWE) problem.

ML-KEM is considered safe even against the threat of quantum attacks. Currently, NIST has three sets for ML-KEM, each offering different levels of security and performance: ML-KEM-512, ML-KEM-768, and ML-KEM-1024. These sets increase in security strength but decrease in performance as the parameters scale up.

ML-KEM consists of three steps, as shown in Figure 17:

i. **ML-KEM.KeyGen():** Generating the key pair i.e. public key and private key. The public key is then sent to the other party i.e. P2 in Figure 17.

ii. **Ml-KEM.Encaps()**: Encapsulation is performed using the public key that was received by P2 which generates cipher text and shared secret. This cipher text is then sent to P1.

iii. **ML-KEM.Decaps()**: Decapsulation of Cipher text is done using the private key that was generated in step 1. This creates the same shared secret on the P1 side as well.

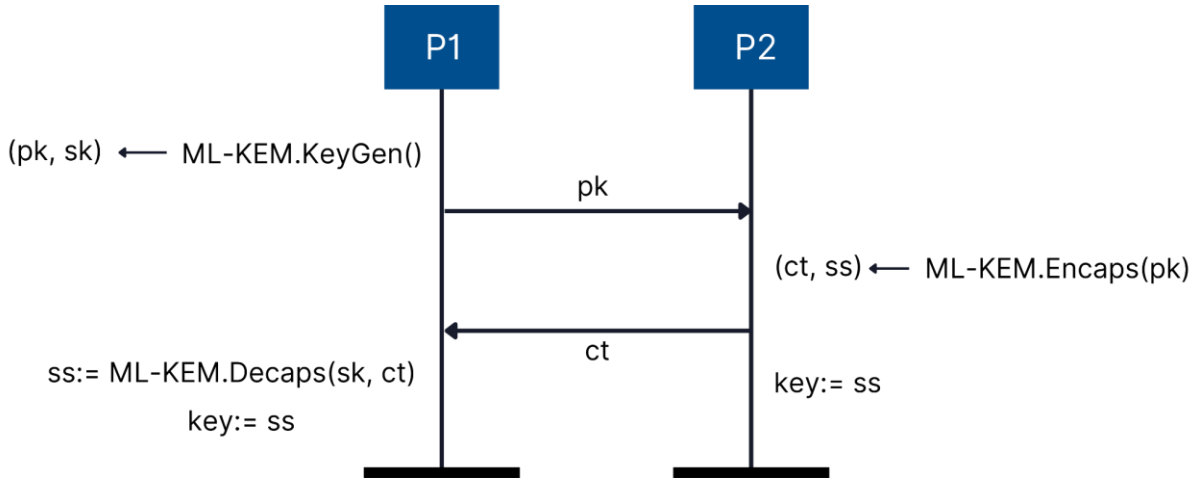


***Figure 17**: ML-KEM*

5.4 ML-DSA

Digital signatures are a cryptographic scheme that allows the recipient to verify the authenticity and integrity of digital data, proving that the data came from a legitimate sender and has not been tampered with. By ensuring the sender's identity and the data's integrity, digital signatures establish trust in a public network, thus, they serve as an essential component for secure communication. NIST has specified [13] ML-DSA, a suite of algorithms designed to generate and verify digital signatures. ML-DSA is based on the computational hardness of the MLWE problem, making it safe against the threats posed by quantum computers.

The security guarantee of ML-DSA means that an adversary who has access to a signing oracle cannot produce a signature of a message whose signature he hasn't yet seen, nor produce a different signature of a message that he already saw signed.

ML-DSA, as a digital signature scheme, consists of three main algorithms as shown in Figure 18:

i. **ML-DSA.KeyGen()**: Generating the keypair, i.e. private and public keys. This algorithm takes in no inputs and outputs the keypair encoded as byte strings. The public key is sent to the other party i.e. P2.

ii. **ML-DSA.Sign()**: Signing of digital data (e.g. messages) is performed using the private key. This algorithm takes the message, context string, and the private key as the input and outputs a byte-encoded signature which is then sent to the party P2.

iii. **ML-DSA.Verify()**: Verification of the digital signature sent by party P1 is done using the signature public key of P1, which was generated in step 1. This algorithm takes in the public key, message, signature & context string as the input. It outputs a Boolean value, i.e. true if the signature is valid with respect to the message and the public key, and a false value is returned if the signature is invalid.

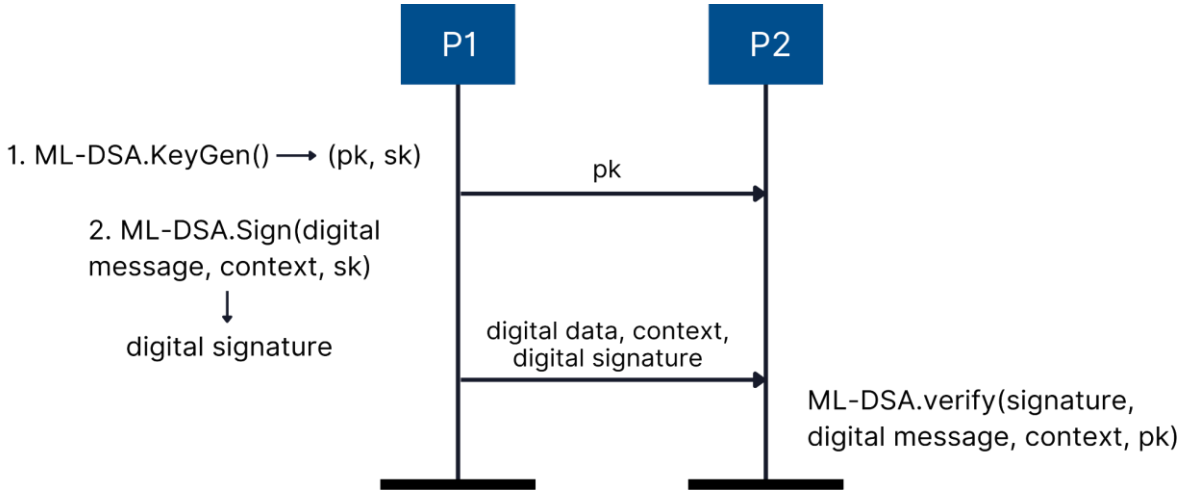


***Figure 18**: ML-DSA*

5.5 PQ-TLS

Post-Quantum Transport Layer Security (PQ-TLS) [18] secures communication channels by post-quantum cryptographic algorithms [16], making sure that data sent between two parties remains confidential and safe against quantum threats.

As shown in Figure 19, PQ-TLS (TLS1.3 with PQ support) introduces homogeneous and hybrid authentication mechanisms that make use of quantum safe signature schemes, such as ML-DSA, SLH-DSA, and Falcon, with a classical scheme in combination (if hybrid authentication is chosen). HMAC, however, is not replaced as it is considered quantum-safe [41]. The Key Exchanges (KEXs) are achieved by Post Quantum Key Exchanges, typically

involving PQ KEMs such as ML-KEM, NTRU-HRSS, BIKE, and FrodoKEM, among others. These KEXs are usually integrated with classical PKC algorithms to form a hybrid design [17] [38], which guarantees as much security as the existing classical standards in case any of the PQ KEX counterparts are found to be insecure.

TLS 1.3 integrated with Post-Quantum Cryptography like ML-DSA and ML-KEM [22] makes PQ-TLS quantum-secure and perfectly forward-secure. As a result, PQ-TLS stands as a splendid replacement for the current TLS protocol and can be seamlessly introduced into most digital networks, including 5G.

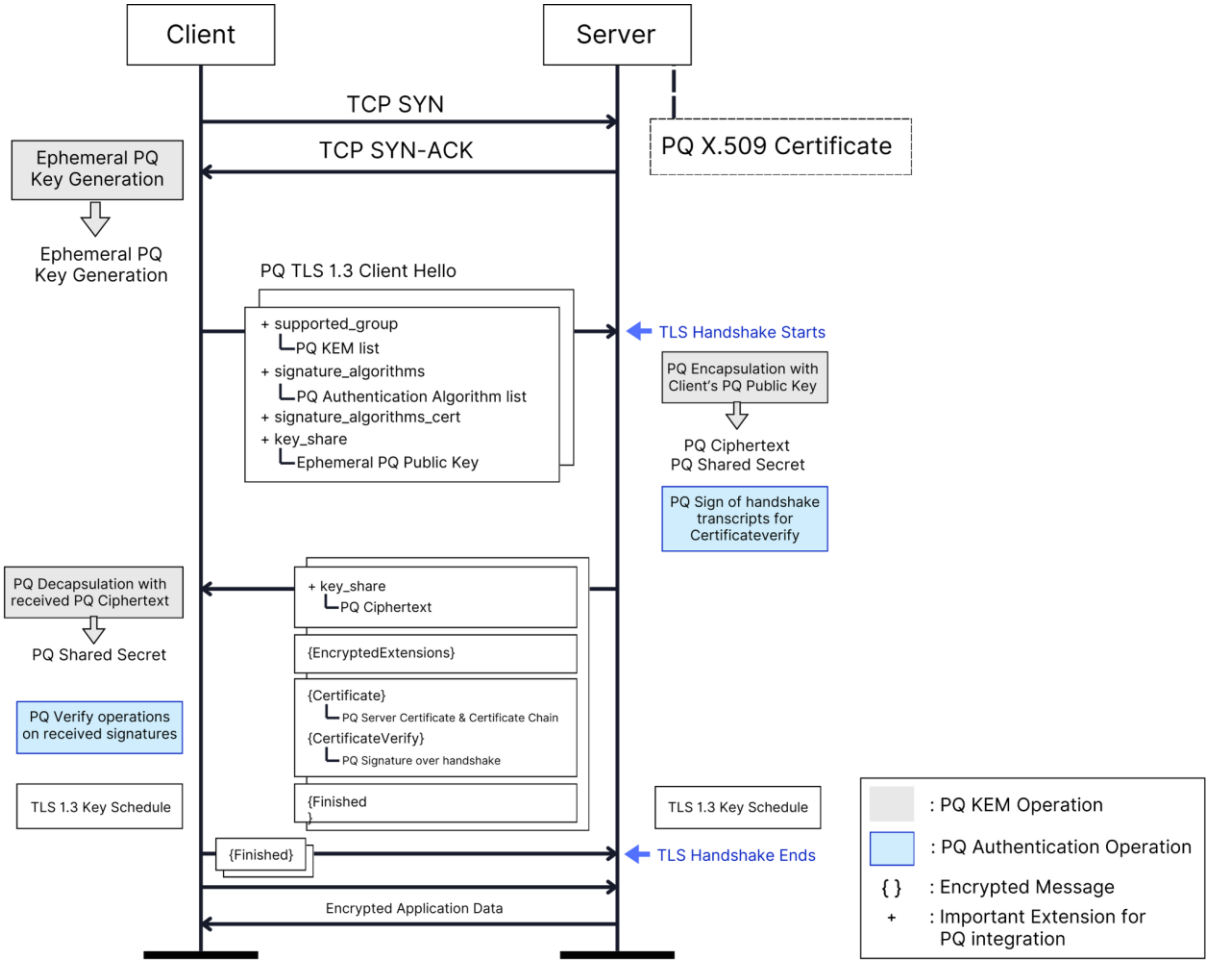


***Figure 19**: Post Quantum TLS 1.3 Handshake*

5.6 PQ-IPSec

Post-Quantum Internet Protocol Security (PQ-IPSec) [19] secures Internet Protocol communications by using post-quantum cryptographic methods [20]. This protocol encrypts and authenticates data packets transmitted over IP networks protecting against quantum adversaries. With this Post-Quantum Pre-Shared Keys & IKEv2 will be upgraded to use Post-Quantum Key Exchanges algorithm along with Post-Quantum Certificates. PQ-IPSec (IKEv2 with PQ support) [39] is crucial for maintaining the confidentiality and integrity of data against quantum threats.

5.7 PQ-DTLS

Post-Quantum Datagram Transport Layer Security (PQ-DTLS) secures datagram-based communications by employing homogeneous and hybrid post-quantum cryptographic algorithms. PQ-DTLS (DTLS1.3 with PQ support) makes sure all the data packets sent between two parties are confidential and authenticated, even when there are any quantum adversaries while still maintaining the efficiency and flexibility required for datagram transmission.

5.8 PQ-mTLS

Post-Quantum Mutual Transport Layer Security (PQ-mTLS) extends [16] the principles of PQ-TLS by requiring both parties in a communication exchange to authenticate each other by using Post-Quantum Digital Certificates as shown in Figure 20. By integrating homogeneous and hybrid post-quantum algorithms, PQ-mTLS (mTLS1.3 with PQ support) makes sure both client and server are authenticated and the data/messages sent between them are in an encrypted format, which is also done using Post-Quantum Cryptographic Algorithms. This post-quantum mutual authentication process & key exchange mechanisms [41] secure bidirectional communications from quantum threats. PQ-mTLS utilizes PQ X.509 certificates which use quantum-resistant digital signature schemes, such as ML-DSA, in either homogeneous or hybrid mode; this guarantees that the authentication of mTLS cannot be compromised by any quantum-capable adversary. Furthermore, it makes use of PQ KEMs as the key exchange mechanism, in a manner identical to its parent protocol, PQ-TLS.

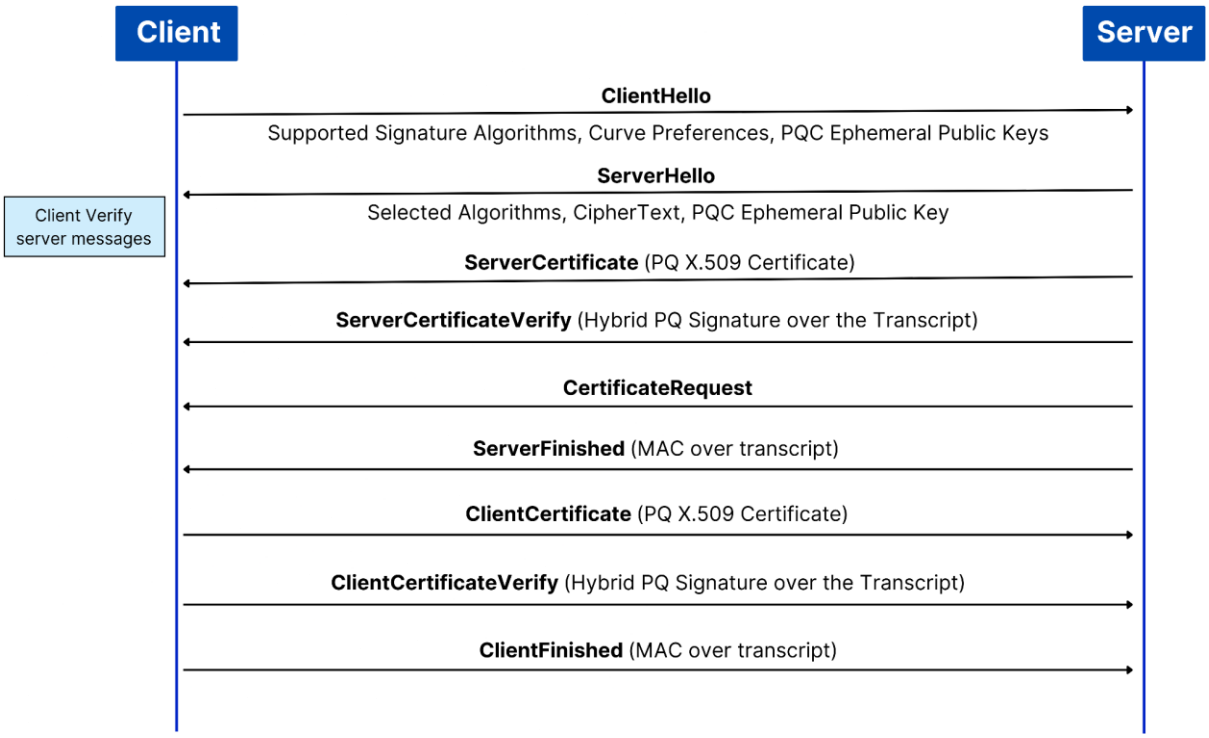


***Figure 20**: PQ-mTLS*

5.9 SLH-DSA

SLH-DSA, or Stateless Hash-Based Digital Signature, is a digital signature algorithm that uses hash-based methods to generate and verify signatures without maintaining state information between operations. SLH-DSA [23] is based on SPHINCS+, which was selected for standardization as part of the NIST Post-Quantum Cryptography Standardization process.

6.0 Migration to Post-Quantum Cryptography in 5G Core

To successfully transition from a conventional 5G Core to a post-quantum Core, several critical areas and protocols can be updated as provided in Figure 21. This includes modifications in the 5G-AKA & user authentication mechanisms to introduce Post Quantum PKE methods [24] upgrading the current ECIES method. Furthermore, it requires changes in the core networks' security protocols like (m)TLS & OAuth 2.0 to incorporate PQ algorithms [26]. Of utter importance is to update roots-of-trusts for firmware update to mitigate that quantum attackers provisions fraudulent firmware and which would enable complete control of base stations and core nodes. Firmware update is a very high-level target, hardware roots-of-trust can typically not be migrated to PQC after manufacturing, and base stations are often deployed for decades. CNSA 2.0 for US national security systems specifies that algorithms for firmware and software update is the first thing to migrate. Software libraries for TLS, IPsec, and SSH can be migrated at any time. These changes must be carried out carefully by making use of proper PQC migration techniques that thoroughly evaluate quantum-safe protocols and prioritize those at the application layer [30], such as TLS.

The table below outlines the necessary changes across different components and areas of the 5G core network to ensure quantum-resistant security.

Functionality	Classical Mechanism	Post Quantum Mechanism
Random Number	DRBG/PRNG	QRNG/TRNG
SBI Communication	mTLS	PQ-mTLS
Digital Signature in x.509 Certificate	Classical Signature Scheme	PQ Signature Scheme (ML-DSA)
Symmetric Key (optional)	AES-128	AES-256
N2 CP Message	DTLS / IPSec	PQ-DTLS / PQ-IPSec
N3 User Data	IPSec	PQ-IPSec

ECIES Scheme	Classical Cryptographic Algorithm (Curve25519, Secp256r1)	Homogeneous: ML-KEM
		Hybrid: ML-KEM + Classical Cryptographic Algorithm

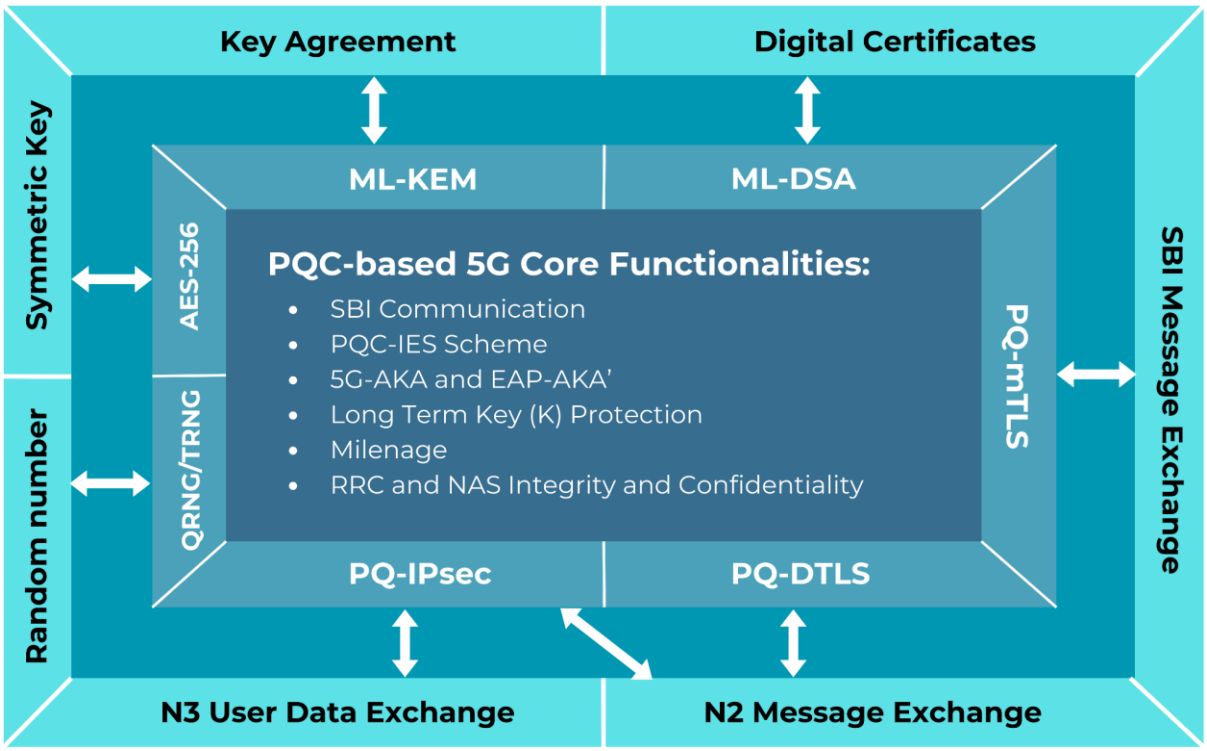


***Figure 21**: Post Quantum Cryptography in 5G Core*

6.1 Random Seed Generation using QRNG/TRNG

Traditional random number generators like PRNG/DRBG are based on deterministic algorithms [60] and even so, the generated random number can be guaranteed to be safe when the entropy of the initial value is high, it is impossible to generate the complete random number in the deterministic system. Hence, in order to achieve truly random numbers and higher entropy [50] QRNGs or TRNGs can be used [58] [59].

The advanced Quantum Random Number Generators that have appeared with the impulse of quantum information research are capable of solving [43] these shortcomings of traditional random number generators by leveraging quantum processes to produce truly random numbers, ensuring high unpredictability and entropy. This level of randomness [42] can be used for cryptographic key generation, as it significantly enhances security by making it nearly impossible to predict or reproduce keys. Therefore, QRNGs can be used for maintaining robust security in telecom networks.

In addition to QRNG, True Random Number Generators (TRNG) can also be used to generate random numbers based on physical processes, such as electronic noise, which are inherently unpredictable. TRNGs provide an alternative to QRNGs, especially in environments where quantum hardware is not yet feasible.

Both QRNGs and TRNGs are crucial for secure cryptographic operations in the 5G Core network, ensuring the integrity of systems like key generation, authentication, and data encryption. There are various areas of the 5G Core where QRNG/TRNG can be used for generating random numbers and seeds for various keys:

i. **Keys for 5G-AKA Procedure** - The 5G-AKA procedure performs various key agreements for the authentication process. QRNG/TRNG can be used to generate these keys and parameters, which can then also be used in the Milenage algorithm.

ii. **Long-Term Keys** - The long-term keys are one the most important keys in the overall network and it is highly required for these keys to be truly random. QRNG/TRNG can be used to provide true randomness while generating the long-term keys.

iii. **Home Network Public and Private Keys**: The security of SUPI concealment relies on how strong and random the home network public and home network private keys are, therefore, these keys can be truly random by using QRNG/TRNG.

iv. **Certificate Generation Between Different NFs** - Digital Certificates are important for the authentication between different NFs and QRNG/TRNG can improve the security of these certificates by providing more randomness to them.

v. **Secure SBI Communication Between NFs** - The SBI helps in the communication between different network functions and this communication is secured using various algorithms. QRNG/TRNG can provide random seeds to these algorithms.

6.2 Transition to AES-256 Symmetric Key

Symmetric encryption is an integral part of maintaining the safety of the core network. It is used to safely cipher the data in transit making it unintelligible for any adversary and hence it is highly necessary to make the symmetric encryption method more secure.

In the 5G networks, AES is highly popular due to the extensive support it has received from major CPU vendors, who have introduced specialized AES SIMD instruction sets, speeding it up even in software-based environments. Thus, it has an edge over other symmetric ciphers, making it a great choice for 5G networks, which are efficiency-focused [47]. Currently, however, the symmetric cryptography doesn't seem to be affected severely by the quantum computers, still in order to make symmetric encryption more secure it is recommended to use AES-256 [51] [54] [56] [57] [28]. In the following areas it can be upgraded to AES-256:

i. **SUPI Concealment** - The final step of SUPI concealment requires AES-128 for encryption and similarly, it is also required for the decryption part. In this case, AES-256 can be used for generating SUCI instead of AES-128.

ii. **AKA Procedure** - Within the AKA procedure, AES-128 can be replaced with AES-256 to improve the security making sure that the authentication remains safe against potential quantum risks.

iii. **Milenage Function** - The Milenage function, used in the 5G AKA, can adopt AES-256 [55], including for generating the Operator's Permanent Key (oPc) value. This transition enhances the security of cryptographic operations, ensuring that the encrypted data & the generated keys are resilient against quantum threats.

iv. **NAS Security** - AES-256 can be used to improve the NAS security [51] (alongwith SNOW-256 [52] & ZUC-256 [53]).

6.3 PQ-mTLS Based SBI Communication between NFs

Communication between NFs currently relies on mTLS which uses classical asymmetric cryptography & symmetric encryption methods, making it quantum unsafe. As a result, the Post Quantum version of mTLS & its parent protocol TLS, is of utmost importance in the present scenario. To address this vulnerability, PQ-mTLS (mTLS1.3 with PQ support) needs to be implemented in the 5G/B5G Core, to ensure that it is quantum-resistant.

PQ-mTLS leverages state-of-the-art cipher suites(provided in below table) that integrate post-quantum cryptographic algorithms. These cipher suites include both homogeneous and hybrid post-quantum algorithms.

Field	Value
CA Type	Private (Internal) CA
Certificate Signature Algorithm	Homogeneous: ML-DSA-44/65/87
	Hybrid: ML-DSA_Ed448, ML-DSA_Ed25519 + Any TLS v1.3/1.2 Classical Signature Schemes
Signature Length	3293 octets + Classical Signature length (e.g., 64 octets for Ed25519)
Key Exchange Mechanism	Homogeneous: ML-KEM (512/768/1024)
	Hybrid: ECDHE_ML-KEM (e.g., X25519MLKEM768)

Key Exchange Length (Public key)	1216 octets (ML-KEM_768: 1184 octets, X25519/P256: 32 octets)
Key Exchange CipherText Length	1088 octets
AEAD - Symmetric Encryption & Authentication Algorithm	AES256_GCM, ChaCha20_Poly1305
enckeylen	32 octets (256 bits)
ivlen	12 octets (96 bits) (AEAD specific)
mackeylen	32/48 octets (256/384 bits)
maclen	32/48 octets (256/384 bits)
TLS KDF	HMAC-based Expand & Extract KDF (HKDF) / PRF for TLS v1.2
TLS Finished MAC algorithm	HMAC-SHA-256/384
Fallback Methods	TLS v1.2, Classical signature algorithms & Classical key exchanges supported

Post-quantum certificates ensure secure and trustworthy communication between NFs. This process validates the authenticity and validity of post-quantum certificates. The network protects itself against quantum-capable adversaries (both active & passive) by using post-quantum cryptographic algorithms to generate and verify certificates. This approach ensures the security of all communications.

PQ-mTLS allows the use of quantum-safe cryptographic algorithms to encrypt the data and messages sent between the NFs. This approach prevents eavesdropping & MITM attacks, keeping the information confidential and tamper-proof, protecting it from interception and unauthorized access. Furthermore, the addition of quantum-safe cryptography guarantees the safety of data against “Store Now, Decrypt Later” attacks & also against active quantum adversaries.

In the 5G/Beyond 5G Core, PQC boosts mTLS-based communication between NFs to PQ-mTLS. This setup allows both homogeneous and hybrid post-quantum signature algorithms in their shared cipher suites.

Also, QRNGs/TRNGs can be utilized to create seeds to produce both post-quantum and classical ephemeral key pairs, like ML-KEM768 and ECC X25519, this allows for true randomness in the Key generation procedure. PQ-mTLS helps NFs swap encrypted data and messages, which keeps information private and safe from tampering. This approach stops others from intercepting or accessing the data without permission.

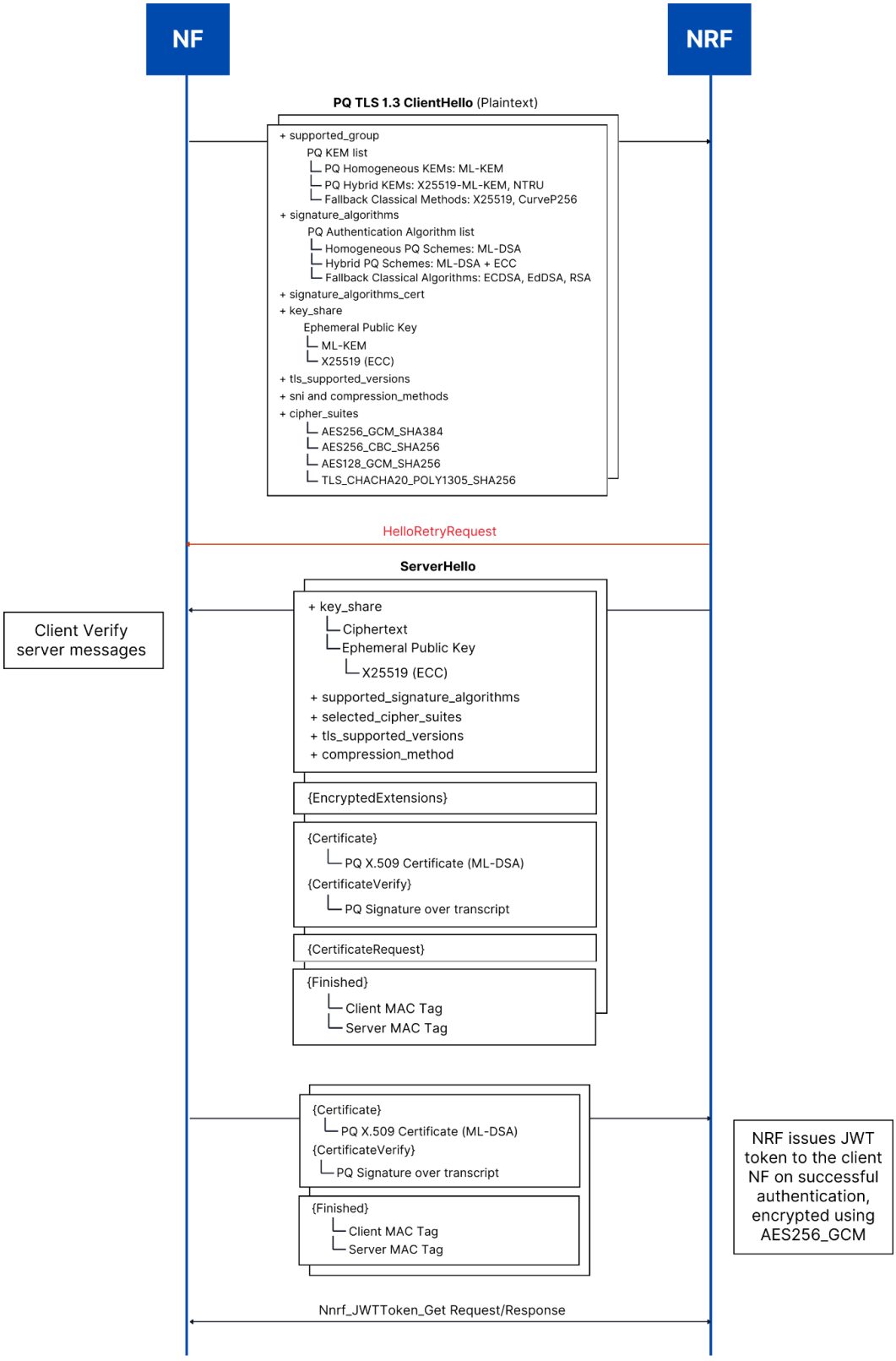


***Figure 22**: Hybrid PQ-mTLS in SBI Communication between NFs*

As shown in Figure 22, Here are the message exchanges [41] between the server (NRF) and client (NF) during the NF registration process with the NRF:

I. The client starts the handshake by sending a **ClientHello** message, which includes the cryptographic algorithms and parameters that the client supports:

   i. The supported TLS **cipher suites**, such as TLS_AES256_GCM_SHA384, which combine an authenticated encryption scheme and a hash function, are represented using code points. A code point is an identifier of a cryptographic algorithm used in TLS.

   ii. Furthermore, these cipher suites include more secure symmetric encryption algorithms, such as AES256 or ChaCha20 as their topmost priority. Quantum unsafe suites are listed at a lower priority level.

   iii. The **signature_algorithms** extension includes the supported signature algorithms, which consist of Homogeneous and Hybrid PQ Signatures Schemes such as ML-DSA (44/65/87), ML-DSA_Ed448, ML-DSA_secp256k1, with fallback support for classical signature schemes when needed.

   iv. The **supported_groups** extension lists the supported key exchange mechanisms which include Homogenous and Hybrid PQ KEMs, such as ML-KEM (512/768/1024), and X25519MLKEM768, SecP256R1MLKEM768 [17] along with fallback support for classical DH and ECDH(E) key exchanges.

   v. The client generates a key pair for each supported key exchange group and includes these public keys in the **key_share** extension. A key share is a public key that is used to compute a shared secret when exchanged between parties. For instance, a public key for a hybrid PQ KEM such as X25519MLKEM768, is a concatenation of the ML-KEM768 public key (1184 octets) and the X25519 public key (32 octets).

   vi. Optionally, the client may send an additional list of signature algorithms in the **signature_algorithms_cert** extension for certificate signatures to indicate preferences.

II. On receiving ClientHello, the server selects supported parameters from the client's proposal and if it chooses any key share group that consists of PQ KEMs, it first encapsulates the public key to compute a shared secret. sharedSecret1, which is then combined with the DH shared secret. sharedSecret2 (if a hybrid scheme is chosen). The final shared secret, sharedSecret (sharedSecret1 + sharedSecret2) is used to derive symmetric keys for securing subsequent messages, and responds as follows:

   i. The server sends the **ServerHello** message containing the server's selected parameters from ClientHello. The server also sends the CipherText which is obtained from encapsulating the client's PQ KEM public key. The server also generates its own key pair for the selected DH group (if a Hybrid Scheme is chosen) and includes its public key in the **key_share** extension.

ii. The **Encrypted Extensions** message contains encrypted extensions such as **supported_groups**, which are encrypted using the derived keys.

iii. If the server wants the client to also authenticate itself, it issues an optional **CertificateRequest** message to the client.

iv. The **certificate** message sent by the server contains the server's certificate chain. This is a PQ Homogenous/Hybrid X.509 certificate which must contain a public key for one of the signature schemes listed in the client's **signature_algorithms** extension. If the client sends the **signature_algorithms_cert** extension, the certificates in the chain must be signed with one of the listed signature algorithms in the extension.

v. The **CertificateVerify** message contains a signature over the hash of all handshake messages up to this point. The signature is computed using the private key corresponding to the public key in the server's certificate. This signature is done via PQ Homogenous/Hybrid Signature schemes which the client is willing to verify.

vi. The **Finished** message contains a MAC over the hash of all handshake messages up to this point. The algorithm is HMAC with the negotiated hash function from the selected cipher suite.

III. The client completes its part of the key exchange by first decapsulating the PQ KEM's CipherText sent by the server to obtain a shared secret - sharedSecret1. Then, it derives the DH shared secret using the server's ECC public key - sharedSecret2 (if a hybrid scheme is chosen). The final shared Secret - sharedSecret is then used to derive subsequent keys as per the TLS v1.3 key schedule.

i. If the server issues a CertificateRequest, the client responds with its own **Certificate** and **CertificateVerify** messages. The client's final handshake message is **Finished**, which includes a MAC over the entire handshake transcript.

ii. Once both the client and server have exchanged the Finished messages and successfully verified all the MACs and signatures, the handshake procedure is complete. The peers can then start exchanging application data protected by the AEAD algorithm. The symmetric keys used in the AEAD/HMAC operations are derived from the shared secret through the TLS 1.3 key schedule, which is determined by the negotiated hash function.

IV. Token Exchange: Next, using the derived secrets, the server (NRF) issues a JWT token to the client (NF), encrypted using AES256_GCM.

6.3.1 PQ JWT Token-based Authentication

For service requests between the NFs, each of the network functions is assigned with PQ JWT token by NRF through SCP, as shown in Figure 23. After the validation of tokens, the SCP is used on the communication path for some service selections and routing processes.

The NRF gets NF Registration and Discovery Requests straight from NF instances. It gives information about found NF instances and keeps NF profiles up to date. When it signs up and updates NF profiles, the NRF checks if the details in the NF profile match those in the Post-Quantum certificate of the NF instance. This check makes sure approved network functions can access the system.

SCP handles all the service requests from each network function, which it then sends to NRF. SCP does this by dealing with access token requests from NF Service Consumers and giving out authorization tokens when needed. As an authorization server, the NRF makes sure both it and the network functions asking for services through SCP are safe. This keeps the service-based setup secure and reliable.

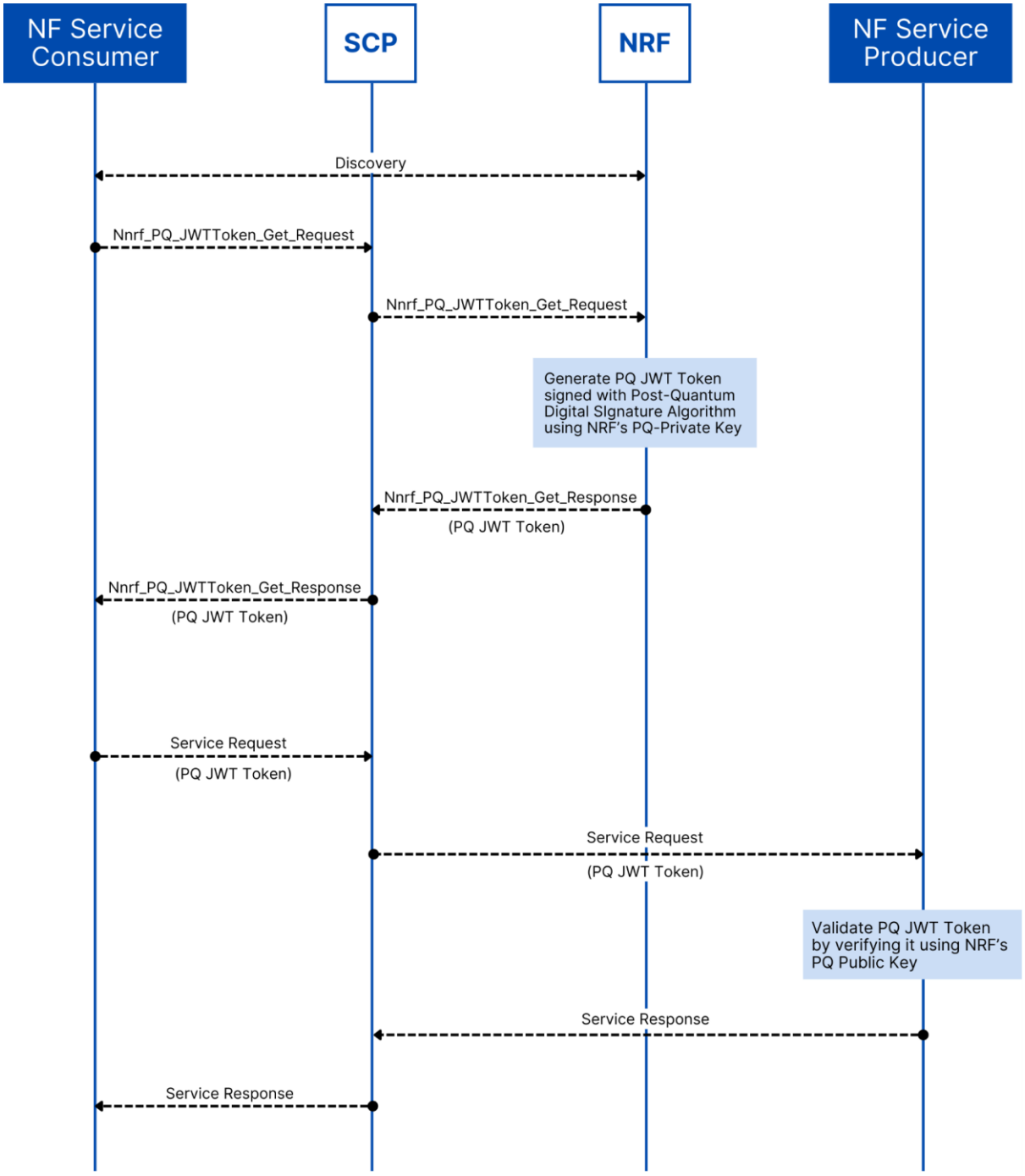


***Figure 23**: PQ JWT token-based Authentication*

6.4 PQ-IES Scheme

In 4G networks, IMSI is transmitted in plain text from UE to the core network, making it vulnerable to man-in-the-middle attacks. To address this vulnerability, 5G networks introduced SUPI. The SUPI is encrypted and converted into SUCI before being transmitted to the core network, enhancing security. This encryption process is currently performed using the ECIES.

However, since ECIES relies on elliptic curves that are vulnerable [45] to quantum attacks, PQC is essential to integrate for the SUPI concealment. This integration can be achieved

through two methods: the homogeneous method or the hybrid approach. The two profiles that were approved by 3GPP for ECIES are not secure against Quantum attacks so two new Post-Quantum profiles i.e. Profile C and Profile D, are added for the SUPI to SUCI conversion, as shown in Figure 24. Profile C uses only Post-Quantum cryptographic algorithms whereas Profile D goes with the Hybrid Post-Quantum approach. Using profile C and D, SUPI is now even secured against Quantum-powered IMSI-Catchers.

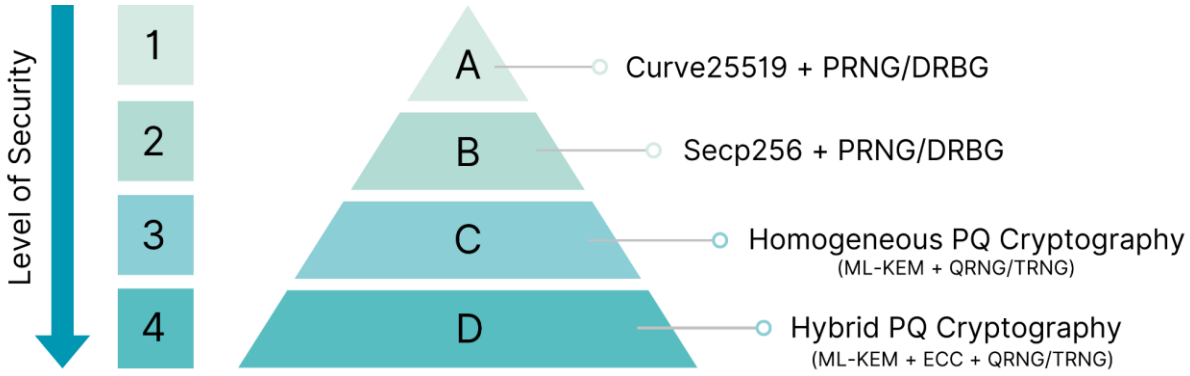


***Figure 24**: PQ-IES (ECIES with PQ Support) Profiles*

PQ-IES Parameters	Profile C (Homogeneous)	Profile D (Hybrid)
PQC domain parameters	ML-KEM + QRNG/TRNG	ML-KEM + ECC (Curve25519/secp256r1) + QRNG/TRNG
PQC Diffie-Hellman primitive	N/A	X25519
Point Compression	N/A	X25519 - N/A secp256r1 - true
KDF	ANSI-X9.63-KDF	ANSI-X9.63-KDF
Hash	SHA-256	SHA-256
SharedInfo1	the empty string	R (the ephemeral ECC public key octet string)
MAC	HMAC-SHA-256/384	HMAC-SHA-256/384

mackeylen	32 octets (256 bits)	32 octets (256 bits)
maclen	8 octets (64 bits)	8 octets (64 bits)
SharedInfo2	empty string	empty string
ENC	AES-256 in CTR mode	AES-256 in CTR mode
enckeylen	32 octets (256 bits)	32 octets (256 bits)
icblen	16 octets (128 bits)	16 octets (128 bits)

6.4.1 Profile C: Homogeneous Post-Quantum Cryptography

This approach employs post-quantum cryptography methods throughout the communication process to safeguard the UE's SUPI from adversaries (classical and quantum) by providing a robust public key encryption technique.

It uses ML-KEM (FIPS 203), along with key generation through QRNG/TRNG, to convert SUPI to SUCI and back, resulting in a strong and secure encryption technique. It uses AES-256 to improve encryption giving more security than older standards. It also supports multiple encryption profiles (ML-KEM 512/768/1024), each made to give stronger levels of security. These profiles fit different security needs letting the network adjust to various threat levels and operational requirements.

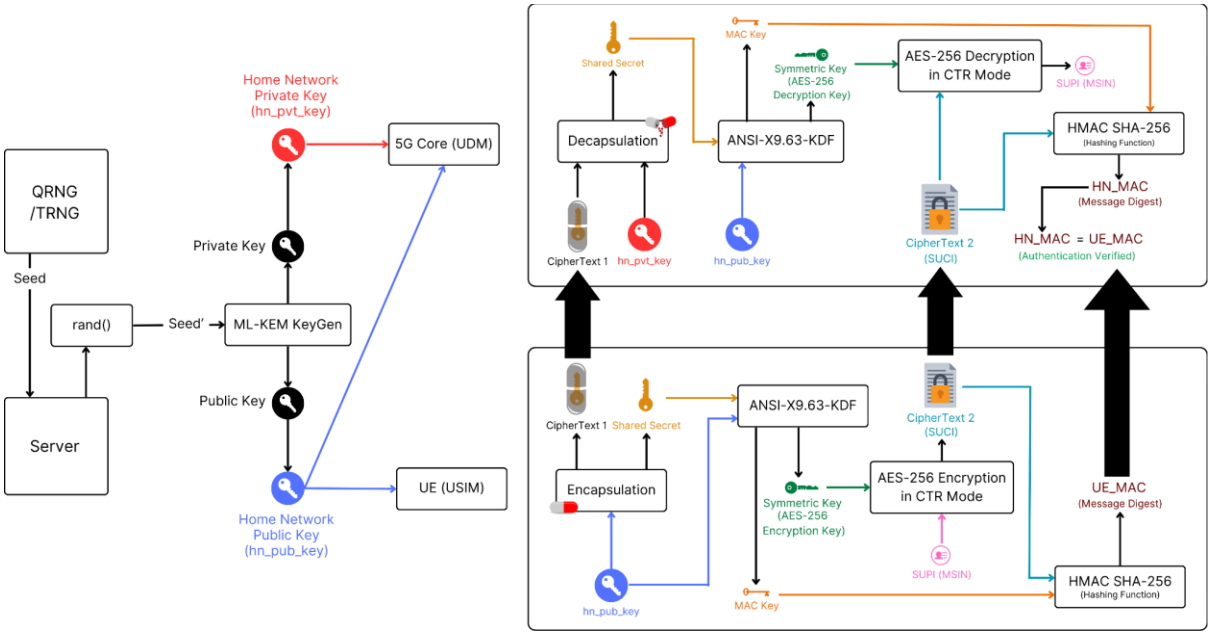


***Figure 25**: Homogeneous Post-Quantum Cryptography Approach in SUPI Concealment*

As shown in Figure 25, Here are the steps involved in securing a user's identity in Quantum Secure 5G Core under Homogeneous Post-Quantum Cryptography:

ML-KEM Keygen using QRNG/TRNG Seeds:

i. The seed generated using QRNG/TRNG can be utilized to create the HN Public Key and HN Private Key via ML-KEM.

Key Distribution:

i. The HN Public Key is securely transmitted to the UE. Simultaneously, the HN key pairs are securely stored in UDM within the 5G Core.

Encryption at the UE Side:

i. The UE performs key encapsulation using the HN Public Key, generating a shared secret and a ciphertext (Ciphertext 1).

ii. The shared secret and HN Public Key are then passed through a Key-Derivation Function (ANSI-X9.63-KDF) to produce 2 keys: a symmetric key and a MAC Key.

iii. The Symmetric Key is used to encrypt SUPI, specifically the MSIN part, using the AES-256-CTR encryption algorithm to generate SUCI (Ciphertext 2).

iv. SUCI and the MAC Key are then passed through the HMAC-SHA256 hashing function, generating a message digest referred to as the UE_MAC.

v. The UE sends Ciphertext 1, SUCI, and UE_MAC to the UDM in the 5G Core.

Decryption at the UDM Side:

i. UDM uses the HN Private Key and the received Ciphertext 1 to perform key decapsulation to reconstruct the shared secret.

ii. The received shared secret and the HN Public Key are then passed through the ANSI-X9.63-KDF again to regenerate the Symmetric Key and MAC Key.

iii. The Symmetric Key is subsequently used to decrypt SUCI via the AES-256-CTR algorithm, obtaining SUPI.

iv. Additionally, Ciphertext 2 and the MAC Key are hashed again using HMAC-SHA256, generating a second message digest called the HN_MAC.

Message Integrity Verification:

i. The UDM compares the HN_MAC with the UE_MAC received from the UE. If both message digests match, the integrity and confidentiality of the transmitted identity data are successfully verified. This ensures that the user's identity is securely protected during transmission and that no tampering occurs.

ii. After the verification, SUCI is decrypted to obtain SUPI.

6.4.2 Profile D: Hybrid Post-Quantum Cryptography

This method [32] will combine classical and post-quantum cryptographic methods, which guarantees that the encryption will be as secure as the proven classical methods of ECC even if Post Quantum cryptographic algorithms turn out to be insecure.

This approach combines the post-quantum algorithm ML-KEM with classical algorithms like Curve25519 [12] and Secp256r1, along with key generation through QRNG/TRNG, for the conversion of SUPI to SUCI and vice versa. This hybrid method [27] [29] enhances security by leveraging both quantum-resistant and classical cryptographic techniques.

By utilizing a 256-bit key, AES-256 significantly strengthens the encryption process, ensuring that even with the advent of quantum computing, the integrity and confidentiality of communications are maintained.

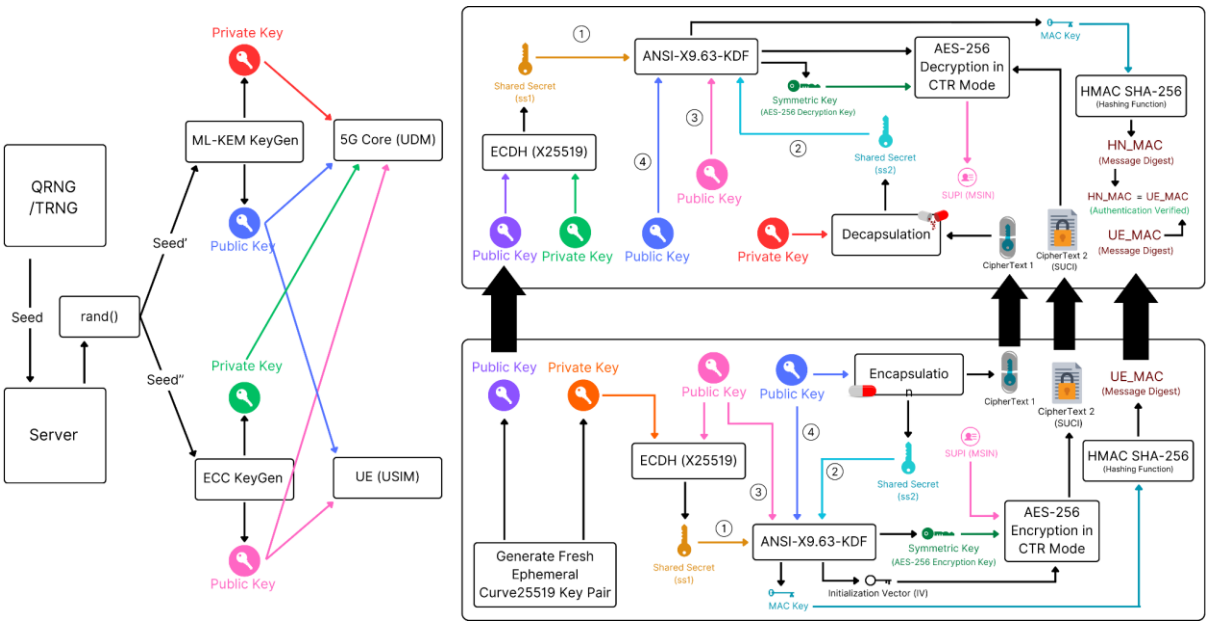


***Figure 26**: Hybrid Post-Quantum Cryptography Approach in SUPI Concealment*

As shown in Figure 26, here are the steps involved in securing a user's identity in Quantum Secure 5G Core under Hybrid Post-Quantum Cryptography:

Long-Term Key Generation:

I. At the HN, a QRNG/TRNG generates two seeds: a 64-byte seed and a 32-byte seed:

   i. The 64-byte seed is used to generate the long-term (LT) ML-KEM private and public keys.

   ii. The 32-byte seed is used to generate another LT Curve25519 (ECC) private key and a corresponding public key.

II. The LT ML-KEM and ECC public keys are securely transmitted to the UE, while both ML-KEM and ECC key pairs are securely stored in the UDM of the 5G Core.

Initial Registration Process:

i. During the initial registration, the UE generates an ephemeral Curve25519 (ECC) key pair, consisting of an ephemeral private key and an ephemeral public key.

ii. The ephemeral ECC private key is combined with the LT HN ECC public key of the Home Network using the X25519 Elliptic Curve Diffie-Hellman (ECDH) protocol to create a shared secret (shared secret 1).

iii. Simultaneously, the LT HN ML-KEM public key is used for key encapsulation, producing a ciphertext and another shared secret (shared secret 2).

Key Derivation and Encryption:

i. The shared secrets (shared secret 1 + shared secret 2) are concatenated and passed through the ANSI-X9.63 KDF. The KDF uses the combined ECC ephemeral public key and the LT HN ML-KEM public key as shared information, resulting in the generation of three keys: a symmetric key, an Initialization Vector (IV), and a MAC key.

ii. The symmetric key and IV are used to encrypt the SUPI using the AES-256-CTR encryption algorithm to generate SUCI.

iii. Next, the HMAC-SHA256 algorithm is used to generate a MAC tag, referred to as UE_MAC, by hashing SUCI along with the MAC key.

iv. The ECC ephemeral public key, ciphertext, SUCI, and UE_MAC are sent to the UDM.

v. Any traces of ciphertext and ECC ephemeral key pair are immediately deleted from the UE.

Decryption and Verification at UDM:

i. UDM combines the ECC ephemeral public key with the LT HN ECC private key using the X25519 ECDH protocol to recreate the first shared secret (shared secret 1).

ii. The ciphertext is decapsulated using the LT HN ML-KEM private key to obtain the second shared secret (shared secret 2).

iii. These shared secrets (shared secret 1 and shared secret 2) are passed to the ANSI-X9.63 KDF (in the same order as before) along with ECC ephemeral public key + LT HN ML-KEM public key as shared information, generating a symmetric key, an IV, and a MAC key.

iv. HMAC-SHA256 is then applied to the SUCI with MAC Key to produce the MAC tag, referred to as, HN_MAC.

v. If the HN_MAC matches the UE_MAC, the integrity and confidentiality of the message are verified. If the values do not match, the process is aborted.

vi. Finally, the symmetric key and IV are used to decrypt the SUCI via the AES-256-CTR algorithm, obtaining SUPI.

vii. All traces of ciphertext and ECC ephemeral public key are immediately deleted, completing the process.

6.5 PQ-DTLS on N2

The N2 interface can now be configured with the added security layer of PQ-DTLS (DTLS1.3 with PQ support) to meet new security needs in the world of quantum computing. PQ-DTLS improves on the usual DTLS protocol by adding quantum-resistant cryptographic algorithms to encrypt datagrams. This improves the security of data that the AMF and the 5G 5G-AN exchange.

PQ-DTLS over the N2 interface creates trust between the AMF and the 5G-AN by offering certificate-based authentication. These certificates have signatures generated through ML-DSA. Shared key agreement is done using ML-KEM, this shared key is used to generate the symmetric encryption key for AES256-GCM, which encrypts the data in transit. This makes the entire communication guarded from unauthorized access.

PQ-DTLS is applied over the SCTP sockets since SCTP ensures the transport of signaling messages among AMF and 5G-AN nodes, hence PQ-DTLS is used on top of SCTP.

6.6 PQ-IPSec on N2

The N2 interface can also make use of the PQ-IPSec (IKEv2 with PQ support) network protocol suite [19] [20] to make data transmission between the AMF and the 5G-AN quantum secure. IKEv2 currently depends on classical cryptographic algorithms in order to generate certificates. IPSec with IKEv2 [21] will be integrated with Post-Quantum Algorithms for it to be called PQ-IPSec, which includes Post-Quantum Key exchange algorithm with Post-Quantum Digital Certificates.

Post Quantum Pre-shared key can be shared between AMF and 5G-AN at the start of the protocol for further securing the complete communication which makes the overall process safe against quantum threats. This way the control plane messages between AMF and 5G-AN are encrypted and authenticated.

6.7 PQ-IPsec on N3

Post-Quantum IPsec [19] [20] also protects the user plane data that is sent through the N3 interface between the 5G-AN and the UPF. PQ-IPSec uses post-quantum IKEv2 [21] with

upgraded support for Post-Quantum key exchange, Post-Quantum Certificate verification, and advanced encryption methods.

Post Quantum Pre-shared key can be shared between UPF and 5G-AN at the start of the protocol for further securing the complete communication which makes the overall process safe against quantum threats making sure that the user plane is secure against any type of attack whether classical or quantum attacks.

6.8 Risk Assessment and Prioritization

i. **Identifying Critical Systems**: First, identify key systems and interfaces in the 5G Core that rely on cryptographic operations, such as Authentication, Session Management, User Plane, and interfaces like N1, N2, and N3. These systems handle sensitive data and require immediate attention for PQC migration.

ii. **Vulnerability Assessment**: Assessing the security of existing cryptographic algorithms, such as RSA and ECC, is crucial in the face of emerging quantum threats. Quantum attacks, particularly Shor's Algorithm, pose a significant risk to these methods, with ECC being especially susceptible. As quantum computing advances, the effective security of ECC is greatly diminished, making it imperative to transition toward quantum-resistant alternatives.

iii. **Prioritization of Migration**: Critical systems involved in user authentication, key exchange, and secure communication (like the 5G-AKA procedure, SUPI concealment, and SBI communication) should be prioritized for migration. Additionally, systems storing encrypted data for extended periods must also be considered to prevent future decryption via HNDL attacks.

iv. **Impact on Performance and Compatibility**: Assess the performance and compatibility impacts of migrating to PQC, as some algorithms might introduce overhead. Hybrid cryptography can be used to bridge the gap between classical and quantum-resistant algorithms during the transition phase.

v. **Migration Roadmap**: A phased migration approach should be implemented, starting with the most critical systems. Hybrid solutions can ensure continued security, and continuous monitoring will help adapt to the rapid developments in quantum computing.

vi. **Compliance and Standardization**: Ensure adherence to NIST-approved PQC algorithms like ML-KEM, ML-DSA, and SLH-DSA. Compliance with regulatory standards and industry best practices will be essential for a smooth and secure transition to PQC.

7.0 Limitations and Future Scope

This report focuses on the incorporation of PQC within the 5G core network. The scope and limitations are outlined below:

i. **Types of Cryptographic Systems**: This technical report addresses the shift from conventional cryptographic methods, such as RSA, AES-128, and ECC, to quantum-resistant solutions within the 5G core network. The focus is on those cryptographic systems that are currently in use. Future versions may expand to cover additional cryptographic systems that are not currently employed in 5G networks.

ii. **Network Components Covered**: The report provides guidelines for implementing PQC in the 5G Core network functions. Currently, it does not address the application of PQC in other network components, such as the RAN, edge computing nodes, or IoT devices, which may be included in future updates.

iii. **PQC Algorithms**: The report outlines the implementation of specific PQC algorithms recommended by NIST, such as ML-KEM (FIPS 203) [14], ML-DSA (FIPS 204) [13], and SLH-DSA (FIPS 205) [23]. Future versions may incorporate additional algorithms once they become standardized and validated.

iv. **Hardware-Specific Guidance**: This version does not include detailed guidelines for hardware-specific implementations of PQC. Guidelines for specialized hardware requirements or optimizations may be included in future updates once the technology becomes more established and integrates with physical network components.

v. **Performance Benchmarks**: This report does not provide specific performance benchmarks for PQC implementations within 5G networks. As PQC algorithms mature and their effects on network performance become unambiguous future versions may include detailed benchmarking guidance.

vi. **Threat Scenarios**: The technical report caters to common and anticipated threat scenarios related to the adoption of PQC in 5G networks. However, it does not comprise all possible threat scenarios, particularly those involving highly sophisticated or emerging quantum attacks. Future versions may expand on this to provide security against a broader range of potential threats.

vii. **Deployment Scenarios**: This version focuses on PQC deployment within 5G networks under general operating conditions. While it covers common deployment environments, this technical report does not address scenarios involving extreme edge cases, hybrid cloud deployments, or highly customized network configurations. These aspects may be explored in more detail in future updates.

viii. **Interoperability**: The technical report prioritizes ensuring interoperability between PQC and existing cryptographic protocols within the 5G core. However, it does not

cover compatibility with legacy systems or non-3GPP networks. This issue may be explored in future versions as the technology evolves.

ix. **PQC Maturity**: Recognizing that PQC is an evolving field still in its budding stages, this technical report does not prescribe final, or immutable solutions. It aims to offer flexible and adaptable guidelines for implementation by reflecting on the current understanding and best practices, with the expectation that future versions may adjust as PQC technology and technical reports continue to evolve.

8.0 References

[1] 3GPP TS 33.501 version 18.6.0 Release 18: “5G; Security architecture and procedures for 5G System”

[2] 3GPP TS 35.205 version 18.0.0 Release 18: “Universal Mobile Telecommunications System (UMTS); LTE; 3G Security; Specification of the MILENAGE algorithm set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 1: General”

[3] 3GPP TS 35.206 version 18.0.0 Release 18: “Universal Mobile Telecommunications System (UMTS); LTE; 3G Security; Specification of the MILENAGE algorithm set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 2: Algorithm specification”

[4] Martin Thomson and Cory Benfield. 2022. HTTP/2. RFC 9113. (June 2022).

[5] Roy T. Fielding, Mark Nottingham, and Julian Reschke. 2022. HTTP Semantics. RFC 9110. (June 2022).

[6] 3GPP TS 33.310 version 19.01.0 Release 19: “Universal Mobile Telecommunications System (UMTS); LTE; Network Domain Security (NDS); Authentication Framework (AF)”

[7] Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture.

[8] Santorinaios, Dimitris. "Privacy evaluation of 5G networks." Master's thesis, 2022.

[9] 3GPP TS 23.003 version 18.6.0 Release 18: “Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; Numbering, addressing and identification”

[10] Michael Tüxen, Eric Rescorla, and Robin Seggelmann. 2011. Datagram Transport Layer Security (DTLS) for Stream Control Transmission Protocol (SCTP). RFC 6083. (Jan. 2011).

[11] 3GPP TS 33.210 version 18.01.0 Release 18: “Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; Network Domain Security (NDS); IP network layer security”

[12] A. Langley, M. Hamburg, and S. Turner. 2016. RFC 7748: Elliptic Curves for Security. RFC Editor, USA.

[13] Gaithersburg M D Nist. 2024. Module-Lattice-Based Digital Signature Technical report. Technical Report. Gaithersburg, MD.

[14] Gaithersburg M D Nist. 2024. Module-lattice-based key-encapsulation mechanism technical report. Technical Report. Gaithersburg, MD.

[15] Arkko, Jari, Vesa Lehtovirta, and Pasi Eronen. “Improved extensible authentication protocol method for 3rd generation authentication and key agreement (eap-aka')”. No. rfc5448. 2009.

[16] Douglas Stebila, Scott Fluhrer, and Shay Gueron. 2024. Hybrid key exchange in TLS 1.3. Internet-Draft draft-ietf-tls-hybrid-design-10. Internet Engineering Task Force.

[17] Kris Kwiatkowski, Panos Kampanakis, Bas Westerbaan, and Douglas Stebila. 2024. Post-quantum hybrid ECDHE-MLKEM Key Agreement for TLSv1.3. Internet-Draft draft-kwiatkowski-tls-ecdhe-mlkem-01. Internet Engineering Task Force.

[18] Thomas Vincent Wiggers. Post-Quantum TLS. Jan 2024.

[19] S. Fluhrer, P. Kampanakis, D. McGrew, and V. Smyslov. 2020. Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security. RFC 8784. RFC Editor.

[20] Panos Kampanakis and Gerardo Ravago. 2024. Post-quantum Hybrid Key Exchange with ML-KEM in the Internet Key Exchange Protocol Version 2 (IKEv2). Internet-Draft draft-kampanakis-ml-kem-ikev2-06. Internet Engineering Task Force.

[21] Valery Smyslov. 2022. Intermediate Exchange in the Internet Key Exchange Protocol Version 2 (IKEv2). RFC 9242. (May 2022).

[22] Stephan Müller. CRYSTALS Kyber Integration into TLS. Jul 2023.

[23] Nist, G. M. D. (2024). Stateless hash-based digital signature technical report.

[24] Damir, Mohamed Taoufiq, et al. "A beyond-5G authentication and key agreement protocol." International Conference on Network and System Security. Cham: Springer Nature Switzerland, 2022.

[25] Niederhagen, Ruben, and Michael Waidner. "Practical post-quantum cryptography." Fraunhofer SIT (2017).

[26] T. Charles Clancy, Robert W. McGwier, and Lidong Chen. 2019. Post-quantum cryptography and 5G security: tutorial. In Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '19). Association for Computing Machinery, New York, NY, USA, 285.

[27] Stephan Müller. Hybrid KEM Specification. April 2024

[28] Bonnetain, Xavier, María Naya-Plasencia, and André Schrottenloher. "Quantum security analysis of AES." IACR Transactions on Symmetric Cryptology 2019.2 (2019): 55-93.

[29] Vuppala, R. C., Kumar, D., Je, D., Sharma, N., Nigam, A., & Kim, D. (2023, December 4). Post-quantum secure hybrid methods for UE primary authentication in 6G with forward

secrecy. GLOBECOM 2023 - 2023 IEEE Global Communications Conference, 2590–2595. Presented at the GLOBECOM 2023 - 2023 IEEE Global Communications Conference, Kuala Lumpur, Malaysia.

[30] Giron, Alexandre Augusto. "Migrating Applications to Post-Quantum Cryptography: Beyond Algorithm Replacement." Cryptology ePrint Archive (2023).

[31] Liu, Yi-Kai, and Dustin Moody. "Post-quantum cryptography and the quantum future of cybersecurity." Physical review applied 21.4 (2024): 040501.

[32] ETSI TR 103 823 version 1.1.1: “CYBER; Quantum-Safe Public-Key Encryption and Key Encapsulation”

[33] Bassham, L. E., III, et al. “A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications”. National Institute of Technical reports and Technology, 2010.

[34] Barker, Elaine, Quynh Dang, Sheila Frankel, Karen Scarfone, and Paul Wouters. “Guide to IPsec VPNs”. Gaithersburg, MD: National Institute of Technical reports and Technology, June 2020.

[35] Magma India: “ECIES in 5G Core: SUPI to SUCI Conversion”. Nov 2022.

[36] Dick Hardt. 2012. The OAuth 2.0 Authorization Framework. RFC 6749. (Oct. 2012).

[37] National Institute of Technical reports and Technology (US). (2023). Digital Signature Technical report (DSS).

[38] Bas Westerbaan and Douglas Stebila. 2023. X25519Kyber768Draft00 hybrid post-quantum key agreement. Internet-Draft draft-tls-westerbaan-xyber768d00-03. Internet Engineering Task Force.

[39] Russ Housley. 2020. TLS 1.3 Extension for Certificate-Based Authentication with an External Pre-Shared Key. RFC 8773. (March 2020).

[40] Magma India: “AKA Procedure”. Nov 2022.

[41] Alnahawi, Nouri, et al. "A Comprehensive Survey on Post-Quantum TLS." IACR Communications in Cryptology 1.2 (2024).

[42] Mannalatha, Vaisakh, Sandeep Mishra, and Anirban Pathak. "A comprehensive review of quantum random number generators: Concepts, classification and the origin of randomness." Quantum Information Processing 22.12 (2023): 439.

[43] Herrero-Collantes, Miguel, and Juan Carlos Garcia-Escartin. "Quantum random number generators." Reviews of Modern Physics 89.1 (2017): 015004.

[44] 3GPP TS 33.105 V18.0.0, Release 18: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Cryptographic Algorithm Requirements".

[45] Tobias Funke and David Rupprecht. “Invalid Curve Attack on the 5G SUCI Privacy Feature”. GSMA: Radix Security (2023).

[46] Hallgren, S., & Vollmer, U. (2009). Quantum computing. In Post-Quantum Cryptography (pp. 15–34).

[47] Yang, J., & Johansson, T. (2020). An overview of cryptographic primitives for possible use in 5G and beyond. Science China Information Sciences, 63(12).

[48] National Institute of Technical reports and Technology (US). (2023). “Advanced Encryption Technical report (AES)”.

[49] Rescorla, E. (2018). “The Transport Layer Security (TLS) Protocol Version 1.3. RFC Editor”.

[50] Lee, Kyungroul, et al. "TRNG (True Random Number Generator) method using visible spectrum for secure communication on 5G network." IEEE access 6 (2018): 12838-12847.

[51] 3GPP TS 35.245 V18.0.0 (2024-03): Specification of the AES based 256-bits algorithm set: Specification of the 256-NEA5 encryption, the 256-NIA5 integrity, and the 256-NCA5 authenticated encryption algorithm for 5G; Document 3: design conformance test data (Release 18)

[52] 3GPP TS 35.242 V18.0.0 (2024-03): Specification of the Snow 5G based 256 bits algorithm set: Specification of the 256-NEA4 encryption, the 256-NIA4 integrity, and the 256-NCA4 authenticated encryption algorithm for 5G; Document 3: design conformance test data (Release 18)

[53] 3GPP TS 35.248 V18.0.0 (2024-03): Specification of the ZUC based 256-bits algorithm set: Specification of the 256-NEA6 encryption, the 256-NIA6 integrity, and the 256-NCA6 authenticated encryption algorithm for 5G; Document 3: design conformance test data (Release 18)

[54] 3GPP TR 33.841 V16.1.0 (2019-03): Study on the support of 256-bit algorithms for 5G (Release 16)

[55] 3GPP TS 35.237 V0.1.0 (2024-02): Specification of the MILENAGE-256 algorithm set; An example set of 256-bit 3GPP Authentication and Key Generation functions f1, f1*, f2, f3, f4, f5, f5* and f5**; Document 4: Summary and Results of Design and Evaluation (Release 19)

[56] 3GPP TR 33.700-41 V19.0.0 (2024-09): Study on enabling a cryptographic algorithm transition to 256 bits (Release 19)

[57] ANSSI views on the Post-Quantum Cryptography transition (2023 follow up)

[58] GSMA Quantum Networking and Service Version 1.0

[59] NIST's New Quantum Method Generates Really Random Numbers

[60] A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications

[61] Michael Tüxen, Randall R. Stewart, Randell Jesup, & Salvatore Loreto. (2017). Datagram Transport Layer Security (DTLS) Encapsulation of SCTP Packets.

9.0 Abbreviations

Abbreviation	Expansion
3GPP	3rd Generation Partnership Project
5G	Fifth Generation
5QI	5G Quality of Service Identifier
AES	Advanced Encryption Standard
AF	Application Function
AKA	Authentication and Key Agreement
AMF	Access and Mobility Management Function
ANSI	American National Standards Institute
API	Application Programming Interface
ARPF	Authentication Credential Repository and Processing Function
AUSF	Authentication Server Function
AUTN	Authentication Token
AV	Authentication Vectors
CK	Ciphering Key
CMAC	Cipher-based Message Authentication Code
CN	Core Network
CP	Control Plane
CRQC	Cryptographically Relevant Quantum Computer
CTR	Counter Mode
DL	Downlink
DN	Data Network
DRBG	Deterministic Random Bit Generator
DSS	Digital Signature Standard
DTLS	Datagram Transport Layer Security

EAP-AKA’	Extensible Authentication Protocol Authentication and Key Agreement
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
ECDLP	Elliptic Curve Discrete Logarithm Problem
ECDSA	Elliptic Curve Digital Signature Algorithm
ECIES	Elliptic Curve Integrated Encryption Scheme
EdDSAs	Edwards Curve Digital Signature Algorithm
ESP	Encapsulating Security Payload
FIPS	Federal Information Processing Standards
GCM	Galois Counter Mode
HE	Home Environment
HMAC-SHA	Hash-Based Message Authentication Code - Secure Hash Algorithm
HN	Home Network
HNDL	Harvest Now, Decrypt Later
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
IK	Integrity Key
IKEv2	Internet Key Exchange version 2
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IPSec	Internet Protocol Security
IV	Initialization Vector
JSON	JavaScript Object Notation
JWT	JSON Web Token
KDF	Key Derivation Function

KEM	Key Encapsulation Mechanisms
KEX	Key Exchange
LBC	Lattice Based Cryptography
LT	Long Term
LWE	Learning with Errors
MAC	Message Authentication Code
MCC	Mobile Country Code
ML-DSA	Module-Lattice-Based Digital Signature Algorithm
ML-KEM	Module-Lattice-Based Key-Encapsulation Mechanism
MLWE	Module Learning with Errors
MNC	Mobile Network Code
MSIN	Mobile Subscriber Identification Number
mTLS	Mutual Transport Layer Security
N3IWF	Non-3GPP Interworking Function
NAS	Non-Access Stratum
NEA	New Radio Encryption Algorithm
NEF	Network Exposure Function
NF	Network Function
NGN	Next Generation Network
NIA	New Radio Integrity Algorithm
NIST	National Institute of Standards and Technology
NR	New Radio
NRF	Network Repository Function
NSSF	Network Slice Selection Function
OAuth	Open Authentication
OTA	Over-The-Air

PCF	Policy Control Function
PDU	Protocol Data Unit
PKE	Public Key Encryption
PKI	Public Key Infrastructure
PQ-DTLS	Post-Quantum Datagram Transport Layer Security
PQ-IPSec	Post-Quantum Internet Protocol Security
PQ-mTLS	Post-Quantum Mutual Transport Layer Security
PQ-TLS	Post-Quantum Transport Layer Security
PQC	Post-Quantum Cryptography
PQ-IES	Post Quantum Integrated Encryption Scheme
PRNG	Pseudo Random Number Generator
QFI	QoS Flow ID
QoS	Quality of Service
QRNG	Quantum Random Number Generators
RAN	Radio Access Network
RAND	Random Number
RAND	Random Challenge
RAT	Radio Access Technology
RSA	Rivest–Shamir–Adleman
S-NSSAI	Single Network Slice Selection Assistance Information
SBA	Service Based Architecture
SBI	Service Based Interfaces
SCP	Service Communication Proxy
SCTP	Stream Control Transmission Protocol
SD	Service Differentiator
SEAF	Security Anchor Function

SEG	Security Gateway
SIDF	Subscription Identifier De-concealing Function
SIM	Subscriber Identity Module
SMF	Session Management Function
SNN	Service Network Name
SST	Slice/Service Type
SUCI	Subscription Concealed Identifier
SUPI	Subscription Permanent Identifier
TLS	Transport Layer Security
TRNG	True Random Number Generator
UDM	Unified Data Management
UDP	User Datagram Protocol
UDR	Unified Data Repository
UE	User Equipment
UL	Uplink
UP	User Plane
UPF	User Plane Function
USIM	Universal Subscriber Identity Module
XRES	Expected Response