Preparing 5G for the Quantum Era: An Analysis of 3GPP Architecture and the Transition to Quantum-Resistant Cryptography

ABSTRACT

This report focuses on the integration of Quantum-Safe Cryptography (QSC) within the 3GPP 5G network standards, which are characterized by their high data rates, low latency, and extensive connectivity. The report evaluates how 5G, as it expands, must adapt its cryptographic standards to combat the emerging quantum threats by transitioning to QSC based algorithms that are secure against both classical and quantum computing attacks. This transition is critical to maintaining the security foundations of telecom networks in the face of quantum computing advancements.

This report's main objective is to provide a practical, phased risk approach from technological and security perspectives regarding the implementation of quantum-resistant cryptography in 5G networks. It assesses the standardization of current cryptographic methods against quantum threats and explores quantum-resistant solutions suitable for integration into the 5G infrastructure. From a security standpoint, the report identifies potential quantum vulnerabilities across various network layers and domains and evaluates the robustness of proposed quantum-resistant technologies against these risks. Furthermore, the report outlines the phased transitional changes and prioritizes updates for forthcoming 3GPP releases. This comprehensive analysis aims to ensure that 5G networks remain secure and resilient, safeguarding against both current and future cyber threats in the quantum computing era.

FOREWORD

As a leading technology and solutions development organization, the Alliance for Telecommunications Industry Solutions (ATIS) brings together the top global ICT companies to advance the industry's most pressing business priorities. ATIS' nearly 200 member companies are currently working to address the All- Internet Protocol (IP) transition, 5G, network functions virtualization, big data analytics, cloud services, device solutions, emergency services, M2M, cyber security, network evolution, quality of service, billing support, operations, and much more. These priorities follow a fast-track development lifecycle — from design and innovation through standards, specifications, requirements, business use cases, software toolkits, open-source solutions, and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). The organization is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of the oneM2M global initiative, a member of and major U.S. contributor to the International Telecommunication Union (ITU), as well as a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit www.atis.org.

TABLE OF CONTENTS

1. INTRODUCTION

The advent of Cryptographic Relevant Quantum Computers (CRQCs) marks a pivotal shift in the computational landscape, with profound implications for current cryptography practices, particularly within telecommunications infrastructure. Traditional cryptographic systems, which form the backbone of security in telecom networks, rely on the computational difficulty of certain mathematical problems, such as factoring large prime numbers or computing discrete logarithms. These systems ensure confidentiality, integrity, and authentication of communications. However, CRQCs promise to possess the capability to solve these problems efficiently, thereby rendering many of the existing cryptographic protocols vulnerable to breaches. This potential breakthrough in quantum computing threatens to compromise encrypted communications, expose private data, and undermine the security foundations of current telecom networks.

As the deployment of 5G technology accelerates, integrating robust Quantum-Safe Cryptography (QSC) becomes imperative to safeguard the next generation of telecommunications from emerging quantum threats. 5G networks, known for their high data rates, low latency, and massive connectivity, incorporate advanced cryptographic standards to secure vast amounts of data transferred across increasingly complex networks. The introduction of CRQCs necessitates a reassessment of these cryptographic standards. 5G must adapt by transitioning to QSC, which is designed to be secure against both conventional and quantum computing attacks. This transition involves replacing vulnerable encryption and key agreement mechanisms with algorithms based on hard mathematical problems that are believed to be resistant to quantum attacks, such as lattice-based, hash-based, and multivariate cryptographic techniques. This shift not only aims to protect data but also ensures the integrity and reliability of communications across 5G networks, maintaining trust and compliance with emerging security standards in a post-quantum world.

The primary aim of this report is to evaluate the integration of Quantum-Resistant Cryptography (QRC) within various segments of 5G networks, particularly in the face of potential quantum attacks and vulnerabilities that current cryptographic methods might soon fail to counteract. As quantum computing progresses, it presents a clear danger to the encryption standards that underpin the security of 5G infrastructure. This analysis will delve into the specific quantum threats that could compromise each aspect of 3GPP 5G networks and assess how QSC can mitigate these risks.

This report's scope is to provide a comprehensive impact analysis from technological and security perspectives for implementing QSC in 5G networks. The report will evaluate the technological readiness of current cryptographic methods to withstand quantum computing advancements and identify the QSC solutions that could be integrated into 5G infrastructure. From a security standpoint, the report aims to pinpoint potential quantum threats and vulnerabilities that could affect various layers of the network. This includes assessing the robustness of proposed quantum-resistant technologies against these emerging risks and implications of deploying these advanced cryptographic solutions, considering the investment needed for implementation and the potential impact on operational deployment. This analysis will help define the key facets of transitioning to QRC in the 5G context.

This report's impact analysis outlines a strategic roadmap of transitional changes and priorities that should focus on upcoming 3GPP releases, guiding network operators, policymakers, and technology providers on critical areas requiring updates to bolster defenses against these emerging quantum challenges. Through this comprehensive approach, we aim to ensure that 5G networks remain robust and secure, safeguarding against both current cyber threats and those anticipated in the quantum computing era.

2. 5G INFRASTRUCTURE SECURITY THREAT FROM CRQC

To effectively prepare 5G networks for the advent of quantum computing, it is crucial to understand the types of quantum attacks (in other words, threat landscape) and assess their relevance across various domains of the network. Below is an overview of potential quantum attack types. The three types of quantum attacks outlined here all focus on decrypting data but differ in approach.

2.1 Types of CRQC Attacks

Harvest-Now, Decrypt-Later (HNDL): Attackers capture encrypted data transmitted today with the intention of decrypting it once a CRQC is available. This is a significant threat for data that needs to remain confidential over a long period.

> An example of a HNDL attack on 5G infrastructure could involve attackers strategically intercepting encrypted communications between users and cell towers or between different network nodes. Imagine a scenario where sensitive communications, such as government or corporate secrets, are transmitted over a 5G network. These communications are encrypted with current standards such as Advanced Encryption Standard (AES)-128 or using Elliptic Curve Integrated Encryption Schemes (ECIES) for subscriber identifier privacy, which are deemed secure against classical computing attacks. Nevertheless, attackers capture and store these communications. The attackers do not attempt to decrypt this information immediately. Instead, they bide their time until the advent of sufficiently powerful quantum computers capable of breaking these encryption methods using algorithms like Shor's quantum factoring algorithm for public key cryptosystems or Grover's search algorithm for symmetric keys. This delay in decryption allows the attackers to circumvent current security measures, making HNDL a particularly insidious threat to long-term data confidentiality in emerging 5G networks. A few years ago, it was widely believed that Grover's algorithm would necessitate doubling symmetric key sizes, meaning AES-256 would be needed instead of AES-128 to achieve equivalent security strength against a quantum adversary. But according to the National Institute of Standards and Technology (NIST) [1], Grover's algorithm does not pose any apparent threat to AES-128 symmetric cryptography.

> Based on NIST's current assessments, AES-128 is likely to remain secure for the foreseeable future, despite the theoretical implications of Grover's algorithm. However, the efficacy of AES-128 is significantly influenced by the quality of entropy used in the key generation process. Poor entropy quality can render AES-128 vulnerable to classical attacks, much less quantum threats, as detailed in the ATIS study "Implications of Entropy on Symmetric Key Encryption Resilience to Quantum" [2]. Therefore, it is crucial to ensure high-quality entropy in key generation to maximize the security of AES-128.

> Furthermore, the nature of HNDL attacks means that the captured encrypted information might remain relevant and sensitive for many decades into the future. Given that AES-128 is deemed secure based on current quantum computing projections, there arises a pertinent question: How long will AES-128 continue to provide secure protection against the evolving capabilities of quantum computing? This concern underscores the importance of not only securing encryption with high entropy but also continuously evaluating the longevity of its effectiveness as quantum technologies advance. Thus, although NIST's current stance reassures the short-term security of AES-128, organizations should also consider strategies for longer-term security assurances, potentially including early transitions to more robust algorithms like AES-256 or other quantum-safe cryptographic solutions. This proactive approach will help safeguard sensitive communications against both present and future threats in the evolving cybersecurity landscape.

Quantum Decryption: In a quantum decryption attack, the decryption by a CRQC is achievable but may take time (i.e., not be instantaneous) while the attacker intercepts encrypted communications. Once the quantum computer successfully decrypts the data, the attacker gains access to sensitive information, all without the knowledge of the communicating parties.

> An example of a passive Quantum Decryption attack on 5G infrastructure could involve the use of Shor's algorithm by attackers to target the public key cryptosystems used within the network. Imagine a scenario where a 5G network employs RSA or ECC for securing communication channels between mobile devices and network nodes. An attacker, equipped with a quantum computer capable of running Shor's algorithm, intercepts encrypted messages exchanged during these communications. Then the attacker could rapidly break the public key system used to exchange keys, thus obtaining the keys used for encryption.

> Once in possession of these encryption keys, the attacker can decrypt all past, present, and future communications encrypted with the corresponding public keys. This could lead to massive data breaches, including the exposure of sensitive personal data, confidential business information, or critical national security data transmitted over the network

Quantum-Impersonation Attack: In a quantum impersonation attack, an adversary uses quantum computational capabilities to exploit vulnerabilities in public key cryptographic systems to impersonate another user or entity. This kind of attack is particularly concerning in environments where public key infrastructure (PKI) is used for encryption and digital signatures. The attacker can use the signature keys to impersonate the original key holders. This allows for unauthorized actions such as signing documents, sending deceptive communications, or conducting transactions that appear to be from legitimate users. This type of attack not only allows for decrypting communications but also for perpetuating frauds and forgeries under the guise of legitimate entities.

> An example of how a quantum impersonation attack could be executed within a 5G infrastructure component that utilizes Public Key Infrastructure (PKI), such as during the authentication process between different network operators in an interconnect scenario. Interconnect authentication often occurs when operators in different geographic regions or separate administrative domains need to authenticate each other to establish a secure communication channel. This process typically uses PKI to ensure each party is communicating with a legitimate counterpart, typically involving digital certificates for identity verification. If compromised by a quantum threat actor performing a Quantum Impersonation attack, specific operational and configuration data accessible via this interface can provide a threat actor with numerous opportunities for exploitation. Examples include information about the network's layout and structure, including locations of key network nodes (such as gNBs, UPFs, and AMFs), routing paths, and interconnection points. A threat actor could use this information to plan targeted attacks, such as denial of service (DoS) attacks on critical nodes or to bypass security measures by understanding the data flow paths.

Quantum Man-in-the-Middle (QMITM)*:* Similar to a classical MITM attack, a QMITM attacker intercepts communications between two parties and, using a Cryptographically Relevant Quantum Computer (CRQC), can tamper with or alter messages. This attack involves real-time decryption and re-encryption of the intercepted message, allowing the attacker to modify data instantly and undetectably, thereby directly undermining the integrity and authenticity of the communication.

> In a QMITM scenario, a quantum-enabled attacker intercepts an encrypted message. By using advanced quantum computing techniques like Shor's algorithm, the attacker can factorize key primitives or compute discrete logarithms to derive the original signature key data without alerting either the user or the server. The attacker can then modify the message content and re-encrypt and forward the message to the recipient undetected. For example, in a financial transaction over a 5G network, the attacker could alter the amount or destination account of a transfer. Each party believes it is securely connected to the other, so the tampering goes unnoticed. This capability to stealthily intercept and manipulate secure communications marks a significant escalation in the threat landscape posed by quantum computing technologies. In contrast, a quantum decryption attack focuses mainly on compromising data confidentiality, allowing unauthorized access to encrypted information without altering the content in transit.

Side-Channel Attacks: Although not specifically an attack by a CRQC, another significant threat to cryptography is the side-channel attack, which poses risks not only to classical cryptographic algorithms but also to Post-Quantum Cryptography (PQC) algorithms. A side-channel attack exploits indirect information, such as timing, power consumption, or electromagnetic emissions and parameter drifts. This observation can be utilized to predict and gain access to the secret keys being used by the device and without directly breaking the encryption itself. PQC protocols are still relatively untested in real-world scenarios, so they may be more susceptible to side-channel attacks.

> A potential example of a side-channel attack on 5G could focus on devices like smartphones or Internet of Things (IoT) devices that connect to the network. These devices, often equipped with cryptographic measures to secure data transmission, also exhibit various physical and operational characteristics that could emit exploitable information. A side-channel attack could also involve quantum algorithms that are particularly efficient at analyzing the minuscule yet detectable fluctuations in power consumption or electromagnetic emissions from these devices as they perform cryptographic operations.

3. OVERVIEW OF IMPACTS TO CURRENT CRYPTOGRAPHY AND QSC

QSC encompasses cryptographic methods including asymmetric and symmetric keying mechanisms, designed to secure data against both classical and future quantum computers-based threats. Today's quantum computers do not yet possess the capability to break current cryptographic algorithms, but advancements in quantum technology suggest that they will eventually be powerful enough to do so. This prospect is particularly anchored in the capabilities of quantum algorithms like Shor's quantum factoring algorithm, which can theoretically factorize large integers, an essential component of many traditional cryptographic systems. This potential has propelled significant research into PQC.

Presently, it is believed that symmetric cryptographic algorithms and hash functions are more resistant to quantum attacks. In contrast, asymmetric cryptographic systems are seen as particularly susceptible. This disparity has shaped the focus of cryptographic research, emphasizing the development and implementation of quantum-resistant methods to secure communications against the unprecedented power of quantum computing.

Symmetric and asymmetric cryptography are two fundamental types of classical cryptographic systems used to secure data, but they function quite differently.

> **Symmetric cryptography**, also known as secret key cryptography, has a key that both the sender and receiver use to encrypt and decrypt messages. This method is highly efficient for confidentiality protection purposes, making it ideal for encrypting large volumes of data. Symmetric key cryptography can also help provide integrity protection and authenticity to messages. However, the key distribution process — ensuring that both parties securely receive the key without interception — presents a significant challenge.
>
> The primary quantum threat to symmetric cryptography comes from Grover's search algorithm, which can theoretically reduce the effective security of symmetric encryption keys by the square root of the number of operations required to brute-force guess them. This means that a symmetric key such as AES-256 that would normally take 2 to the power 256 operations to crack could potentially be compromised with only 2 to the power 128 operations using a quantum computer [3]. To counter this threat, one straightforward solution is to increase the key length.
>
> Doubling the key length in symmetric systems can counteract the square root reduction in brute-force complexity brought about by Grover's search algorithm. Although Grover's algorithm theoretically enhances the capability of quantum computers to perform brute-force attacks on symmetric keys with a quadratic reduction in time, practical applications and existing technological limits significantly temper its immediate threat. NIST recognizes that algorithms such as AES-128 are currently considered secure against quantum threats for the foreseeable future. Likewise, industry believes that SNOW 3G (using 128 bit) could also be safe. However, the evolving capabilities of quantum computing indicate that transitioning to larger key sizes provides stronger encryption methods, such as AES-256, which should be part of future planning to enhance resilience against potential quantum attacks. This proactive approach aims to ensure continued security against increasingly sophisticated attacks, safeguarding sensitive data across various domains. By planning for such a migration, organizations can stay ahead of potential security challenges, maintaining the confidentiality and integrity of their communications as quantum computing technology matures.
>
> **Asymmetric cryptography**, or public key cryptography, uses a pair of keys: a public key, which can be shared openly, and a private key, which remains confidential to the owner. This system facilitates not only encryption and decryption but also digital signatures and key distribution (achieving authentication, integrity, and non-repudiation) without the need for a pre-shared secret. Although asymmetric methods offer greater flexibility and security in environments where secure key distribution is impractical, they are generally more computationally intensive than symmetric techniques, making them less suitable for encrypting large datasets. Their dependency on complex mathematical problems also makes asymmetric cryptography more vulnerable to potential quantum computing breakthroughs, such as those enabled by Shor's quantum factoring algorithm.
>
> Asymmetric key cryptography faces significant vulnerabilities from quantum computing, particularly due to Shor's quantum factoring algorithm, which can efficiently factor large integers and compute discrete logarithms — the mathematical foundations of widely used asymmetric encryption methods like RSA and ECC. This means that quantum computers could, in theory, decrypt data encrypted with these systems and compromise digital signatures made by them, posing a profound security risk.
>
> To secure asymmetric cryptography against quantum threats, researchers are developing and proposing new quantum-resistant algorithms, often referred to as PQC. These new cryptographic algorithms do not rely on the factorization of large integers or the computation of discrete logarithms and are instead based on problems believed to be resistant to both classical and quantum computing attacks.

3.1 Post-Quantum Cryptography (PQC)

PQC ia an area of cryptography that researches and advances the use of quantum-resistant primitives, with the goal of keeping existing PKI intact in a future era of quantum computing. It is intended to be secure against both quantum and classical computers and deployable without drastic changes to existing communication protocols and networks. With the progression of quantum technology, the implementation of these quantum-resistant solutions becomes increasingly urgent to secure the long-term integrity of data and communications.

These algorithms are built on mathematical problems believed to be insurmountable even for quantum algorithms like Shor's. The primary classes of quantum-resistant algorithms include:

- Lattice-based
- Code-based
- Hash-based
- Multivariate polynomial

Recognizing the need for standardized solutions, NIST has been at the forefront of evaluating and endorsing PQC algorithms. As of August 2024, NIST has published new Federal Information Processing Standards (FIPS) that officially endorses a suite of PQC algorithms. These standards, which were anticipated in previous announcements and are detailed further on NIST's official page [4], include:

- **ML-KEM (Module-Lattice-Based Key-Encapsulation Mechanism) NIST FIPS 203 Standard [5]**: Designated for key encapsulation. ML-KEM (based on CRYSTALS-Kyber) was selected for its compact key sizes and rapid operational capabilities, making it ideal for secure communication across public networks.
- **ML-DSA (Module-Lattice-Based Digital Signature Algorithm) NIST FIPS 204 Standard [6]**: Designated for digital signatures, which are vital for verifying identities in digital transactions, remotely signing documents and verifying the source of software provisioning. ML-DSA (based on CRYSTALS-Dilithium) is recommended as the primary algorithm for digital signatures due to its efficiency and reliability.
- **SLH-DSA (Stateless Hash-Based Digital Signature Algorithm) FIPS 205 NIST Standard [7]**: SLH-DSA based on Stateless Practical Hash-based Incredibly Nice Cryptographic Signature (SPHINCS+), which, despite having larger signature sizes, provides a distinctive mathematical structure that offers robust alternatives within the cryptographic landscape for digital signatures.

Table 1 and the paragraph that follows present the latest NIST-approved PQC algorithms, the mathematical problems they are based on, an overview of their performance, and key and signature sizes.

PQC Algorithm	Mathematical Basis	Cryptographic Application Use	Cryptographic Characteristics i.e., Key Size, Signature Size
ML-KEM NIST FIPS 203 Standard [5]:	ML-KEM is derived from the round-3 version of the CRYSTALS-KYBER KEM. The security relies on the computational difficulty of the Module Learning with Errors (LWE) problem	Key Encapsulation which includes Key Gen, Key Enc, and Key Dec	Key Sizes ML-KEM: Typically features larger key sizes compared to classical algorithms. These key sizes are defined by the parameter sets. Three parameter sets have been defined by NIST: 1. ML-KEM Level 1 (Security Category 1): ML-KEM-512 with Ciphertext of 768 bytes. The RBG security level shall be of at least 128 bits. 2. ML-KEM Level 2 (Security Category 3): ML-KEM-768 with Ciphertext of 1088 bytes. The RBG security level shall be at least 192 bits. It is worth mentioning that NIST recommends using this ML-KEM security level as the default parameter set because it provides a large security margin at reasonable performance cost in case it is practical to use. 3. ML-KEM Level 3 (Security Category 5): ML-KEM-1024 with Ciphertext of 1568 bytes. The Random Bit Generator (RBG) security level shall be at least 256 bits.

ML-DSA NIST FIPS 204 Standard [6]:	Module-Lattice-based LWE. ML-DSA is derived from v3.1 of Crystal Dilithium. The scheme security relies on LWE and Short Integer Solution (SIS)	Digital Signature	Key and Signature sizes ML-DSA: Generally, features larger public and private key sizes compared to classical digital signature algorithms. It uses an Approved RBG to generate a 256-bit random seed which is expanded using an eXtendable-Output Function (XOF) which is a byte variant of (Secure Hash Algorithm and KECCAK) SHAKE-256 The following sizes are parameterized to provide different levels of security: 1. ML-DSA-44 (Category 2): uses a private key of 2560 Bytes, and a public key of 1312 byte sizes, while the signature size is 2420 bytes. 2. ML-DSA-65 (Category 3): uses a private key of 4032 Bytes, and a public key of 1952 bytes, while the signature size is 3309 bytes. 3. ML-DSA-87 (Category 5): uses a private key of 4896 Bytes, and a public key of 2592 bytes, while the signature size is 4627 bytes. According to the above, these can be considered relatively medium key sizes.
SLH-DSA FIPS 205 NIST Standard [7]:	SLH-DSA based on SPHINCS+ (Version 1.3)	Digital Signature	Key Size and Signatures: SLH-DSA: Tends to have larger key sizes compared to classical algorithms. SLH-DSA was designed to sign up to 2^{64} messages (as the rest of all the signature schemes in the NIST PQC process) and offers three security levels to enhance the robustness of the scheme and depending on key size the signature could have varying lengths: 1. Level 1: comparable to AES-128 o Public Key: 32 bytes o Signature: 7,856 to 17,088 bytes 2. Level 3: Comparable to AES-192 o Public Key: 48 bytes o Signature: 16,224 to 35,664 bytes 3. Level 5: Comparable to AES-256 o Public Key: 64 bytes o Signature: 29,792 to 49,856 bytes

Table 1: Cryptographic Algorithms Characteristics

PQC Performance Characteristics:

- **Key Encapsulation, Signature Generation and Verification Speed:** A typical characteristic of new PQC algorithms like ML-DSA, this may exhibit slower signature generation and verification speeds compared to classical algorithms such as ECDSA and RSA. A significant factor contributing to perceived delays is the increased amount of data transmitted over the network, especially as certificate chains that incorporate hybrid (RSA, ECC and PQC) to keys to support interoperability processes can become substantially larger with PQC implementations. Although PQC offers robust security against quantum attacks, it is less efficient in terms of computational and bandwidth requirements compared to classical algorithms. The need to manage larger key sizes and signature outputs means that more data must be processed and transmitted. This can notably affect performance in environments where bandwidth is a critical constraint or is limited.
- **Computational Overhead:** PQC algorithms demand increased computational resources due to the complexity of its underlying cryptographic operations. These algorithms will increase computational processing needs and increase storage capabilities to manage the larger keys and signatures effectively. This can pose challenges, particularly in

embedded systems or mobile devices where computational resources and power availability are constrained. Despite this, it is noteworthy that private keys in some PQC systems can often be compactly stored as small seeds, which may offer some storage advantages. However, the overall memory requirements for PQC may still differ significantly from those for ECC, and the infrastructure and resource demands for implementing PQC may be higher.

In summary, SLH-DSA provides very small public key sizes but has larger signature sizes and slower performance compared to ML-DSA. Additionally, the confidence in the classical and quantum security of the hash functions SHA2 and SHAKE extends to SLH-DSA. Although less efficient than ML-DSA, SLH-DSA may be a preferable choice for hardware applications that are difficult to access and update, where the performance trade-off is justified by the increased confidence in long-term security.

4. IMPACT ANALYSIS ON 3GPP 5G INFRASTRUCTURE ARCHITECTURE

The impact analysis on 3GPP 5G infrastructure architecture will focus on the scope of the 3GPP standards within the 5G infrastructure. This analysis delves into the vulnerabilities that emerging quantum technologies might exploit and evaluates potential mitigating solutions that could be implemented to mitigate the threat. Furthermore, this report outlines the challenges that these solutions might present, such as compatibility with existing technologies, implementation costs, and operational or performance impacts. By assessing these factors, the report aims to provide a risk assessment, helping to prioritize areas within the 3GPP standards roadmap that require urgent attention to enhance resilience against quantum threats.

The scope of the impact analysis is specific to the following 3GPP 5G specifications:

Technical Specification (TS) 33.501 - Security Architecture and Procedures for 5G System: [8]

> This standard continues to be the foundational document outlining the security architecture for the 5G system, detailing mechanisms for authentication, security context management, encryption, and integrity protection.

TS 33.310- Network Domain Security (NDS); Authentication Framework (AF) [9]

> Outlines the standards and protocols for security and authentication within network domains, focusing on ensuring robust security measures and reliable identity verification mechanisms across telecommunications networks.

TS 33.210 - NDS; IP Network Layer Security [10]

> Specifies the security architecture for network domain IP-based control planes, which covers the control plane security and on selected interfaces between network elements of NDS/IP networks.

Note: Lawful intercept has not been included as part of this study.

We will focus on the specific 3GPP 5G interfaces defined in TS 23.501, examining how they are structured and interact within the overall network architecture, indicated in Figure 1.

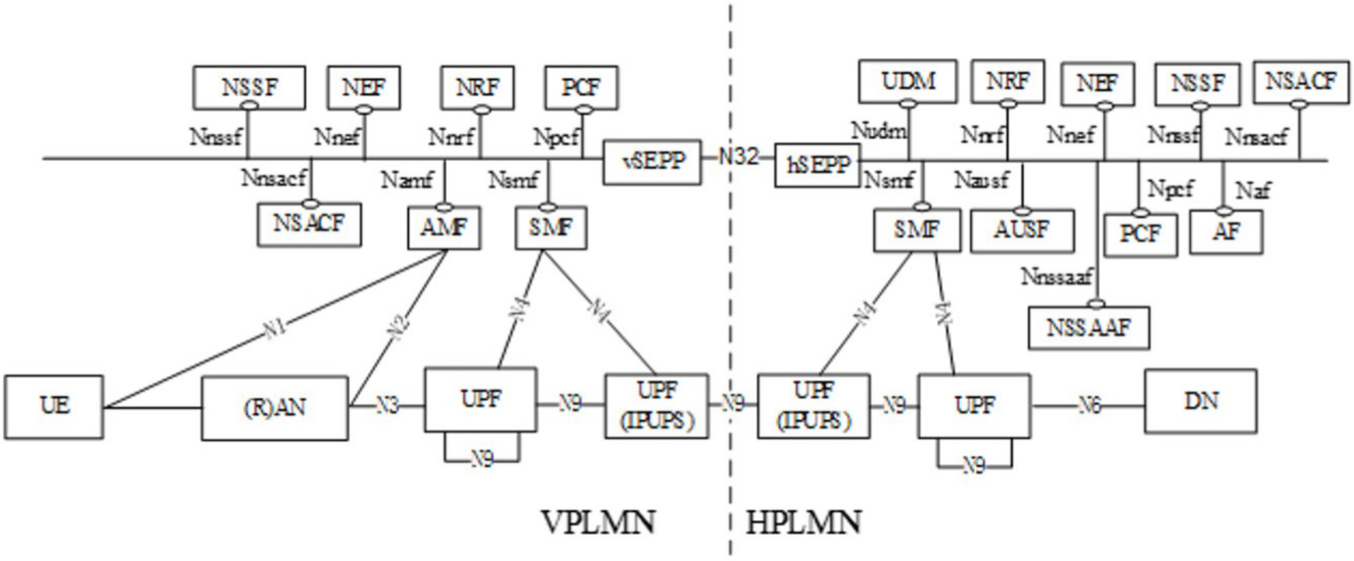

Figure 1: 3GPP TS 23.501 Roaming 5G System architecture

For each domain of the 3GPP 5G architecture, we consider both the control plane (which carries signaling traffic and controls network connections) and the user plane (which carries the actual user data). Figure 2 outlines the four domains (device, access network, serving and home core network, and interconnect network) indicating the specific security protocols employed across both the user plane and control plane.

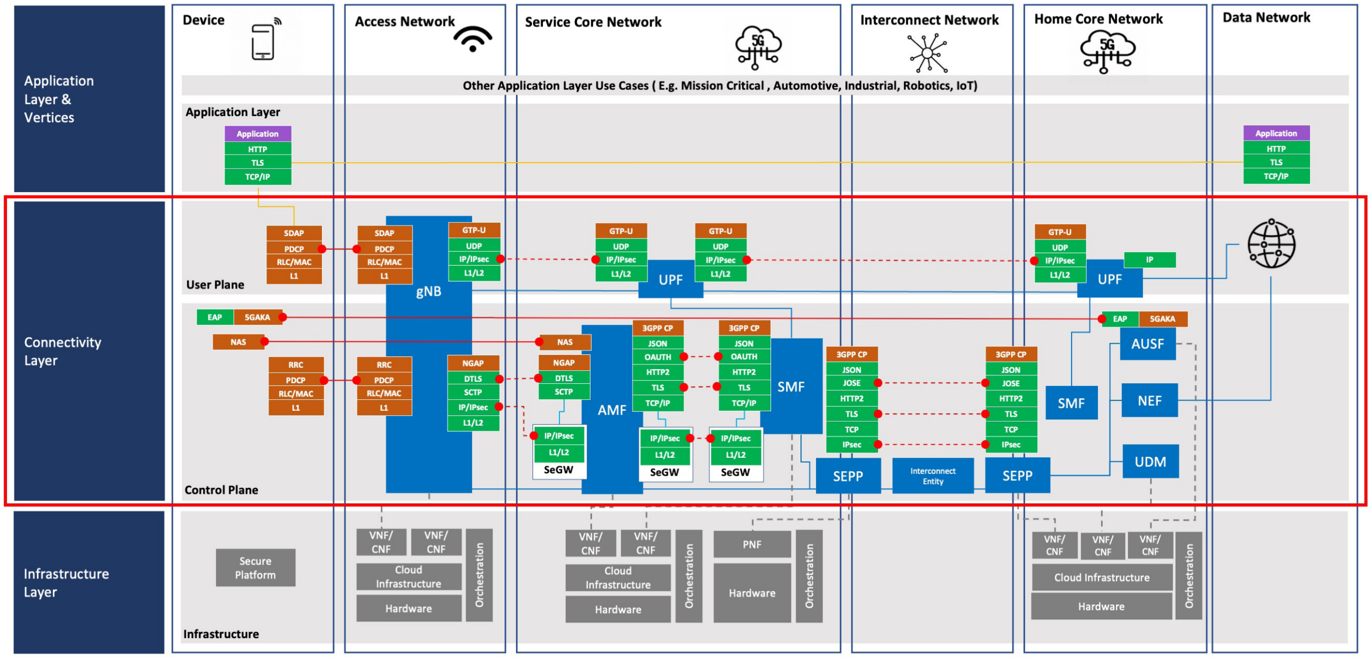

Figure 2: Overview of 3GPP 5G Domains Security Protocols [Source: Ericsson Blog]

Control Plane Implications:

The control plane, which manages signaling and network controls, is fundamentally based on protocols that ensure the security and integrity of communication between network nodes and devices. Incorporating QSC into this plane involves not only updating cryptographic measures but also ensuring that these updates do not impair the real-time operational demands of network signaling. Protocols that handle mobility management and security mode control, such as the Non-Access Stratum (NAS), must be carefully adapted to incorporate QSC. The adaptation must consider the latency and computational overhead introduced by QSC, which could greatly differ from existing solutions. For instance, lattice-based cryptographic solutions are secure against quantum attacks, but typically involve larger key sizes and more complex computations, potentially impacting the protocol efficiency and response times crucial for control plane operations.

User Plane (UP) Implications:

In the user plane, which handles the actual data transmitted between users and the network, the requirements for data throughput and latency are extremely stringent, especially with the increasing volume of high-speed mobile data traffic. Transitioning to QSC within the user plane protocols, such as PDCP (Packet Data Convergence Protocol), which is responsible for data encryption and integrity checks, requires a careful balancing act. The cryptographic agility of the user plane must be maintained to manage the diverse and intensive demands of video streaming, virtual reality, and other bandwidth-intensive applications. The impact of QSC on data throughput and encryption processing times must be thoroughly assessed to ensure that the transition does not degrade user experience.

For both planes, each protocol must be individually assessed to understand how the proposed QSC's unique cryptographic characteristics will impact its functionality. This understanding will guide 3GPP in prioritizing and implementing specific changes. The transition strategy must also consider the interoperability between existing and future quantum-resistant systems to ensure a smooth evolution of the network infrastructure. The complexity of this task underscores the need for ongoing research, multi-stakeholder collaboration, and phased testing to implement QSC effectively across the 3GPP 5G architecture.

Figure 2 illustrates the architectural framework of the 3GPP 5G infrastructure, with a specific focus on identifying the protocol stacks underpinning both the user plane and control plane. This visual representation is designed to elucidate the intricate network of protocols that facilitate the myriad functions necessary for the seamless operation of 5G networks. By delineating the user plane and control plane protocols, the diagram serves as a foundational tool to understand where and how PQC algorithms or adaptations to the symmetric key cryptography can be integrated effectively. This integration is critical for enhancing the security measures against potential quantum computing threats without compromising the operational efficiency and performance standards essential for next-generation wireless communication systems.

4.1 5G Devices Impact Analysis

Mobile device endpoints, commonly referred to as User Equipment (UE), encompass a broad range of devices including smartphones, tablets, mobile IoT and industrial sensors, autonomous vehicles, and personal computing devices. These devices connect to and communicate through the 5G network, necessitating robust security measures, to protect the privacy, confidentiality, integrity, and authenticity of the communications. Figure 3 illustrates the security protocols used at each layer.

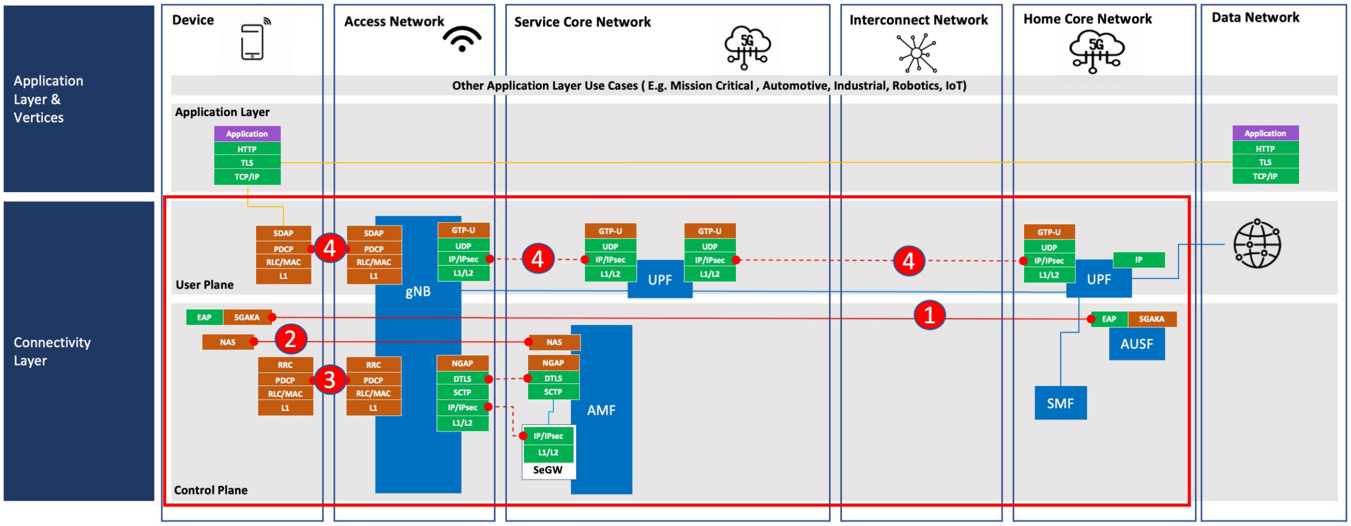

Figure 3: 3GPP 5G Device Security Protocols

5G Subscriber Identity Authentication Process (1)

The main protocol used in securing the end user device with the mobile core network is the 5G Authentication and Key Agreement (AKA) protocol. It is an essential security mechanism within the 5G network infrastructure, specifically designed to authenticate users and ensure the privacy and security of their communications.

MILENAGE is a set of cryptographic algorithms designed for use in mobile telecommunications, particularly for authentication and key generation processes. It is based on the AES and is part of the AKA protocols used in Universal Mobile Telecommunications Service (UMTS) and Long-Term Evolution (LTE), which have been adapted for 5G systems. This protocol is a continuation and improvement of the AKA protocol used in previous mobile communication generations, tailored to meet the increased security requirements of 5G networks. Here, we will delve into the technical specifics of the 5G AKA process, focusing on user authentication and the provision of a Subscription Concealed Identifier (SUCI) for user privacy. It is important to note that 5G AKA doesn't use asymmetric cryptography, so it is not an immediate threat.

Encryption of the Subscriber's Permanent Identifier (SUPI):

> The SUCI is an encrypted form of the SUPI, designed to protect user identities within 5G networks. This encryption employs a hybrid approach, combining public key cryptography and symmetric key encryption. Specifically, the SUCI is generated using the network's public key, which is provisioned on the device by the network, along with a device-specific private key, typically derived using ECC. This method ensures that only the network, which holds the corresponding private key to the public key used, can decrypt the SUCI back into the SUPI, safeguarding the user's identity from interception and unauthorized tracking. The risk here is that ECC algorithms are known to be vulnerable to quantum attack, so this needs to be evaluated for quantum resistance.

Key Derivation from Authentication Vectors:

> The symmetric keys derived during the authentication process (such as K_AUSF and K_SEAF) are generally considered more resistant to quantum attacks. However, the process to derive these keys often involves cryptographic hashes and Hash-Based Message Authentication Codes (HMACs), which might need to be evaluated for quantum resistance. The risk here is that the keys may be potentially hacked during key derivation, so this needs to be evaluated for quantum resistance.

Device/UE to gNodeB (gNB) on the Control Plane and User Plane (2,3,4)

In a 5G network, the security protocols designed to protect communications between the UE, the gNB, and the User Plane Function (UPF) on the user plane are crucial for ensuring the confidentiality and integrity of the data transmitted.

PDCP Layer Security (3,4): In the 5G architecture, the PDCP layer in the radio protocol stack at the gNB handles the encryption and decryption of user data as it travels between the UE and the network. PDCP also manages the sequence numbering of packets to provide replay protection.

The integrity and encryption protection provided at this layer ensures that the data remains secure as it traverses potentially vulnerable paths between network components.

- **User Plane Encryption (UPE):** Data transmitted over the user plane between the UE and the gNB, and onward to the UPF, is encrypted to ensure confidentiality. In the 5G device communications over the user plane, data encryption primarily relies on symmetric key algorithms such as AES, which is utilized within Network Encryption Algorithms (NEA) protocols defined as NEA1, NEA2, and NEA3.
- **User Plane Integrity (UPI) Protection**: To protect the integrity of the data, Network Integrity Algorithms (NIA) are used. These include NIA1 (based on AES-CMAC) and NIA2 (based on SNOW 3G), specifically used for the North American market. Integrity protection is critical to ensure that the data has not been altered or tampered with during transmission.

NAS Protocol Security (2): In 5G networks, NAS is responsible for carrying out signaling and control information related to session management and mobility management between the UE and the core network components. The keys used for NAS security and those used for user plane security are related but distinct, each serving specific security purposes within their respective domains.

- The specific encryption and integrity algorithms used for NAS security are determined during the SMC process. Commonly, these could involve algorithms like NEA1 or NEA2 for encryption and NIA1 or NIA2 for integrity protection, depending on the security capabilities and preferences of both the network and the UE.

In the case of both encryption and integrity security over PDCP and NAS, the use of symmetric key mechanisms like AES may face vulnerabilities from quantum computational advancements in the future. Encryption and integrity checks are crucial for ensuring that data has not been tampered with during transit, and weakening these could allow undetected manipulations of critical data.

Relevant 3GPP Specifications:

3GPP TS 33.501 addresses the security needs of these UEs comprehensively, focusing on essential aspects such as authentication on the control plane and encryption on the user plane. TS 33.501 outlines the protocols for securing interactions within the network, ensuring that user identities are authenticated effectively on the control plane to establish trust between the device and the network. Concurrently, encryption on the user plane ensures that data exchanged between the network and the device is protected against interception and unauthorized access.

Potential Quantum Threats:

- **HNDL:** Because device communications data exchanged during the 5G AKA process often includes long-term credentials or session keys that remain sensitive for extended periods. .
- **QMITM:** Particularly in IoT devices, which might lack robust quantum-resistant measures.
- **Side-Channel Attacks:** Although not exclusively a quantum threat, due to the physical accessibility of devices.

Current Cryptography Usage:

- Current Methods: AES-128, SHA256, Public Key Cryptography algorithms

Specific Vulnerabilities:

- AES-128, recognized for its robustness against classical attacks because of its computational complexity and key size, currently maintains a strong defense in conventional security. Although NIST indicates that AES-128 remains secure against quantum attacks for now, the theoretical implications of Grover's algorithm suggest the need for eventual migration to more secure standards such as AES-256 at some time in the future.

Security Protocol Updates:

To safeguard the integrity and confidentiality of UE communications within future 5G networks against emerging security challenges posed by quantum computing, it is crucial for the authentication and encryption protocols to transition to QRC. This will ensure that both the authentication of user identities and the encryption of data transmissions remain secure and effective, even as quantum computing capabilities evolve.

> **Increased Key Sizes:** As previously indicated, AES-128 is currently believed to be resilient to quantum attacks. However, in anticipation of advancements in quantum computing and particularly the potential impact of Grover's algorithm, future standards should consider migrating to AES-256 if the implementation allows. This transition would effectively double the key length used in symmetric encryption algorithms, restoring and enhancing the effective security level against quantum threats.
>
> **Adoption of PQC Algorithms:** Incorporating PQC algorithms where applicable is crucial. For example, key exchange mechanisms or key establishments can provide robust protection against quantum threats.

The move toward making the user plane communication in 5G networks quantum resistant is critical, not only for maintaining the confidentiality and integrity of data but also for ensuring the overall resilience of mobile communications in the quantum era. This transition will require careful consideration of performance impacts, especially for applications requiring real-time or ultra-low-latency communications and must be integrated smoothly to maintain user experience and system efficiency.

Potential Challenges in Migration To QSC:

While MILENAGE is inherently quantum-resistant due to its reliance on AES, integrating it within hybrid cryptographic frameworks can enhance its resilience against quantum threats. Continuous evaluation and adaptation in line with advancements in quantum computing and cryptography are vital for maintaining the security integrity of 5G networks using MILENAGE.

Migrating device/UE communications to QSC on 5G networks presents several challenges. Not all devices may be able to be updated immediately — or even ever — to support 5G implementation of QSC. Ensuring that these devices can communicate securely without requiring immediate upgrades to QSC-compatible hardware or software is a significant challenge. Often, to maintain backward compatibility, the network may need to support both QSC and classical cryptographic algorithms simultaneously. This hybrid approach requires the network infrastructure to be flexible and capable of dynamically selecting the appropriate cryptographic suite based on the device's capabilities. This dual support increases the complexity of the network and can lead to potential vulnerabilities if not managed carefully.

Authentication of the device/UE in 5G network transition to QSC presents significant challenges, especially regarding the management of dual Ki keys for 5G-enabled QSC security and seamless roaming across 5G networks that have not yet adopted QSC. The device's Universal Subscriber Identity Module (USIM) needs to support dual key types, which can lead to compatibility and performance issues due to the increased computational requirements of QSC algorithms. The AUSF must handle the complexities of managing and switching between legacy and QSC keys for authentication, increasing the risk of misconfigurations and security breaches. This dual key management system adds operational complexity and can lead to potential disruptions and increased overhead during the transition.

Proposed Phased Implementation:

- ***Phase 1: Test QSC Implementation for Initial Connections*:**
  - Implement a test phase for a small set of devices/UEs, using PQC algorithm (e.g., ML-KEM) for key establishment, along with quantum-safe symmetric algorithms (e.g., AES-128 or preferably AES-256, if the implementation allows) for SUPI protection:
    - Test a small set of devices/UEs using quantum-safe symmetric algorithms (e.g., TUAK with 256 bits) for 5G Authentication and Key Agreement. (by means of 5G-AKA or EAP-AKA').

- **Phase 2: Start to Implement QSC to Critical Communication Paths**
  - Upgrade Security for Critical Control Plane Interfaces:
    - For NAS confidentiality and Integrity, which is based on symmetric key cryptography (e.g., AES-128, and SNOW 3G), should preferably be 256 bits if the implementation allows.
  - Enhance Security for Authentication and Identity Management:
    - In the communication between the UE and AUSF, specifically with the primary authentication and the key agreement (e.g., EAP-AKA').

        - Update the key establishment procedure with a QSC-compliant algorithm (e.g. ML-KEM) along with a quantum-safe symmetric algorithm (e.g., AES-128 or AES-256 if the implementation allows) for SUPI protection.
        - Update the 5G AKA and EAP-AKA' protocol with quantum-safe symmetric algorithm (e.g., TUAK-128 /256 or MILENAGE-128/256, preferably 256 bits if the implementation allows).
        - NEA1-128 and NEA2-128 should preferably be 256 bits if the implementation allows.

- **Phase 3: Full QSC Deployment for User Plane Data and Wide-Scale Rollout**
    - Secure User Plane Data with QSC:
        - Ensure that all data exchanged between the UE and the 5G network, including both user and control plane data, are fully protected using QSC.
    - Wide-Scale Rollout to All Devices/UEs:
        - Gradually expand the deployment of QSC algorithms to all devices/UEs across the network, prioritizing devices that handle sensitive data or are used in critical applications.
        - Continue to monitor and optimize the performance and security of QSC implementations, ensuring minimal impact on user experience and network operations.

- **Phase 4: Full Transition to QSC**
        - Complete migration to QSC
        - Where possible, plans should be made to decommission protocols using algorithms that have been deprecated.
        - Continuous performance and security validation after the full transition to QSC.
        - Post-migration support and maintenance such as patching vulnerabilities, updating cryptographic algorithms as needed, and responding to new security challenges.

4.2 Access/Radio Access Network (RAN)

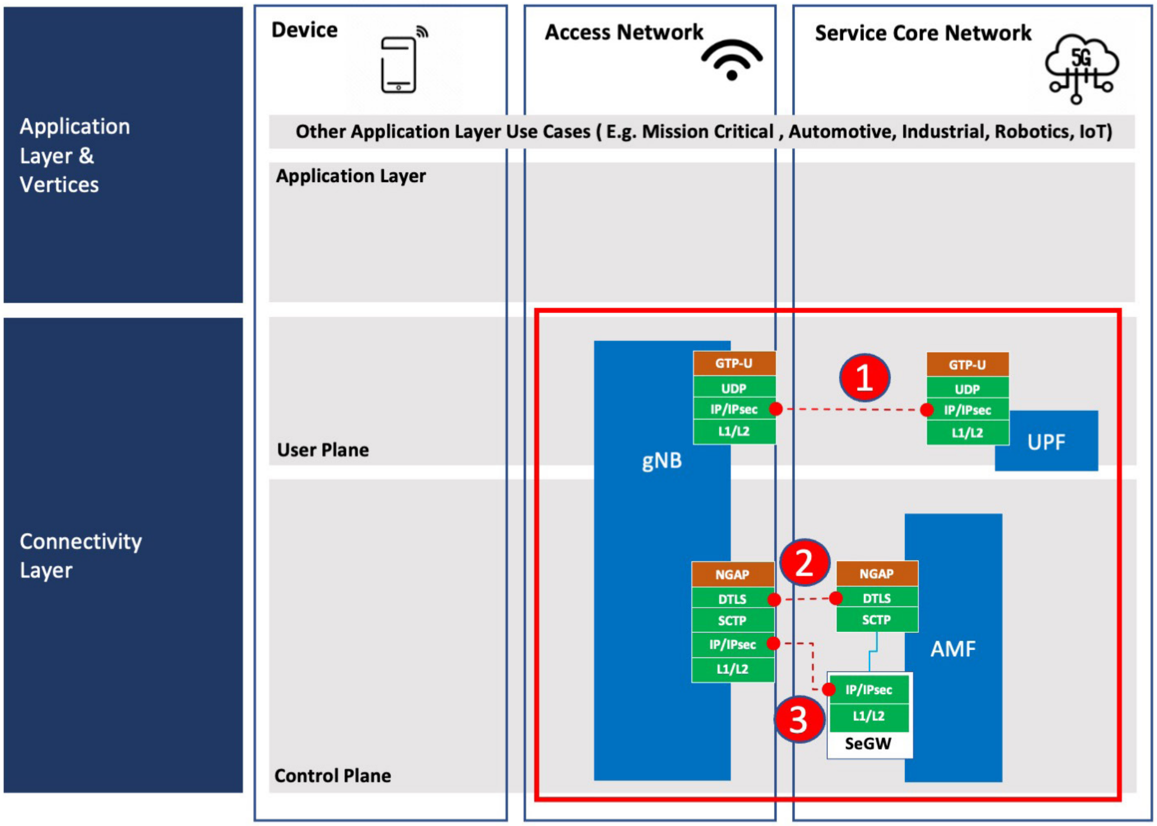

Figure 4: 3GPP 5G Radio Access Network Security Architecture

Figure 4 illustrates how the 5G RAN consists of several key components and technologies that work together to provide enhanced mobile communication services. Here is an overview of the main elements that make up the 5G RAN:

gNB: The gNB is the 5G equivalent of the base station in previous generations. It handles radio resource management, beamforming, and scheduling. In addition, it manages communication with UEs over the air interface. Moreover, the gNB acts as intermediary between the UE and 5G core network as it handles control plane with AMF (over N2 interface) for tasks such as registration authentication and mobility management. It also manages user plane traffic with the UPF (over N3 interface) for efficient data forwarding and quality of service (QoS) enforcement to ensure seamless connectivity, secure communication, and optimized performance for 5G network users. The gNB can be deployed as more than one entity by splitting the gNB into gNB-Centralized Units (CU) and gNB-Distributed Units (DU) and possibly further splitting the gNB-CU into gNB-CU-CP and gNB-CU-UP, which introduces F1 and E1 interfaces standardized in 3GPP TS 38.470 [11] and TS 38.460 [12].

- **Distributed Units (DUs):** DUs handle lower-layer protocol processing and are usually located closer to the user to reduce latency and improve performance.
- **Centralized Units (CUs):** CUs manage higher-layer protocol processing and control plane functions, coordinating with multiple DUs for efficient resource management. By centralizing certain functions, CUs can optimize network performance and enable more advanced features like network slicing.
- **Radio Units (RUs):** Remote Radio Heads (RRHs) are part of the gNB that handles the transmission and reception of radio signals.
- **Fronthaul and Backhaul Networks (AKA Transport Networks):** Fronthaul connects the RUs to the DUs, requiring high-capacity, low-latency links to support 5G's high data rates and processing demands. Backhaul connects the DUs and CUs to the core network, ensuring reliable and efficient data transport across the network infrastructure.

Along with these networks components, the RAN employs key technologies to provide enhanced mobile communication services such as network slicing, edge computing, virtualization, cloud native, and Self-Organizing Networks (SON). Some of these technologies necessitate particular security controls and mechanisms to ensure secure services. The following subsections elaborate how PQC would help or impact these security protocols, mechanisms, and requirements.

Control Plane Security (2,3) The control plane in the RAN section refers to the information transported over the N2 interface between the gNB and the AMF. This interface is used, among other functions, to carry NAS signaling traffic between the UE and the AMF. According to 3GPP TS 33.501, control plane traffic over N2 shall be protected for confidentiality, integrity, and replay attacks. To ensure protection of control traffic over the N2 interface, 3GPP SA3 recommends the implementation of one or both of the following security protocols:

- **IPsec Encapsulating Security Payload (ESP) with IKEv2 (3)**: This option involves using IPsec ESP in conjunction with IKEv2 for certificate-based authentication. Implementing this protocol may necessitate a Security Gateway (SEG) to effectively terminate the IPsec tunnel, ensuring secure communication over the network.
- **Datagram Transport Layer Security (DTLS) (2):** Alternatively, as specified in RFC 6083, the DTLS security implementation should align with the TLS profile as detailed in TS 33.210, while the certification handling should conform to the guidelines set forth in TS 33.310.

Both options offer effective means to secure control plane communications, with the choice depending on specific network requirements and existing infrastructure capabilities.

In case of split DU-CU, as shown in Figure 5 which is a zoomed-in view of the 5G RAN diagram included in Figure 4. for split gNB, using F1 interface defined in TS 38.470. Signaling traffic (i.e. both F1-C interface management traffic defined in TS 38.470 and F1-C signaling bearer are carried on the F1-C interface). The F1-C interface shall support confidentiality, integrity, and replay protection, too. The E1 interface connects CU-CP to CU-UP as defined in TS 38.460. The E1 interface shall be confidentiality, integrity, and replay protected. According to TS 33.501, the security for F1-C and E1 interfaces shall support both IPsec with IKEv2 (3) and DTLS (2).

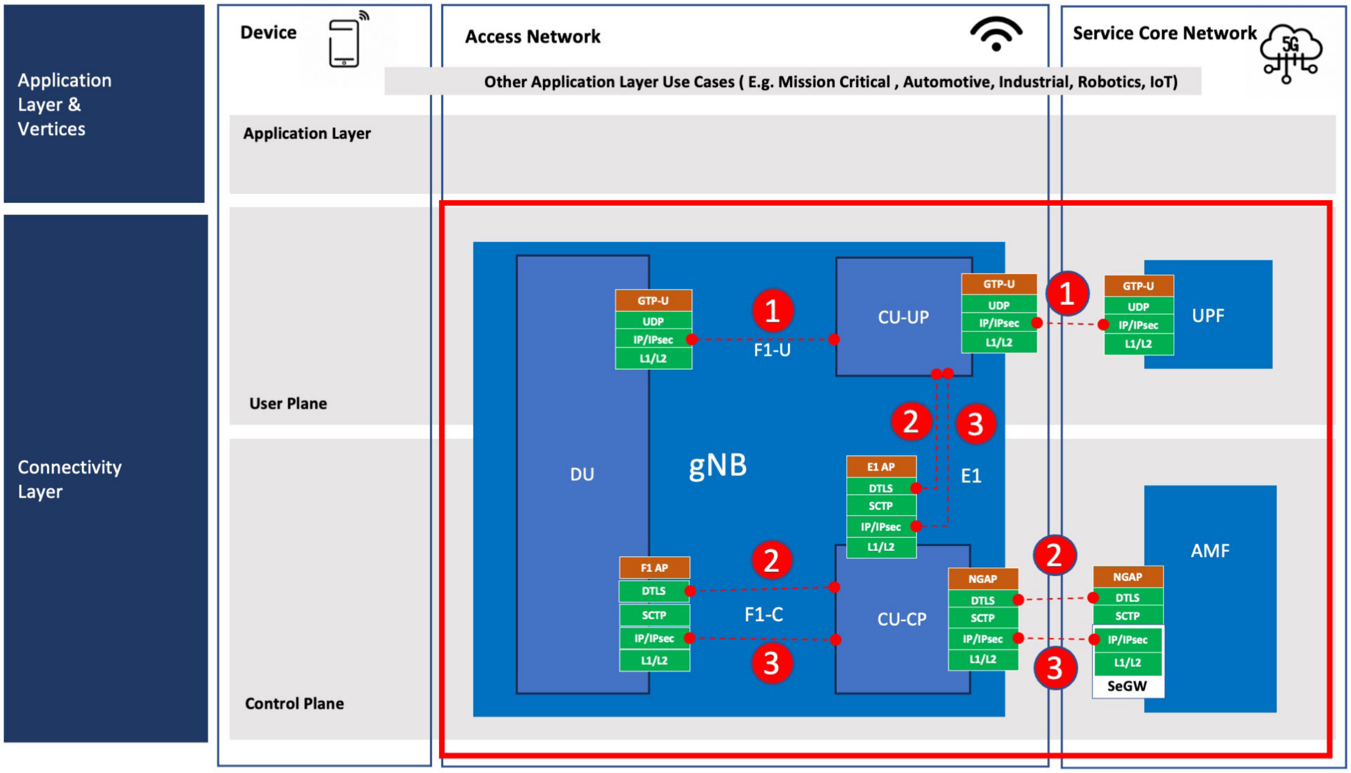

Figure 5: 3GPP 5G RAN Security Architecture with split gNB

User Plane Security (1): User plane protection can be approached from different perspectives. The first perspective focuses on the southbound direction, which is toward the UE. The second perspective is on the northbound direction, which is towards the UPF. The southbound traffic is covered in section 4.1, "5G Devices Impact Analysis," while the discussion below focuses on the northbound traffic.

The N3 interface carries network traffic between the RAN (specifically the gNB) and the UPF. According to TS 33.501, the transport of user data over N3 shall be protected for integrity, confidentiality, and against replay attacks. This requires the implementation of IPsec ESP and IKEv2 for certificate-based authentication, as outlined in the control plane specifications. In case of gNB split, the F1-U interface shall use IPsec with IKEv2 (1) to protect data in transit.

Relevant 3GPP Specifications:

- **3GPP Specification TS 33.501** specifies the security architecture and procedures for 5G systems, covering mechanisms for authentication, confidentiality, integrity protection, and key management. It defines how 5G networks ensure secure communication between UEs and network entities, including encryption and integrity algorithms, as well as measures to protect sensitive data and signaling across the network.
- **3GPP Specification TS 33.210** profiles both IPsec with IKEv2 and TLS including the Cipher suites used in the negotiation of IPsec Security Associations (SAs).
- **3GPP Specification TS 33.310** outlines how Certificate Authorities (CAs) are organized. It also provides requirements for the protocols and certificate profiles used, ensuring that operator IPsec and PKI implementations can interoperate effectively.

Potential Quantum Threats:

- ***HNDL*:** Presents a risk due to the transmission of potentially sensitive control signaling data over time, potentially exposing long-term secrets or operational details of the network.
- ***Quantum Decryption***: If the encryption used in the control interface is based on asymmetric cryptographic methods, an attacker could exploit weaknesses in asymmetric cryptography that are used for key exchange, such as RSA or ECC.
- ***QMITM***: Depending on the implementation, this threat involves an attacker using quantum techniques to break the

signature key in advance and sit undetected as a MitM and potentially alter the communication between the gNB and the AMF or between the gNB and the UE. Such an attack could compromise the integrity of the control messages, leading to unauthorized control of network operations or disclosure of sensitive user information.

- **Side-Channel Attack (SCA)**: Presents a risk to both the northbound and southbound sides. By leveraging huge quantum computation capabilities, an attacker potentially could get information about how the transmitted information has been encrypted at different layers. This could involve exploiting some encryption-related information inadvertently provided by the non-cryptographic physical parameters of the communicating nodes such as time delay and electromagnetic parameters to disturb.

Current Cryptography Usage:

Current Methods: TLS 1.2, TLS1.3, IPsec with IKEv2, DTLS1.2

Specific Vulnerabilities:

The cryptographic algorithms traditionally used in IPsec with IKEv2 and DTLS include Diffie-Hellman Key Exchange (DHE) for key exchange, and RSA and ECC for digital signatures and key exchange. These are all vulnerable to quantum attacks. Both DTLS and IPsec with IKEv2 offer a wide range of cipher suites, which need to get migrated to withstand quantum-based attacks.

Security Protocol Updates:

Employing quantum-safe algorithms to secure both IPsec with IKEv2 and DTLS can have higher time requirements in case of server-to-server communication due to potentially longer certificate chains. Implementing these in the real-time environment requires careful considerations to avoid degrading the performance or increasing the latency beyond acceptable limits. DTLS, and IPsec with IKEv2, need to be updated to post-quantum-safe algorithms. For example, all DH-style key exchanges need to be replaced by ML-KEM.

Potential Challenges in Migration to QSC:

Migrating the 5G RAN to PQC presents several challenges:

1. **Performance Impact:** Selecting the appropriate algorithm is a crucial step that must be taken carefully because it depends on various performance and complexity factors. For instance, real-time communication requires algorithms that are less complex and have faster processing times. For example, referring to Table ML-KEM and ML-DSA seem to relatively offer lower computational overhead and faster processing

2. **Compatibility Issues:** Integrating PQC into existing 5G infrastructure may pose compatibility challenges with current hardware and software. Many components of the 5G RAN domain, such as base stations, and other 5G domains such as user devices, might not support the new algorithms without significant updates or replacements.

3. **Network Architecture**: Non-Standalone deployment requires 4G networks to get updated concurrently with the RAN part. Implementation of PQC in 5G is potentially easier than 4G due to 5G's updated infrastructure and standards, which may provide more flexibility and support for new security protocols.

4. **Resource Constraints**: The RAN environment is resource-constrained compared to the core environment in terms of computational power, memory, and energy. Post-quantum algorithms often require larger key sizes and more complex computations, which may strain these limited resources.

5. **Security Assurance and Testing**: New cryptographic algorithms need extensive testing and validation to ensure they provide the expected security levels against both classical and quantum attacks. This process is time-consuming and costly, requiring rigorous testing in various scenarios.

Proposed Phased Implementation:

Migrating the 5G RAN to PQC requires a carefully planned and phased approach to ensure minimal disruption and maximize interoperability and security. Here's a proposed transition:

- **Phase 1: Preparation and Assessment**
  - Inventory and Audit: Identify components and information that rely on classical asymmetric cryptographic algorithms. Moreover, identify protocols that are not planned to migrate to PQC, such as TLS1.2 [13], to define potential alternatives.
  - Risk Assessment and Impact Analysis: Evaluate the risks associated with quantum computing threats and assess the impact of adopting PQC on 5G RAN performance and security.
  - Algorithm Selection: Focus on algorithms recommended by standard bodies like NIST with less processing time, fewer keys, and smaller signatures.
  - Proof of Concept (PoC) Development: Develop a PoC to test selected PQC algorithms within a controlled environment. Analyze the impact on computational resources, latency, and throughput to refine algorithm choices.

- **Phase 2: Initial Deployment and Testing**
  - Hybrid Cryptography Implementation: This paper recommends adopting a hybrid cryptographic approach that combines classical and quantum-resistant algorithms. This may ensure interoperability and allow a gradual transition.
  - Performance Optimization: Optimize the network and PQC implementations to minimize latency and computational overhead.

- **Phase 3: Broader Rollout**
  - Gradual Rollout to Key Network Components: Starting by migrating key network components to PQC, such as gNBs and UPFs. Continue using the hybrid model that would maintain interoperability during the transition.
  - Update Key Management Systems: Implement new key management systems designed to support the new algorithms.
  - Compliance and Security Testing: Conduct extensive compliance checks and security testing to ensure that the new cryptographic methods meet regulatory requirements and protect against both quantum and classical threats.
  - Monitoring and Feedback Loop: Establish a continuous monitoring system to detect any performance or security issues.

- **Phase 4: Full Transition to QSC**
  - Complete migration to QSC
  - Where possible, plans should be made to decommission protocols using algorithms that have been deprecated.
  - Continuous performance and security validation after the full transition to QSC.
  - Post-migration support and maintenance such as patching vulnerabilities, updating cryptographic algorithms as needed, and responding to new security challenges.

4.3 Core Network (Serving and Home Core Networks) Impact Assessment

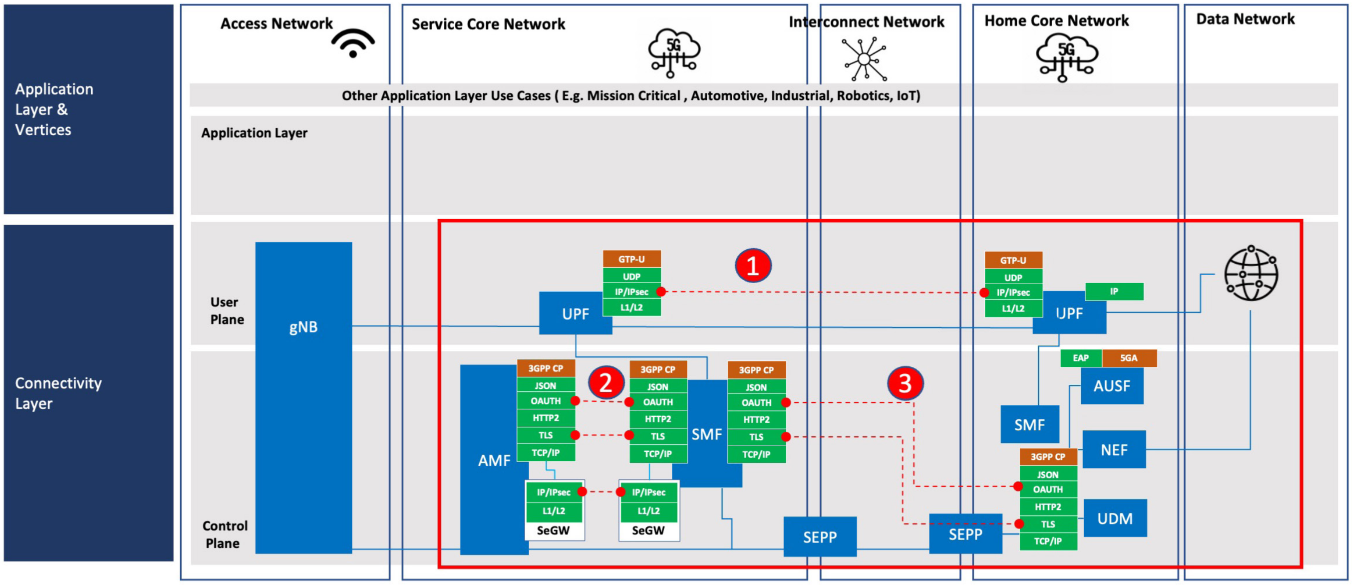

Figure 6: 3GPP 5G Core Network Security Architecture

The core network consists of functions that may be logically split into serving core and home core functions. The serving core functions primarily manage the connectivity and session contexts of active users, while home core functions deal with user data and subscription details, regardless of the user's location. A key aspect of the 5G core network's architecture, the Service-Based Interfaces (SBI) facilitate communication between the different network functions (NFs).

Serving Core Network Functions include the AMF, Session Management Function (SMF), and the UPF. In a roaming scenario, these NFs are located within a visited network.

> The **AMF** is responsible for all aspects of access and mobility management for the UE. It supports registration and deregistration processes, connection and reachability management, and mobility handling. The AMF ensures that UEs are authenticated and authorized to access the network services securely and efficiently. It also coordinates with other functions to manage any changes in the UE's network connection state or mobility.

> The **SMF** provides session management, establishing, modifying, and releasing session contexts associated with each user. The SMF coordinates with the UPF to ensure data flows are properly set up for the UE's service needs. It allocates the necessary network and radio resources required to maintain connectivity, manages the QoS levels, and handles session continuity during the UE's mobility phases.

> The **UPF** is involved in handling user data packets. It manages and routes data packets between the UE and the data network, facilitating connectivity to various services such as the internet, network slices, or voice services.

Home Core Network Functions, include the Unified Data Management (UDM), AUSF, and Network Exposure Function (NEF). They are central to managing subscriber/subscription data, UE authentication and authorization, and securely exposing network capabilities to third-party applications, ensuring comprehensive service and security management across the network.

> The **UDM/UDR** stores all subscriber-specific information. The UDM leverages this data to support various network operations, including service authorization, user identity confidentiality, subscription validation, and service access configuration.

> The **AUSF** manages the UE security, handling authentication and authorization of UEs. It verifies the user credentials provided by the AMF and confirms the legitimacy of access attempts, safeguarding against unauthorized use and ensuring network integrity.

> The **NEF** provides an interface for external networks to securely access network capabilities and services. It exposes network functionalities to third-party service providers while maintaining control over which information and features are accessible.

These NFs communicate with one another using the SBI, based on HTTP/2 where a Network Function Consumer (NF-C) requests services from a Network Function Producer (NF-P). To ensure secure transactions, the following security protocols are implemented on the SBI interface:

- The NFs mutually authenticate one another leveraging the Mutual Transport Layer Security ((mTLS) 1.2/1.3) protocol.
- Digital certificates compliant to X.509 specifications (RFC 5280) and using ECC, curve P-256, or P-384 with Elliptic Curve Digital Signature Algorithm (ECDSA) signatures are used for mutual authentication between the NFs.
- Authorization of services requested from an NF-P by an NF-C are carried out using OAuth 2.0 tokens, which are issued by the Network Repository Function (NRF) based on authorization rules. Network Function to Network Function (NF-NF) authorization is performed using OAuth 2.0 tokens, which are digitally signed using ECDSA by the NRF. The OAuth 2.0 tokens are validated for authenticity and integrity by the producer NFs using the pre-provisioned public keys of the NRF.

The SMF and UPF communicate using Packet Forwarding Control Protocol (PFCP), which uses the User Datagram Protocol (UDP) as a transport mechanism over the N4 interface. The communications between the gNB and the AMF over the N2 interface uses the Stream Control Transmission Protocol (SCTP), while the gNB to the UPF uses the N3 interface are based on the Generic Tunneling Protocol (GTP).

The N2, N3 and N4 are not based on SBI, so they are protected using IPSec or DTLS. There is no explicit authorization carried out on the non-SBI interfaces.

Relevant 3GPP Specifications:

- **TS 33.501:** Describes 5G subscriber authentication, NF-NF authentication and authorization, Authentication and Key Management for Applications (AKMA), and secondary and slice-specific authentications/authorizations. The protocols described and specified include symmetric key-based schemes (e.g., 5G-AKA, EAP-AKA'), Elliptic Curve Integrated Encryption Schemes (ECIES), and asymmetric-based mechanisms used for key agreement to protect the SUPI and generate SUCI.
- **TS 33.310**: Specifies the authentication of network elements that use NDS/IP or TLS, and Certificate Enrolment for Base Stations. In the case of NDS/IP, the specification includes both the authentication of SEG and the network elements.
- **TS 33.210**: Specifies the security architecture for network domain IP-based control planes, which covers the control plane security and on selected interfaces between network elements of NDS/IP networks.

Potential Quantum Threats:

- **HNDL**: Is a risk to the 5G core network that carries subscriber data, including charging data, location information, and subscriber profile information, which are protected using TLS1.2/IPSec. A CRQC can be used to decrypt to obtain a certain user behavior, subscriber profile, and thus compromising subscriber privacy.
- **Quantum Decryption:** Because the core networks rely heavily on encryption for user data and signaling.
- **QMITM:** Presents a risk, particularly in signaling and control plane operations.
- **Quantum Side-Channel Attacks:** Presents a risk mostly related to the secure environment (e.g., HSM), which may be deployed deeper into the home network.

Current Cryptography Usage:

- **Current Methods:** TLS 1.2/1.3 with OAuth, IKEv2/IPSec, DTLS

Specific Vulnerabilities:

- **SBI Interfaces:**
  - **Mutual Authentication of TLS endpoints:** Mutual authentication between the NFs are carried out using X.509 certificates that carry ECDSA-based signatures. Thus they are vulnerable to QMITM attacks, where an attacker can modify signatures and impersonate a legitimate NF.
  - **Encryption using TLS**: The TLS 1.2 cipher suites that are mandated to be supported are based on ECDHE (e.g., curve secp256r1/P-256, secp384r1) or DHE, with key sizes greater than 256 bits and 4096 bits, respectively, which are

known to be vulnerable to HNDL attacks. Only PSK-based would be spared if the key lengths are greater than 128 bits.

  - **NF Authorization using Access Tokens:** Integrity and authenticity are of primary importance in JSON Web Token (JWT) with JSON Web Signature (JWS), so they are not vulnerable to HNDL. However, if JSON Web Encryption (JWE) is used for certain use-cases, then the encrypted JSON payload that is encrypted using ECDHE is known to be vulnerable to HNDL. The JWS is vulnerable to QMITM, where an attacker can tamper with the claims in the OAuth token and issue bogus tokens digitally signed by the attacker that can then be used to obtain services from an NF-P.

- **Non-SBI Interfaces:**
  - **Authentication and Encryption using IKEv2/IPSec:** The IKEv2 profiles that are used for authentication as part of negotiating IPSec SAs are based on ECDSA and RSA and thus vulnerable to QMITM attacks. Additionally, the key-establishment mechanisms used are based on ECDHE or DHE and therefore vulnerable to HNDL and QMITM attacks.
  - **Authentication and Encryption using DTLS**: The protocol is very similar to TLS and therefore highly vulnerable to HNDL and QMITM attacks.

Security Protocol Updates:

The SBI interface (HTTPS/2.0) is protected using mTLS1.2/1.3, and the profiles are currently based on DHE/ECDHE, making them susceptible to HNDL attacks. TLS1.3 will have to be updated with PQC-compliant crypto suites for mutual authentication and key establishment. Similarly, the interfaces N2, N3, and N4 that are protected using IPSec/DTLS, so the crypto suites within IPSec will have to be updated with PQC-compliant crypto suites. All NF-NF authentication is carried out using X.509 certificates with ECDSA signatures that will have to be upgraded to certificates that contain PQC-compliant digital signatures (e.g., ML-DSA). The digital signatures within the OAuth access tokens will have to be upgraded to PQC-compliant signature schemes (e.g., ML-DSA). In summary the following upgrades will have to be performed:

1. **PKI with PQC:** The upgraded PKI systems must be able to issue and manage certificates with PQC-compliant digital signature algorithms (e.g., ML-DSA) for NF client/server certificates and the NRF signing certificate.

2. **Upgrade NFs to Support PQC-Capable mTLS 1.3:** The NFs must have the capability to validate ML-DSA signatures from the issuing CA as part of the mutual authentication process and then use ML-KEM public keys to perform key establishment. The NFs must use AES-128 (AES-256 preferred) as the encryption algorithm and for integrity protection use SHA-256 at a minimum (SHA-384 preferred) using GCM mode.

3. **Upgrade to PQC Capable IKE/IPSec:** Upgrade the SEG and IKEv2 protocol to have the capability to authenticate endpoints using ML-DSA certificates and use ML-KEM as the key establishment algorithm. Ensure that the IPSec SAs uses AES-128 (256 bits preferred) for encryption and integrity protection based on SHA-256 bits (SHA-384 preferred).

4. **Upgrade NRF to PQC Compliant Signatures:** The NRF must be capable of generating PQC-compliant signatures (e.g., ML-DSA) as part of the JWS in the OAuth 2.0 access tokens. Additionally, ensure that the hashing algorithm used for generating the digital signatures uses SHA-256 bits (SHA-384 preferred).

5. **Upgrade the UDM/SIDF:** The UDM/SIDF that hosts the Subscriber Identifier De-Concealment Function (SIDF) will have to be upgraded to be capable of decrypting the SUCI that has been generated using a PQC-compliant key establishment (ML-KEM).

6. **Upgrade HSM:** If the UDM utilizes a HSM to store and decrypt the UE subscriber credentials (e.g., authentication vectors) then the HSM must be upgraded to PQC-compliant authentication and key establishment algorithms using ML-DSA and ML-KEM, respectively.

Potential Challenges in Migration to QSC:

Migrating the 5G core network to PQC entails several challenges that mirror some of those faced by the RAN but also include unique issues associated with core network operations:

- **Performance Impact:** PQC algorithms typically require more computational resources, which could lead to increased latency and reduced throughput in the core network. This is particularly critical in the 5G core, which needs to manage not only user data but also extensive signaling data.
- **Compatibility Issues:** Integrating PQC into the existing 5G core infrastructure may lead to compatibility issues with

current systems and software. NFs and services that rely on traditional cryptographic standards may require significant updates or reengineering to accommodate new quantum-resistant algorithms.

- **Network Architecture Adaptation:** Unlike the RAN, the core network uses a Service-Based Architecture (SBA) that might offer more flexibility in updating cryptographic protocols. However, this also means that every service and interface might need individual attention to ensure coherent security upgrades across the board.
- **Resource Constraints:** Although the core network generally has access to more substantial computational resources than the RAN, the increased demands of PQC for key management and data processing still pose challenges. These include managing larger key sizes and the additional overhead of secure session management.
- **Security Assurance and Validation:** New cryptographic implementations in the 5G core will require comprehensive testing to confirm their effectiveness against quantum attacks. This validation process must ensure that no new vulnerabilities are introduced and that all aspects of core network operations remain secure and robust.
- **Risk of Transition Period Attacks:** During the transition to PQC, the 5G core may have to operate in a mixed environment where old and new cryptographic standards coexist. Managing this transition carefully is crucial to avoid creating temporary vulnerabilities that could be exploited by attackers.

Addressing these challenges requires a strategic approach that involves careful planning, phased implementation, and ongoing collaboration with technology providers, standards bodies, and security experts. This will ensure that the migration enhances the security of the 5G Core network without compromising its performance and reliability.

Proposed Phased Implementation:

It is assumed that a PQC-compliant PKI is made available so the lifecycle management of certificates issued to NFs can be performed.

- **Phase 1: Preparation and Assessment**
  - **Inventory and Audit:** Identify components and information that rely on classical asymmetric cryptographic algorithms that may require alternatives or hybrid solutions.
  - **Risk Assessment and Impact Analysis:** Evaluate the risks associated with quantum computing threats and assess the impact of adopting PQC on the 5G core network's performance and security.
  - **Algorithm Selection:** Focus on algorithms recommended by standard bodies like NIST with less processing time, fewer keys, and smaller signatures. Consider algorithms that balance security requirements with minimized processing overhead, ensuring compatibility with 5G core performance standards.
  - **Proof of Concept (PoC) Development:** Develop a PoC to test selected PQC algorithms within a controlled environment. Analyze the impact on computational resources, latency, and throughput to refine algorithm choices.

- **Phase 2: Upgrade NFs that use or transport confidential data using PQC:**
  - **PQC-compliant PKI:** Ensure that the NFs are provisioned with PQC-compliant digital certificates. It is important to provide crypto agility to NFs that use these certificates and that there is an automated management of these certificates using a PQC-compliant PKI.
  - **Identify and protect interfaces that carry subscriber data using PQC:** Identify control plane messages that carry subscriber data and are vulnerable to HNDL attacks. These include authentication data carried between the AMF and the AUSF, authentication/subscriber data between the UDR and the UDM, etc. Additionally, the Charging Data Records (CDR) that are transferred between the SMF and Charging Function (CHF) over the N_{CHF} interface, as well as other interfaces that carry charging and call details data, and analytics data that is shared with the NWDAF all must be protected using TLS 1.3 with ML-KEM. Ensure interfaces (e.g., N2) that carry session keys are protected using PQC-compliant IKEv2/IPSec.
  - **Update AUSF to Support QSC Authentication:** The AUSF must be updated to handle dual authentication processes, supporting both legacy and QSC authentication mechanisms. This update ensures that devices with QSC-enabled USIMs can perform secure, quantum-resistant authentication while still allowing compatibility with networks using traditional cryptographic methods.

- **Phase 3: Broader implementation of QSC across NFs**
  - **Upgrade NRF to have PQC digital signature capability:** The NRF must be upgraded to have the capability to issue access tokens that are digitally signed using PQC-compliant (e.g., ML-DSA) algorithms and the NF-P have the capability to validate the PQC compliant digital signatures of the NRF.

- **Upgrade NFs that perform important functions:** The interfaces that are used for carrying configuration information (e.g., PFCP) and that warrant high integrity/authenticity may be the next set of interfaces that are protected using IKEv2/IPSec with certificates signed using ML-DSA for mutual authentication and secured for integrity using ML-KEM.
- **User Plane Protection:** The interface between the gNB and UPF that carries user plane data over N3 is protected using IKEv2/IPSec or DTLS1.3 with ML-KEM.

- **Phase 4: Full Transition to QSC**
  - Complete migration to QSC
  - Where possible, plans should be made to decommission protocols using algorithms that have been deprecated.
  - Continuous performance and security validation after the full transition to QSC.
  - Post-migration support and maintenance such as patching vulnerabilities, updating cryptographic algorithms as needed, and responding to new security challenges.

4.4 Interconnect Network

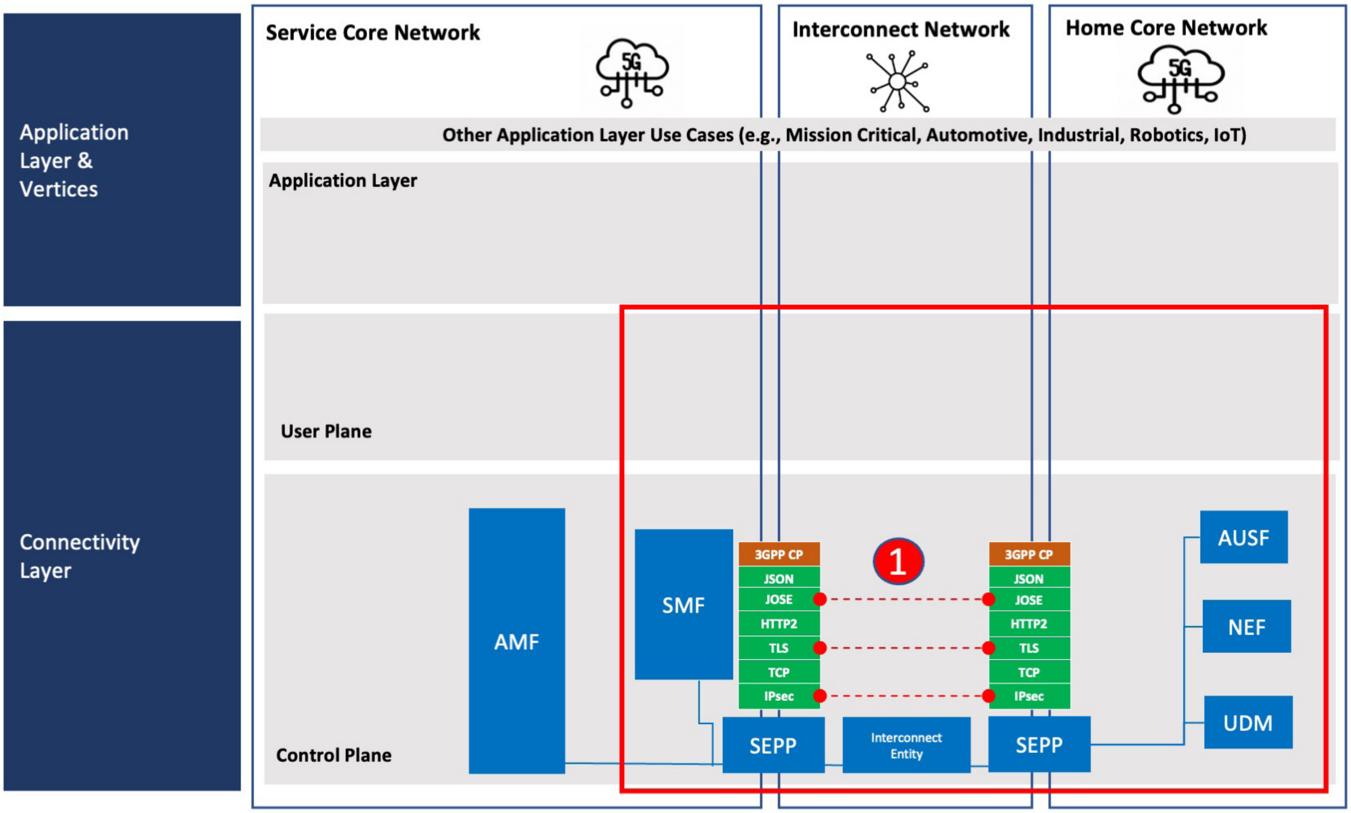

Figure 7: 3GPP 5G Interconnect Network Security Architecture

In the context of 5G networks, the Security Edge Protection Proxy (SEPP) plays a pivotal role in enhancing the security and integrity of inter-operator communications. The Internetwork Packet Exchange (IPX) provides a global, private, and secure IP network framework that enables the seamless exchange of IP traffic among Mobile Network Operators (MNOs) and other service providers. This infrastructure is crucial for ensuring high-quality, scalable, and interoperable connectivity across various telecommunications services and geographical boundaries.

SEPP Functionality for 5G Interconnect: The SEPP enhances the security measures for data exchanged between the serving core network and the home network core. It utilizes robust encryption and authentication mechanisms to safeguard the integrity and confidentiality of cross-network communications.

In 5G interconnect security, SEPP-to-SEPP communications can be implemented in two ways. The direct SEPP-to-SEPP connection uses TLS on the N32c interface to provide end-to-end encryption and integrity directly between the home and visited networks. Alternatively, when an IPX provider is involved, SEPP utilizes application-layer security using PRotocol for N32 INterconnect Security (PRINS). PRINS incorporates TLS for transport-layer encryption while adding JSON Object Signing and Encryption (JOSE) for message-level integrity and confidentiality. This allows intermediaries like IPX providers to inspect or modify messages as permitted by policy, without compromising overall security.

The primary security protocols typically used between the SEPPs in these networks to safeguard data integrity, confidentiality, and authenticity:

- **TLS:** Used for securing the N32c and establish keys that can then be used for securing the N32f interface.
- **JOSE**: Used between the two SEPPs in the context of 5G networks, particularly for securing JSON-based message exchanges.
    - Data Integrity and Authentication (JWS): Used to digitally sign objects exchanged between the SEPPs to provide authentication, data integrity, and non-repudiation.
    - Data Confidentiality (JWE): Used to encrypt objects, providing confidentiality and security for sensitive information transmitted between SEPPs.

Relevant 3GPP Specifications:

- **TS 33.501**, "Security architecture and procedures for 5G System." This specification includes detailed descriptions of the security features and mechanisms required to protect the signaling data exchanged between SEPPs, which are essential components in ensuring the overall security and integrity of the network.

Potential Quantum Threats:

- **HNDL:** This threat involves adversaries capturing encrypted SEPP-to-SEPP communications with the intent to decrypt them later once powerful quantum computers are available. The longevity and sensitivity of the data exchanged make this a critical risk, as data harvested now could still be valuable when quantum decryption becomes feasible.
- **Quantum Decryption:** Currently SEPP-to-SEPP communications rely on traditional encryption methods such as RSA or ECC for securing exchanges. These could be susceptible to decryption by quantum computers using Shor's algorithm. This poses a risk where future quantum computers could decrypt currently secure communications, potentially exposing sensitive network configuration and user data.
- **QMITM:** Where the attacker could modify or forge encrypted communications between SEPPs undetected. This could undermine the integrity and authenticity of the security protocols in place.

Current Cryptography Usage:

Current Methods: TLS 1.2/1.3, JOSE, JWE, JWT/SHA256

Specific Vulnerabilities:

- **TLS**: Most of the crypto suites supported within TLS 1.2 are based on ECC/Elliptic Curve Diffie-Hellman (ECDH) or RSA Diffie-Hellman key exchange, making it susceptible to HNDL attacks where encrypted data can be harvested now and potentially decrypted later with advanced quantum computing capabilities.
- **JOSE**: This is a framework for securing data using JSON-based data structures, including JWT. It heavily relies on RSA and ECC for key management and digital signatures, making it highly vulnerable to quantum attacks due to Shor's algorithm. The use of JWT hash functions such as SHA-256 is currently considered secure against quantum attacks. However, in alignment with CNSA 2.0 [14] guidance, transitioning to SHA-3 for enhanced resilience is recommended as part of a broader strategy to mitigate quantum threats. This is particularly relevant for algorithms like RS256 (RSA with SHA-256) and ES256 (ECDSA with P-256 and SHA-256), which remain susceptible to quantum-enabled HNDL attacks.

Security Protocol Updates:

SEPP-to-SEPP N32 interface communications are protected using HTTPS over HTTP/2.0 with mTLS 1.2/1.3. Thus the cryptographic suites used in TLS 1.3 must be updated to be compliant with PQC standards for both mutual authentication and key establishment. This ensures that SEPP communications remain secure against quantum computing threats.

In summary, the following upgrades are necessary for SEPP-to-SEPP communications to maintain robust security against future quantum threats:

1. Upgrade to use mTLS 1.3 (Mutual Transport Layer Security) with PQC-compliant crypto-suites (e.g., ML-KEM) for key establishment to secure SEPP-to-SEPP communications.
2. Upgrade the PKI systems to issue and manage certificates with PQC-compliant digital signature algorithms (e.g., ML-DSA) used for IPX client/server signing certificate to enhance the security of message authentication.
3. For JWS, although SHA-256 is believed to be quantum secure for the moment, transition to hash functions with larger security margins, such as SHA-384 or SHA512, should be part of the future planning.

These updates will ensure that SEPP-to-SEPP communications remain secure and resistant to quantum computing threats, maintaining the integrity and confidentiality of the 5G network.

Potential Challenges in Migration to Quantum-Safe Cryptography:

Migrating the SEPP-to-SEPP communications to QSC involves several potential challenges. These challenges can impact performance, compatibility, and overall network operations. Below are some key challenges that may arise during this migration:

- **Performance Impact**
  - Increased Computational Requirements: PQC algorithms generally require more computational resources than classical algorithms. This can lead to increased CPU usage and power consumption, especially in devices with limited processing capabilities. Implementing PQC may reduce throughput and increase latency, particularly in high-traffic scenarios.
- **Compatibility Issues**
  - Interoperability with Legacy Systems: Ensuring interoperability between PQC-enabled SEPPs and legacy systems that do not support PQC can be challenging. A hybrid approach, where both classical and quantum-resistant algorithms are supported, may be necessary during the transition period, complicating network management and increasing operational complexity.
- **IPX Provider Limitations**
  - Dependence on IPX Providers: SEPP-to-SEPP communications often rely on IPX providers for secure interconnectivity between different networks. Not all IPX providers may be ready to support PQC, leading to potential delays in the migration process. Coordination with IPX providers to ensure that they can support a hybrid approach to QSC is essential for a smooth transition.
  - Security Policy Misalignment: IPX providers may have their own security policies and cryptographic standards, which could differ from those required for QSC. Aligning these policies to ensure end-to-end security can be complex and require significant collaboration and negotiation.
- **Implementation and Management Complexity**
  - Complex Implementation Process: Migrating to PQC is not a straightforward process and involves updating multiple layers of network architecture. This includes updating protocols, key management systems, and security policies. The complexity of this process can lead to errors or misconfigurations, potentially exposing the network to security vulnerabilities.

Proposed Phased Implementation:

- **Phase 1:** Identify SEPP-to-SEPP communications that handle sensitive data and are vulnerable to quantum threats. This includes communications involving sensitive subscriber information and signaling data that are exchanged over various SEPP interfaces. Initially, focus on protecting these communications using TLS 1.3 with PQC-compliant cryptographic suites, such as ML-KEM for key establishment. Ensure that critical data exchanges, such as those between SEPPs in different network slices or geographical locations, are prioritized for early migration to quantum-safe cryptography.
- **Phase 2:** Upgrade the SEPP-to-SEPP interfaces responsible for carrying configuration and management information, which require high integrity and authenticity. Implement TLS 1.3, IKE/IPSec, or DTLS 1.3 with PQC-compliant digital signature algorithms to secure these communications. This includes updating the PRINS interface to incorporate PQC-compliant algorithms for both TLS and JOSE, ensuring robust protection of signaling messages, as well as enhancing key management systems to support quantum-safe key exchange and digital signatures, such as ML-DSA.
- **Phase 3:** Broader Integration of PQC for SEPP and IPX Interworking. Transition to hybrid cryptographic solutions that combine classical and PQC algorithms, ensuring backward compatibility while progressively introducing quantum-safe

measures. This hybrid approach is particularly important for ensuring interoperability across different operators and IPX providers during the transition phase.

- **Phase 4:** Full Transition to QSC
  - Complete migration to QSC
  - Where possible, plans should be made to decommission protocols using algorithms that have been deprecated.
  - Continuous performance and security validation after the full transition to QSC.
  - Post-migration support and maintenance such as patching vulnerabilities, updating cryptographic algorithms as needed, and responding to new security challenges.

5. CNSA 2.0 CONSIDERATIONS

The Commercial National Security Algorithm (CNSA) Suite 2.0 [14] is a set of cryptographic algorithms selected and recommended by the U.S. National Security Agency (NSA) for securing classified and sensitive information. It represents an update to the original CNSA Suite, reflecting advancements in cryptographic research and the evolving landscape of cybersecurity threats, including those posed by quantum computing.

Note: CNSA 2.0 updates and clarifications were published in the form of a Q&A on April 18, 2024 [14], which was prior to the publication of the NIST FIPS standards on PQC. When this report was written in late 2024, NIST indicated that AES-128 is safe from Grover's algorithm attacks by quantum computers for decades to come [1].

Algorithm	Function	Specification	Parameters
Advanced Encryption Standard (AES)	Symmetric block cipher for information protection	FIPS PUB 197	Use 256-bit keys for all classification levels.
ML-KEM (aka CRYSTALS-Kyber)	Asymmetric algorithm for key establishment	FIPS PUB 203	Use Category 5 parameter, ML-KEM1024, for all classification levels.
ML-DSA (aka CRYSTALS-Dilithium)	Asymmetric algorithm for digital signatures in any use case, including signing firmware and software.	FIPS PUB 204	Use Category 5 parameter, ML-DSA87, for all classification levels.
Secure Hash Algorithm (SHA)	Algorithm for computing a condensed representation of information	FIPS PUB 180-4	Use SHA-384 or SHA512 for all classification levels.
Leighton-Micali Signature (LMS)	Asymmetric algorithm for digitally signing firmware and software	NIST SP 800-208	All parameters approved for all classification levels. LMS SHA-256/192 is recommended.
Extended Merkle Signature Scheme (XMSS)	Asymmetric algorithm for digitally signing firmware and software	NIST SP 800-208	All parameters approved for all classification levels

Table 2: CNSA 2.0 Suite Considerations

Migrating 3GPP 5G standards for compliance with CNSA 2.0 involves several considerations:

AES-256 Symmetric Key Encryption:

- **Status**: AES-256 is part of the CNSA 2.0 Suite and is considered secure against quantum attacks when used in symmetric key encryption.
- **Usage in 5G**: AES-256 would need to be implemented in 5G networks for data encryption at various layers:
  - *User Plane Encryption:* Secure user data transmission between the UE and the 5G network.
  - *Control Plane Encryption:* Encrypt control signaling to protect signaling messages between the UE, base stations (gNB), and core NFs.
  - *Transport Network Layer Security:* Protects data in transit over backhaul and core networks.
- **Changes Required**: Replace any existing use of AES-128 with AES-256 to meet CNSA 2.0 compliance.

Public Key Cryptography and Key Exchange, Elliptic Curve Cryptography (ECC):

- **Status**: ECC, specifically algorithms like ECDH and ECDSA, are considered vulnerable to quantum attacks and are **not** CNSA 2.0 compliant.

Quantum-Resistant Alternatives:

- **Post-Quantum Key Encapsulation Algorithms**: Implement algorithms such as ML-KEM, designed to be secure against quantum attacks.
- **Post-Quantum Digital Signatures**: Replace ECDSA with post-quantum digital signature schemes like ML-DSA and SLH-DSA.

Changes Required:

- **Authentication Protocols**: Update the AKA protocols in 5G (such as 5G-AKA) to use QSC.
- **Digital Signatures**: Ensure that any digital signature schemes used in certificate-based authentication or integrity checks are updated to quantum-resistant algorithms.

Hash Functions

SHA-2 (SHA-256, SHA-384):

- **Status:** SHA-2 is part of CNSA 2.0 and is considered secure against quantum attacks for now. SHA-256 and SHA-384 can be used for integrity checks and HMACs

SHA-3:

- **Status:** At the time this report was written, CNSA had not approved SHA-3 as a hash algorithm.

Changes Required:

- **Integrity Protection**: Continue to use SHA-256 or SHA-384 for HMAC in integrity protection but plan for the potential future adoption of SHA-3 where appropriate.
- **Protocol Updates**: Ensure all cryptographic functions in protocols that rely on hashing (like IPSec, TLS, and application-level protocols) are capable of using SHA-256/SHA-384.

TLS:

- **TLS 1.3**: Ensure that all network elements use at least TLS 1.3, which supports more robust cryptographic algorithms and has eliminated older, insecure algorithms.
- **Post-Quantum TLS**: As quantum-resistant algorithms become standardized, update TLS configurations to include quantum-safe key exchanges and digital signatures.

Changes Required:

- **TLS Handshake**: Modify the TLS handshake process to use quantum-resistant key exchange algorithms and digital signatures.
- **PKI and Certificates**: Transition to quantum-resistant PKI to issue digital certificates that use quantum-resistant signatures.

IKEv2/IPSec:

- **IKEv2**: Update to support post-quantum key exchanges.
- **IPSec**: Use QSC encryption and integrity algorithms (AES-256 for encryption and SHA-3 for hashing).

Changes Required:

- **Protocol Negotiation**: Ensure that IKEv2 and other key exchange mechanisms can negotiate quantum-resistant algorithms.
- **PKI and Certificates**: In the case of certificate-based IPsec, transition to quantum-resistant PKI cryptography algorithms issued with digital certificates that use quantum-resistant signatures.

Summary of Specific 3GPP Protocol Adaptations for CNSA 2.0 compliance:

- **User Plane and Control Plane Encryption**: Update to AES-256 for all encryption tasks.
- **Authentication and Key Exchange**: Transition from ECC-based key exchanges to post-quantum algorithms like NIST ML-KEM.
- **Digital Signatures**: Replace ECDSA with quantum-resistant signatures like ML-DSA or in certain cases SLH-DSA.
- **Integrity Protection**: Utilize SHA-256, SHA-384, or SHA-3 for hashing and integrity checks.
- **TLS and IPSec**: Modify to support quantum-safe key exchanges and certificates.

By making these changes, 5G networks will be compliant with CNSA 2.0 and prepared for a future where quantum computing could threaten traditional cryptographic security.

6. RECOMMENDATIONS FOR 3GPP

STAGES FOR MIGRATION TO QUANTUM-SAFE CRYPTOGRAPHY:

To enable an effective transition to QSC across the 3GPP standards for devices, RAN, Core Network, and Interconnect Network, the following recommendations outline prioritized actions to implement quantum-resistant cryptography. These priorities are designed to address critical vulnerabilities and threats posed by CRQC while ensuring a coordinated and seamless approach across these domains. It is recommended that 3GPP specify support for quantum-resistant cryptographic mechanisms in its future specifications, ensuring that standardized security frameworks align with evolving quantum threats. By embedding these priorities into the 3GPP standardization roadmap, the industry can proactively safeguard 5G infrastructure and beyond against emerging quantum threats.

Priority 1: Addressing HNDL Attack Vulnerabilities

Given the nature of HNDL attacks, where adversaries capture encrypted data with the intention of decrypting it once powerful quantum computers are available, the focus should be on enhancing encryption methods to remain secure both now and in the future. Here are recommendations to the 3GPP specifications to protect the user and control plane from such attacks. The standards should consider:

- Considering the requirements outlined in CNSA 2.0, the adoption of AES-256 into 3GPP specifications should be evaluated as a future-proof option. AES-256 offers increased resilience against quantum attacks and aligns with evolving security frameworks. Reassessing and potentially expediting the adoption of AES-256 should be considered, given the long-term implications of HNDL attacks and the potential for quantum computing capabilities to evolve beyond the current projected security lifespan of AES-128.
- Prioritize the adoption of quantum-resistant key encapsulation mechanisms, such as ML-KEM, to securely exchange key material to establish a shared secret for classical symmetric encryption algorithms like AES. This ensures protection against HNDL attacks by safeguarding key exchange processes from future quantum threats.
- Allowing for hybrid cryptographic approaches that combine classical (E.g. ECDHE) and or PQC (ML-KEM) algorithms. This ensures backward compatibility with legacy cryptographic systems while enabling a seamless transition for critical network components to adopt quantum-resistant solutions while maintaining interoperability with existing infrastructure.

Device/UE:

- Specify quantum-resistant key encapsulation (e.g. ML-KEM) for SUPI protection with optional support for hybrid cryptography (e.g. ECIES with ML-KEM).
- Support for AES-256 should be considered for SUPI protection.

RAN/Core Network:

- Support for quantum-resistant cryptographic algorithms (e.g. ML-KEM) for key encapsulation as part of IKEv2/IPsec and DTLS protection toward the Core NFs (UPF, AMF) over N3 and N2 interfaces, respectively, and in the gNBs (CU-DU in split RAN architecture) to protect the F1 interface.

  Note: During this period, any use case that requires digital signatures can exist using existing classical algorithms.

Core Network:

- Specify one or more quantum-resistant algorithms (e.g. ML-KEM) to be used for key encapsulation within TLS1.3/DTLS and NDS/IP (IKEv2/IPSec) to secure SBI and non-SBI interfaces that carry highly confidential data (e.g., subscriber data, session keys, call details) that are vulnerable to HNDL attacks.
- SUCI de-concealment process should support the use of quantum-resistant key encapsulation (e.g. ML-KEM) and optionally support hybrid cryptography (e.g. ECIES with ML-KEM).
- Additionally, support for AES-256 should be considered.

Interconnect Network:

- Support for quantum-resistant cryptographic algorithms (e.g., ML-KEM) as key establishment between the SEPPs and use of AES-256 (if implementation allows) for confidentiality protection of the control and forwarding planes (N32-C, N32-F interfaces).

Priority 2: Expanding QSC to Critical Communication Paths

The focus of this next phase is to expand QSC to critical communication paths, with a particular focus on protecting the signature and authentication mechanisms across the 5G domains. This involves securing key channels and nodes against quantum-enabled attacks such as impersonation (e.g., forging identities using broken public keys), spoofing (e.g., injecting false data into control channels), and tampering attacks (e.g., altering encrypted communications in transit). 3GPP standards should consider:

- Implementation of PKI that is capable of issuing and managing the lifecycle of PQC certificates used as part of mutual authentication between network entities.
- Support for quantum-resistant digital signature algorithms (e.g. ML-DSA) to be used for signature generation and validation as well as classical/quantum-resistant hashing algorithms (e.g. SHA-256, SHA-384)
- Allowing for hybrid PKI cryptographic approaches that combine classical and or PQC algorithms (e.g ECDSA, ML-DSA). This ensures backward compatibility with legacy cryptographic systems while enabling a seamless transition for critical network components to adopt quantum-resistant solutions while maintaining interoperability with existing infrastructure.

Device/UE:

- Support NEA-256 and NIA-256 algorithms based on AES/SNOW 3G as an option when specified by 3GPP for providing confidentiality and integrity protection, respectively, on the RRC control plane, user plane, and NAS messaging.
- Upgrade algorithms and procedures used as part of the UE authentication procedure (e.g., 5G-AKA, EAP-AKA') to support larger key sizes in addition to TUAK with 256 bit and specify MILENAGE-256 as an additional option.

RAN Network:

- Specify PQC (e.g., ML-DSA) for digital signatures between gNB and Core NFs (UPF, AMF) and CU-DU in split RAN architecture as part of IKEV2/IPsec.

Core Network:

- Protection of SBI interfaces and non-SBI (e.g. PFCP/N4 interface) that carry configuration information using TLS 1.3 with PQC-compliant digital signature algorithms (e.g., ML-DSA), to ensure integrity, authenticity, and non-repudiation.
- Specify PQC-compliant digital signature algorithm (e.g., ML-DSA) for JSON Web Signature (JWS) as part of OAuth 2.0 token and Client Credential Assertion (CCA).

Interconnect Network:

- Specify PQC-compliant digital signature algorithms (e.g., ML-DSA) on SEPP-to-SEPP interfaces handling configuration and management information.
- Specify the use of PQC-compliant digital signature algorithm (e.g., ML-DSA) for JWS to protect JSON objects that are modified by the IPX intermediaries when using the PRINS mode.

Continuous Monitoring and Improvement

In the evolving landscape of quantum computing and cryptographic security, it is critical for 3GPP standardization to incorporate continuous monitoring of PQC protocols at every stage of its development and implementation. PQC algorithms are still relatively new, so ongoing scrutiny is required to identify potential vulnerabilities or inefficiencies that may emerge in their real-world applications. Regular evaluations will ensure that any weaknesses are addressed promptly, maintaining the integrity and reliability of the cryptographic solutions adopted for securing 5G infrastructure.

Equally important is the need to monitor advancements in quantum computing technologies, particularly breakthroughs that could accelerate the development of CRQCs. These advancements may compress the projected timeline for when current cryptographic protocols become vulnerable. Additionally, the discovery or refinement of quantum algorithms could potentially reduce the computational requirements (e.g., qubit count or fidelity) to break existing cryptographic standards sooner than anticipated. Such developments would necessitate revisiting migration timelines and reprioritizing areas of the 3GPP architecture for earlier transitions to quantum-safe alternatives.

By continuously assessing these variables — emerging quantum capabilities, the effectiveness of PQC protocols, and evolving threat landscapes — 3GPP can ensure that its standardization efforts remain proactive and adaptive. This vigilance is essential for maintaining the security and resilience of telecommunications networks in the face of quantum-era challenges, allowing standardization priorities to evolve in alignment with the latest risks and technological realities.

Summary

The transition to QSC across the 3GPP 5G network represents a vital proactive measure against the potential risks posed by quantum computing advancements. This report provides a structured approach for a prioritized phased migration to enhance the cryptographic resilience of the device/UE, RAN, Core Network, and Interconnect Network. The recommendations are aimed at addressing immediate vulnerabilities, particularly those associated with HNDL attacks, and preparing for broader security enhancements through the integration of quantum-resistant algorithms.

By methodically upgrading to QSC, 3GPP 5G networks can ensure the integrity, confidentiality, and availability of communications against both current and future quantum threats, thereby maintaining trust and compliance with emerging security standards. This phased transition emphasizes the use of hybrid cryptographic implementations, combining classical and quantum-resistant algorithms to ensure interoperability, seamless operations, and support backward compatibility during the migration. Over time, this approach will support the gradual phase-out of algorithms that are not quantum-safe, aligning with global security frameworks and minimizing disruptions to critical infrastructure while enhancing the network's overall security posture in the quantum computing era.

7. ACRONYMS AND ABBREVIATIONS

AES	Advanced Encryption Standard
AF	Authentication Framework
AH	Authentication Header
AKA	Authentication and Key Agreement
AKMA	Authentication and Key Management for Applications
AMF	Access Management Function
AUSF	Authentication Server Function
CA	Certificate Authority
CDR	Charging Data Records
CHF	Charging Function
CNSA	Commercial National Security Algorithm
CRQCs	Cryptographic Relevant Quantum Computers
CUs	Centralized Units
DHE	Diffie–Hellman Key Exchange
DTLS	Datagram Transport Layer Security
DUs	Distributed Units
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
ECDHE	Elliptic Curve Diffie Hellman Ephemeral
ECDSA	Elliptic Curve Digital Signature Algorithm
ECIES	Elliptic Curve Integrated Encryption Schemes
ESP	Encapsulating Security Payload
FIPS	Federal Information Processing Standards
FN-DSA	FFT (fast-Fourier transform) over NTRU-Lattice-Based Digital Signature Algorithm
gNB	gNodeB
GTP	Generic Tunneling Protocol
HMACs	Hash-Based Message Authentication Codes
HNDL	Harvest-Now, Decrypt Later
IKE	Internet Key Exchange
IoT	Internet of Things
IP	Internet Protocol
IPsec	Internet Protocol Security
IPsec SAs	Internet Protocol Security Associations
IPX	Internet Protocol Exchange
IPX	Internetwork Packet Exchange
JOSE	JavaScript Object Signing and Encryption
JWE	JSON Web Encryption
JWS	JSON Web Signature
JWT	JSON Web Token
KA	Key Agreement

KDFs	Key Derivation Functions
LGE	Long Term Evolution
LMS	Leighton-Micali Signature
LWE	Learning with Errors
MITM	Man-In-The-Middle
ML-DSA	Module Lattice-Based Digital Signature Algorithm
ML-KEM	Module Lattice-Based Key Encapsulation Mechanism
MNOs	Mobile Network Operators
mTLS	Mutual Transport Layer Security
NAS	Non-Access Stratum
NDS	Network Domain Security
NEA	Network Encryption Algorithms
NEF	Network Exposure Function
NF-C	Network Function Consumer
NF-NF	Network Function to Network Function
NF-P	Network Function Producer
NIA	Network Integrity Algorithms
NIST	National Institute of Standards and Technology
NRF	Network Repository Function
PDCP	Packet Data Convergence Protocol
PFCP	Packet Forwarding Control Protocol
PKI	Public Key Infrastructure
PoC	Proof of Concept
PRINS	PRotocol for N32 INterconnect Security
PQC	Post Quantum Cryptography
PSK	Pre-Shared Key
QMITM	Quantum Man-in-the-Middle
QoS	Quality of Service
QRC	Quantum-Resistant Cryptography
QSC	Quantum-Safe Cryptography
QSCA	Quantum Side Channel Attack
RAN	Radio Access Network
RBG	Random Bit Generator
RRHs	Remote Radio Heads
RSA	Rivest-Shamir-Adleman
RUs	Radio Units
SA	Security Association
SBAs	Service-Based Architecture
SBIs	Service-Based Interfaces
SCTP	Stream Control Transmission Protocol
SEG	Security Gateway
SEPP	Security Edge Protection Proxy
SHA	Secure Hash Algorithm
SIDF	Subscriber Identifier De-Concealment Function

SIS	Short Integer Solution
SLH-DSA	Stateless Hash-Based Digital Signature Algorithm
SMC	Security Mode Command
SMF	Session Management Function
SON	Self-Organizing Networks
SPHINCS+	Stateless Practical Hash-based Incredibly Nice Cryptographic Signature
SUCI	Subscription Concealed Identifier
SUPI	Subscription Permanent Identifier
TLS	Transport Layer Security
TS	Technical Specification
UDM	Unified Data Management
UDP	User Datagram Protocol
UE	User Equipment
UMTS	Universal Mobile Telecommunications Service
UP	User Plane
UPE	User Plane Encryption
UPF	User Plane Function
UPI	User Plane Integrity
USIM	Universal Subscriber Identity Module
XMSS	Extended Merkle Signature Scheme

8. REFERENCES

[1] National Institute of Standards and Technology (NIST). Post Quantum Cryptography FAQs, https://csrc.nist.gov/projects/post-quantum-cryptography/faqshttps://csrc.nist.gov/projects/post-quantum-cryptography/faqs

[2] ATIS, Implications of Entropy on Symmetric Key Encryption Resilience to Quantum: https://atis.org/resources/implications-of-entropy-on-symmetric-key-encryption-resilience-to-quantum/

[3] UK National Cyber Security Centre, On the practical cost of Grover for AES key recovery: https://csrc.nist.gov/csrc/media/Events/2024/fifth-pqc-standardization-conference/documents/papers/on-practical-cost-of-grover.pdf

[4] NIST. Post-Quantum Cryptography, https://csrc.nist.gov/projects/post-quantum-cryptographyhttps://csrc.nist.gov/projects/post-quantum-cryptography

[5] NIST. (2023). FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard, https://csrc.nist.gov/pubs/fips/203/finalhttps://csrc.nist.gov/pubs/fips/203/final

[6] NIST. (2023). FIPS 204: Module-Lattice-Based Digital Signature Standard, https://csrc.nist.gov/pubs/fips/204/finalhttps://csrc.nist.gov/pubs/fips/204/final

[7] NIST. (2023). FIPS 205: Stateless Hash-Based Digital Signature Standard, https://csrc.nist.gov/pubs/fips/205/finalhttps://csrc.nist.gov/pubs/fips/205/final

[8] 3GPP TS 33.501. "Security Architecture and Procedures for 5G System."

[9] 3GPP TS 33.310. "Network Domain Security (NDS); Authentication Framework (AF)."

[10] 3GPP TS 33.210. "Network Domain Security (NDS); IP network layer security."

[11] 3GPP TS 38.470. "NG-RAN; F1 general aspects and principles.", https://www.3gpp.org/ftp/Specs/archive/38_series/38.460/38460-i00.zip

[12] 3GPP TS 38.460. "NG-RAN; E1 general aspects and principles." https://www.3gpp.org/ftp/Specs/archive/38_series/38.460/38460-i00.zip

[13] IETF - TLS 1.2 is in Feature Freeze , https://www.ietf.org/archive/id/draft-ietf-tls-tls12-frozen-00.html

[14] NSA. (2024). " The Commercial National Security Algorithm Suite 2.0 and Quantum Computing FAQ," https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/1/CSI_CNSA_2.0_FAQ_.PDF

ACKNOWLEDGEMENTS

Contributors:

Ian Deakin , ATIS

Spondon Dey, AT&T

William Trost, AT&T

Hisham Sarhan, Ericsson

John Strassner, Futurewei

Martin McGrath, Nokia

Vinod Choyi, Verizon

COPYRIGHT AND DISCLAIMER

ATIS-I-0000101

Published February 2025

Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER, NO REPRESENTATION OR WARRANTY IS MADE OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

www.atis.org

For information, contact ATIS at (202) 628-6380.