Quantum-safe Cryptography for 4G and 5G Roaming

Version 1.0

26 June 2025

Security Classification: Non-confidential

Access to and distribution of this document is restricted to the persons permitted by the security classification. This document is subject to copyright protection. This document is to be used only for the purposes for which it has been supplied and information contained in it must not be disclosed or in any other way made available, in whole or in part, to persons other than those permitted under the security classification without the prior written approval of the Association.

Copyright Notice

Disclaimer

The GSM Association ("Association") makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

Compliance Notice

The information contain herein is in full compliance with the GSM Association's antitrust compliance policy.

Table of Contents

1 Introduction

The GSMA PQTN Task Force has published a series of documents about the impact of Post Quantum Cryptography (PQC) on telecoms.

This document is an extension of PQ.03 v2 - Quantum Safe User Cases and Migration [1] and address 4G and 5G the roaming.

1.1 Overview

3GPP and GSMA have developed a standardised roaming architecture, specifications and requirements for use-cases where a UE roams from its Home PLMN (HPLMN) to a Visited PLMN (VPLMN) and vice-versa. This document provides an overview of threats, impacts and mitigation mechanisms against a Cryptographically Relevant Quantum Computer (CRQC) targeting the roaming architecture and its interfaces.

1.2 Scope

This document covers mechanisms that may be employed to protect UEs and operator networks from a CRQC when a UE roams between HPLMN and VPLMN and connects to the visitor network. The roaming architecture considers the scenarios where a Security Edge Protection Proxy (SEPP) is responsible for protecting the operator's core network from attacks targeting (or originating from) the inter-connect interfaces (N32-c, N32-f). The interfaces may be secured using either:

1. Direct TLS between SEPPs
2. PRotocol for N32 INterconnect Security (PRINS)

Diameter inter-connect security is included in the analysis: when a 5G UE connects to a 4G roaming network and vice-versa.

1.3 Abbreviations.

Term	Description
3GPP	Third Generation Partnership Program
CDR	Call Data Record
CRQC	Cryptologically relevant quantum computer
DEA	Diameter Edge Agent
DoS	Denial of service
DRA	Diameter Relay Agent
ECDHE	Elliptic Curve Diffie-Hellman Ephemeral
GSMA	GSM Association
GTP-U	GPRS Tunnelling Protocol User Plane
HNDL	Harvest Now Decrypt Later
HPLMN	Home PLMN

Term	Description
hSEPP	Home SEPP (Security Edge Protection Proxy)
IMS	IP Multimedia Subsystem
IPUPS	Inter-PLMN User Plane Security
IPX	IP exchange
JWE	JSON Web Encryption
JWS	JSON Web Signature
MITM	Man in the middle
ML-DSA	Module-Lattice-Based Digital Signature Algorithm
ML-KEM	Module-Lattice-Based Key-Encapsulation Mechanism
NDS/IP	Network Domain Security for IP based protocols
OCSP	Online Certificate Status Protocol
PDU	Protocol Data Unit
PGW	Packet Data Network Gateway
PKI	Public Key Infrastructure
PLMN	Public Land Mobile Network
PRINS	PRotocol for N32 INterconnect Security
RSA	Rivest-Shamir-Adleman
RTP	Real-time Transport Protocol
SBI	Service Based Interface
SEPP	Security Edge Protection Proxy
SGW	Serving Gateway
SIP	Session Initiation Protocol
SRTP	Secure RTP
TEID	Tunnel End-Point Identifier
TLS	Transport Level Security
UE	User Equipment
UPF	User Plane Function
VoLTE	Voice over LTE
VoNR	Voice over New Radio
VPLMN	Visited PLMN
vSEPP	Visited SEPP (Security Edge Protection Proxy)

Table 1 Abbreviations

1.4 References

Ref	Doc Number	Title
[1]	PQ.03 v2	Post Quantum Cryptography – Guidelines for Telecom Use Cases, GSMA PQTN, PQ.03 Version 2.0, 04 Oct 2024
[2]	RFC 8446	The Transport Layer Security (TLS) Protocol Version 1.3, RFC 8446, IETF, Aug 2018 https://datatracker.ietf.org/doc/html/rfc8446
[3]	TS 23.501	System architecture for the 5G System (5GS)
[4]	TS 33.501	Security architecture and procedures for 5G system
[5]	NG.113	Official Document NG.113 5GS Roaming Guidelines, Version 11.0 October 2024, GSMA,
[6]	IR.34	Official Document IR.34 - Guidelines for IPX Provider networks (Previously Inter-Service Provider IP Backbone Guidelines), Version 13.0 October 2016, GSMA
[7]	TS 33.210	Network Domain Security (NDS); IP network layer security
[8]	TS 33.310	Network Domain Security (NDS); Authentication Framework (AF)
[9]	RFC 7516	JSON Web Encryption (JWE), RFC 7516, May 2015, IETF https://datatracker.ietf.org/doc/html/rfc7516
[10]	RFC 7515	JSON Web Signature (JWS), RFC 7515, May 2015, IETF https://datatracker.ietf.org/doc/html/rfc7515
[11]	IR.88	Official Document IR.88 - EPS Roaming Guidelines. Nov 2021, GSMA
[12]	IR.92	Official Document IR.92 IMS Profile for Voice and SMS, June 2024, GSMA
[13]	NG.114	NG.114 IMS Profile for Voice, Video and Messaging over 5GS, Jan 2024, GSMA
[14]	X.509	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, RFC 5280, May 2008, IETF https://datatracker.ietf.org/doc/html/rfc5280
[15]	FIPS 203	National Institute of Standards and Technology (2024) Module-Lattice-Based Key-Encapsulation Mechanism Standard. (Department of Commerce, Washington,D.C.), Federal Information Processing Standards Publication (FIPS) NIST FIPS 203. https://doi.org/10.6028/NIST.FIPS.203 (Accessed 2025-02-17)
[16]	FIPS 204	National Institute of Standards and Technology (2024) Module-Lattice-Based Digital Signature Standard. (Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) NIST FIPS 204.

Ref	Doc Number	Title
		https://doi.org/10.6028/NIST.FIPS.204 (Accessed 2025-02-17)
[17]	FIPS 205	National Institute of Standards and Technology (2024) Stateless Hash-Based Digital Signature Standard. (Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) NIST FIPS 205. https://doi.org/10.6028/NIST.FIPS.205 Accessed 2025-02-17
[18]	FS.40	Official Document FS.40 - 5G Security Guide, July 2024, GSMA
[19]	FS.36	FS.36 – 5G Interconnect Security
[20]	RFC 7518	JSON Web Algorithms (JWA), RFC 7518, May 015, IETF https://datatracker.ietf.org/doc/html/rfc7518
[21]	RFC 7519	JSON Web Token (JWT), RFC 7519, May 2015, IETF https://datatracker.ietf.org/doc/html/rfc7519
[22]	RFC 4210	Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP), TFC 4210, May 2005, IETF https://datatracker.ietf.org/doc/html/rfc4210
[23]	RFC 9509	X.509 Certificate Extended Key Usage (EKU) for 5G Network Functions, RFC 9509, Mar 2024, IETF https://datatracker.ietf.org/doc/html/rfc9509
[24]	TS 23.401	E-UTRAN access, TS 23.401, 3GPP
[25]	TS 23.402	Architecture enhancements for non-3GPP accesses, TS23.402, 3GPP
[26]		ML-KEM Post-Quantum Key Agreement for TLS 1.3, Oct 2024 https://datatracker.ietf.org/doc/draft-ietf-tls-mlkem/
[27]		Post-Quantum Key Encapsulation Mechanisms (PQ KEMs) for JOSE and COSE, Nov 2024 https://datatracker.ietf.org/doc/html/draft-ietf-jose-pqc-kem-01
[28]	RFC 8784	Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security, RFC 8784 June 2020, IETF https://datatracker.ietf.org/doc/rfc8784/
[29]		Post-quantum hybrid ECDHE-MLKEM Key Agreement for TLSv1.3, Sep 2024, draft-ietf-tls-ecdhe-mlkem-00

Ref	Doc Number	Title
		https://datatracker.ietf.org/doc/draft-ietf-tls-ecdhe-mlkem/
[30]		Post-quantum Hybrid Key Exchange with ML-KEM in the Internet Key Exchange Protocol Version 2 (IKEv2), Apr 2025, draft-kampanakis-ml-kem-ikev2-09 https://datatracker.ietf.org/doc/draft-kampanakis-ml-kem-ikev2/
[31]		X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, RFC 6960, DOI 10.17487/RFC6960, June 2013, IETF https://www.rfc-editor.org/info/rfc6960

Table 2 References

2 Executive Summary

2.1 Migration Plan

A threat actor may use a CRQC when available, to decrypt messages transported between mobile operators when a UE roams. The attacker may be an un-authorized Man-in-the-Middle (MITM) or a compromised entity with access to the roaming intermediaries that can harvest the messages (e.g. IPX providers). Since the messages carry subscriber information (including session keys, profile, call data, CDRs, etc.) data leakage may impact the privacy of subscribers. Internal network function deployment and identifiers may be exposed to attackers, which can be used to perform secondary attacks (e.g. DoS). Networks should protect the roaming interfaces using PQC-compliant key encapsulation mechanisms (e.g. ML-KEM [15]) in order that the interfaces remain protected both from classical as well as from CRQC.

Impersonation, spoofing and tampering attacks on the roaming interface may cause service degradation, stealing of services and even Denial-of-Service. Quantum safe (e.g. ML-DSA [16]) certificates and signature generation and verification capabilities must be built into the roaming entities.

2.2 Migration Prioritization

Mitigation against Harvest Now Decrypt Later (HNDL) attacks are more immediate, it is imperative to specify the use of quantum-safe key encapsulation (e.g. ML-KEM) as part of TLS1.3 [2] for protecting the n32 interfaces.

Mutual authentication, authorization and integrity are the building blocks for securing the roaming interfaces. The threat posed by CRQC is not considered immediate and they are not the highest priority.

Building the trust framework for authentication and authorization takes time and therefore immediate work must be carried out for building the trust framework including the Public Key Infrastructure (PKI).

3 Standards

3.1 3GPP Standards

3GPP created technical specifications TS 23.501 [3] and associated specifications that describe a high-level roaming architecture as well as network functions and interfaces for roaming. In TS 33.501 [4], it provides guidance for developing 5G security architecture, including secure roaming architectures and interconnect networks. It also provides security requirements and details on the protocols for securing the n32 interfaces. The n32-c is used for establishing security context between the partners, by means of the Security Edge Protection Proxy (SEPP). The security context is then used for securing the n32-f, the forwarding plane. An NF (e.g. AMF) in one operator network would use the n32-f interface for communicating with an NF (e.g. AUSF) in another operator network.

The security architecture depends on the roaming partners involved, which may vary and may involve the use of intermediaries (e.g. IPX providers). 3GPP describes two security mechanisms for securing the interfaces. The two modes are: Direct TLS and Protocol for N32 Inter-connect Security (PRINS).

3.2 GSMA Recommendations & Guidelines

GSMA developed NG.113 5GS roaming guidelines [5], based on the roaming architectures and requirements specified by 3GPP, which detail the technical requirements, architectures, procedures, call flows for the control and user plane, and the security architectures for deployment. It also describes four models of SEPPs, some of which enable a mobile operator to provide the N32-endpoint to an operator or on behalf of another operator. The detailed designs of different security architectures for the deployment models are described to enable different protection schemes.

4 Roaming Use-cases

4.1 5G Roaming Architecture

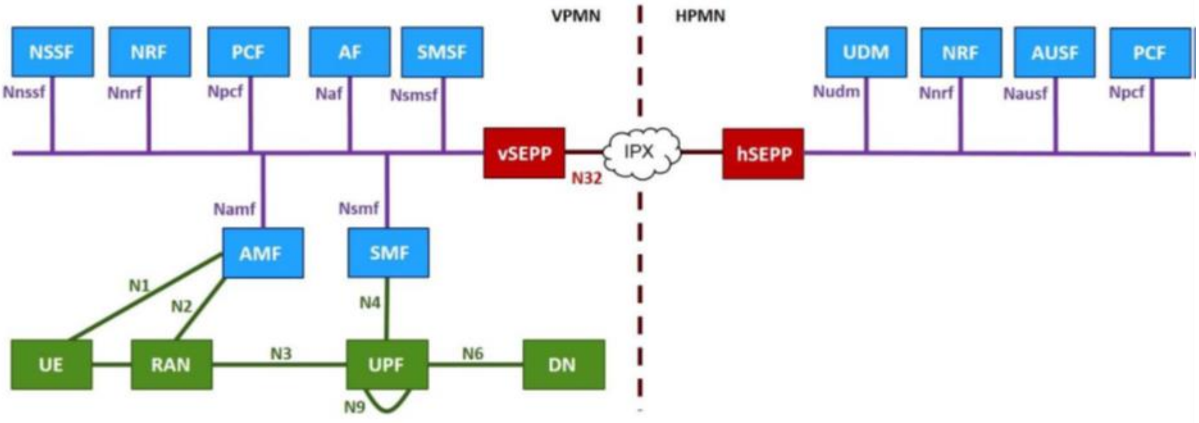


Figure 1 Roaming Architecture – Source: TS 23.501 (Local Breakout)

The SEPP acts as the roaming firewall for 5G roaming interfaces between PLMNs over the N32 interface. The N32 interface is used by the SEPPs to communicate HTTP/2 application-level control plane messages between operators. The N32 interface consists of the N32-c (control), that is used to perform handshake between the SEPPs and the N32-f performs the forwarding of the NF control plane messages using the security parameters that had been established as part of the N32-c handshake procedure. The SEPP performs security actions based on protection profiles configured by the PLMNs and is responsible for enforcing the protection policies that have been agreed upon with the roaming partners. The protection policies may include the confidentiality and integrity protection of information elements exchanged between the PLMNs.

4.1.1 Direct TLS

Direct TLS mode is used when there are no intermediaries (e.g. IPX) between the two operators. The SEPPs perform mutual TLS authentication and negotiate cipher-suites and key management to secure the N32-f messages based on agreed protection policies.

Hop-by-Hop TLS may be used between an operator and one or more intermediate roaming entity (e.g. IPX, roaming hub) and another operator. TLS 1.2 or 1.3 enable secure connections in a hop-by-hop manner, using X.509 certificates for authentication. The intermediaries are privy to the signaling messages carried over N32, since they decrypt and then re-encrypt the messages for each hop.

4.1.2 Protocol for N32 Interconnect Security (PRINS)

A SEPP uses the PRINS mode when there are roaming intermediaries (e.g. IPX) present between the operators. The roaming intermediaries may be allowed to modify the application layer messages based on policies and therefore the SEPPs shall be able to verify the validity and integrity of the modification performed by the intermediaries. Additional transport mechanisms may be used for communications between the SEPP and the roaming intermediaries that includes NDS/IP [7, 8] and TLS VPN.

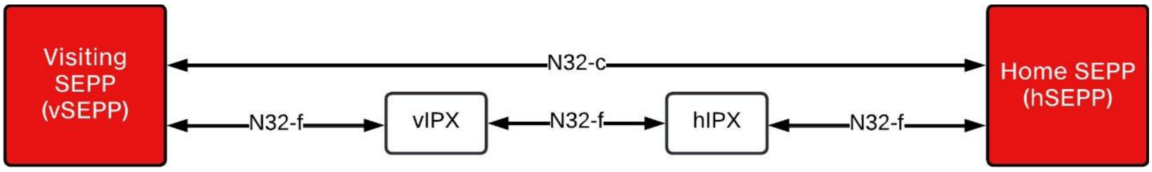


Figure 2PRINS control and forwarding interfaces

The SEPPs rely on JSON Web Encryption (JWE) [9] for encrypting attributes deemed to be confidential. The JWE Authenticated Encryption with Associated Data (AEAD) algorithm generates JWE encrypted text (ciphertext) and a JWE authentication tag (Message Authentication Code).

The roaming intermediaries use JSON Web Signature (JWS) [10] to provide authentication and integrity for the modifications performed by them.

4.1.3 Inter-PLMN User Plane Security

The Inter-PLMN User Plane Security (IPUPS) function is used to enforce GTP-U security on the N9 interface between UPFs of home and visited PLMNs when using home routed mode [4]. The N9 interface can be protected using NDS/IP, where X.509 certificates [14] are used for mutual authentication between the home UPF (hUPF) and the visiting UPF (vUPF) and uses IKEv2 / IPSec Encapsulated Security Payload (ESP) for integrity, authenticity and confidentiality. In addition to protecting the N9 interface, the IPUPS is required to discard malformed GTP-U packets and forward only those packets that contain a valid Tunnel End-Point Identifier (TEID) that belongs to an active PDU session.

4.2 4G Roaming

A Diameter Edge Agent (DEA) is the entry and exit point between mobile network operators' networks [11]. For 4G roaming, only the relay agent, the proxy agent and the translation agent are relevant. A Diameter Relay Agent (DRA) is responsible for forwarding Diameter messages. A Diameter proxy has the capability to process non-routing related Attribute Value Pairs (AVP) and can inspect the actual contents of the message to perform admission control, policy control etc. A Diameter proxy is application aware and maintains states of downstream peers to enforce resources usage, provide admission control and provisioning.

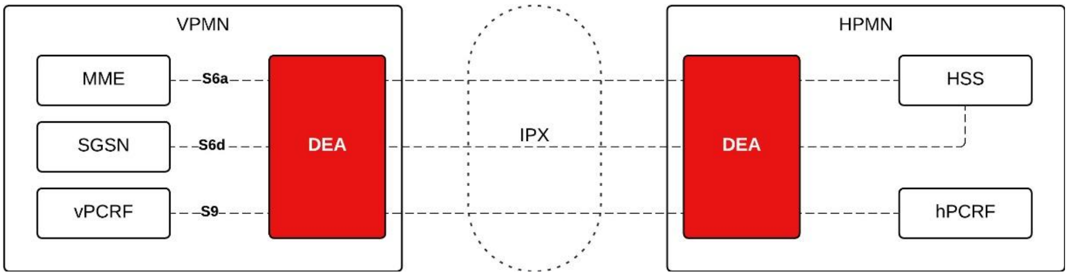


Figure 34G Diameter Edge Agent Architecture

The DEA is mainly used for route addressing and forwarding of Diameter signaling, including mobility management, charging policy, and charging information about roaming users, for control / signaling plane messages transmitted over the S6a, S6d, and S9 interfaces.

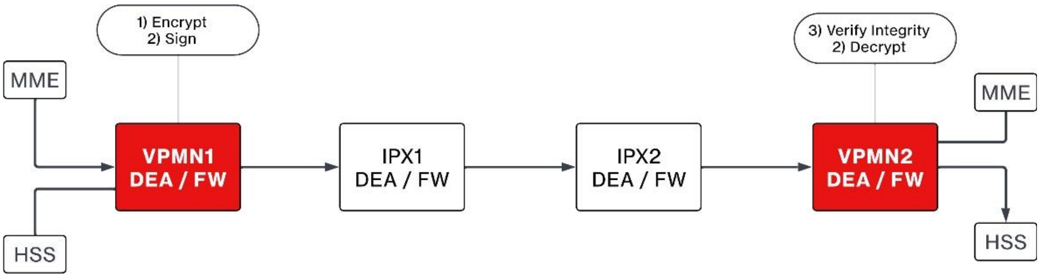


Figure 44G Diameter network entity interactions

The Diameter messages exchanged between service providers do not provide integrity or confidentiality protection by default. Therefore IPSec / TLS, specified as part of NDS/IP is used to provide hop-by-hop protection (no end-to-end protection is provided).

There is no 3GPP requirement to protect the user plane traffic over the S8 interface between a SGW in one operator network to a PGW in another roaming partner network in a home-routed scenario. The traffic therefore is only expected to be protected at the application layer without any network or transport layer protections and therefore considered out-of-scope here.

VoNR / VoLTE Roaming

VoNR [13] and VoLTE [12] roaming are enabled through the IP Multimedia Subsystem (IMS), where SIP is used for signaling and RTP/SRTP for media transport. In typical deployments, the S8 Home-Routed (S8HR) architecture is used, anchoring both signaling and media in the Home PLMN (HPLMN) via the IPX interconnect. Control plane signaling traverses interfaces such as S6a/Nh between the Visited PLMN (VPLMN) and HPLMN, while the user plane is established through the S8 or N9 interface, depending on whether the UE is in LTE or 5G SA/NSA. Dedicated Quanity of Service (QoS) bearers (e.g., QCI 1 for voice, QCI 5 for signaling) are used for voice sessions.

Quantum-specific risks in VoNR/VoLTE roaming:

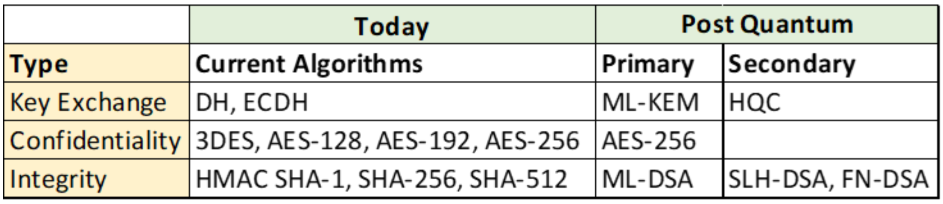
- The susceptibility of signaling and media traffic to Harvest Now, Decrypt Later (HNDL) attacks, especially when key exchanges use classical algorithms such as ECDHE or RSA.

3. Authentication vectors transmitted over Diameter (S6a) or HTTP/2 interfaces may be targeted by future quantum adversaries, compromising user privacy and allowing impersonation.

   - To mitigate these risks, PQC-based key encapsulation mechanisms such as ML-KEM should be integrated into TLS sessions securing SIP and Diameter transport. Hybrid key exchange may provide a transitional safeguard. Symmetric encryption algorithms used for SRTP and user plane protection should use quantum-safe algorithms such as AES.

- During VoLTE or VoNR sessions, IPSEC sessions are established to ensure confidentiality and integrity protection. The IMS AKA procedure is used during these IPSEC sessions. The IMS AKA procedure relies on keys stored on the SIM card and the AuC/AUSF on the HSS/UDM. During the establishment of the IMS IPSEC tunnel, quantum-secured algorithms should be employed, and support for multiple algorithm options should be provided.
- In VoLTE/VoNR for key exchange, DH (Diffie-Hellman) or ECDH (Elliptic Curve Diffie-Hellman) algorithms are currently used. These should be replaced with ML-KEM or HQC (Hamming Quasi-Cyclic) once standardsed.
- For encryption, 3DES or AES algorithms are used in VoLTE/VoNR, with AES being highly recommended.
- For integrity control and signature, HMAC or SHA algorithms can be utilized. In the post-quantum era, ML-DSA (FIPS 204) [16] or SLH-DSA (FIPS 205) [17] algorithms should be used. Considering the computational power requirements on the terminal side, ML-DSA is highly recommended. FN-DSA may be added to the list once standardised. Other DSA algorithms necessitate larger key sizes, which could be inefficient for mobile terminals today.

A summary table is given below.



	Today	**Post Quantum**	
Type	**Current Algorithms**	**Primary**	**Secondary**
Key Exchange	DH, ECDH	ML-KEM	HQC
Confidentiality	3DES, AES-128, AES-192, AES-256	AES-256	
Integrity	HMAC SHA-1, SHA-256, SHA-512	ML-DSA	SLH-DSA, FN-DSA

Table 3 Proposed Cryptographic Suites for Post Quantum Security

5 Scope

The roaming interfaces carry subscriber profile information as well as subscriber authentication data and session keys. The roaming interfaces are protected using TLS 1.3 and / or IPSec based on mutual authentication using X.509 certificates.

The N32 interface uses X.509 certificates for mutual authentication and uses JWS for integrity and authentication of the JSON payload added by the intermediaries in the PRINS mode. Attacks by a CRQC against integrity and authentication are not considered to be an imminent threat, when a CRQC becomes available, it could launch tampering as well as impersonation attacks between roaming partners.

5.1 Sensitive Data Discovery

5.1.1 5G Roaming

Data at Rest

- Subscriber data including SUPI, and other subscriber data including location info
- Roaming agreements and policies associated with roaming partners
- Private Key associated with a hSEPP
- Certificate chain(s) associated with vSEPP of roaming partners and IPX providers
- Private Key associated with hUPF and certificate chain(s) associated with vUPF
- Session keys (e.g. keying material) used by the SEPP and keying material to be provided to the IPX providers as part of PRINS (in case PRINS is being used) for protecting the N32 interface(s).
- Session keys associated with the N9 interface at the UPF
- Security policies and configuration parameters for Cat 1, Cat 2 and Cat3 protection logic

Data in Transit

Based on TS 33.501 [4], the following attributes must be protected for confidentiality when transmitted over the N32 interface:

IE Type	Description
UEID	IE of type user equipment (UE) identity (e.g SUPI).
LOCATION	IE carrying location information.
KEY_MATERIAL	IE carrying keying material.
AUTHENTICATION_MATERIAL	IE carrying authentication material like authentication vectors and Extensible Authentication Protocol (EAP) payload.

AUTHORIZATION_TOKEN	IE carrying authorization token
OTHER	IE carrying other data requiring encryption.
NONSENSITIVE	IE carrying information that are not sensitive.

Figure 5 5GControl Plane Attributes that are to be Protected for Confidentiality

5.1.2 4G Roaming

Data at Rest

- Private key associated with hDEA and certificate chains associated with roaming partners (vDEAs, IPX providers).
- Session keys

Data in Transit

- Subscriber data
- Authentication material and session keys
- Subscriber location info

VoNR / VoLTE Roaming

Data at Rest

- Subscriber credentials (e.g. SUPI/IMSI, permanent keys like K and OPc) stored in HSS/UDM at HPLMN.
- Private keys and certificates for IMS functions (e.g. P-CSCF, S-CSCF, I-CSCF).
- Call Detail Records (CDRs), SIP signaling logs, and metadata stored for billing and compliance purposes.
- Session-related keys and derived key material (e.g. K_ASME, K_SEAF) cached in core entities (MME/AMF).
- Stored routing policies or QoS profiles including APN and bearer identifiers.
- Temporary session data cached at IPX or visited network nodes (e.g. MME/VLR) during voice session.

Data in Transit

- SIP signaling between UE and HPLMN (e.g. REGISTER, INVITE, 200 OK) transmitted over TLS via IPX.
- Authentication vector exchange (AV) over S6a/Nh interfaces between VPLMN and HPLMN.

- RTP or SRTP voice traffic carrying user conversations across S8/N9 interface.
- NAS signaling (attach/registration) transporting subscriber ID (SUCI) and session setup messages.
- Diameter signaling between IMS and charging systems (e.g. Rf/Ro) including user identifiers and call metadata.

5.2 Cryptographic Inventory

Based on 3GPP specifications 33.501 [4], SEPPs are deployed between operator domains in a roaming scenario. Either a direct TLS or PRINS with JSON Web Signature (JWS) is required for security protection.

If the direct mechanism is used between the SEPPs, then mutual TLS 1.3 is the process for mutual authentication and key exchange. The cryptographic suites supported by the TLS stack should include: ECDHE_ECDSA_with_AES_128_GCM_SHA256, DHE_RSA_with_AES_128_GCM_SHA256 for key establishment and ECDSA_SEPCP384r1_SHA384, RSA_PSS_RSAE, secp2256r1 and secp384r1 algorithms for digital signatures.

In some cases, IKE/IPSec may be used between the mobile operators and the IPX provider to transport keys used by the intermediaries for JSON patch.

IPSec or TLS may be used for protecting Diameter interfaces and in cases, where SCTP is used as a transport mechanism, DTLS may be used.

5.3 Threats and Attacks against Roaming Interfaces

Threats pertaining to DoS, privilege escalation, and other threats that cannot be addressed by PQC are considered out of scope and therefore only those threats impacting cryptographic capabilities to the roaming interfaces are addressed here.

Harvest Now Decrypt Later attacks (HNDL): These attacks are carried out by an adversary on data that is encrypted as a result of classical asymmetric key establishment process (e.g. elliptic-curve), where the attacker obtains encrypted data that is transmitted today and stores it, with the intent to decrypt it when a CRQC becomes available. HNDL attacks are particularly concerning for data that needs to be protected for long periods of time.

The key establishment process on the n32 interface using TLS 1.2 / 1.3 relies on either ECDHE or DHE, and therefore the N32-c and N32-f interfaces are highly susceptible to HNDL type of attacks where an adversary using a CRQC would be able to decrypt and obtain subscriber over the control plane and decrypt harvested user plane communications at a later point in time.

Spoofing, Impersonation and Repudiation Attacks: These attacks not generally considered imminent attacks since spoofing and impersonation type attacks are generally carried out in near real-time (e.g. as part of TLS handshake) and therefore only generally possible when a CRQC becomes available. When a CRQC becomes available:

- it could be used to break ECDSA and obtain the private key associated with a SEPP / IPX intermediaries used for impersonation over the N32 between roaming partner networks.
- JSON web tokens (JWT), that are authenticated using JSON web signatures based on ECDSA can be spoofed by IPX intermediaries.
- Tampering of N32-C / N32-f messages and JSON data is another attack that can be carried out causing degradation, denial of service and stealing of services.

6 Migration Strategy Analysis and Dependencies

6.1 Standards

The 5G roaming specifications are based on 3GPP TS 33.501 [4] and protection mechanisms have been specified in 3GPP TS 33.210 [7], and TS 33.310 [8] (NDS/IP). Additionally, GSMA has defined protection profiles and developed security guidelines which have been documented in FS.36 [19] and in FS.40 [18] respectively.

3GPP TS 33.501 and TS 33.210 defines JWS profiles. JWT, and JWS that are to be used in the PRINS mode have been specified in IETF RFC 7519 [21], RFC 7515 [10] and RFC 7516 [9] respectively and the cipher-suites are described in RFC 7518 [20]. The algorithm ("alg") parameter that has been specified to be used for signing the JWT is ES256 (ECDSA using P-256 curve with SHA-256). If JWE is used, then ECDH may be used as one of the key agreement mechanisms.

Other relevant standards include, PKI and certificate life-cycle management protocols, such as Certificate Management Protocol (CMPv2), that uses X.509 certificates as described in RFC 4210 [22], as well as the extended key purpose 5G network functions described in RFC 9509 [23]. Certificate validation and certificate revocation lists may also be used.

3GPP TS 23.401 [24] and TS 23.402 [25] define a direct Diameter interface between the network elements of the visited network (Mobility Management Entity (MME), Visited Policy and Charging Rules Function (vPCRF) and SGSN and the network elements of the home Network (HSS and Home Policy and Charging Rules Function (hPCRF)). The Diameter protocol is used by the DEA for communications between the Operators.

6.1.1 Public Key Infrastructure & Certificate Management (Not just a QSC issue)

The potential solutions of migration include post-quantum key encapsulation algorithm (e.g., ML-KEM) or hybrid key exchange. When a TLS connection is being established, the SEPP needs to verify the validly of certificate issued by the CA/RA. This requires migration to a quantum-safe solution for the root CAs/RAs and intermediate CAs/RAs when generating and managing the keys and certificates.

Further, if PRINS is used between SEPP instead of direct link with TLS connection, the JWE/JWS and IPX server shall be used in the PRINS between SEPP, as specified in 3GPP TS 33.501 [4]. The cIPX and pIPX may generate JWSs attaching to the JWE with the signature of cIPX or pIPX. The public key used for signature of the related IPXs should be quantum safe. Therefore, PKI and the certificate management protocols should consider migration.

For the above requirements, quantum-safe management protocol and an improved profile are required. For example, quantum-safe management protocol requires quantum-safe security link to CAs/RAs. Because of the root certificate, the certificate needs to be replaced gradually in the CA/RA. The certificate may need to be supported by having a new root certificate and a legacy root certificate at the same time during the migration. Also, migration of certificate profile should also be used. Including a quantum-safe signature algorithm and the agility of transmission size between SEPPs. Large-size signatures need to be supported and may require additional extension key slots. Overall, it is important to migrate PKI and certificates to prevent the potentially forged SEPP identity from quantum attacks.

6.1.2 TLS 1.3

The IETF specification for TLS 1.3 in RFC 8446 [2], describes mechanism for a client and server to establish a secure connection over the transport layer. A client SEPP and a server SEPP use TLS 1.3 to establish a secure connection that provides mutual authentication by means of X.509 certificates, message integrity and authenticity, replay protection and confidentiality. The key exchange process may involve either Elliptic Curve Diffie Hellman (ECDHE) or Diffie Hellman when using public key cryptography. The specifications also support Pre-shared Key (PSK) mechanisms which may be shared offline which is then used as part of the TLS handshake to establish the session keys.

There are efforts in the IETF LAMPS WG to create specification for TLS 1.3 with ML-KEM [26] and efforts to specify ML-KEM for JOSE objects, and one such effort is [27].

6.1.3 IKEv2 / IPSec

The Internet Key Exchange (IKE) protocol enables communicating parties (e.g. mobile operator and IPX providers) to establish an IPSec channel by using X.509 certificates for mutual authentication. The key exchange protocol is based on Diffie-Hellman (DH). IETF RFC 8784 [28] provides an extension of IKEv2 to allow for the use of pre-shared keys to make it resistant to HNDL type attacks.

6.1.4 Hybrid Cryptography

The IETF LAMPS group is currently in the process of developing standards for providing hybrid cryptographic mechanisms by combining ML-KEM along with ECDHE / DHE schemes. One such proposal [29] draft-ietf-tls-ecdhe-mlkem-00 proposes to combine SecP256r1 with ML-KEM for TLS 1.3. Another IETF draft [30] draft-kampanakis-ml-kem-ikev2-09 proposes to use ML-KEM as an additional key exchange along with traditional key exchange for IKEv2.

6.2 Regulations & Migration Strategy with Roaming Partners

6.2.1 National Guidelines: Regulation (Intra-PLMN) and Inter-PLMN

There may be efforts carried out by GSMA, Alliance for Telecommunications Industry Solutions (ATIS) in addition to NIST guidelines for securing TLS 1.3, IKEv2 / IPSec and JWT tokens, that would recommend the use of PQC based key encapsulation mechanisms, certificate management protocols and digital signature schemes.

6.2.2 Vendors

As standards mature, it is anticipated that vendors will increasingly support quantum-safe services in their products. Vendors may find that providing pre-standard protocols or algorithms for testing may help facilitate the full migration towards standards-based solutions.

Vendors, operators and roaming partners need to jointly develop roadmaps for the transition, to assist migration planning and manage security risk during migration.

6.2.3 Operators

Based on risk profile, operators may use PQC when available from the vendors or PQ/T hybrid schemes for certain use cases where the risk is higher (e.g. N-32-c and N-32) such as when TLS 1.3 is used or when using JWE to mitigate against HNDL type attacks. In PRINS mode, where JWS is used the threat is not imminent and therefore a migration to PQC signatures schemes should be undertaken in a phased manner. Similarly, the Diameter interfaces should be secured using IPSec with PQC support (e.g. ML-KEM) to protect against HNDL attacks.

6.2.4 3rd-parties (e.g. IPX providers)

IPX providers that use TLS 1.3, IKEv2 / IPSec, and JWE must prioritize the use of protection mechanisms such as ML-KEM for key establishment to mitigate against HNDL attacks. This effort must be coordinated in conjunction with other roaming partners and mobile operators and conform to industry best practices (e.g. GSMA roaming guidelines).

6.2.5 LEAs

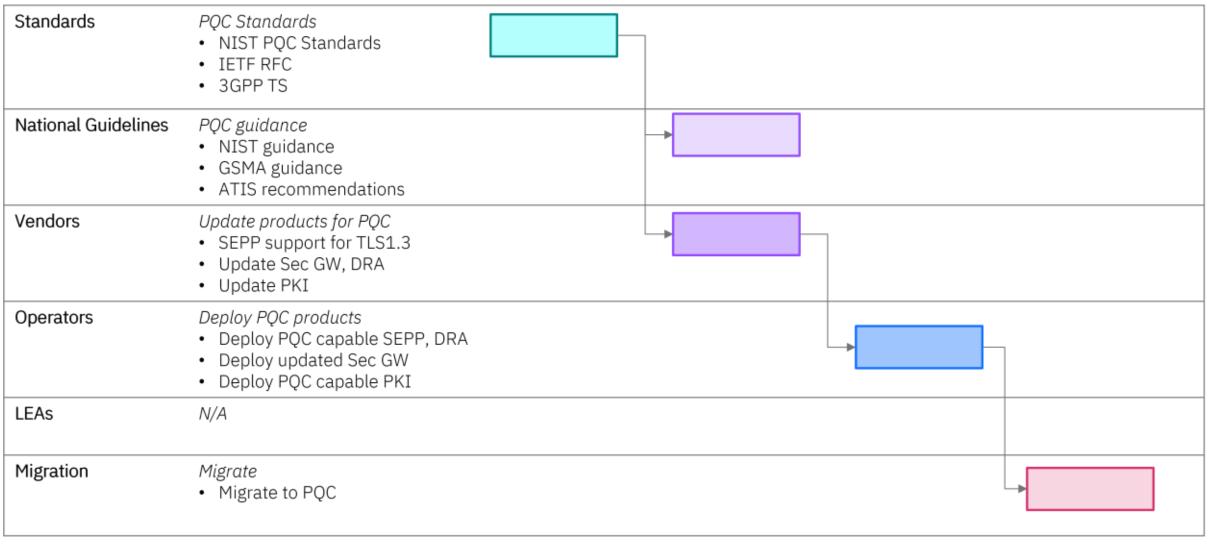
There does not appear to be impacts of PQC on LEA.

6.2.6 Performance

The immediate impact is for the SEPPs to support ML-KEM within their TLS 1.3 crypto suite. The performance impact may be minimal. Once the more latency-oriented TLS1.3 handshake protocol between the SEPPs is established, then the TLS security association can be a longer lasting association that accommodates N32 traffic for any number of UEs that roam between a pair of mobile operators.

The bigger impact may be when PRINS mode is used, where ML-KEM is used between the operator and the IPX provider either as part of TLS 1.3 or IKEv2 / IPSec for transferring session keys from the operator to the IPX provider.

6.2.7 Gantt Chart for PQC Migration



Standards	*PQC Standards* • NIST PQC Standards • IETF RFC • 3GPP TS
National Guidelines	*PQC guidance* • NIST guidance • GSMA guidance • ATIS recommendations
Vendors	*Update products for PQC* • SEPP support for TLS1.3 • Update Sec GW, DRA • Update PKI
Operators	*Deploy PQC products* • Deploy PQC capable SEPP, DRA • Deploy updated Sec GW • Deploy PQC capable PKI
LEAs	*N/A*
Migration	*Migrate* • Migrate to PQC

Figure 6Gantt Chart for PQC Migration for Roaming

6.2.8 PQC Migration Process Description

The primary concern is for the protection of the N32 interfaces from HNDL attacks. Therefore the number one priority is to use ML-KEM as the cryptographic suite within the TLS 1.3 handshake as the key encapsulation mechanism between the SEPPs. Similarly, ML-KEM must be used as the key encapsulation process (as part of either TLS 1.3 or IKEv2 / IPSec) between the SEPP and the IPX provider for sending the session keys.

The digital signature within a JWS object should be updated with ML-DSA [16] or an other standardized PQC digital signature algorithm. Firstly, the ML-DSA will have to be specified in the IETF and based on such a specification, a mechanism that uses the IETF specs will have to be described and specified within the 3GPP TS 33.210 specs. In the interim, a hybrid scheme for digital signature that combines ECDSA and ML-DSA can be used if there is a near-term availability of a viable quantum computer. Algorithms that are being standardized within the IETF, that includes generating composite signatures (e.g. draft-ounsworth-pq-composite-sigs) may be good candidate schemes. It must be noted that “harvest now, decrypt later” type attacks are less of a concern when only JWS is being used which may be the case for almost all of the use-cases.

There may be some use cases where encrypted JSON objects are needed, e.g. when confidentiality or privacy related data needs to be shared within a JWE. If key agreement is being used, then one of the standardized key encapsulation mechanisms must be used. The “harvest now, decrypt later” type attacks are a genuine concern when JWE is used and therefore quickly pivoting to PQ/Traditional hybrid key agreement mechanisms and later to ML-KEM type schemes when PQC matures.

In a hybrid environment, the certificate life-cycle management must include certificates that are used for both ML-DSA as well as for the traditional algorithms (e.g. ECDSA, ECDH). The certificates used for signature generation / verification by the SEPP must be provisioned and managed by PQ PKI systems and that also has the ability to support hybrid schemes. Also, PQ compliant capabilities within the certificate revocation list (CRL) and Online Certificate Status Protocol (OCSP) [31] must be developed and standardized.

6.2.9 Synergy with Internal Programs

Synergies with internal programs where SBI interface protection using PQC based methods for NF-NF communications. Similarly, for non-SBI interface protections based on IKEv2 / IPSec where PQC methods are being developed. Internal PKI that can manage the lifecycle of PQC certificates including support for protocols such as CMPv2 with ML-DSA certificates.

6.2.10 Synergy with External Programs

Synergy with national cybersecurity initiatives and recommendation including PQC (e.g. CNSA 2.0 in the US). Synergy with roaming partners, PKI vendors and organization involved in developing global partnerships (e.g. GSMA). Synergy with 3GPP standards development, IETF PQUIP, LAMPS WGs to coordinate and discuss use-cases and to avoid any conflicts about the migration plan. Synergy with vendors about the operator migration plan, and standards compliance which will affect the product development of vendors.

Document Management

A.1 Document History

Version	Date	Brief Description of Change	Approval Authority
1.0	26 June 2025	New document	Technology Group

Table 4 Document History

A.2 Other Information

Type	Description
Document Owner	PQTN
Editor / Company	Vinod Choyi, Verizon

Table 5 Other Information

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at prd@gsma.com

Your comments or suggestions & questions are always welcome.