Post-Quantum Use In Protocols
Internet-Draft
Intended status: Informational
Expires: 4 January 2026

L. Li
F. Liu
Huawei

3 July 2025

PQC migration use cases for the telecom network
draft-li-pquip-teleco-pqc-migration-01

Abstract

Telecommunications (Telecom) networks are important infrastructure. 3rd Generation Partnership Project (3GPP) provides security specifications for telecom networks, including network devices and user terminals. Meanwhile, the security protocols from IETF widely used in telecom systems. This docuemnt presents some post-quantum risks and assessments that exist in current telecom network, analyzes possible post-quantum migration cases and potential strategy in typical telecom network, the strategy includes the suggestion of related IETF protocols and profiles.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 4 January 2026.

Copyright Notice

Copyright (c) 2025 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components

extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction

Cryptographic technologies are used throughout ICT(Information and communications technology) industry to authenticate the source and protect the confidentiality and integrity of information that we communicate and store. However, quantum computing technology poses significant threats to classical cryptography, especially to widely-used cryptographic algorithms.

Today’s 5G network widely uses both symmetric and asymmetric cryptography above across different layers of the network to ensure the security, privacy, and integrity of communications. The permanent identity of device (named Subscription Permanent Identifier, SUPI) is protected by asymmetric key encryption algorithms when the UE initially accesses the 5G systems. Then, symmetric key encryption (e.g., AES) is used to protect the signaling control and data when the UE (e.g., the cellphone) communicates with the network. In addition, a network entity (for example, a base station) uses IPsec tunnels to protect the user data and control plane. network functions in the core network use TLS connection for security transmission. The PRINS [RFC8784] can be used to protect

communications between different operator domains through SEPP. These are all related to both symmetric and asymmetric key cryptography

In fact, servral procedures should considered be migrated to quantum-safe, becase quantum computers endanger both symmetric and asymmetric cryptography:

* For asymmetric encryption schemes, for example, ECIES (based on Elliptic Curve Cryptography), and IKEv2 (Dbased on iffie-Hellman key exchanges), Shor's algorithm [shor], running on a sufficiently powerful quantum computer, can break these systems by making these hard mathematical problems easy to solve (e.g., ECC used in ECIES and Diffie-Hellman used in IKEv2 relying the difficulty of solving discrete logarithm problems). As a result, public-key cryptosystems that secure digital signatures, encrypted communications, and key exchanges would become vulnerable to quantum attacks.

* For symmetric encryption schemes, for example, AES (Advanced Encryption Standard) / SNOW-5G / ZUC and SHA-256 (hash functions), their vulnerability to quantum computing algorithm (e.g., Grover's algorithm) is still in active discussions in post-quantum cryptography research community. The major concern is that quantum computer can speed up the process of brute-forcing symmetric keys.

Applying post quantum cryptography algorithms to telecom networks is called PQC migration, this document proposes the telecom use case for PQC migration, contains potential PQC risk, assessment and migration strategy. Some of the cases are referred from the guideline of GSMA [PQ03]. Further, this document points out the connections between the IETF protocols and the telecom system for the information of each WG in contributing the PQC protocol current design as well as in future.

2. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

3. Typical Telecom Scenarios and Potential Risks

This section is the core of this document. each introduced telecom scenarios may contain more than one risks and threats and it will link to the reference use cases in the next section.

3.1. Certificate Enrollment Procedure of the Base station

Given the standardized process of certificate enrolment for base stations defined in 3GPP TS 33.310[TS33310], we consider the procedure where a base station (e.g., 5G base station = gNB, or 4G base station = eNodeB) bootstraps and tries to apply a certificate from the operator's CA with a preconfigured certificate from the vendor CA.

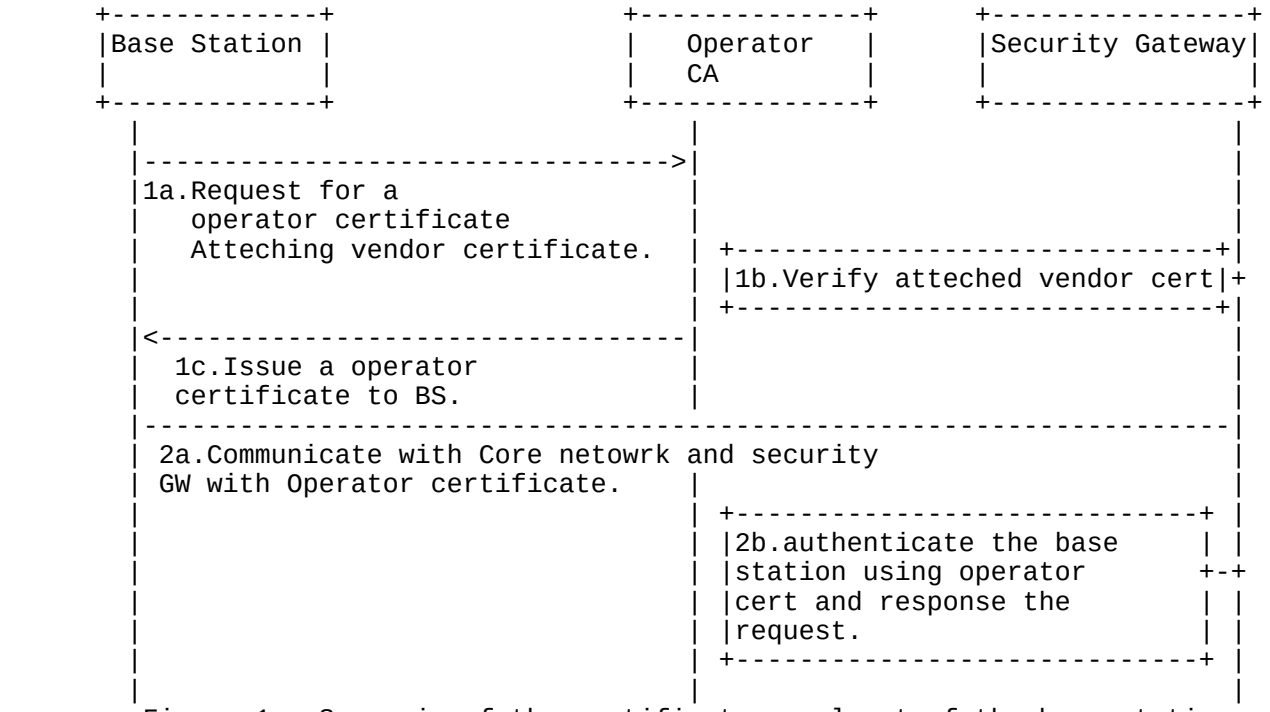

Figure 1 Scenario of the certificate enrolment of the base station

As shown in Figure 1, the following steps are performed by gNB/eNodeB to initially establish a secure connection and depend on the certificate, which can be an example to show the quantum risk in the current telecom system:

* 0. The base station pre-installs vendor certificate from vendor CA (out of band). Then, the base station pre-establishes the IPsec tunnel connection with operator's CA.

* 1. The base station request to apply the operator's certificate through the IPsec Tunnel.

* 2. The base station communicate to core network through IPsec tunnel used the operator certificate.

There are two risks related to the quantum computation attack that need to be considered in the above steps.

Risk A: attacking the IPsec tunnel

* 1. The base station establishes the secure connection with operator’s CA through IPsec Tunnel. During the establishment, the base station exchanges the session key with operator’s CA using IKEv2/IPsec.

* 2. Attackers in Risk A eavesdropping and storing the traffic of IPsec tunnel can analyze and corrupted the key exchange packet in IKEv2 with quantum computing capabilities.

* 3. If the traffic is protected by quantum-resistant algorithm, the attacker will fail to derive the IPsec session key used for base station and operator CA.

Risk B: attacking the certificates

* 1.The attacker in risk B establishes a connection with the operator CA and obtains the X.509 profile of a stolen vendor certificate from other entities.

* 2.The attacker attempts to forge a valid X.509 profile (including the certificate signature) of a vendor certificate.

* 3.If a quantum-resistant signature approaches is used in certificate; the attacker will fail to forge a valid vendor certificate with a valid signature.

Risk A is non-quantum security protocols such as the CMPv2 and IPsec (e.g., secure key exchange procedure). Risk B is the non-quantum security X.509 certificate (e.g., ECC signatures in the certificate). Two possible quantum risks threaten the security of base station and requires PQC migration to defense the potential attacker.

4. Reference Migration Use Cases

This section is the core of this document. For each use case, we present a concise overview and highlight the features that can help to categorize it. This list is not exhaustive, and if you think we have missed some important use case please consider contributing to it.

4.1. Overview of Telecom network

In today's the 5G Telecom network, a variety of cryptographic algorithms and IETF protocols are used ,both symmetric and asymmetric cryptography, a summury is provided in Table 1.

Migration Protocols	Usage in 5G	Symmetric Cryptography	Asymmetric Cryptography	Reference in Existing 3GPP specifications	Relative IETF WG
Key Derivation	Key agreement between UE and individual NF (e.g., K_AMF)	KDF based on symmetric cryptography	N/A	Annex A.1 in 3GPP TS 33.501[TS33501], TS 33.220[TS33220]	N/A
Secure Key Exchange	Two entities (e.g., NF/RAN/Security gateway, etc.) to securely exchange keys over an insecure channel for deriving symmetric session keys	Integrity and confidential protection in IPsec	Diffie-Hellman (DH) or Elliptic Curve Diffie-Hellman (ECDH)	Clause 9 in 3GPP TS 33.501	IPSECME
Authentication	UE registration and authentication	5G-AKA and EAP-AKA'	EAP-TLS	Annex I.2 in 3GPP TS 33.501	EMU
Authentication for Network function	Two NFs mutual authentication	N/A	Digital Certificate and PKI	Clause 13 in 3GPP TS 33.501	Lamps
Identity Protection	Concealing SUPI by generating SUCI	N/A	Public key encryption (ECIES)	Clause 6.12 in TS 33.501, 3GPP TS 23.003 [TS23003]	N/A
Data Confidentiality and integrity	Encryption to protect user plane data and/or control	AES / SNOW-5G / ZUC	N/A	Clause 5.11 in 3GPP TS 33.501, TS 35.215[TS35215],	CFRG

	plane signaling			TS 35.221[TS35221]		
Public key Infrastructure	Signature of the certificate for security establishment, such as transport layer security	N/A	Signature algorithm, for example, ECC, etc.	3GPP TS 33.310[TS33310]	ACME /Lamps	

Table 1: Summary of symmetric and asymmetric cryptography in 5G Telecom network

As shown in the table, some common issues have been discussing in the relevant IETF WGs, but there are some unique characteristics, in terms of the deployment of telecom networks. Specific use cases are discussed in the following sections, which are proposed based on the scenario in section 3 to address the identified risks.

4.2. N2/N3 migration between base station and security gateway

4.2.1. Description

In the current telecom network, the base station and the core network need to transmit control signaling and the user’s data. Control signaling is for example non-access stratum information of the UE, including important messages such as user authentication and authorization information. The user’s data is for example, the communication data between the UE and the website of data network (aka., user plane data). The foregoing content is transmitted through interface N2 and N3 respectively. Generally, it can be concluded that N2 is used for control plane signaling, and N3 is used for user plane data.

As described in the threat analysis in Section 2, both the secure connection of the N2 and the N3 use the IPsec protocol. Specifically, the core network uses a security gateway (SEG) as the endpoint of the IPSec tunnel, and the other end point is base station. As specified if 3GPP TS 33.501, When an IPsec tunnel is established, IKEv2 is executed and authenticated by the certificate with specified profile.

For post-quantum migration of N2/N3, Although IPsec itself uses symmetric encryption for transmission, the current 3GPP recommended IKEv2 protocol version and certificate format do not include post-quantum considerations. In this use case of N2/N3, the post-quantum migration of IKEv2 should be considered.

4.2.2. Migration Suggestion

From the perspective of IETF PQUIP and this use case, the following analysis can be considered.

About key exchange:

* A pre-shared key may be considered as a way, for example, as specified in RFC 8784[RFC8784], which includes the pre-shared hybrid key, and the non-hybrid key (e.g, AES only). The reason is same as hybrid key exchange. Moreover, considering that base stations and SEGs are usually provided by different vendors, extra coordination may be required or the key pre-configuration can be implemented by operators during the deployment.

* Directly use the post-quantum algorithm to negotiate keys, which can be considered when the post-quantum algorithm is mature. Besides, some additional issues also need to be considered, such as increased payload size and IKE fragmentation.

About authentication:

* PKIs that support post-quantum signatures need to be considered. Otherwise, certificate-based authentication may be risky between the base station and the SEG.

4.2.3. Other Information

For other SDOs, 3GPP has not yet proposed post-quantum migration considerations. The GSMA proposed post-quantum migration guideline[PQ03] partially including the use case.

4.3. Concealment of the Cellphone’s Subscription Permanent Identifier

TODO

5. IANA Considerations

This document has no IANA considerations.

6. Security Consideration

TODO

7. References

7.1. Normative Reference

[PQ03] GSMA, "Post Quantum Cryptography Guidelines for Telecom Use Cases v2.0", PQ 03, Task Force PQTN, October 2024, <https://www.gsma.com/newsroom/gsma_resources/pq-03-post-quantum-cryptography-guidelines-for-telecom-use-cases/>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC8784] Fluhrer, S., Kampanakis, P., McGrew, D., and V. Smyslov, "Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security", RFC 8784, DOI 10.17487/RFC8784, June 2020, <https://www.rfc-editor.org/info/rfc8784>.

[TS23003] 3GPP, "Numbering, addressing and identification", TS 23.003, Group 3GPP/CT4, January 2025, <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=729>.

[TS33220] 3GPP, "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)", TS 33.220, Group 3GPP/SA3, March 2024, <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2280>.

[TS33310] 3GPP, "Network Domain Security (NDS); Authentication Framework (AF)", TS 33.310, Group 3GPP/SA3, January 2025, <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2293>.

[TS33501] 3GPP, "Security architecture and procedures for 5G System", TS 33.501, Group 3GPP/SA3, January 2025, <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169>.

[TS35215] 3GPP, "Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 and UIA2; Document 1: UEA2 and UIA2 specifications", TS 35.215, Group 3GPP/SA3, April

2024,
<https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2395>.

[TS35221] 3GPP, "Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 and UIA2; Document 1: UEA2 and UIA2 specifications", TS 35.221, Group 3GPP/SA3, April 2024,
<https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2395>.

7.2. Informative References

[PRINS] Green, G., "5G Security when Roaming Part 2", 21 May 2021, <https://www.mpirical.com/blog/5g-security-when-roaming-part-2>.

[shor] Shor, P.W., "Algorithms for Quantum Computation: Discrete Logarithms and Factoring", DOI 10.1109/SFCS.1994.365700, 6 August 2002, <https://ieeexplore.ieee.org/document/365700/authors#authors>.

Acknowledgments

TODO

Authors' Addresses

Lun Li
Huawei
Email: lilun20@huawei.com

Faye Liu
Huawei
Email: liufei19@huawei.com