A Study on Enhancing Security in Private 5G Networks Using Post-Quantum Cryptography (PQC)-Based X.509 Certificates*

Juseoung Lee*, Jihoon Choi, and Sookhyun Jeon

Telecommunications Technology Association, Republic of Korea
{jslee, jihoonchoi, shjeon}@tta.or.kr

Abstract

The expansion of private 5G networks into critical sectors like defense and public services creates a long-term security vulnerability, as their current authentication systems are susceptible to future quantum computing threats. To proactively address this risk, this paper proposes a security profile integrating Post-Quantum Cryptography (PQC) into the X.509 certificate framework for device authentication.

1 Introduction

As private 5G networks become to security-critical sectors like defense and public transportation, ensuring trusted device authentication is paramount. However, their reliance on conventional public-key cryptosystems such as RSA and ECC creates a significant long-term vulnerability, as these systems will be rendered insecure by the advent of quantum computers. To address this impending threat, this paper proposes a security model that integrates PQC algorithms into the X.509 certificate framework.

2 A Proposed Device Certification Profile

This section details the proposed PQC-based certificate profile designed to counter the quantum computing threats identified previously. Within private 5G networks, mutual authentication via X.509 certificates constitute the foundational layer of security, ensuring that only authorized devices can access application server[1].

The structure of the proposed certificate is shown in Figure 1, with key fields defined as follows. Serial Number: A unique identifier assigned by the Certificate Authority (CA) to each device, with a maximum length of 20 bytes. Uniqueness must be guaranteed within the issuing CA. Signature Algorithm: Specifies the algorithm used to sign the certificate. This profile employs CRYSTALS-Dilithium3, one of the algorithms standardized by NIST for PQC, to guarantee signature integrity. Subject: Identifies the certificate's owner. The Subscription Permanent Identifier, the standard permanent identifier in 5G networks, is used to unequivocally link the certificate to the device. X.509v3 Basic Constraints: Set to 'CA: FALSE', this designates the certificate as an End-Entity, preventing it from being misused to issue subordinate certificates in a Man-in-the-Middle attack. X.509v3 Subject Key Identifier: A hash of the certificate's public key, which serves as a unique identifier for the certificate corresponding to the end-entity device. X.509v3 Authority Key Identifier: Contains the public key identifier of the

*Proceedings of the 9th International Conference on Mobile Internet Security (MobiSec'25), Article No. P-40, December 16-18, 2025, Sapporo, Japan.

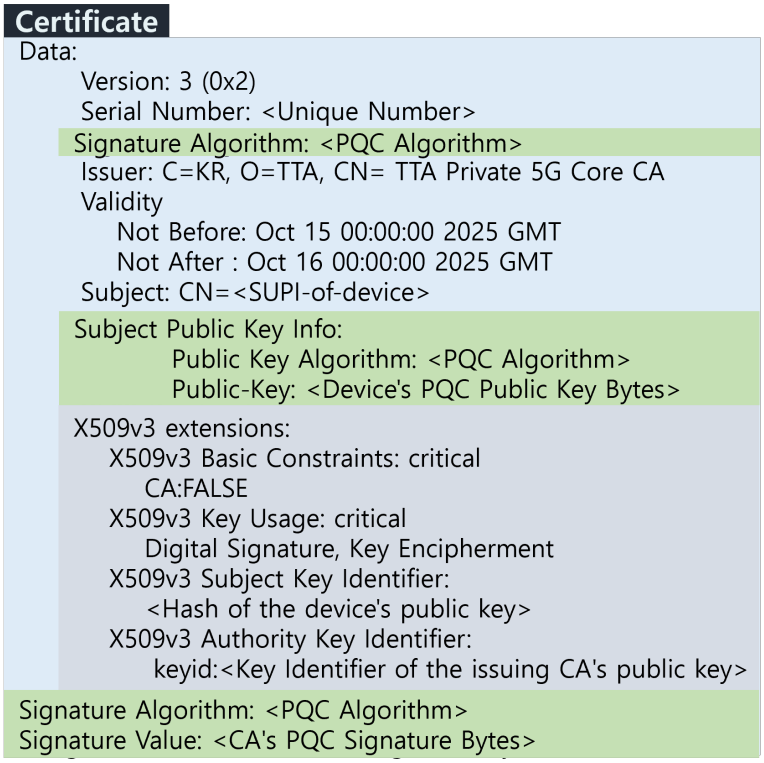

Figure 1: A Proposed PQC-based Certificate Structure for 5G Private Devices

issuing CA's certificate. This provides an authentication path and optimizes the path-building process for establishing the trust chain.

3 Conclusion

In this paper proposes a PQC-based X.509 certificate profile incorporating the NIST algorithm to protect private 5G networks from quantum threats. Future work should focus on implementing this profile in a live PKI system.

4 Acknowledgments

- This work was supported by Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korea government (MIST) (No. RS-2024-00398312, Development of Quantum Security Based Device Identification and Test Verification Technologies for 5G Non-Public Network).

References

[1] Jihoon Choi, Hyesu Oh, Juseoung Lee, and Sukhyeon Jeon. "an adaptive device authentication framework for private 5g networks: Key considerations for implementation". in Proc. of Mobisec '24, 2024.