**3GPP TSG-SA3 Meeting #124 S3-253381-r1 (merging 3489)**

**Wuhan, China, 13 – 17 October 2025**

**Source: Huawei, HiSilicon, Ericsson**

**Title: PQC migration for PKI certificates**

**Document for: Approval**

**Agenda item: 5.2.1**

**Spec: 3GPP TR 33.703**

**Version: 0.1.0**

**Work Item: FS\_CryptoPQC**

**Comments**

It is proposed to study the PQC migration scheme of the PKI certificates in 3GPP.

\* \* \* First Change \* \* \* \*

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[y2] IETF RFC 9763: "Related Certificates for Use in Multiple Authentications within a Protocol "

[y3] IETF RFC 9802: "Use of the HSS and XMSS Hash-Based Signature Algorithms in Internet X.509 Public Key Infrastructure"

[y4] IETF Draft (Standards Track): "Internet X.509 Public Key Infrastructure - Algorithm Identifiers for the Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM) ", https://datatracker.ietf.org/doc/draft-ietf-lamps-kyber-certificates/.

[y5] IETF Draft (Standards Track): "Internet X.509 Public Key Infrastructure: Algorithm Identifiers for SLH-DSA", <https://datatracker.ietf.org/doc/draft-ietf-lamps-x509-slhdsa/>.

[y6] IETF Draft (Standards Track): "Internet X.509 Public Key Infrastructure - Algorithm Identifiers for the Module-Lattice-Based Digital Signature Algorithm (ML-DSA)", <https://datatracker.ietf.org/doc/draft-ietf-lamps-dilithium-certificates/>.

[y7] IETF Draft (Standards Track): "Composite ML-KEM for use in X.509 Public Key Infrastructure", <https://datatracker.ietf.org/doc/draft-ietf-lamps-pq-composite-kem/>.

[y8] IETF Draft (Standards Track): "A Mechanism for Encoding Differences in Paired Certificates", <https://datatracker.ietf.org/doc/draft-bonnell-lamps-chameleon-certs/>.

[y9] IETF Draft (Standards Track): "Root CA Certificate Rekeying in the Scenario of Post Quantum Migration", https://datatracker.ietf.org/doc/draft-wang-lamps-root-ca-cert-rekeying/.

[y10] IETF Draft (Standards Track): "A Mechanism for X.509 Certificate Discovery", <https://datatracker.ietf.org/doc/draft-ietf-lamps-certdiscovery/>.

[y11] NIST FIPS 203: “Module-Lattice-Based Key-Encapsulation Mechanism Standard”.

[y12] NIST FIPS 204: “Module-Lattice-Based Digital Signature Standard”.

[y13] NIST FIPS 205: “Stateless Hash-Based Digital Signature Standard”.

\* \* \* Next Change \* \* \* \*

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [1].

ECIES Elliptic Curve Integrated Encryption Scheme

MIKEY-SAKKE Multimedia Internet KEYing – Sakai-Kasahara Key Encryption

PQC Post Quantum Cryptography

SDO Standards Development Organizations

SECG Security Engineering & Consulting Group

SUCI Subscription Concealed Identifier

PKI Public Key Infrastructure

PKIX Public Key Infrastructure X.509

HBS Hash-Based Signature

HSS Hierarchical Signature System

XMSS eXtended Merkle Signature Scheme

CRL Certificate Revocation Lists

KEM key encapsulation mechanism

ML-KEM Module-Lattice-Based Key-Encapsulation Mechanism

ML-DSA Module-Lattice-Based Digital Signature

SLH-DSA Stateless Hash-Based Digital Signature

CA Certification Authority

\* \* \* Next Change \* \* \* \*

## 6.X Protocol #X：PKI certificate

6.X.1 General

The IETF LAMPS group has introduced multiple Drafts to enable a smooth transition to PQC in PKIX to provide quantum-resistant security for PKIX.

### 6.X.2 Current Work in IETF

#### 6.X.2.1 IETF RFCs

### **Introduction of PQC algorithms**

The IETF RFC 9802 [y3] has specified algorithm identifiers and ASN.1 encoding format for several stateful Hash-Based Signature (HBS) schemes: Hierarchical Signature System (HSS), eXtended Merkle Signature Scheme (XMSS), and a multi-tree variant of XMSS, XMSS^MT. These schemes are applicable to the Internet X.509 Public Key Infrastructure (PKI) when digital signatures are used to sign certificates and certificate revocation lists (CRLs).

### **Support for Hybrid Mechanisms**

The IETF RFC 9763 [y2] defines a method for requesting and issuing two X.509 end-entity certificates for the same entity, in order to perform two authentications using the two certificates where each certificate corresponds to a distinct digital signature.

#### 6.X.2.2 IETF Adopted Drafts

### **Introduction of PQC algorithms**

The IETF standards track draft “Internet X.509 Public Key Infrastructure - Algorithm Identifiers for the Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM)” [y4] proposes to use the ML-KEM [y11] in X.509 Public Key Infrastructure. The conventions for the subject public keys and private keys are specified.

The IETF standards track draft “Internet X.509 Public Key Infrastructure: Algorithm Identifiers for SLH-DSA” [y5] proposes to use the SLH-DSA [y13] in X.509 Public Key Infrastructure. The conventions for the associated signatures, subject public keys, and private keys are specified.

The IETF standards track draft “Internet X.509 Public Key Infrastructure - Algorithm Identifiers for the Module-Lattice-Based Digital Signature Algorithm (ML-DSA)” [y6] proposes to use the ML-DSA [y12] in X.509 Public Key Infrastructure. The conventions for the associated signatures, subject public keys, and private keys are specified.

### **Support for Hybrid Mechanisms**

The IETF standards track draft “Composite ML-KEM for use in X.509 Public Key Infrastructure” [y7] defines a specific instantiation of the PQ/T Hybrid paradigm called "composite" where multiple cryptographic algorithms (i.e. ML-KEM [y11] in hybrid with traditional algorithms RSA-OAEP, ECDH, X25519, and X448) are combined to form a single key encapsulation mechanism (KEM) presenting a single public key and ciphertext such that it can be treated as a single atomic algorithm at the protocol level.

### **Certificate Discovery**

The IETF standards track draft “A Mechanism for X.509 Certificate Discovery” [y10] specifies a method to discover a secondary X.509 certificate associated with an X.509 certificate to enable efficient multi-certificate handling in protocols.

#### 6.X.2.3 IETF Non-Adopted Drafts

### **Support for Hybrid Mechanisms**

The IETF standards track draft “A Mechanism for Encoding Differences in Paired Certificates” [y8] specifies a method to efficiently convey the differences between two certificates in an X.509 version 3 extension, which allows a relying party to extract information sufficient to reconstruct the paired certificate and perform certification path validation using the reconstructed certificate.

### **root CA certificate rekeying**

The IETF standards track draft “Root CA Certificate Rekeying in the Scenario of Post Quantum Migration” [y9] proposes a newWithOld root CA certificate rekeying solution such that old entities are transparent to root CA certificate rekeying, the solution works in both traditional PKIs and PQC PKIs, where the certificate can either contain standalone PQC algorithms or contain PQT hybrid algorithms.

6.X.3 3GPP Considerations\* \* \* End of Changes \* \* \* \*