**3GPP TSG-SA3 Meeting #119 S3-244621-r1**

**Orlando, US, 11 -15 November 2024**

**Source: Nokia, Nokia Shanghai Bell**

**Title: Technical Content for 3GPP Cryptographic Inventory**

**Document for: Approval**

**Agenda Item: 3.2**

# 1 Decision/action requested

***The SA3 is kindly asked to review and approve the proposed changes to the 3GPP cryptographic inventory TR.***

# 2 References

None.

# 3 Rationale

It is proposed to add the following technical content into the TR 33.9xy.

# 4 Detailed proposal

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of 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] NIST US Government, [link](https://csrc.nist.gov/Projects/post-quantum-cryptography/faqs)

[2] NCSC UK Government, [link](https://www.ncsc.gov.uk/whitepaper/next-steps-preparing-for-post-quantum-cryptography#:~:text=In%20contrast%20with%20PKC%2C%20the,can%20continue%20to%20be%20used.)

[3] draft IETF, “Post-Quantum Cryptography for Engineers”

[4] draft IETF, “Terminology for Post-Quantum Traditional Hybrid Schemes”

[5] FIPS 186, “Digital Signature Standard (DSS)”

[6] NIST Special Publications (SP) 800-56 A “Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography”

[7] NIST Special Publications (SP) 800-56 B ”Recommendation for Pair-Wise Key-Establishment Using Integer Factorization Cryptography”

[8] FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard,

 Published August 13, 2024

[9] FIPS 204, Module-Lattice-Based Digital Signature Standard,

 Published August 13, 2024

[10] FIPS 205, Stateless Hash-Based Digital Signature Standard,

 Published: August 13, 2024

[11] NIST SP 800-227, Recommendations for key-encapsulation mechanisms,
 2024

[12] FIPS 202, SHA-3 Standard: Permutation-Based Hash and Extendable-Output
 Functions

[13] draft-ietf-pquip-pqt-hybrid-terminology-03

[14] draft-ietf-pquip-pqc-engineers-04

[15] draft-ietf-tls-hybrid-design-10

[16] RFC 8446, The Transport Layer Security (TLS) Protocol Version 1.3

[17] ETSI TC CYBER, ETSI QSC, “Quantum Safe Cryptographic Protocol Inventory”, S3-240223

[18] GSMA, “LS regarding the publication of the Post Quantum Cryptography – Guidelines for Telecom Use Cases document in Feb 24”

[19] ETSI TR 103 619 V1.1.1 (2020-07), “Migration strategies and recommendations to Quantum Safe schemes”

[20] GSMA, “Post Quantum Cryptography – Guidelines for Telecom Use Cases”

[21] S3-243812, LS reply to 3GPP Reply-LS on PQC Migration

[22] S3-244307, Reply-LS on PQC Migration

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

## 3.1 Terms

For the purposes of the present document, the terms given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

**Cryptographically Relevant Quantum Computer (CRQC):**“Quantum computers use properties of quantum mechanics to compute in a fundamentally different way from today's digital, 'classical', computers. They are, theoretically, capable of performing certain computations that would not be feasible for classical computers.” [2]

“If such a computer could exist in the future, most traditional public key cryptography (PKC) algorithms in use today will be vulnerable to attacks from it.” [2]

Traditional Public Key Cryptography (PKC) Algorithms:
“These traditional PKC algorithms include:

* algorithms based on integer factorisation such as RSA
* algorithms based on the discrete logarithm problem such as Finite Field Diffie-Hellman, ECDH, DSA, ECDSA, EdDSA” [2]

**Classical Computer / Traditional Computer:**In the context of quantum computing and in comparison, to a CRQC, in classical/traditional computers the bits of data can exist either on zero (0) or one (1).

**Hybrid Mode:**Implementation and coexistence of traditional cryptographic algorithms and post-quantum cryptographic algorithms.

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

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP 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 3GPP TR 21.905 [1].

AES Advanced Encryption Standard

AKA Authentication and Key Agreement

API Application Programming Interface

CRQC Cryptographically Relevant Quantum Computer

CSRC Computer Security Resource Center

DSA Digital Signature Algorithm

ECDH Elliptic Curve Diffie-Helman

ECDHE Elliptic Curve Diffie-Helman Ephemeral

ECDSA Elliptic Curve Digital Signature Algorithm

EdDSA Edwards-Curve Digital Signature Algorithm

FIPS Federal Information Processing Standards

GSM Global System for Mobile Communications

GSMA GSM Association

HMAC Hash-based Message Authentication Code

JSON JavaScript Object Notation

JWE JSON Web Encryption

JWS JSON Web Signature

LS Liaison Statement

MAC Message Authentication Code

ML-DSA Module-Lattice-Based Digital Signature Standard

ML-KEM Module-Lattice-Based Key Encapsulation

NCSC UK National Cyber Security Centre United Kingdom

NIST US National Institute of Standards and Technology United States

NSSAA Network Slice-Specific Authentication and Authorization

PKC Public Key Cryptography

PQ Post Quantum

PQC Post Quantum Computing

PQS Post Quantum Security

RSA Rivest-Shamir-Adleman

SECG Security Gateway

SEPP Security Edge Protection Proxy

SHA Secure Hash-Algorithm

SLH-DSA Stateless Hash-Based Digital Signature Standard

SNPN Stand-alone Non-Public Network

SoR Steering of Roaming

TLS Tranport Layer Security

UE User Equipment

UPU UE Parameter Update

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

## 4.1 General

This 3GPP cryptographic inventory is separated in three main topics, the first is providing the 3GPP algorithms which refer to traditional algorithms, while the second is providing the mapping to the post-quantum related algorithms, and the last is for the reference to the IETF specifications.

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

## 4.2 Introduction of PQ Security Levels - Defined by NIST

According to NIST the “quantum computers would completely break many public-key cryptosystems, including RSA, DSA, and elliptic curve cryptosystems. These cryptosystems are used to implement digital signatures and key establishment and play a crucial role in ensuring the confidentiality and authenticity of communications on the Internet and other networks.” [1]

And according to the [1] and [2] the following can be assumed:

“In contrast with PKC, the security of symmetric cryptography is not significantly impacted by quantum computers, and existing symmetric algorithms with at least 128-bit keys (such as AES) can continue to be used. The security of hash functions such as SHA-256 is also not significantly affected, and secure hash functions can also continue to be used.”

The below Table 4.2-1 is providing the list of PQ security levels and is mapping those to traditional and post-quantum algorithms.

Table 4.2-1: PQ Security Levels – Defined by NIST

|  |  |  |
| --- | --- | --- |
| **PQ Security Level** | **AES/SHA(2/3) hardness** | **PQC Algorithm** |
| 1 | AES-128 (exchaustive key recovery) | ML-KEM-512, FN-DSA-512, SLH-DSA-SHA2/SHAKE-128f/s |
| 2 | SHA-256/SHA3-256 (collision search) | MH-DSA-44 |
| 3 | AES-192 (exchaustive key recovery) | ML-KEM-768, ML-DSA-65, SLH-DSA-SHA2/SHAKE-192f/s |
| 4 | SHA-384/SHA3-384 (collision search) | No algorithm tested at this level. |
| 5 | AES-256 (exchaustive key recovery) | ML-KEM-1024, FN-DSA-SHA2/SHAKE-256f/s |

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

## 4.3 3GPP Cryptographic Inventory – 5G System

The below Table 4.3-1 provides an overview of 3GPP specific cryptographic algorithms which exist in 5G System and the ownership/development organisation of the cryptographic algorithms. These algorithms are seen to be 3GPP specific, because the cryptographic algorithms for the air-interface are specific to 3GPP. These algorithms are going to be adapted according to a 3GPP defined API. For each of the existing algorithm the corresponding PQS algorithm is listed, as well as the PQS related reference documentation.

### 4.3.1 Symmetric Cryptographic Algorithms

The security for the NAS messages between UE and AMF and the RRC signalling as well as the UP data between UE and gNB is based on symmetric algorithms.

The two primary authentication methods, i.e., the 5G AKA and the EAP-AKA, are challenge-and-response protocols which are based on a shared secrete key (K). The shared secrete is classified as being a symmetrical key. The 5G-AKA is computing hash values (see Annex A.5 of TS 33.501). The EAP-AKA’ is based on EAP-TLS procedures (see Annex B of TS 33.501).

For the NPN the two authentication methods (e.g., 5G AKA and EAP-AKA’ might apply.

Table 4.3-1: 3GPP specific algorithms (5G System)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Traditional Algorithm | 3GPP Interface | Impacted by quantum computing | Referred Document (Note 14) | PQS Algorithm | PQS Level | Development Organization |
| 128-NxA1  | Uu interface protection | No | 3GPP 256-bitConfidentiality and Integrity Algorithms for the Air Interface | 256-NxA1 | TBD (Note 12) | ETSI SAGE |
| 128-NxA1  | Uu interface protection | No | 3GPP 256-bitConfidentiality and Integrity Algorithms for the Air Interface | 128-NxA1 (Note 11) | 1(Note13) | ETSI SAGE |
| 128-NxA2 | Uu interface protection | No | 3GPP 256-bitConfidentiality and Integrity Algorithms for the Air Interface | 256-NxA2 | TBD (Note 12) | ETSI SAGE |
| 128-NxA2 | Uu interface protection | No | 3GPP 256-bitConfidentiality and Integrity Algorithms for the Air Interface | 128-NxA2 (Note 11) | 1 | ETSI SAGE |
| 128-NxA3 | Uu interface protection | No | 3GPP 256-bitConfidentiality and Integrity Algorithms for the Air Interface | 256-NxA3 | TBD (Note 12) | ETSI SAGE |
| 128-NxA3 | Uu interface protection | No | 3GPP 256-bitConfidentiality and Integrity Algorithms for the Air Interface | 128-NxA3 (Note 11) | 1(Note 13) | ETSI SAGE |
| MILENAGE-128 | AKA | No | Specification of the MILENAGE-256 algorithm set | MILENAGE-256 | 5 | ETSI SAGE |
| TUAK-128/256 | AKA | No | - | TUAK-128/256 (Note 11) | TBD (Note 12) | ETSI SAGE |

The following applies:

* NxA1 is Snow 5G based encryption/integrity protection algorithm, NxA2 is AES based encryption/integrity protection algorithm, NxA3 is ZUC based encryption/integrity protection algorithm.
* MILENAGE-128 is AES based algorithm for authentication and key generation, while the MILENAGE-256 employs Rijndael-256-256.
* TUAK is Keccak based algorithm for authentication and key generation.
* NOTE 11: For 128-bit symmetric cryptographic algorithms the NIST [1] and the NCSC [2] have declared those to be NOT significantly impacted by quantum computing and therefore cryptographic algorithms with at least 128-bit key length can continue to be used and can be rated to as PQS level 1.
* NOTE 12: (TBD) in PQS level collumn means there is no corresponding PQ security level defined by NIST for the algorithm.
* NOTE 13: The PQ level is assumed to be one, because of the [1] and [2] statement.
* NOTE 14: The specifications can be obtained from the following 3GPP specifications portal [35-series](https://www.3gpp.org/dynareport?code=35-series.htm).

Editor’s Note: NIST is benchmarking AES for PQS, therefore other than AES will be marked as TBD. In this case the PQS must wait for first/initial benchmarking.

### 4.3.2 Combined Cryptographic Algorithms

The Elliptic Curve Integrated Encryption Scheme (ECIES) specified in SECG is used to encrypt a SUPI.

The ECIES specification combines the ECC-based asymmetric cryptography with symmetric ciphers to provide data encryption.

The below Table 4.3-2 shows the cryptographic algorithms which are directly used by 3GPP functions. The term ‘directly used’ refers to the fact that these algorithms are used without any modification/adaptation.

Table 4.3-2: 3GPP Directly Used Algorithms (5G System)

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Traditional Algorithm | 3GPP Interface | Impacted by quantum computing | Ref. Doc. Traditional Algorithm | PQS Algorithm | PQS Level | Development Organisation | PQS Alg. Dev. Org. | PQ Referred Document |
|  ECIES  | SUCI | Yes | Standards for Efficient Cryptography: Elliptic Curve Cryptography | ML-KEM-512 | 1 | SECG | NIST/SECG | FIPS 203 (ML-KEM) |
|  ECIES  | SUCI | Yes | Standards for Efficient Cryptography: Elliptic Curve Cryptography | ML-KEM-768 | 3 | SECG | NIST/SECG | FIPS 203 (ML-KEM) |
|  ECIES  | SUCI | Yes | Standards for Efficient Cryptography: Elliptic Curve Cryptography | ML-KEM-1024 | 5 | SECG | NIST/SECG | FIPS 203 (ML-KEM) |
| HMAC-SHA-256 | Key derivation | No | FIPS 180-2 | HMAC-SHA-256 (Note 21) | 2 | IETF/NIST | - | - |
| HMAC-SHA-256 | Key derivation | No | FIPS 180-2 | HMAC-SHA3-256 | 2 | IETF/NIST | IETF/NIST | FIPS 202 |
| HMAC-SHA-256 | Key derivation | No | FIPS 180-2 | HMAC-SHA3-384 (Note 22) | 4 | IETF/NIST | IETF/NIST | FIPS 202 |

The following applies:

* Curve Integrated Encryption Scheme” (ECIES) is specified in SECG with adaptation in SA3. From the cryptographic standpoint, this is a Diffie-Hellman key exchange between the UE (which generates an ephemeral key pair) and the home network (which uses a long-term public key already provisioned on the UE). The Diffie-Hellman key share is then used as an input to a key derivation function so as to generate an encryption key EK and a MAC key MK. Two profiles (profile A and profile B) are defined whose main difference lies in the elliptic curve parameters (curve 25519 vs secp256). In all cases, EK is used as an AES-128 key in CTR mode whereas MK is a 256-bit key used for HMAC-SHA-256.
* NOTE 21: HMAC-SHA2-256 algorithm is not confirmed as PQ vulnerable, nor secure.
* NOTE 22: It is not clear if NIST security level 4 is needed for key derivation.

### 4.3.3 Asymmetric Cryptographic Algorithms

All the NFs based on SBI support mutually authenticated TLS and HTTPS. The SBI authentication is based on OAuth 2.0 framework.

There are various interfaces in 5G systems are non-SBI, e.g., N2, N3, Xn, N6, and other interfaces, e.g., Rx based on DIAMETER or GTP. In general the protection of the interfaces is based on IPsec ESP and IKEv2. In addition DTLS is to be supported in the split-gNB scenario.

The procedures for the secondanry authentication between UE and external data networks (see clause 11 of TS 33.501) is based on EAP framework.

The mutual authentication and security protection between the NEF and AF interface and the management interface between the clice management service consumer and producer are based on TLS. The Authorization of requests from the AF or the clice management service consumers is based on OAuth 2.0.

For the Non-3GPP access the IKEv2 to setup one or more IPsec ESP security associations, and the DTLS may also to be involved.

For the EDGE computing the DNS over TLS is specified, in this case the TLS means apply.

The below Table 4.3-3 shows the cryptographic algorithms which are going to be used because of use of TLS, IPsec, and JSON features/functions. The listed algorithms are being used implicit, because if the one is using these features/functions, then associated algorithms will be used implicit.

Table 4.3-3: 3GPP indirectly used algorithms (5G System)

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Security Protocol | Traditional Algorithm | 3GPP Interface | Impacted by quantum computing | Ref. Doc. Existing Algorithm | PQS Algorithm | PQS Level | Algorithm Dev. Org. | PQ Ref. Doc. | PQS Alg. Dev. Org. | PQ Ref. RFC (Note35) |
| TLS | (EC)DHE (Note 31) | N2, N3, N4, N6, N9, N33, Gm, TLS based SBA, N32-c, N32-f (Note 33) | Yes | RFC 8446 | ML-KEM-512/768/1024 | 1/3/5 | NIST/IETF | FIPS 203 (ML-KEM) | IETF |  |
|  | RSA (Note 31) | Same | Yes |  | ML-KEM-512/1024 | 1/5 | NIST/IETF | FIPS 203 (ML-KEM) | IETF |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  | (EC)DHE (Note 32) | Same | Yes |  | ML-DSA-44/65/87 | 2/3/5 | NIST/IETF | FIPS 204 (ML-DSA) | IETF |  |
|  | (EC)DHE (Note 32) | Same | Yes |  |  SLH-DSA-SHA2/ SHAKE- 128f/s / 192f/s 256f/s  | 1/3/5 | NIST/IETF | FIPS 205 (SLH-DSA) | IETF |  |
|  | (EC)DHE (Note 32) | Same | Yes |  |  FN-DSA-512/1024 | 1/5 | NIST/IETF | FIPS 205 (SLH-DSA) | IETF |  |
|  | RSA (Note 32) | Same | Yes |  | ML-DSA-44/65/87 | 2/3/5 | NIST/IETF | FIPS 204 (ML-DSA) | IETF |  |
|  | RSA (Note 32) | Same | Yes |  |  SLH-DSA-SHA2/ SHAKE- 128f/s / 192f/s 256f/s  | 1/3/5 | NIST/IETF | FIPS 205 (SLH-DSA) | IETF |  |
|  | RSA (Note 32) | Same | Yes |  |  FN-DSA-512/1024 | 1/5 | NIST/IETF | FIPS 205 (SLH-DSA) | IETF |  |
| OAuth 2.0 |  |  | Yes | RFC8252, RFC8996 |  |  |  |  |  |  |
| DTLS |  |  | Yes | RFC8996 |  |  |  |  |  |  |
| IPSec | Diffie-Hellman (Note 31) | N2, N3, N4, N6, N9, Gm (Note 33) | Yes | TS 33.210 | ML-KEM-512/768/1024 | 1/3/5 | NIST/IETF | FIPS 203 (ML-KEM) | IETF |  |
|  | (EC)DHE (Note 32) | Same | Yes |  | ML-DSA-44/65/87 | 2/3/5 | NIST/IETF | FIPS 204 (ML-DSA) | IETF |  |
|  | (EC)DHE (Note 32) | Same | Yes |  | SLH-DSA-SHA2/ SHAKE- 128f/s / 192f/s 256f/s  | 1/3/5 | NIST/IETF | FIPS 205 (SLH-DSA) | IETF |  |
|  | (EC)DHE (Note 32) | Same | Yes |  | FN-DSA-512/1024 | 1/5 | NIST/IETF | FIPS 205 (SLH-DSA) | IETF |  |
|  | RSA (Note 32) | Same | Yes |  | ML-DSA-44/65/87 | 2/3/5 | NIST/IETF | FIPS 204 (ML-DSA) | IETF |  |
|  | RSA (Note 32) | Same | Yes |  | SLH-DSA-SHA2/ SHAKE- 128f/s / 192f/s 256f/s  | 1/3/5 | NIST/IETF | FIPS 205 (SLH-DSA) | IETF |  |
|  | RSA (Note 32) | Same | Yes |  | FN-DSA-512/1024 | 1/5 | NIST/IETF | FIPS 205 (SLH-DSA) | IETF |  |
|  |  |  |  |  |  |  |  |  |  |  |
| JWS | ECDSA | OAuth2.0 token signing | Yes | RFC 7515 | ML-DSA-44/65/87 | 2/3/5 | NIST/IETF | FIPS 204 (ML-DSA) | IETF |  |
|  |  | OAuth2.0 token signing | Yes |  | SLH-DSA-SHA2/ SHAKE-128f/s / 192f/s 256f/s  | 1/3/5 | NIST/IETF | FIPS 205 (SLH-DSA) | IETF |  |
|  |  | Same | Yes |  | FN-DSA-512/1024 | 1/5 | NIST/IETF | FIPS 205 (SLH-DSA) | IETF |  |
| JWE | (EC)DHE (Note 34) | N32-c, N32-f | Yes | RFC 7516 | ML-KEM-512/768/1024 | 1/3/5 | NIST/IETF | FIPS 203 (ML-KEM) | IETF |  |
|  | RSA (Note 34) | Same | Yes |  | ML-KEM-512/1024 | 1/5 | NIST/IETF | FIPS 203 (ML-KEM) | IETF |  |

NOTE 31: Algorithm for key agreement.

NOTE 32: Algorithm for digital signature and authentication.

NOTE 33: The list of interfaces is not exhausted but only included main interfaces, other interfaces introduced by new features are not listed.e.g., IMS media plane, Edge computing, ProSe, Location related interface, and SNPN, NSSAA, secondary authentication related interfaces and protocols, etc.

NOTE 34: JWE is used for the message encryption between the SEPPs and it uses ECDHE or RSA (e.g., TLS based key exchanged via separate N32c) for key exchange.

NOTE 35: Will have to be edited once the corresponding RFC(s) have been published.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*