ETSI TR 133 938 V19.1.0 (2026-01)

TECHNICAL REPORT

5G;
3GPP Cryptographic Inventory
(3GPP TR 33.938 version 19.1.0 Release 19)

Reference
DTR/TSGS-0333938vj10

Keywords
5G,SECURITY

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI IPR online database.

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Legal Notice

This Technical Report (TR) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 3GPP and ETSI identities can be found at 3GPP to ETSI numbering cross-referencing.

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

In the present document, modal verbs have the following meanings:

shall indicates a mandatory requirement to do something

shall not indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

should indicates a recommendation to do something

should not indicates a recommendation not to do something

may indicates permission to do something

need not indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

can indicates that something is possible

cannot indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

will indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

will not indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

might indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

might not indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

is (or any other verb in the indicative mood) indicates a statement of fact

is not (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

1 Scope

The present document lists the security protocols that use cryptography in 3GPP specifications for the 5G System in the Standalone mode. They

- include the type of cryptography used by the protocol (symmetric/asymmetric)
- include the pointers to the protocol specification
- include the pointers to the relevant 3GPP cryptographic profiles
- include usage type (e.g., integrity, confidentiality, and/or authentication)

NOTE 1: the present document does not include resolution to PQC migration, and does not contain solutions that lead to any specification/normative work.

NOTE 2: the present document does not include protocols for Lawful Interception systems. The cryptographic inventory for those protocols is documented in TS 33.128 [49].

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".

[2] 3GPP TS 33.210: "3G security; Network Domain Security (NDS); IP network layer security".

[3] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

[4] 3GPP TS 33.501: “Security architecture and procedures for 5G system”.

[5] IETF RFC 9190: "EAP-TLS 1.3: Using the Extensible Authentication Protocol with TLS 1.3".

[6] IETF RFC 5216: "The EAP-TLS Authentication Protocol".

[7] SECG SEC 1: “Recommended Elliptic Curve Cryptography”, Version 2.0, 2009. Available at http://www.secg.org/sec1-v2.pdf.

[8] SECG SEC 2: “Recommended Elliptic Curve Domain Parameters”, Version 2.0, 2010. Available at http://www.secg.org/sec2-v2.pdf.

[9] IETF RFC 9001: "Using TLS to Secure QUIC".

[10] IETF RFC 8152: "CBOR Object Signing and Encryption (COSE)".

[11] 3GPP TS 33.220: “Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)”.

[12] IETF RFC 8613: "Object Security for Constrained RESTful Environments (OSCORE)".

[13] 3GPP TS 33.180: "Security of the Mission Critical (MC) service".

[14] IETF RFC 6509: "MIKEY-SAKKE: Sakai-Kasahara Key Encryption in Multimedia Internet KEYing (MIKEY)".

[15] IETF RFC 5448: "Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')".

[16] 3GPP TS 35.205: "3G Security; Specification of the MILENAGE algorithm set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*".

[17] 3GPP TS 35.231: "Specification of the TUAK algorithm set: A second example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 1: Algorithm specification".

[18] 3GPP TS 35.234: "Specification of the MILENAGE-256 algorithm set; An example set of 256-bit 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5, f5* and f5**; Document 1: General".

[19] NIST IR 8547 ipd: “Transition to Post-Quantum Cryptography Standards”

[20] IETF RFC 9147: "The Datagram Transport Layer Security (DTLS) Protocol Version 1.3".

[21] IETF RFC 8446: "The Transport Layer Security (TLS) Protocol Version 1.3".

[22] IETF RFC 6960: " X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP".

[23] IETF RFC 7296: " Internet Key Exchange Protocol Version 2 (IKEv2)".

[24] IETF RFC 4303: "IP Encapsulating Security Payload (ESP)".

[25] IETF RFC 8221: "Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)".

[26] IETF RFC 8750: "Implicit Initialization Vector (IV) for Counter-Based Ciphers in Encapsulating Security Payload (ESP)".`

[27] IETF RFC 7516: "JSON Web Encryption".

[28] IETF RFC 7515: "JSON Web Signature (JWS)".

[29] IETF RFC 6507: “Elliptic Curve-Based Certificateless Signatures for Identity-Based Encryption (ECCSI)”

[30] IETF RFC 6508: “Sakai-Kasahara Key Encryption (SAKKE)"

[31] IETF RFC 5869: "HMAC-based Extract-and-Expand Key Derivation Function (HKDF)".

[32] IETF RFC 4303: "IP Encapsulating Security Payload (ESP)".

[33] IETF RFC 3602: "The AES-CBC Cipher Algorithm and Its Use with IPsec".

[34] IETF RFC 4106: "The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)".

[35] IETF RFC 4543: "The Use of Galois Message Authentication Code (GMAC) in IPsec ESP and AH".

[36] IETF RFC 4868: "Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPs".

[37] IETF RFC 6347: “Datagram Transport Layer Security Version 1.2”.

[38] IETF RFC 5246: “The Transport Layer Security (TLS) Protocol Version 1.2”.

[39] IETF RFC 5281: "Extensible Authentication Protocol Tunnelled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0)".

[40] IETF RFC 6749: "The OAuth 2.0 Authorization Framework".

[41] IETF RFC 6750: "The OAuth 2.0 Authorization Framework: Bearer Token Usage".

[42] IETF RFC 7519: "JSON Web Token (JWT)".

[43] 3GPP TS 29.500: "Technical Realization of Service Based Architecture".

[44] 3GPP TS 38.323: "Packet Data Convergence Protocol (PDCP) specification".

[45] IETF RFC 8017: "PKCS#1: RSA Cryptography Specifications Version 2.2".

[46] IETF RFC 4754: "IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA)".

[47] NIST FIPS PUB 180-4: "Secure Hash Standard (SHS)".[48]IETF RFC 8442: "ECDHE_PSK with AES-GCM and AES-CCM Cipher Suites for TLS 1.2 and DTLS 1.2”.

[49] 3GPP TS 33.128: " Protocol and procedures for Lawful Interception (LI)".

3 Definitions of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in 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 TR 21.905 [1].

Asymmetric Cryptography (NIST IR 8547 [19]): Also known as public-key cryptography, it is the cryptography that uses two separate keys to exchange data: one to encrypt or digitally sign the data and one to decrypt the data or verify the digital signature.

Key Agreement (NIST IR 8547 [19]): A (pair-wise) key-establishment procedure where the resultant secret keying material is a function of information contributed by two participants so that no party can predetermine the value of the secret keying material independently from the contributions of the other party.

Key Derivation (NIST IR 8547 [19]): The process of deriving a key in a non-reversible manner from shared information, some of which is secret.

Symmetric Key Cryptography (NIST IR 8547 [19]): A cryptographic algorithm that uses the same secret key for its operation and, if applicable, for reversing the effects of the operation.

3.2 Symbols

Void

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].

5G-AKA	5G Authentication and Key Agreement
AEAD	Authenticated Encryption with Associated Data
BSF	Bootstrapping Server Function
CBOR	Concise Binary Object Representation
COSE	CBOR Object Signing and Encryption
CSK	Client-Server Key
DTLS	Datagram Transport Layer Security
EAP-AKA’	Improved Extensible Authentication Protocol Method for 3GPP Mobile Network Authentication and Key Agreement
EAP-TLS	Extensible Authentication Protocol Transport Layer Security

EAP-TTLS	Extensible Authentication Protocol Tunnelled Transport Layer Security
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
ECIES	Elliptic Curve Integrated Encryption Scheme
ESP	Encapsulating Security Payload
GMK	Group Master Key
HKDF	HMAC-based Key Derivation Function
HMAC	Hash-Based Message Authentication Code
IKE	Internet Key Exchange
IKEv2	Internet Key Exchange Protocol Version 2
IPsec	Internet Protocol Security
JSON	JavaScript Object Notation
JWE	JSON Web Encryption
JWS	JSON Web Signature
JWT	JSON Web Token
KDF	Key Derivation Function
MIKEY-SAKKE	Multimedia Internet KEYing – Sakai-Kasahara Key Encryption
MPQUIC	Multipath QUIC
MuSiK	Multicast Signalling Key
NAS	Non-Access Stratum
NDS	Network Domain Security
OAuth	Open Authorization
OCSP	Online Certificate Status Protocol
OSCORE	Object Security for Constrained RESTful Environments
PCK	Private Call Key
PDCP	Packet Data Convergence Protocol
PKI	Public Key Infrastructure
QUIC	Quick UDP Internet Connections
REST	Representational State Transfer
RSA	Rivest-Shamir-Adleman
SA	Security Association
SECG	Standards for Efficient Cryptography
SHA	Secure Hash Algorithm
SUPI	Subscription Permanent Identifier
TLS	Transport Layer Security
UDP	User Datagram Protocol

4 3GPP Cryptographic Inventory – 5G System

4.1 General

This clause provides inventory of security protocols that use cryptography in 3GPP specifications for 5G systems (limited to the standalone mode). The clause 4.2 presents inventory in detailed lists, and the clause 4.3 summarizes them in tables.

4.2 Detailed Protocol List

4.2.1 DTLS

DTLS specified in IETF RFC 9147 [20] is used in 5G system in standalone mode to protect the following:

- N2 interface (see clause 9.2 of TS 33.501 [4]).
- Xn interface (see clause 9.4 of TS 33.501 [4]).
- DIAMETER or GTP-based interfaces (see clause 9.5 of TS 33.501 [4]).
- gNB internal interfaces (see clause 9.8 of TS 33.501 [4]).

Security profiles for DTLS implementation and usage in 3GPP are given in clause 6.2 of TS 33.210 [2] and the certificate profile is given in clause 6.1.3a of TS 33.310 [3].

DTLS employs symmetric cryptography for confidentiality and integrity protection.

DTLS employs asymmetric cryptography for digital signature and key agreement.

4.2.2 TLS

TLS specified in IETF RFC 8446 [21] is used in 5G system in standalone mode to protect the following:

- NIDD interfaces (see clause 6.16.3 of TS 33.501 [4]).
- DIAMETER or GTP-based interfaces (see clause 9.5 of TS 33.501 [4]).
- NEF – AF interface (see clauses 12.2 and 12.3 of TS 33.501 [4]).
- Interfaces between network functions (see clauses 13.1, 13.2, 13.5 of TS 33.501 [4]).
- N32 interface (see clause 13.2 of TS 33.501 [4]).
- Network slice management interfaces (see clauses 15.2 and 15.3 of TS 33.501 [4]).
- Message Service interfaces for MIoT over the 5G System (see clauses Y.2 – Y.4 of TS 33.501 [4]).

Security profiles for TLS implementation and usage in 3GPP are given in clause 6.2 of TS 33.210 [2] and the certificate profile is given in clause 6.1.3a of TS 33.310 [3].

TLS employs symmetric cryptography for confidentiality and integrity protection.

TLS employs asymmetric cryptography for digital signature and key agreement.

4.2.3 EAP-TLS

EAP-TLS [5][6] is used in 5G system in standalone mode to realise the following:

- Mutual authentication between UE and AUSF (see Annex B, Annex I of TS 33.501 [4])
- Mutual authentication between UE and AAA (see Annex I of TS 33.501 [4])
- Mutual authentication between N5GC and AUSF (see Annex O of TS 33.501 [4])

The 3GPP TLS protocol profile related to supported TLS versions and supported TLS cipher suites in 3GPP networks is specified in clause 6.2 of TS 33.210 [2]. The 3GPP profile of TLS certificates is specified in clause 6.1.3a of TS 33.310 [3].

EAP-TLS employs asymmetric cryptography for authentication and key agreement.

EAP-TLS employs symmetric cryptography for authentication and key agreement.

EAP-TLS employs hash function for session key derivation.

4.2.4 ECIES

ECIES is used in 5G system in standalone mode for the following:

- Confidentiality and Integrity Protection of the SUPI (see Annex C.3 of TS 33.501 [4]).

The ECIES profiles follow the terminology and processing specified in SECG version 2 [7] and [8]. The security profiles for the ECIES implementation and usage in 3GPP is given in clause C.3.4 of TS 33.501 [4].

ECIES employs asymmetric cryptography for the key agreement of the symmetric keys.

ECIES employs symmetric cryptography for the confidentiality and integrity protection of the SUPI.

4.2.5 PKI

PKI is used in 5G system in standalone mode for the following:

- Issuing of X.509 certificates (see Clause 4 of TS 33.310 [3]).
- PKI architecture for NDS/AF (see Clause 5.1 of TS 33.310 [3]).

PKI employs asymmetric cryptography for certificate signing and verification.

PKI employs hash function for computation of digests.

4.2.6 Online Certificate Status Protocol (OCSP)

Online Certificate Status Protocol (OCSP) specified in IETF RFC 6960 [22] is used in 5G system in standalone mode for the following:

- Certificate status request, i.e., OCSP stapling (see clause B.2.2 of TS 33.501 [4]).
- Revocation of subscriber certificates (see Clause B.2.2 of TS 33.501 [4]).

OCSP and the related profiles are in Clause 6.1b of TS 33.310 [3].

OCSP employs asymmetric cryptography for digital signing and signature verification.

OCSP employs hash algorithms for computation of digests.

4.2.7 QUIC and MPQUIC

The QUIC and MPQUIC are used in 5G system in standalone mode for the following:

- QUIC is used for the security of connection between UPF and AS proxy (see Clause 18 of TS 33.501 [4]).
- MPQUIC steering functionality is used for ATSSS (see Clause AA of TS 33.501 [4]).

For the QUIC establishment, the RFC 9001 [9] mandates the use of TLS with the exception of TLS_AES_128_CCM_8_SHA256.

4.2.8 CBOR Object Signing and Encryption (COSE)

The COSE [10] is used in 5G system in standalone mode for the following:

- OSCORE [12] for cryptographic algorithm selection between UE and BSE (reference point Ua) (see Clause P.3.3 of TS 33.220 [11]).

COSE employs asymmetric cryptography for digital signature and key agreement.

COSE employs symmetric cryptography for confidentiality and integrity protection.

COSE employs hash functions for session key derivation.

4.2.9 MIKEY-SAKKE

MIKEY-SAKKE is used in the 5G system to securely transport cryptographic keys for Mission Critical Services. It is used in the following scenarios:

- Group Master Keys (GMKs) from a Group Management Server to a Group Management Client on a MC UE (see Annex E clause E.2 TS 33.180 [13])
- Private Call Keys (PCKs) between MC UEs (see Annex E clause E.3 TS 33.180 [13])
- Client-Server keys (CSKs) between MCX Server and MC client (see Annex E clause E.3 TS 33.180 [13])
- Multicast Signalling Keys (MuSiK) from MCX Servers to MC clients (see Annex E clause E.3 TS 33.180 [13])

Security profiles for MIKEY-SAKKE are left for implementation.

MIKEY-SAKKE is specified in IETF RFC 6509 [14].

MIKEY-SAKKE employs asymmetric cryptography for key distribution.

4.2.10 IKEv2

IKEv2 protocol is specified in IETF RFC 7296 [23] to perform authentication and setup Security Associations (SA) for IPsec tunnels. The IPsec ESP protocol is described in clause 4.2.15.

IKEv2 is used in 5G system to provide security for the following:

- Untrusted non-3GPP access to the 5G core network (see clause 7 of TS 33.501 [4]) and trusted non-3GPP access to the 5G core network (see clause 7 of TS 33.501 [4])
- IP based interfaces for 5GC and 5G-AN according to NDS/IP (see clause 9 of TS 33.501 [4])
- N2 interface between the AMF and the 5G-AN (see clause 9.2 of TS 33.501 [4])
- N3 interface between the UPF and 5G-AN (see clause 9.3 of TS 33.501 [4])
- Xn interface between 5G-AN (see clause 9.4 of TS 33.501 [4])
- F1 and E1 of the gNB internal interfaces (see clause 9.8 of TS 33.501 [4])
- Non-SBA interfaces internal to 5GC and between PLMNs (see clause 9.9 of TS 33.501 [4])
- F1 interface between the IAB-node (gNB-DU) and the IAB-donor-CU (see clause M3.3 and M5 of TS 33.501 [4])

Security profiles for IKEv2 implementation and usage in 3GPP are given in clauses 5.2, 5.4, and 5.6 of TS 33.210 [2] and clauses 5, 6.2, and 7.5 of TS 33.310 [3].

IKEv2 employs symmetric cryptography for confidentiality and integrity protection.

IKEv2 employs asymmetric cryptography for digital signature and key agreement.

IKEv2 employs both symmetric cryptography and asymmetric cryptography for authentication.

4.2.11 PDCP security

The PDCP security protocol between the UE and the NG-RAN is responsible for the security protection of the following scenarios in 5G system:

- RRC integrity and confidentiality protection between UE and gNB (see clause 6.5.1 and 6.5.2 of TS 33.501 [4]).
- User plane data integrity and confidentiality protection between UE and gNB (see clause 6.6.3 and 6.6.4 of TS 33.501 [4]).

PDCP security protocol employs symmetric cryptography for confidentiality and integrity protection.

4.2.12 NAS security

The NAS security mechanisms are to protect NAS signaling and data between the UE and the AMF over the N1 reference point in 5G system:

- NAS signaling integrity and confidentiality protection between UE and AMF (see clause 6.4.3 and 6.4.4 of TS 33.501 [4]).
- Integrity and confidentiality protection for small user data or SMS as payload of a NAS message between UE and AMF (see clauses 6.16.1 and 6.4.7 of TS 33.501 [4]).

NAS security protocol employs symmetric cryptography for confidentiality and integrity protection.

4.2.13 EAP-AKA’

EAP-AKA’ enables mutual authentication between the UE and AUSF and provides keying material that can be used between the UE and the serving network in subsequent security procedures.

The long term key K and the SUPI are preconfigured in the USIM (in the UE) and in the UDM/ARPF.

EAP-AKA' is specified in RFC 5448 [15].

The 3GPP 5G profile for EAP-AKA' is specified in the normative Annex F of TS 33.501 [4].

KDF for key generation is HMAC-SHA-256 as per Annex B.2.0 of TS 33.220 [11].

EAP-AKA’ requires functions as described for 128 Bit MILENAGE in TS 35.205 [16], 128 Bit or 256 Bit TUAK in TS 35.231 [17] and in TS 35.234 [18] for 256 Bit MILENAGE.

EAP-AKA’ employs symmetric cryptography for authentication and key agreement.

EAP-AKA’ employs hash function for session key derivation.

4.2.14 5G-AKA

5G-AKA enables mutual authentication between the UE and AUSF with proof of successful authentication of the UE from the visited network. 5G-AKA provides keying material that can be used between the UE and the serving network in subsequent security procedures.

The long term key K and the SUPI are preconfigured in the USIM (in the UE) and in the UDM/ARPF.

- 5G-AKA is specified in TS 33.501 [4].
- KDF for key generation is HMAC-SHA-256 as per Annex B.2.0 of TS 33.220 [11].

5G-AKA requires functions as described for 128 Bit MILENAGE in TS 35.205 [16], 128 Bit or 256 Bit TUAK in TS 35.231 [17] and in TS 35.234 [18] for 256 Bit MILENAGE.

5G-AKA employs symmetric cryptography for authentication and key agreement.

5G-AKA employs hash function for session key derivation.

4.2.15 IPsec ESP

IPsec ESP specified in IETF RFC 4303 [24], RFC 8221 [25], RFC 8750 [26] is used in 5G system to provide security for the following:

- Untrusted non-3GPP access to the 5G core network (see clause 7 of TS 33.501 [4]) and trusted non-3GPP access to the 5G core network (see clause 7 of TS 33.501 [4])
- IP based interfaces for 5GC and 5G-AN according to NDS/IP (see clause 9 of TS 33.501 [4])
- N2 interface between the AMF and the 5G-AN (see clause 9.2 of TS 33.501 [4])
- N3 interface between the UPF and 5G-AN (see clause 9.3 of TS 33.501 [4])
- Xn interface between 5G-AN (see clause 9.4 of TS 33.501 [4])
- F1 and E1 of the gNB internal interfaces (see clause 9.8 of TS 33.501 [4])
- Non-SBA interfaces internal to 5GC and between PLMNs (see clause 9.9 of TS 33.501 [4])
- F1 interface between the IAB-node (gNB-DU) and the IAB-donor-CU (see Annex M3.3 and M5 of TS 33.501 [4])
- Policy discrimination of GTP-C, GTP-U and protection of GTP-C transport protocol (see Annex B of TS 33.210 [2])

- Protection of IMS protocols and interfaces for all SIP signalling traversing inter-security domain boundaries. (see Annex C of TS 33.210 [2])
- Protection of UTRAN/GERAN IP transport protocols and interfaces for all RANAP and RNSAP messages traversing inter-security domain boundaries. (see Annex D of TS 33.210 [2])

Security profile for IPsec ESP implementation in 3GPP are given in clause 5.3 of TS 33.210 [2].

IPSec ESP employs symmetric cryptography for confidentiality, integrity and replay protection.

Keying happens using IKEv2 (Internet Key Exchange Protocol Version 2 (IKEv2) as mentioned in clause 4.2.10.

4.2.16 Key Derivation Function (KDF)

The KDF is used in 5G system in standalone mode and is defined in the normative Annex A of TS 33.501 [4].

- The generic KDF for the purpose of a cryptographic key computation is specified in the normative Annex B.2 of TS 33.220 [11].

The KDF employs hash function for key derivation.

4.2.17 JWE and JWS

JSON Web Encryption (JWE) specified in IETF RFC 7516 [27] and/or JSON Web Signature (JWS) specified in IETF RFC 7515 [28] are used in 5G system in standalone mode to protect the following:

- N32 interface (see clause 13.2 of TS 33.501 [4]).
- NF service access (see clause 13.4 of TS 33.501 [4]).

Profiles for JWE/JWS implementation and usage in 3GPP are given in clause 6.3 of TS 33.210 [2].

JWE/JWS employ symmetric cryptography for confidentiality and integrity protection.

JWE/JWS employ asymmetric cryptography for digital signature and key agreement.

4.2.18 EAP-TTLS

EAP-TTLS is an authentication protocol specified in RFC 5281 [39].

EAP-TTLS is used in 5G system to provide security for the following:

- Security of UE onboarding in SNPNs (clause I.9 of TS 33.501 [4])
- Primary authentication using EAP-TTLS in SNPNs (clause U of TS 33.501 [4])
- Authentication of AUN3 devices using additional EAP methods (clause Z.2 of TS 33.501 [4])

EAP-TTLS employs both asymmetric cryptography and symmetric cryptography for authentication and key agreement.

EAP-TTLS employs hash function for session key derivation.

4.2.19 OAuth 2.0

The OAuth 2.0 protocol is an authorization framework enabling a third-party application to obtain limited access to an HTTP service as specified in RFC 6749 [40]. The usage of bearer tokens in OAuth 2.0 and JSON Web Token (JWT) are specified in RFC 6750 [41] and RFC 7519 [42] respectively. The former requires TLS (see also in the clause 4.2.2) to secure transmission of token whereas the latter uses JSON Web Signature (JWS) (see also in the clause 4.2.17) for integrity protection of token.

OAuth 2.0, using JWT bearer token, is used in 5G system to provide security for the following:

- Authorization of Application Function (clause 12.4 of TS 33.501 [4])

- Authorization for the Service Based Interface (clauses 13 and 14 of TS 33.501 [4] and clause 6.7 of TS 29.500 [43])
- Authentication for the management service for network slices (clause 15 of TS 33.501 [4])
- Authorization of NF Service for network automation (clause X.2 of TS 33.501 [4])

Cryptographic algorithms, features and usage types for TLS and JWT are described in clauses 4.2.2 and 4.2.17 respectively.

4.3 Summary Tables

4.3.1 3GPP Symmetric Cryptographic Algorithms

The following table summarizes the security related protocols used in 3GPP employing symmetric cryptographic algorithms including hash functions (5G System).

Table 4.3.1-1: Protocols Used in 3GPP Employing Symmetric Cryptographic Algorithms (5G System)

Protocol/Function	Protocol Profile, Clauses	Cryptographic Algorithm(s)	Feature(s), Usage Type
COSE (IETF RFC 8152[10])	TS 33.220 [11], Clause P.3.3	HMAC-based KDF with SHA-256 [31]	Session Key Derivation / Hash Function
		AES-CCM-16-64-128	Confidentiality and Integrity Protection
DTLS 1.2 (IETF RFC 6347 [37])	TS 33.210 [2] clause 6.2.1	See TLS 1.2 in this table	Confidentiality and Integrity Protection
DTLS 1.3 (IETF RFC 9147 [20])	TS 33.210 [2] clause 6.2.1	See TLS 1.3 in this table	Confidentiality and Integrity Protection
EAP-TLS (IETF RFCs 9190 [5], 5216 [6])	TS 33.501 [4], Clause B.2.1	AEAD_AES_128_GCM	Confidentiality and Integrity Protection
		HKDF (RFC5869 [31])	Session Key Derivation
EAP TTLS (IETF RFC 5281 [39])	TS 33.501 [4], Annex U TS 33.210 [2] clause 6.2 for TLS	See TLS in this table	Confidentiality and Integrity Protection
			Session Key Derivation
ECIES ([7], [8])	TS 33.501 [4], Clause C.3	SHA-256, HMAC-SHA-256,	Session Key Derivation
		HMAC–SHA-256	Integrity Protection
		AES-128-CTR	Confidentiality Protection
IKEv2 (IETF RFC 7296 [23])	TS 33.210 [2] clause 5.4	128-AES GCM SHA-256 (IETF RFC 8442 [48]) 256-AES GCM SHA-384 (IETF RFC 8442 [48])	Confidentiality and Integrity Protection
	TS 33.310 [3] clauses 5,6,7	SHA2-256/384 [47]	Hash Function
IPsec ESP (IETF RFCs 4303 [32], 8221 [25], 8750 [26])	TS 33.210 [2]	ENCR_AES_CBC (IETF RFC 3602 [33])	Confidentiality Protection
		ENCR_AES_GCM_16 (IETF RFC 4106 [34]) ENCR_AES_GCM_16_IIV (IETF RFC 8750 [26])	Confidentiality and Integrity Protection
		AUTH_AES_128_GMAC (IETF RFC 4543 [35]) AUTH_HMAC_SHA2_256_128 (IETF RFC 4868 [36])	Authentication

Protocol/Function	Protocol Profile, Clauses	Cryptographic Algorithm(s)	Feature(s), Usage Type
JWE (IETF RFC 7516 [27])	TS 33.210 [2] clauses 6.3.1, 6.3.2	AES_128_GCM, AES_256_GCM	Confidentiality and Integrity Protection
JWS (IETF RFC 7515 [28])	TS 33.210 [2] clauses 6.3.1, 6.3.3	SHA-256	Hash Function
KDF (TS 33.220, Clause B.2 [11])	TS 33.220 [11], Clause B.2.0	HMAC-SHA-256	Session Key Derivation
	TS 33.501 [4], Clause C.3	ANSI-X9.63-KDF	Session Key Derivation
MIKEY-SAKKE (IETF RFC 6509) [14]	IETF RFC 6509 [14], Appendix A	SHA-256	Hash Function
NAS security (TS 33.501 [4])	TS 33.501 [4], Annex D	128-NEA1, 128-NIA1 128-NEA2, 128-NIA2 128-NEA3, 128-NIA3	Confidentiality and Integrity Protection
OAuth 2.0 (IETF RFC 6749 [40], 6750 [41])	TS 33.210 [2] clause 6.2 for TLS	See TLS 1.2 and TLS 1.3 in this table	Confidentiality and Integrity Protection
			Hash Function
	TS 33.210 [2] clause 6.3 for JWE/JWS	See JWE and JWS in this table	Confidentiality and Integrity Protection
			Hash Function
OCSP (IETF RFC 6960 [22])	TS 33.310 [3], Clause 6.1b	SHA-256 SHA-384	Hash Function
PDCP security (TS 38.323 [44])	TS 33.501 [4], Annex D	128-NEA1, 128-NIA1 128-NEA2, 128-NIA2 128-NEA3, 128-NIA3	Confidentiality and Integrity Protection
PKI	TS 33.310 [3], Clause 6.1.1	SHA-256 SHA-384	Hash Function
TLS 1.2 (IETF RFC 5246 [38])	TS 33.210 [2] clauses 6.2.1, 6.2.3	AES_128_GCM, AES_256_GCM	Confidentiality and Integrity Protection
		SHA256, SHA384	Hash Function
TLS 1.3 (IETF RFC 8446 [21])	TS 33.210 [2] clauses 6.2.1, 6.2.2	AES_128_GCM, AES_256_GCM, CHACHA20_POLY1305	Confidentiality and Integrity Protection
		SHA-256, SHA-384	Hash Function

4.3.2 3GPP Asymmetric Cryptographic Algorithms

The following table summarizes the security related protocols used in 3GPP employing asymmetric cryptographic algorithms (5G System).

Table 4.3.2-1: Protocols Used in 3GPP Employing Asymmetric Cryptographic Algorithms (5G System)

Protocol/Function	Protocol Profile, Clauses	Cryptographic Algorithm(s)	Feature(s), Usage Type
DTLS 1.2 (IETF RFC 6347 [37])	TS 33.210 [2] clause 6.2.1	See TLS 1.2 in this table	Confidentiality and Integrity Protection
DTLS 1.3 (IETF RFC 9147 [20])	TS 33.210 [2] clause 6.2.1	See TLS 1.2 in this table	Confidentiality and Integrity Protection
EAP-TLS (IETF RFCs 9190 [5], 5216 [6])	TS 33.501 [4], Clause B.2.1	See TLS in this table.	Authentication / Digital Signature / Confidentiality Protection / Hash Function
	TS 33.501 [4] RFC 9190 (TLS1.3) [5]	ECDHE	Key Agreement
EAP-TTLS (IETF RFC 5281 [39])	TS 33.501 [4], Annex U TS 33.210 [2] clause 6.2 for TLS	See TLS in this table	Key Agreement
		See TLS in this table	Authentication / Digital Signature / Confidentiality Protection / Hash Function
ECIES ([7], [8])	TS 33.501 [4], Clause C.3	ECDH	Key Agreement
IKEv2 (IETF RFC 7296 [23])	TS 33.210 [2] clause 5.4	DH	Key Agreement

Protocol/Function	Protocol Profile, Clauses	Cryptographic Algorithm(s)	Feature(s), Usage Type
	TS 33.310 [3] clauses 5,6,7	RSA Sha-256/384 (IETF RFC 8017 [45]) ECDSA SHA-256/384/512 (IETF RFC 4754 [46]) RSASSA-PSS SHA-256 [47]	Digital Signature
		SHA2-256/384 [47]	Hash Function
JWE (IETF RFC 7516 [27])	TS 33.210 [2] clauses 6.3.1, 6.3.2	ECDH-ES	Key Agreement
JWS (IETF RFC 7515 [28])	TS 33.210 [2] clauses 6.3.1, 6.3.3	ECDSA	Digital Signature
MIKEY-SAKKE (IETF RFC 6509) [14]	IETF RFC 6507 [29]	ECCSI	Digital signature
	IETF RFC 6508 [30]	SAKKE	Key agreement
OAuth 2.0 (IETF RFC 6749 [40], 6750 [41])	TS 33.210 [2] clause 6.2 for TLS	See TLS 1.2 and TLS 1.3 in this table	Key Agreement
			Digital Signature
	TS 33.210 [2] clause 6.3 for JWE/JWS	See JWE and JWS in this table	Key Agreement
			Digital Signature
OCSP (IETF RFC 6960 [22])	TS 33.310 [3], Clause 6.1b	RSA ECDSA	Authentication / Digital Signature
PKI	TS 33.310 [3], Clause 6.1.1	RSA, ECDSA	Authentication / Digital Signature
TLS 1.2 (IETF RFC 5246 [38])	TS 33.210 [2] clauses 6.2.1, 6.2.3	ECDHE	Key Agreement
		ECDSA, RSA	Digital Signature
TLS 1.3 (IETF RFC 8446 [21])	TS 33.210 [2] clauses 6.2.1, 6.2.2	ECDHE	Key Agreement
		ECDSA, RSA	Digital Signature

Annex A:
Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2025-06	SA#108	SP-250647				Presented for information and approval	1.0.0
2025-06	SA#108					Upgrade to change control version	19.0.0
2025-09	SA#109	SP-251014	0003	1	F	Adding references, formatting tables and providing corrections to 4.2.12 for TR 33.938	19.1.0

History

Document history		
V19.1.0	January 2026	Publication