**3GPP TSG-SA3 Meeting #124 S3-253314-r1**

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

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** |  | **rev** | **-** | **Current version:** |  |  |
|  | | | | | | | | |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* | | | | | | | | |
|  | | | | | | | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME |  | Radio Access Network |  | Core Network |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Adding MOBIKE protocol to inventory list | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Huawei, HiSilicon | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | FS\_CryptoInv | | | | |  | ***Date:*** | | | 2025-10-06 |
|  |  | | | |  | |  | | |  |
| ***Category:*** |  |  | | | | | ***Release:*** | | | Rel-19 |
|  | *Use one of the following categories:* ***F*** *(correction)* ***A*** *(mirror corresponding to a change in an earlier release)* ***B*** *(addition of feature),* ***C*** *(functional modification of feature)* ***D*** *(editorial modification)*  Detailed explanations of the above categories can be found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | | | | | | | | *Use one of the following releases: Rel-8 (Release 8) Rel-9 (Release 9) Rel-10 (Release 10) Rel-11 (Release 11) … Rel-15 (Release 15) Rel-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | Missing MOBIKE protocol using cryptographic algorithms | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Addition of a subclause for the MOBIKE protocol | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Incomplete TR | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | |  | **x** | Other core specifications | | | | TS/TR ... CR ... | | |
| ***affected:*** | |  | **x** | Test specifications | | | | TS/TR ... CR ... | | |
| ***(show related CRs)*** | |  | **x** | O&M Specifications | | | | TS/TR ... CR ... | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | | 2, 3.3, 4.2.x (new), 4.3.1, 4.3.2 | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | |  | | | | | | | | |

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".

[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)".

[x] IETF RFC 4555: "IKEv2 Mobility and Multihoming Protocol (MOBIKE)".

\* \* \* 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].

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

IAB Integrated Access and Backhaul

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

MOBIKE IKEv2 Mobility and Multihoming Protocol

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

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

### 4.2.x MOBIKE

The MOBIKE protocol, a mobility and multihoming extension to the IKEv2, is specified in IETF RFC 4555 [x].

MOBIKE is used in 5G systems to provide security association negotiation in the following scenarios:

- Security for trusted non-3GPP access to the 5G core network (see clause 7A of TS 33.501 [4])

- IAB inter-CU IPsec migration procedure (see clause M of TS 33.501 [4])

Security profiles for MOBIKE are left for implementation.

MOBIKE employs the same cryptography as the IKEv2 protocol described in clause 4.2.10, for confidentiality and integrity protection, digital signature and key agreement, and authentication.

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

### 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 |
| 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 |
| MOBIKE (IETF RFC 4555 [x]) | Left for implementation | See IKEv2 in this table | See IKEv2 in this table |
| 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 |

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

### 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 |
| 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 |
| MOBIKE (IETF RFC 4555 [x]) | Left for implementation | See IKEv2 in this table | See IKEv2 in this table |
| 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 |

\* \* \* End of Changes \* \* \* \*