3GPP TSG-SA3 Meeting #117 S3‑243642r1

Maastricht, Netherlands 19 - 23 August 2024

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  |  | **CR** | **DRAFT** | **rev** | 1 | **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 | **X** |

|  |
| --- |
|  |
| ***Title:***  | Living document of the Non3GPPMobEnh study |
|  |  |
| ***Source to WG:*** | Nokia |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | Non3GPPMob\_Sec |  | ***Date:*** | 2024-08-10 |
|  |  |  |  |  |
| ***Category:*** | B |  | ***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 canbe 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:*** | Draft Living CR of the Non3GPPMobEnh for normative work |
|  |  |
| ***Summary of change:*** | Draft Living CR is proposed. |
|  |  |
| ***Consequences if not approved:*** | Living CR is not available |
|  |  |
| ***Clauses affected:*** | 2, 7A, 7A.1, 7A.2.X, S.3.2 |
|  |  |
|  | **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:*** |  |
|  |  |
| ***This CR's revision history:*** | S3-242821, S3-243643 |

 **\* \* \* \* 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] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 23.501: "System Architecture for the 5G System".

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

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

[5] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

[6] IETF RFC 4301: "Security Architecture for the Internet Protocol".

[7] 3GPP TS 22.261: "Service requirements for next generation new services and markets".

[8] 3GPP TS 23.502: "Procedures for the 5G System".

[9] 3GPP TS 33.102: "3G security; Security architecture".

[10] 3GPP TS 33.401: "3GPP System Architecture Evolution (SAE); Security architecture".

[11] 3GPP TS 33.402: "3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses".

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

[13] 3GPP TS 24.301: " Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3".

[14] 3GPP TS 35.215: " Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2; Document 1: UEA2 and UIA2 specifications".

[15] NIST: "Advanced Encryption Standard (AES) (FIPS PUB 197)".

[16] NIST Special Publication 800-38A (2001): "Recommendation for Block Cipher Modes of Operation".

[17] NIST Special Publication 800-38B (2001): "Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication".

[18] 3GPP TS 35.221: " Specification of the 3GPP Confidentiality and Integrity Algorithms EEA3 & EIA3; Document 1: EEA3 and EIA3 specifications".

[19] 3GPP TS 23.003: "Numbering, addressing and identification".

[20] 3GPP TS 22.101: "Service aspects; Service principles".

[21] IETF RFC 4187: "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)".

[22] 3GPP TS 38.331: "NR; Radio Resource Control (RRC); Protocol specification".

[23] 3GPP TS 38.323: "NR; Packet Data Convergence Protocol (PDCP) specification".

[24] 3GPP TS 33.117: "Catalogue of general security assurance requirements".

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

[26] Void

[27] IETF RFC 3748: "Extensible Authentication Protocol (EAP)".

[28] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)".

[29] SECG SEC 1: Recommended Elliptic Curve Cryptography, Version 2.0, 2009. Available <http://www.secg.org/sec1-v2.pdf>

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

[31] 3GPP TS 38.470: "NG-RAN; F1 General aspects and principles".

[32] 3GPP TS 38.472: "NG-RAN; F1 signalling transport".

[33] 3GPP TS 38.474: "NG-RAN; F1 data transport".

[34] 3GPP TS 38.413: "NG-RAN; NG Application Protocol (NGAP)"

[35] 3GPP TS 24.501: "Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3".

[36] 3GPP TS 35.217: "Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2; Document 3: Implementors' test data".

[37] 3GPP TS 35.223: "Specification of the 3GPP Confidentiality and Integrity Algorithms EEA3 & EIA3; Document 3: Implementors' test data".

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

[39] Void

[40] IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2".

[41] 3GPP TS 38.460: "NG-RAN; E1 general aspects and principles".

[42] Void.

[43] IETF RFC 6749: "OAuth2.0 Authorization Framework".

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

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

[46] IETF RFC 7748: "Elliptic Curves for Security".

[47] IETF RFC 9113: "HTTP/2".

[48] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

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

[50] IETF RFC 6066: "Transport Layer Security (TLS) Extensions: Extension Definitions".

[51] 3GPP TS 37.340: "Evolved Universal Terrestrial Radio Access (E-UTRA) and NR; Multi-connectivity; Stage 2".

[52] 3GPP TS 38.300: "NR; NR and NG-RAN Overall Description; Stage 2".

[53] 3GPP TS 33.122: "Security Aspects of Common API Framework for 3GPP Northbound APIs".

[54] 3GPP TS28.533: " Management and orchestration; Architecture framework".

[55] 3GPP TS28.531: "Management and orchestration of networks and network slicing; Provisioning".

[56] Void

[57] IETF RFC 7542: "The Network Access Identifier".

[58] IETF RFC 6083: " Datagram Transport Layer Security (DTLS) for Stream Control Transmission Protocol (SCTP)".

[59] IETF RFC 7516: "JSON Web Encryption (JWE)".

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

[61] IETF RFC 5705,"Keying Material Exporters for Transport Layer Security (TLS)".

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

[63] NIST Special Publication 800-38D: "Recommendation for Block Cipher Modes of Operation: Galois Counter Mode (GCM) and GMAC".

[64] IETF RFC 6902: "JavaScript Object Notation (JSON) Patch".

[65] 3GPP TS 31.115: "Secured packet structure for (Universal) Subscriber Identity Module (U)SIM Toolkit applications.

[66] 3GPP TS 31.111: "Universal Subscriber Identity Module (USIM), Application Toolkit (USAT)".

[67] IETF RFC 9048: "Improved Extensible Authentication Protocol Method for 3GPP Mobile Network Authentication and Key Agreement (EAP-AKA')".

[68] 3GPP TS 29.510: "5G System; Network function repository services".

[69] 3GPP TS 36.331: "Radio Resource Control (RRC); Protocol specification".

[70] 3GPP TS 29.505: "5G System; Usage of the Unified Data Repository services for Subscription Data; Stage 3".

[71] 3GPP TS 24.302: "Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks; Stage 3".

[72] 3GPP TS 23.216: "Single Radio Voice Call Continuity (SRVCC)".

[73] 3GPP TS 29.573: " Public Land Mobile Network (PLMN) Interconnection; Stage 3".

[74] 3GP TS 29.500: "5G System; Technical Realization of Service Based Architecture; Stage 3".

[75] IEEE TSN network aspects: see 3GPP TS 23.501 [2] references [95], [96], [97], [98], [104], and [107].

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

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

[78] 3GPP TS 38.401: "NG-RAN; Architecture description".

[79] 3GPP TS 23.316: "Wireless and wireline convergence access support for the 5G System (5GS)"

[80] IEEE Std 802.11-2016 (Revision of IEEE Std 802.11-2012) - IEEE Standard for Information technology—Telecommunications and information exchange between systems Local and metropolitan area networks—Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.

[81] IETF RFC 2410 "The NULL Encryption Algorithm and Its Use With IPsec".

[82] Void

[83] RFC 7858: "Specification for DNS over Transport Layer Security (TLS)".

[84] RFC 8310: "Usage Profiles for DNS over TLS and DNS over DTLS".

[85] RFC 4890: "Recommendations for Filtering ICMPv6 Messages in Firewalls".

[86] 3GPP TS 23.273: "5G System (5GS) Location Services (LCS); Stage 2".

[87] 3GPP TS 38.305: "Stage 2 functional specification of User Equipment (UE) positioning in NG-RAN".

[88] 3GPP TS 36.300: "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access (E-UTRAN); Overall description; Stage 2".

[89] IANA: "Transport Layer Security (TLS) Parameters".

[90] Void

[91] 3GPP TS 33.535: "Authentication and key management for applications based on 3GPP credentials in the 5G System (5GS)".

[92] 3GP TS 29.573: "5G System; Public Land Mobile Network (PLMN) Interconnection".

[93] 3GPP TS 29.503: "5G System; Unified Data Management Services".

[94] 3GPP TS 29.501: "5G System; Principles and Guidelines for Services Definition".

[95] 3GPP TS 29.502: "5G System; Session Management Services".

[96] 3GPP TS 29.526: "5G System; Network Slice-Specific Authentication and Authorization (NSSAA) services".

[97] 3GPP TS 23.402: "Authentication enhancements for non-3GPP accesses".

[98] 3GPP TS 23.548: "5G System Enhancements for Edge Computing; Stage 2".

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

[100] RFC 6678: "Requirements for a Tunnel-Based Extensible Authentication Protocol (EAP) Method".

[101] General Data Protection Regulation, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02016R0679-20160504&from=EN>.

[102] 3GPP TS 33.246: "Security of Multimedia Broadcast/Multicast Service (MBMS)".

[103] 3GPP TS 23.247: "Architectural enhancements for 5G multicast-broadcast services".

[104] 3GPP TS 33.535: "Authentication and Key Management for Applications (AKMA) based on 3GPP credentials in the 5G System (5GS)".

[105] 3GPP TS 23.288: "Architecture enhancements for 5G System(5GS) to support network data analytics services".

[106] 3GPP TS 23.554 Application architecture for MSGin5G Service; Stage 2.

[107] 3GPP TS 22.262 Message service with the 5G System (5GS); Stage 1.

[108] 3GPP TS 26.502: "5G multicast–broadcast services; User Service architecture".

[109] 3GPP TS 33.503: "Security Aspects of Proximity based Services (ProSe) in the 5G System (5GS)".

[110] NIST Special Publication 800-90A (2015): "Recommendation for Random Number Generation Using Deterministic Random Bit Generators".

[111] IETF RFC 4555 (2006-06): "RFC IKEv2 Mobility and Multihoming Protocol (MOBIKE)".

[112] 3GPP TS 24.008: "Mobile radio interface Layer 3 specification; Core network protocols; Stage 3".

[113] RFC 9110: "HTTP Semantics".

[114] 3GPP TS 23.401: "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access".

[I] IEEE Std 802.11™-2020 Part 11: "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications

# 7A Security for trusted non-3GPP access to the 5G core network

## 7A.1 General

Security for trusted non-3GPP access to the 5G Core network is achieved when the UE registers to the 5GC via the TNAN. The UE registers to 5GC and, at the same time, it authenticates with the TNAN by using the EAP-5G procedure, similar to the one used with the registration procedure for untrusted non-3GPP access.

The link between the UE and the TNAN can be any data link (L2) that supports EAP encapsulation. The requirement on the Ta interface between the TNAP and TNGF can be found in clause 4.2.8.3.2 of TS 23.501[2]. The TNGF terminates the EAP-5G signalling andfowards the NAS message to the 5GC when the UE attempts to register to 5GC via the TNAN. The security relies on Layer-2 security between UE and TNAP, which is a trusted entity so that no IPSec encryption would be necessary between UE and TNGF, i.e. NULL encryption is sufficient for the user plane and signalling. However, integrity protection would be provided.

NOTE: The encryption protection over Layer-2 between UE and TNAP is assumed to be enabled.

Separate IPSec SAs may be used for NAS transport and PDU Sessions. At the end of the UE’s registration to 5GC, an IPSec SA (NWt) is established between the UE and TNGF. This is used to protect NAS messages between the UE and TNGF. Later when the UE initiates a PDU session establishment, the TNGF initiates establishment of one or more IPSec child SAs per PDU session. This results in additional IPSec SA’s (NWt) to be setup between the UE and TNGF-UP which are then for user plane transport between the two.

Clause 7A.2.X describes when UE moves from one TNAP to another TNAP, optimized authentication of UE from the previous context without performing the full primary authentication.

Clause 7A.2.4 describes how WLAN UEs that do not support 5GC NAS (N5CW) register via trusted non-3GPP access. Those N5CW devices are able to authenticate to the network with 3GPP credentials and register with the help of an interworking function (TWIF) that provides the 5GC NAS protocol stack towards the AMF.

As defined in clause 7.1, it is the home operator policy decision if a non-3GPP access network is treated as trusted non-3GPP access network. When all of the security domains in clause 4.1 of the present specification related to the non-3GPP access network are considered sufficiently secure by the home operator, the non-3GPP access may be identified as a trusted non-3GPP access for that operator. However, this policy decision may additionally be based on reasons not related to security feature groups.

NOTE: It is specified in clause 7.1a of the current document how the UE gets the operator policy and how it will behave accordingly.

### 7A.2.X Authentication for UE moving from one TNAP to another TNAP without performing the full authentication

Editor’s Note: to be added.

S.3.2 5G NSWO procedures

****

**Figure: S.3-1: Authentication procedure for NSWO in 5GS**

1. The UE establishes a WLAN connection between the UE and the WLAN Access Network (AN), using procedures specified in IEEE 802.11[80].

2. The WLAN AN sends an EAP Identity/Request to the UE.

3. The UE sends an EAP Response/Identity message. If the UE determines to use the NSWO service, the UE shall use the SUCI in NAI format (as specified in TS 23.003 [19], clause 28.7.12 and clause 28.7.9.2) as its identity irrespective of whether SUPI Type configured on the USIM is IMSI or NAI. If the SUPI Type configured on the USIM is IMSI, the UE shall construct the SUCI in NAI format with username containing the encrypted MSIN and the realm part containing the MCC/MNC.

4. The EAP Response/Identity message shall be routed over the SWa interface towards the NSWOF based on the realm part of the SUCI.

NOTE 1: NSWOF acts as SBI/AAA proxy between the AUSF and the WLAN Access Network.

5. The NSWOF shall send the message Nausf\_UEAuthentication\_Authenticate Request with SUCI, Access Network Identity and NSWO indicator towards the AUSF. NSWO\_indicator is used to indicate to the AUSF that the authentication request is for Non-seamless WLAN offload purposes. The NSWOF shall set the Access Network Identity to "5G:NSWO".

6. Based on the NSWO\_indicator, the AUSF (acting as the EAP authentication server) shall send a Nudm\_UEAuthentication\_Get Request to the UDM, including SUCI and the Access Network Identity and NSWO indicator.

7. Upon reception of the Nudm\_UEAuthentication\_Get Request, the UDM shall invoke SIDF. SIDF shall de-conceal SUCI to gain SUPI before UDM can process the request. Based on the NSWO indicator and if NSWO is allowed based on the UE subscription data, the UDM/ARPF shall select the EAP-AKA´ authentication method and generate an authentication vector using the Access Network Identity as the KDF input parameter. The UDM shall include the EAP-AKA’ authentication vector (RAND, AUTN, XRES, CK´ and IK´) and may include SUPI to AUSF in a Nudm\_UEAuthentication\_Get Response message.

8. The AUSF shall store XRES for future verification. The AUSF shall send the EAP-Request/AKA'-Challenge message to the NSWOF in a Nausf\_UEAuthentication\_Authenticate Response message.

NOTE 2: The Access Network Identity is carried in the AT\_KDF\_INPUT attribute in EAP-AKA' as defined in RFC 5448 [12].

9. The NSWOF shall send the EAP-Request/AKA'-Challenge message to the WLAN AN over the SWa interface.

10. The WLAN AN forwards the EAP-Request/AKA'-Challenge message to the UE.

11. At receipt of the RAND and AUTN in the EAP-Request/AKA'-Challenge message, the ME shall obtain the Access Network Identity from the EAP signalling and the USIM in the UE shall verify the freshness of the AV' by checking whether AUTN can be accepted as described in TS 33.102 [9]. If so, the USIM computes a response RES. The USIM shall return RES, CK, IK to the ME. The ME shall derive CK' and IK' using the Access Network Identity as the KDF input parameter. If the verification of the AUTN fails on the USIM, then the USIM and ME shall proceed as described in sub-clause 6.1.3.3. The UE may derive MSK from CK’ and IK’ as per Annex F and as described in RFC 5448[12]. When the UE is performing NSWO authentication, the KAUSF shall not be generated by the UE.

12. The UE shall send the EAP-Response/AKA'-Challenge message to the WLAN AN.

13. The WLAN AN forwards the EAP-Response/AKA'-Challenge message over the SWa interface to the NSWOF.

14. The NSWOF shall send the Nausf\_UEAuthentication\_Authenticate Request with EAP-Response/AKA'-Challenge message to AUSF.

15. The AUSF shall verify if the received response RES matches the stored and expected response XRES. If the AUSF has successfully verified, it continues as follows to step 16, otherwise it returns an error to the NSWOF. The AUSF shall derive the required MSK key from CK’ and IK’ as per Annex F and as described in RFC 5448[12], based on the NSWO indicator received in step 5. The AUSF shall not generate the KAUSF.

16. The AUSF shall send Nausf\_UEAuthentication\_Authenticate Response message with EAP-Success and MSK key to NSWOF. The AUSF may optionally provide the SUPI to NSWOF. The AUSF/UDM shall not perform the linking increased home control to subsequent procedures (as stated in present document clause 6.1.4).

17. The NSWOF shall send the EAP-success and MSK to WLAN AN over the SWa interface. The EAP-Success message is forwarded from WLAN AN to the UE.

18. Upon receiving the EAP-Success message, the UE derives the MSK as specified in step 11, if it has not derived the MSK earlier. The UE uses the first 256-bit of MSK as PMK to perform 4-way handshake to establish a secure connection with the WLAN AN.

NOTE 3: An alternative deployment when both the UE and WLAN AN support FT procedure as specified in IEEE 802.11 [I] is to use FT relying on MSK (available to the WLAN AN and UE) to generate the keys necessary.

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