**3GPP TSG-SA3 Meeting #106-e *draft\_S3-220368-r1***

**e-meeting, 14 - 25 February 2022**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  |  | **CR** | **1329** | **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:***  | SBA service operations for Prose L3 U2N security CP solution |
|  |  |
| ***Source to WG:*** | Ericsson |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** |  5G\_ProSe  |  | ***Date:*** | 2022-02-07 |
|  |  |  |  |  |
| ***Category:*** |  |  | ***Release:*** |  |
|  | *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:*** | SBA service operations for Prose CP based solution for L3 U2N security needs to be defined. |
|  |  |
| ***Summary of change:*** | Adding SBA service operations definition to support Prose CP based solution for L3 U2N security. Adds references to TS 33.503 where the new SBA service operations for ProSe are defined for the AUSF and UDM. |
|  |  |
| ***Consequences if not approved:*** | Missing service operation definitions. |
|  |  |
| ***Clauses affected:*** | 14.1.1, 14.1.2.1 (new), 14.1.2.2 (new), 14.1.2.3 (new), 14.1.5, 14.2.1, 14.2.y |
|  |  |
|  | **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:*** |  |

\*\*\* BEGINNING OF CHANGES \*\*\*

# 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] IETF RFC 4346: "The Transport Layer Security (TLS) Protocol Version 1.1".

[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 7540: " Hypertext Transfer Protocol Version 2 (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] Internet draft draft-ietf-emu-rfc5448bis: "Improved Extensible Authentication Protocol Method for 3rd Generation 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] Internet draft draft-ietf-emu-eap-tls13: "Using EAP-TLS 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] RFC 2818: "HTTP Over TLS".

[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.

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

\*\*\* NEXT CHANGES \*\*\*

## 14.1 Services provided by AUSF

### 14.1.1 General

The AUSF provides UE authentication service to the requester NF by Nausf\_UEAuthentication. For AKA based authentication, this operation can be also used to recover from synchronization failure situations. Clause 14.1.2 describes the Nausf\_UEAuthentication service. The service operations listed here are used in procedures that are described in clause 6 of the present document and in TS 33.503 [xx].

Clause 14.1.3 describes the Nausf\_SoRProtection service used in procedures that are described in clause 6.14 of the present document.

Clause 14.1.4 describes the Nausf\_UPUProtection service used in procedures that are described in clause 6.15 of the present document.

Since AUSF is completely security-related, all service operations are described in the present document. TS 23.501 [2], clause 7.2.7, only lists the services and TS 23.502 [8], clause 5.2.10, provides the reference to the present document.

### 14.1.2 Nausf\_UEAuthentication service

### 14.1.2.1 Nausf\_UEAuthentication\_Authenticate service operation

**Service operation name:** Nausf\_UEAuthentication\_authenticate.

**Description:** Authenticate the UE and provides related keying material.

**Input, Required:** One of the options below.

1. In the initial authentication request: SUPI or SUCI, serving network name.

2. In the subsequent authentication requests depending on the authentication method:

a. 5G AKA: Authentication confirmation message with RES\* as described in clause 6.1.3.2 or Synchronization Failure indication and related information (i.e. RAND/AUTS).

b. EAP-AKA’: EAP packet as described in RFC 4187 [21] and RFC 5448 [12], and Annex F.

**Input, Optional:** None.

**Output, Required:** One of the options below.

1. Depending on the authentication method:

a. 5G AKA: authentication vector, as described in clause 6.1.3.2 or Authentication confirmation acknowledge message.

b. EAP-AKA’: EAP packet as described in RFC 4187 [21] and RFC 5448 [12], and Annex F.

2. Authentication result and if success the master key which are used by AMF to derive NAS security keys and other security key(s).

**Output, Optional:** SUPI if the authentication was initiated with SUCI.

### 14.1.2.2 Nausf\_UEAuthentication\_deregister service operation

**Service operation name:** Nausf\_UEAuthentication\_deregister

**Description:** Deletion of stale security parameters (KAUSF, SOR counter and UE parameter update counter) in AUSF. UDM uses this service operation to request the AUSF to clear the stale security parameters, after the UE has been successfully (re)authenticated in different AUSF Instance.

**Input, Required:** SUPI

**Input, Optional:** None

**Output, Required:** None

**Output, Optional:** None

### 14.1.2.3 Nausf\_UEAuthentication\_ProseAuthenticate service operation

See TS 33.503 [xx].

### 14.1.3 Nausf\_SoRProtection service

The following table illustrates the security related services for SoR that AUSF provides.

Table 14.1.3-1: NF services for SoR provided by AUSF

|  |  |  |  |
| --- | --- | --- | --- |
| Service Name | Service Operations | Operation Semantics | Example Consumer(s) |
| Nausf\_SoRProtection | Protect | Request/Response | UDM |

**Service operation name:** Nausf\_SoRProtection.

**Description:** The AUSF calculates the SoR-MAC-IAUSF as specified in the Annex A.17 of this document using UE specific home key (KAUSF), the Steering Information List and ACK Indication received from the requester NF and delivers the SoR-MAC-IAUSF and CounterSoR to the requester NF. If the ACK Indication input is set to indicate that the acknowledgement is requested, then the AUSF shall compute the SoR-XMAC-IUE and return it in the response.

NOTE: At reception of Nausf\_SoRProtection\_Protect request from the UDM, the AUSF constructs the SOR header, as described in clause 9.11.3.51 of TS 24.501 [35], based on the information received from the requester NF, i.e. ACK Indication and list of preferred PLMN/access technology combinations or a secured packet (if provided).

**Input, Required:** Requester ID, SUPI, service name, ACK Indication.

**Input, Optional:** list of preferred PLMN/access technology combinations or secured packet.

**Output, Required:** SoR-MAC-IAUSF, CounterSoR or error (counter\_wrap).

**Output, Optional:** SoR-XMAC-IUE (if the ACK Indication input is set to indicate that the acknowledgement is requested, then the SoR-XMAC-IUE shall be computed and returned).

### 14.1.4 Nausf\_UPUProtection service

The following table illustrates the security related services for UE Parameters Update that AUSF provides.

Table 14.1.4-1: NF services for UE Parameters Update provided by AUSF

|  |  |  |  |
| --- | --- | --- | --- |
| Service Name | Service Operations | Operation Semantics | Example Consumer(s) |
| Nausf\_UPUProtection | Protect | Request/Response | UDM |

**Service operation name:** Nausf\_UPUProtection.

**Description:** The AUSF calculates the UPU-MAC-IAUSF as specified in the Annex A.19 of this document using UE specific home key (KAUSF) along with the UE Parameters Update Data received from the requester NF (see clause A.19) and delivers the UPU-MAC-IAUSF and CounterUPU to the requester NF. If the ACK Indication input is present, then the AUSF shall compute the UPU-XMAC-IUE and return the computed UPU-XMAC-IUE in the response. The details of the UE Parameters Update Data is specified in TS 24.501 [35].

**Input, Required:** Requester ID, SUPI, service name, UE Parameters Update Data.

**Input, Optional:** ACK Indication.

**Output, Required:** UPU-MAC-IAUSF, CounterUPU or error (counter\_wrap).

**Output, Optional:** UPU-XMAC-IUE (if the ACK Indication input is present, then the UPU-XMAC-IUE shall be computed and returned).

### 14.1.5 Void

## 14.2 Services provided by UDM

### 14.2.1 General

UDM provides within Nudm\_UEAuthentication service all authentication-related service operations, which are Nudm\_UEAuthentication\_Get (clause 14.2.2), Nudm\_UEAuthentication\_ResultConfirmation (clause 14.2.3) and Nudm\_UEAuthentication\_GetProseAv (clause 14.2.y).

The complete list of UDM services is defined in TS 23.501 [2], clause 7.2.5, and further refined in TS 23.502 [8], clause 5.2.3.1.

### 14.2.2 Nudm\_UEAuthentication\_Get service operation

**Service operation name:** Nudm\_UEAuthentication\_Get

**Description:** Requester NF gets the authentication data from UDM. For AKA based authentication, this operation can be also used to recover from synchronization failure situations. If SUCI is included, this service operation returns the SUPI.

**Inputs, Required:** SUPI or SUCI, serving network name.

**Inputs, Optional:** Synchronization Failure indication and related information (i.e. RAND/AUTS).

**Outputs, Required:** Authentication method

Editor's note: How the UDM indicates to the AUSF to run primary authentication with an external Credentials holder is FFS.

Outputs, Optional**:** SUPI if SUCI was used as input. Depending on the authentication method, authentication data (e.g. AKA authentication vector) for the SUPI. AKMA Indication and Routing indicator, if the subscriber has an AKMA subscription (see TS 33.535 [91]).

### 14.2.3 Nudm\_UEAuthentication\_ResultConfirmation service operation

**Service operation name:** UEAuthentication\_ResultConfirmation

**Description:** Requester NF informs UDM about the result of an authentication procedure with a UE.

**Inputs, Required:** SUPI, timestamp of the authentication, the authentication type (e.g. EAP method or 5G-AKA), and the serving network name.

**Inputs, Optional:** None.

**Outputs, Required:** None.

**Outputs, Optional:** None.

### 14.2.y Nudm\_UEAuthentication\_GetProseAv service operation

See TS 33.503 [xx].

\*\*\* END OF CHANGES \*\*\*