**3GPP TSG-CT WG1 Meeting #134-eC1-22xxxx**

**E-Meeting, 17th – 25th February 2022**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **24.501** | **CR** | **3995** | **rev** | **1** | **Current version:** | **17.5.0** |  |
|  | | | | | | | | |
| *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:*** | Update to NAS security mode command during PC5 link establishment | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | vivo, Nokia, Nokia Shanghai Bell, InterDigital | | | | | | | | | |
| ***Source to TSG:*** | C1 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | 5G\_ProSe | | | | |  | ***Date:*** | | | 2022-02-24 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | B |  | | | | | ***Release:*** | | | *Rel-17* |
|  | *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:*** | | When Remote UE establishes a PC5 link between a remote UE and a UE-to-network relay, the Remote UE needs to be authenticated by remote UE’s AUSF via relay UE and relay UE's AMF during 5G ProSe PC5 link establishment. As per TS 33.503 states that,  *6-7. The AUSF shall retrieve the Authentication Vectors from the UDM and trigger* *primary authentication of the remote UE using existing procedure as specified in TS 33.501 [3].* *This authentication* *is performed between the AUSF and the remote UE via the relay AMF and relay UE. AUSF shall not make the newly derived KAUSF as the latest KAUSF. At the remote UE, the newly derived KAUSF shall not be taken as latest KAUSF as NAS SMC procedure is not performed between remote UE and relay AMF.*  and  *10-11. The AUSF shall send the 5GPRUK ID, KNR\_ProSe, Nonce\_2 in Nausf\_UEAuthentication\_Authenticate Response message to the UE-to-Network relay via relay AMF.* *When receiving a KNR\_ProSe from AUSF, the AMF shall not attempt to trigger NAS SMC procedure with Remote UE. Relay UE derives PC5 session key Krelay-sess and confidentiality and integrity keys from KNR\_ProSe, using the KDF defined in clause 6.3.3.3.4 of this document. KNR\_ProSe ID and Krelay-sess ID are established in the same way as KNRP ID and KNRP-sess ID in TS 33.536 [6].*  According to the text above,  (1) When L3 relay UE’s AMF assists the L3 remote UE do the primary authentication, since AUSF would not make the newly derived *KAUSF* as the latest *KAUSF*, so the relay UE’s AMF shall not trigger the NAS security mode control (SMC) procedure.  (2) When the primary authentication procedure successfully authenticates a L3 remote UE, the AMF shall not perform a SMC procedure for remote UE. Also, the AMF instead will use relay key response message to send the *KNR\_ProSe* to relay UE.  These above need to be reflected in 24.501.  Besides, the following EN is added since the relay key request message has not been defined yet:  Editor’s note: The definition of relay key request message is FFS. | | | | | | | | |
| ***r*** | |  | | | | | | | | |
| ***Summary of change:*** | | (1) Clarify that when relay UE’s AMF assists the remote UE do the primary authentication, the relay UE’s AMF shall not trigger the NAS SMC.  (2) Clarify with a NOTE that when the primary authentication procedure successfully authenticates a L3 remote UE, the AMF does not perform a security mode control procedure for relay UE or for remote UE;  (3) An EN is added because relay key request message has not been defined. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | The network would wrongly initiate the NAS SMC procedure. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 2, 5.4.1.3.1, 5.4.2.1 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | | -In rev1, the cover page is enriched, proposed changes in clause 5.4.2.1 has been transferred into a NOTE, the proposed changes in clause 5.4.1.3.1 is reformulated, and an EN is added in clause 5.4.1.3.1. | | | | | | | | |

**\*\*\*\*\*\*\***

\* \* \* 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".

[1A] 3GPP TS 22.011: "Service accessibility".

[2] 3GPP TS 22.101: "Service aspects; Service principles".

[3] 3GPP TS 22.261: "Service requirements for the 5G system; Stage 1".

[4] 3GPP TS 23.003: "Numbering, addressing and identification".

[4A] 3GPP TS 23.040: "Technical realization of Short Message Service (SMS)".

[5] 3GPP TS 23.122: "Non-Access-Stratum functions related to Mobile Station (MS) in idle mode".

[6] 3GPP TS 23.167: "IP Multimedia Subsystem (IMS) emergency sessions".

[6A] 3GPP TS 23.216: "Single Radio Voice Call Continuity (SRVCC); Stage 2".

[6AB] 3GPP TS 23.256: "Support of Uncrewed Aerial Systems (UAS) connectivity, identification and tracking; Stage 2".

[6B] 3GPP TS 23.273: "5G System (5GS) Location Services (LCS); Stage 2".

[6C] 3GPP TS 23.287: "Architecture enhancements for 5G System (5GS) to support Vehicle-to-Everything (V2X) services".

[6D] 3GPP TS 23.316: "Wireless and wireline convergence access support for the 5G System (5GS)".

[6E] 3GPP TS 23.304: "Proximity based Services (ProSe) in the 5G System (5GS)".

[7] 3GPP TS 23.401: "GPRS enhancements for E-UTRAN access".

[8] 3GPP TS 23.501: "System Architecture for the 5G System; Stage 2".

[9] 3GPP TS 23.502: "Procedures for the 5G System; Stage 2".

[10] 3GPP TS 23.503: "Policy and Charging Control Framework for the 5G System; Stage 2".

[10A] 3GPP TS 23.548: "5G System Enhancements for Edge Computing; Stage 2".

[11] 3GPP TS 24.007: "Mobile radio interface signalling layer 3; General aspects".

[12] 3GPP TS 24.008: "Mobile Radio Interface Layer 3 specification; Core Network Protocols; Stage 3".

[13] 3GPP TS 24.011: "Point-to-Point Short Message Service (SMS) support on mobile radio interface".

[13A] 3GPP TS 24.080: "Mobile radio interface layer 3 Supplementary services specification; Formats and coding".

[13B] 3GPP TS 24.193: "Access Traffic Steering, Switching and Splitting; Stage 3".

[13C] 3GPP TS 24.173: "IMS Multimedia telephony communication service and supplementary services; Stage 3".

[14] 3GPP TS 24.229: "IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

[14A] 3GPP TS 24.250: "Protocol for Reliable Data Service; Stage 3".

[15] 3GPP TS 24.301: "Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3".

[16] 3GPP TS 24.302: "Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks; Stage 3"

[17] 3GPP TS 24.368: "Non-Access Stratum (NAS) configuration Management Object (MO)".

[18] 3GPP TS 24.502: "Access to the 3GPP 5G System (5GS) via non-3GPP access networks; Stage 3".

[19] 3GPP TS 24.526: "UE policies for 5G System (5GS); Stage 3".

[19BA] 3GPP TS 24.539: "5G System (5GS); Network to TSN translator (TT) protocol aspects; Stage 3".

[19A] 3GPP TS 24.535: "Device-Side Time-Sensitive Networking (TSN) Translator (DS-TT) to Network-Side TSN Translator (NW-TT) protocol aspects; Stage 3".

[19B] 3GPP TS 24.587: "Vehicle-to-Everything (V2X) services in 5G System (5GS); Protocol aspects; Stage 3"

[19C] 3GPP TS 24.588: "Vehicle-to-Everything (V2X) services in 5G System (5GS); User Equipment (UE) policies; Stage 3"

[19D] Void.

[19E] 3GPP TS 24.554: "Proximity-service (ProSe) in 5G System (5GS) protocol aspects; Stage 3".[19F] 3GPP TS 24.555: "Proximity-services (ProSe) in 5G System (5GS); User Equipment (UE) policies; Stage 3".

[20] 3GPP TS 24.623: "Extensive Markup Language (XML) Configuration Access Protocol (XCAP) over the Ut interface for Manipulating Supplementary Services".

[20AA] 3GPP TS 29.500: "5G System; Technical Realization of Service Based Architecture; Stage 3".

[20A] 3GPP TS 29.502: "5G System; Session Management Services; Stage 3".

[20AB] 3GPP TS 29.503: "5G System; Unified Data Management Services; Stage 3".

[20B] 3GPP TS 29.518: "5G System; Access and Mobility Management Services; Stage 3".

[21] 3GPP TS 29.525: "5G System; UE Policy Control Service; Stage 3".

[21A] 3GPP TS 29.526: "5G System; Network Slice-Specific Authentication and Authorization (NSSAA) services; Stage 3".

[21B] 3GPP TS 29.256: "5G System; Uncrewed Aerial Systems Network Function (UAS-NF); Aerial Management Services; Stage 3.

[22] 3GPP TS 31.102: "Characteristics of the Universal Subscriber Identity Module (USIM) application".

[22A] 3GPP TS 31.111: "USIM Application Toolkit (USAT)".

[22B] 3GPP TS 31.115: "Secured packet structure for (Universal) Subscriber Identity Module (U)SIM Toolkit applications".

[23] 3GPP TS 33.102: "3G security; Security architecture".

[23A] 3GPP TS 33.401: "3GPP System Architecture Evolution; Security architecture".

[24] 3GPP TS 33.501: "Security architecture and procedures for 5G System".

[24A] 3GPP TS 33.535: "Authentication and Key Management for Applications (AKMA) based on 3GPP credentials in the 5G System (5GS)".

[25] 3GPP TS 36.323: "NR; Packet Data Convergence Protocol (PDCP) specification".

[25A] 3GPP TS 36.331: "Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC) protocol specification".

[25B] 3GPP TS 36.300: "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description".

[25C] 3GPP TS 36.304: "Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) procedures in idle mode".

[25D] 3GPP TS 36.306: "Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) radio access capabilities".

[25E] 3GPP TS 36.321: "Evolved Universal Terrestrial Radio Access (E-UTRA); Medium Access Control (MAC) protocol specification".

[26] 3GPP TS 37.355: "LTE Positioning Protocol (LPP)".

[27] 3GPP TS 38.300: "NR; NR and NG-RAN Overall Description; Stage 2".

[28] 3GPP TS 38.304: "New Generation Radio Access Network; User Equipment (UE) procedures in Idle mode".

[29] 3GPP TS 38.323: "Evolved Universal Terrestrial Radio Access (E-UTRA); Packet Data Convergence Protocol (PDCP) specification".

[30] 3GPP TS 38.331: "NR; Radio Resource Control (RRC); Protocol Specification".

[31] 3GPP TS 38.413: "NG Radio Access Network (NG-RAN); NG Application Protocol (NGAP)".

[31A] IEEE Std 802.3™-2018: "Ethernet".

[31AA] 3GPP TS 38.509: "Special conformance testing functions for User Equipment (UE)".

[32] IETF RFC 768: "User Datagram Protocol".

[33] IETF RFC 793: "Transmission Control Protocol."

[33A] IETF RFC 3095: "RObust Header Compression (ROHC): Framework and four profiles: RTP, UDP, ESP and uncompressed".

[33B] Void.

[33C] Void.

[33D] IETF RFC 8415: "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)".

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

[34A] IETF RFC 3843: "RObust Header Compression (ROHC): A Compression Profile for IP".

[35] Void.

[35A] IETF RFC 4122: "A Universally Unique IDentifier (UUID) URN Namespace".

[36] IETF RFC 4191: "Default Router Preferences and More-Specific Routes".

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

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

[38A] IETF RFC 4815: "RObust Header Compression (ROHC): Corrections and Clarifications to RFC 3095".

[38B] IETF RFC 4861: "Neighbor Discovery for IP version 6 (IPv6)".

[39] IETF RFC 4862: "IPv6 Stateless Address Autoconfiguration".

[39A] IETF RFC 5225: "RObust Header Compression (ROHC) Version 2: Profiles for RTP, UDP, IP, ESP and UDP Lite".

[39B] IETF RFC 5795: "The RObust Header Compression (ROHC) Framework".

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

[40A] IETF RFC 6603: "Prefix Exclude Option for DHCPv6-based Prefix Delegation".

[40B] IETF RFC 6846: "RObust Header Compression (ROHC): A Profile for TCP/IP (ROHC-TCP)".

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

[42] ITU-T Recommendation E.212: "The international identification plan for public networks and subscriptions", 2016-09-23.

[43] IEEE Std 802-2014: "IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture" (30 June 2014).

[43A] IEEE Std 802.1AS-2020: "IEEE Standard for Local and metropolitan area networks--Timing and Synchronization for Time-Sensitive Applications".

[43B] IEEE Std 1588™-2019: "IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems".

[43C] Void.

[43D] Void.

[43E] Void.

[44] Void.

[45] Void.

[46] Void.

[47] Void.

[48] IEEE "Guidelines for Use of Extended Unique Identifier (EUI), Organizationally Unique Identifier (OUI), and Company ID (CID)".

[49] BBF TR-069: "CPE WAN Management Protocol".

[50] BBF TR-369: "User Services Platform (USP)".

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

[52] IETF RFC 8106:"IPv6 Router Advertisement Options for DNS Configuration".

[53] 3GPP TS 23.247: "Architectural enhancements for 5G multicast-broadcast services; Stage 2".

[54] 3GPP TS 23.380: "IMS Restoration Procedures".

[55] IETF RFC 3948: "UDP Encapsulation of IPsec ESP Packets".

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

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

##### 5.4.1.3.1 General

The purpose of the 5G AKA based primary authentication and key agreement procedure is to provide mutual authentication between the UE and the network and to agree on the keys KAUSF, KSEAF and KAMF (see 3GPP TS 33.501 [24]). The cases when the 5G AKA based primary authentication and key agreement procedure is used are defined in 3GPP TS 33.501 [24].

The network initiates the 5G AKA based primary authentication and key agreement procedure by sending an AUTHENTICATION REQUEST message to the UE without the EAP message IE. The network shall include the ngKSI and the ABBA in AUTHENTICATION REQUEST message.

The 5G AKA based primary authentication and key agreement procedure is always initiated and controlled by the network. However, the UE can reject the 5G authentication challenge sent by the network.

The UE shall proceed with a 5G authentication challenge only if a USIM is present.

A partial native 5G NAS security context is established in the UE and the network when a 5G authentication is successfully performed. During a successful 5G AKA based primary authentication and key agreement procedure, the CK and IK are computed by the USIM. CK and IK are then used by the ME as key material to compute new keys KAUSF, KSEAF and KAMF. KAMF is stored in the 5G NAS security contexts (see 3GPP TS 33.501 [24]) of both the network and in the volatile memory of the ME while registered to the network, and is the root for the 5GS integrity protection and ciphering key hierarchy.

NOTE 1: Generation of the new KAUSF and the new KSEAF does not result into deletion of the valid KAUSF and the valid KSEAF, if any.

The 5G AKA based primary authentication and key agreement procedure is initiated by an AUTHENTICATION REQUEST message without the EAP message IE.

Upon successful completion of the 5G AKA based primary authentication, the AMF shall initiate a security mode control procedure (see subclause 5.4.2) to take the new partial native 5G NAS security context into use, except for:

- the 5G AKA based primary authentication is triggered by relay key request message as defined in clause 6.3.3.3.2 of 3GPP TS 33.503 [X].

Editor’s note: The definition of relay key request message is FFS.

NOTE 2: The AMF shall immediately initiate a security mode control procedure (see subclause 5.4.2) after 5G AKA primary authentication is successful to avoid KAUSF key mismatch between the UE and the network.

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

#### 5.4.2.1 General

The purpose of the NAS security mode control procedure is to take a 5G NAS security context into use, and initialise and start NAS signalling security between the UE and the AMF with the corresponding 5G NAS keys and 5G NAS security algorithms.

Furthermore, the network may also initiate the security mode control procedure in the following cases:

a)- in order to change the 5G NAS security algorithms for a current 5G NAS security context already in use;

b) in order to change the value of uplink NAS COUNT used in the latest SECURITY MODE COMPLETE message as described in 3GPP TS 33.501 [24], subclause 6.9.4.4; and

c) in order to provide the Selected EPS NAS security algorithms to the UE.

For restrictions concerning the concurrent running of a security mode control procedure with other security related procedures in the AS or inside the core network see 3GPP TS 33.501 [24], subclause 6.9.5.

If the security mode control procedure is initiated after successful 5G AKA based primary authentication and key agreement procedure and the security mode control procedure intends to bring into use the partial native 5G NAS security context created by the 5G AKA based primary authentication and key agreement procedure and the UE accept received security mode command (see subclause 5.4.2.3), the ME shall:

a) delete the valid KAUSF and the valid KSEAF, if any; and

b) consider the new KAUSF to be the valid KAUSF, and the new KSEAF to be the valid KSEAF, reset the SOR counter and the UE parameter update counter to zero, and store the valid KAUSF, the valid KSEAF , the SOR counter and the UE parameter update counter as specified in annex C and use the valid KAUSF in the verification of SOR transparent container and UE parameters update transparent container, if any are received.

NOTE: The AMF does not perform a security mode control procedure when the 5G AKA based primary authentication procedure successfully authenticates a 5G ProSe layer-3 remote UE accessing the network via a 5G ProSe layer-3 UE-to-network relay UE served by the AMF.

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