**3GPP TSG-CT WG1 Meeting #136-eC1-22XXXX**

**E-meeting, 12th – 20th May 2022 (revision of C1-223796, C1-222695)**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **24.501** | **CR** | **4166** | **rev** | **2** | **Current version:** | **17.6.1** |  |
|  | | | | | | | | |
| *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 | **X** | Radio Access Network |  | Core Network | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** |  | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Intel | | | | | | | | | |
| ***Source to TSG:*** | C1 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | eNPN | | | | |  | ***Date:*** | | | 17-MAY-2022 |
|  |  | | | |  | |  | | |  |
| ***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:*** | | SA3 has agreed in CR 1326 to TS 33.501 clause I.9.2.4.1 (see S3-220471) that in case of secondary authentication using DCS the ON-SNPN may trigger secondary authentication procedure with the DCS using Default UE credentials. *“I.9.2.4.1 Secondary authentication using DCS* *After successful primary authentication as described in I.9.2.2 (i.e. primary authentication without using DCS), upon the establishment of the Onboarding PDU Session, the ON-SNPN may trigger secondary authentication procedure with the DCS using Default UE credentials as described in clause 11.1.“*  CR 1326 to TS 33.501 further clarifies in clause I.9.2.4.2 that in case of secondary authentication using DN-AAA the ON-SNPN may trigger secondary authentication procedure with a DN-AAA server. *“I.9.2.4.2 Secondary authentication using DN-AAA* *After successful primary authentication as described in I.9.2.2 or I.9.2.3, upon the establishment of the Onboarding PDU Session, the ON-SNPN may trigger secondary authentication procedure with a DN-AAA server as described in clause 11.1.”*  Furthermore, CR 1388 to TS 33.501 (S3-220939-r4) submitted in SA3#107-e introduces Default UE credentials for primary authentication and Default UE credentials for secondary authentication instead of Default UE credentials. Default UE credentials for secondary authentication are used in case of secondary authentication using DCS or DN-AAA server in onboarding SNPN.  However, 24.501 currently does not specify Onboarding SNPN with secondary authentication support with a DCS or DN-AAA. It is proposed to add Onboarding SNPN with secondary authentication support with a DCS or DN-AAA server using default UE credentials for secondary authentication. | | | | | | | | |
| ***;*** | |  | | | | | | | | |
| ***Summary of change:*** | | 1. Add Onboarding SNPN with secondary authentication support. 2. Rename “default UE credentials” to “default UE credentials for primary authentication” | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | No support for Onboarding SNPN with secondary authentication. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 3.1, 4.14.2, 5.3.2, 5.4.1.2.2.3, 5.4.1.2.2.8, 5.4.1.2.3.1, 5.4.1.2.3A.1, 6.3.1.1 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | | **X** |  | Other core specifications | | | | TS 33.501 CR 1388 | | |
| ***affected:*** | |  | **X** | Test specifications | | | | TS/TR ... CR ... | | |
| ***(show related CRs)*** | |  | **X** | O&M Specifications | | | | TS/TR ... CR ... | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | | Rev 1   * Updates for supporting default PDU session authentication and authorization credentials * merged last two paragraphs on UE behaviour into single paragraph * “default UE credentials” instead of “UE default credentials” * Changed category to B * Added reference to SA3 stage 2 CR   Rev 2   * Updated reference to SA3 stage 2 CR * Specify to use only default UE credentials for secondary authentication for the PDU session authentication and authorization procedure in onboarding SNPN. * “default UE credentials for primary authentication” instead of “default UE credentials” | | | | | | | | |

\*\*\* First change \*\*\*

## 3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP 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 3GPP TR 21.905 [1].

**5GMM-IDLE mode:** In this specification, if the term is used standalone, a UE in 5GMM-IDLE mode means the UE can be either in 5GMM-IDLE mode over 3GPP access or in 5GMM-IDLE mode over non-3GPP access.

**5GMM-CONNECTED mode:** In this specification, if the term is used standalone, a UE in 5GMM-CONNECTED mode means the UE can be either in 5GMM-CONNECTED mode over 3GPP access or in 5GMM-CONNECTED mode over non-3GPP access.

**5GMM-IDLE mode over 3GPP access:** A UE is in 5GMM-IDLE mode over 3GPP access when no N1 NAS signalling connection between the UE and network over 3GPP access exists. The term 5GMM-IDLE mode over 3GPP access used in the present document corresponds to the term CM-IDLE state for 3GPP access used in 3GPP TS 23.501 [8].

**5GMM-CONNECTED mode over 3GPP access:** A UE is in 5GMM-CONNECTED mode over 3GPP access when an N1 NAS signalling connection between the UE and network over 3GPP access exists. The term 5GMM-CONNECTED mode over 3GPP access used in the present document corresponds to the term CM-CONNECTED state for 3GPP access used in 3GPP TS 23.501 [8].

**5GMM-IDLE mode over non-3GPP access:** A UE is in 5GMM-IDLE mode over non-3GPP access when no N1 NAS signalling connection between the UE and network over non-3GPP access exists. The term 5GMM-IDLE mode over non-3GPP access used in the present document corresponds to the term CM-IDLE state for non-3GPP access used in 3GPP TS 23.501 [8].

**5GMM-CONNECTED mode over non-3GPP access:** A UE is in 5GMM-CONNECTED mode over non-3GPP access when an N1 NAS signalling connection between the UE and network over non-3GPP access exists. The term 5GMM-CONNECTED mode over non-3GPP access used in the present document corresponds to the term CM-CONNECTED state for non-3GPP access used in 3GPP TS 23.501 [8].

**5GS services:** Services provided by PS domain. Within the context of this specification, 5GS services is used as a synonym for EPS services.

**5G-EA:** 5GS encryption algorithms. The term 5G-EA, 5G-EA0, 128-5G-EA1, 128-5G-EA2, 128-5G-EA3, 5G-EA4, 5G-EA5, 5G-EA6 and 5G-EA7 used in the present document corresponds to the term NEA, NEA0, 128-NEA1, 128-NEA2, 128-NEA3, NEA4, NEA5, NEA6 and NEA7 defined in 3GPP TS 33.501 [24].

**5G-IA:** 5GS integrity algorithms. The term 5G-IA, 5G-IA0, 128-5G-IA1, 128-5G-IA2, 128-5G-IA3, 5G-IA4, 5G-IA5, 5G-IA6 and 5G-IA7 used in the present document corresponds to the term NIA, NIA0, 128-NIA1, 128-NIA2, 128-NIA3, NIA4, NIA5, NIA6 and NIA7 defined in 3GPP TS 33.501 [24].

**Access stratum connection:** A peer to peer access stratum connection:

- between the UE and the NG-RAN for 3GPP access;

- between the UE and the N3IWF for untrusted non-3GPP access;

- between the UE and the TNGF for trusted non-3GPP access used by the UE;

- within the TWIF acting on behalf of the N5CW device for trusted non-3GPP access used by the N5CW device;

- between the 5G-RG and the W-AGF for wireline access used by the 5G-RG;

- within the W-AGF acting on behalf of the FN-RG for wireline access used by the FN-RG; or

- within the W-AGF acting on behalf of the N5GC device for wireline access used by the N5GC device.

The access stratum connection for 3GPP access corresponds to an RRC connection via the Uu reference point. The creation of the access stratum connection for untrusted non-3GPP access corresponds to the completion of the IKE\_SA\_INIT exchange (see IETF RFC 7296 [41]) via the NWu reference point. The creation of the access stratum connection for trusted non-3GPP access used by the UE corresponds to the UE reception of an EAP-request/5G-start via NWt reference point (see 3GPP TS 23.502 [9]). The creation of the access stratum connection for trusted non-3GPP access used by the N5CW device corresponds to the TWIF's start of acting on behalf of the N5CW device. The creation of the access stratum connection for wireline access used by the 5G-RG corresponds to the 5G-RG reception of an EAP-request/5G-packet over the W-CP EAP connection via the Y4 reference point (see 3GPP TS 23.316 [6D]). The creation of the access stratum connection for wireline access used by the FN-RG corresponds to the W-AGF's start of acting on behalf of the FN-RG. The creation of the access stratum connection for wireline access used by the N5GC device corresponds to the W-AGF's start of acting on behalf of the N5GC device.

**Access to SNPN services via a PLMN/To access SNPN services via a PLMN:** A UE is accessing SNPN services via a PLMN when the UE is connecting to the 5GCN of the SNPN using the 3GPP access of the PLMN.

**Aggregate maximum bit rate:** The maximum bit rate that limits the aggregate bit rate of a set of non-GBR bearers of a UE. Definition derived from 3GPP TS 23.501 [8].

**Always-on PDU session:** A PDU session for which user-plane resources have to be established during every transition from 5GMM-IDLE mode to 5GMM-CONNECTED mode. A UE requests a PDU session to be established as an always-on PDU session based on indication from upper layers and the network decides whether a PDU session is established as an always-on PDU session.

NOTE 1: How the upper layers in the UE are configured to provide an indication is outside the scope of the present document.

**Applicable UE radio capability ID for the current UE radio configuration in the selected network:** The UE has an applicable UE radio capability ID for the current UE radio configuration in the selected network if:

a) the UE supports RACS; and

b) the UE has:

1) a stored network-assigned UE radio capability ID which is associated with the PLMN ID or SNPN identity of the serving network and which maps to the set of radio capabilities currently enabled at the UE; or

2) a manufacturer-assigned UE radio capability ID which maps to the set of radio capabilities currently enabled at the UE.

**CAG cell:** A cell in which only members of the CAG can get normal service. Depending on local regulation, the CAG cell can provide emergency services also to subscribers who are not members of the CAG.

**CAG-ID:** A CAG-ID is a unique identifier within the scope of one PLMN defined in 3GPP TS 23.003 [4] which identifies a Closed Access Group (CAG) in the PLMN associated with a cell or group of cells to which access is restricted to members of the CAG.

**CAG restrictions:** Restrictions applied to a UE in accessing a PLMN's 5GCN via:

a) a non-CAG cell if the entry for the PLMN in the UE's "CAG information list" includes an "indication that the UE is only allowed to access 5GS via CAG cells"; or

b) a CAG cell if none of the CAG-ID(s) supported by the CAG cell is included in the "allowed CAG list" for the PLMN in the UE's "CAG information list".

The CAG restrictions are not applied in a PLMN when a UE accesses the PLMN due to emergency services.

**Cleartext IEs:** Information elements that can be sent without confidentiality protection in initial NAS messages as specified in subclause 4.4.6.

**Configuration of SNPN subscription parameters in PLMN via the user plane:** Configuration of a UE in a PLMN with one or more entries of the "list of subscriber data” via the user plane.

**Control plane CIoT 5GS optimization:** Signalling optimizations to enable efficient transport of user data (IP, Ethernet, Unstructured or SMS) over control plane via the AMF including optional header compression of IP data and Ethernet data.

**DNN determined by the AMF:** If no DNN requested by the UE is provided, a DNN determined by the AMF based subscription information or local policy. Otherwise DNN determined by the AMF is the DNN requested by the UE.

**DNN requested by the UE:** A DNN explicitly requested by the UE and included in a NAS request message.

**DNN selected by the network:** If DNN replacement applies, a DNN selected and indicated to the AMF by PCF. Otherwise DNN selected by the network is the DNN determined by the AMF.

**Default S-NSSAI**: An S-NSSAI in the subscribed S-NSSAIs marked as default.

**Globally-unique SNPN identity:** An SNPN identity with an NID whose assignment mode is not set to 1 (see 3GPP TS 23.003 [4]).

**User plane CIoT 5GS optimization:** Signalling optimizations to enable efficient transport of user data (IP, Ethernet or Unstructured) over the user plane.

**UE supporting CIoT 5GS optimizations:** A UE that supports control plane CIoT 5GS optimization or user plane CIoT 5GS optimization and one or more other CIoT 5GS optimizations when the UE is in N1 mode.

**Registered for 5GS services with control plane CIoT 5GS optimization:** A UE supporting CIoT 5GS optimizations is registered for 5GS services, and control plane CIoT 5GS optimization along with one or more other CIoT 5GS optimizations have been accepted by the network.

**Registered** **for 5GS services with user plane CIoT 5GS optimization:** A UE supporting CIoT 5GS optimizations is registered for 5GS services, and user plane CIoT 5GS optimization along with one or more other CIoT 5GS optimizations have been accepted by the network.

**Registered** **for 5GS services with CIoT 5GS optimization:** A UE is registered for 5GS services with control plane CIoT 5GS optimization or registered for 5GS services with user plane CIoT 5GS optimization.

**DNN based congestion control:** Type of congestion control at session management level that is applied to reject session management requests from UEs or release PDU sessions when the associated DNN is congested. DNN based congestion control can be activated at the SMF over session management level and also activated at the AMF over mobility management level.

**Emergency PDU session:** A PDU session established with the request type "initial emergency request" or "existing emergency PDU session".

**General NAS level congestion control:** Type of congestion control at mobility management level that is applied at a general overload or congestion situation in the network, e.g. lack of processing resources.

**Initial NAS message:** A NAS message is considered as an initial NAS message, if this NAS message can trigger the establishment of an N1 NAS signalling connection. For instance, the REGISTRATION REQUEST message is an initial NAS message.

**Initial registration for emergency services:** A registration performed with 5GS registration type "emergency registration" in the REGISTRATION REQUEST message.

**Initial registration for onboarding services in SNPN:** A registration performed with 5GS registration type "SNPN onboarding registration" in the REGISTRATION REQUEST message.

**Initial registration for disaster roaming services:** A registration performed with 5GS registration type "disaster roaming initial registration" in the REGISTRATION REQUEST message.

**Last visited registered TAI:** A TAI which is contained in the registration area that the UE registered to the network and which identifies the tracking area last visited by the UE.

**Mapped 5G-GUTI:** A 5G-GUTI which is mapped from a 4G-GUTI previously allocated by an MME. Mapping rules are defined in 3GPP TS 23.003 [4].

**Mapped S-NSSAI:** An S-NSSAI in the subscribed S-NSSAIs for the HPLMN, which is mapped to an S-NSSAI of the registered PLMN in case of a roaming scenario.

**Mobility registration for disaster roaming services:** A registration performed with 5GS registration type "disaster roaming mobility registration updating" in the REGISTRATION REQUEST message.

**MUSIM UE:** A UE with multiple valid USIMs, capable of initiating and maintaining simultaneous separate registration states over 3GPP access with PLMN(s) using identities and credentials associated with those USIMs and supporting one or more of the N1 NAS signalling connection release, the paging indication for voice services, the reject paging request, the paging restriction and the paging timing collision control (see 3GPP TS 23.501 [8]).

**N1 mode:** A mode of a UE allowing access to the 5G core network via the 5G access network.

**Native 5G-GUTI:** A 5G-GUTI previously allocated by an AMF.

**Non 5G capable over WLAN (N5CW) device:** A device that is not capable to operate as a UE supporting NAS signalling with the 5GCN over a WLAN access network. However, this device may be capable to operate as a UE supporting NAS signalling with 5GCN using the N1 reference point as specified in this specification over 3GPP access. An N5CW device may be allowed to access the 5GCN via trusted WLAN access network (TWAN) that supports a trusted WLAN interworking function (TWIF) as specified in 3GPP TS 24.502 [18].

**Non-CAG Cell:** An NR cell which does not broadcast any Closed Access Group identity or an E-UTRA cell connected to 5GCN.

**Non-globally-unique SNPN identity:** An SNPN identity with an NID whose assignment mode is set to 1 (see 3GPP TS 23.003 [4]).

**In NB-N1 mode:** Indicates this paragraph applies only to a system which operates in NB-N1 mode. For a multi-access system this case applies if the current serving radio access network provides access to network services via E-UTRA connected to 5GCN by NB-IoT (see 3GPP TS 36.300 [25B], 3GPP TS 36.331 [25A], 3GPP TS 36.306 [25D]).

**In WB-N1 mode:** Indicates this paragraph applies only to a system which operates in WB-N1 mode. For a multi-access system this case applies if the system operates in N1 mode with E-UTRA connected to 5GCN, but not in NB-N1 mode.

**In WB-N1/CE mode:** Indicates this paragraph applies only when a UE, which is a CE mode B capable UE (see 3GPP TS 36.306 [25D]), is operating in CE mode A or B in WB-N1 mode.

**Initial small data rate control parameters:** Parameters that, if received by the UE during the establishment of a PDU session, are used as initial parameters to limit the allowed data for the PDU session according to small data rate control after establishment of a PDU session as described in subclause 6.2.13. At expiry of the associated validity period, the initial small data rate control parameters are no longer valid and the small data rate control parameters apply.

**Initial small data rate control parameters for exception data:** Parameters corresponding to initial small data rate control parameters for small data rate control of exception data.

**N1 NAS signalling connection:** A peer to peer N1 mode connection between UE and AMF. An N1 NAS signalling connection is either the concatenation of an RRC connection via the Uu reference point and an NG connection via the N2 reference point for 3GPP access, or the concatenation of an IPsec tunnel via the NWu reference point and an NG connection via the N2 reference point for non-3GPP access.

**N5CW device supporting 3GPP access:** An N5CW device which supports acting as a UE in 3GPP access (i.e. which supports NAS over 3GPP access).

**N6 PDU session:** A PDU session established between the UE and the User Plane Function (UPF) for transmitting the UE's IP data, Ethernet data or Unstructured data related to a specific application.

**NEF PDU session:** A PDU session established between the UE and the Network Exposure Function (NEF) for transmitting the UE's Unstructured data related to a specific application.

**Network slicing information:** information stored at the UE consisting of one or more of the following:

a) default configured NSSAI for PLMN or SNPN;

b) configured NSSAI for a PLMN or an SNPN;

c) mapped S-NSSAI(s) for the configured NSSAI for a PLMN;

d) pending NSSAI for a PLMN or an SNPN;

e) mapped S-NSSAI(s) for the pending NSSAI for a PLMN;

f) rejected NSSAI for the current PLMN or SNPN;

g) mapped S-NSSAI(s) for the rejected NSSAI for the current PLMN;

h) rejected NSSAI for the failed or revoked NSSAA;

and

i) for each access type:

1) allowed NSSAI for a PLMN or an SNPN;

2) mapped S-NSSAI(s) for the allowed NSSAI for a PLMN;

3) rejected NSSAI for the current registration area;

4) mapped S-NSSAI(s) for the rejected NSSAI for the current registration area;

5) rejected NSSAI for the maximum number of UEs reached; and

6) mapped S-NSSAI(s) for the rejected NSSAI for the maximum number of UEs reached.

**Non-cleartext IEs:** Information elements that are not cleartext IEs.

**Non-emergency PDU session:** Any PDU session which is not an emergency PDU session.

**Onboarding SUCI:** SUCI derived from onboarding SUPI.

**Onboarding SUPI:** SUPI with the SUPI format "network specific identifier" containing a network specific identifier or with the SUPI format "IMSI" containing an IMSI, derived by a UE in SNPN access mode, from default UE credentials for primary authentication and used to identify the UE during initial registration for onboarding services in SNPN and while registered for onboarding services in SNPN.

**PDU address:** An IP address assigned to the UE by the packet data network.

**PDU session for LADN:** A PDU session with a DNN associated with a LADN.

**PDU session with suspended user-plane resources:** A PDU session for which user-plane resources were established or re-established, and for which data radio bearers were suspended when transition to 5GMM-CONNECTED mode with RRC inactive indication.

**Persistent PDU session:** either a non-emergency PDU session contains a GBR QoS flow with QoS equivalent to QoS of teleservice 11 and where there is a radio bearer associated with that PDU session over 3GPP access, or an emergency PDU session where there is a radio bearer associated with that PDU session over 3GPP access.

NOTE 2: An example of a persistent PDU session is a non-emergency PDU session with 5QI = 1 where there is a radio bearer associated with that context.

**Procedure transaction identity:** An identity which is dynamically allocated by the UE for the UE-requested 5GSM procedures or allocated by the UE or the PCF for the UE policy delivery procedures. The procedure transaction identity is released when the procedure is completed but it should not be released immediately.

**RAT frequency selection priority index:** A parameter provided by the AMF to the NG-RAN via the N2 reference point. The AMF selects an RFSP index for a particular UE based on the subscribed RFSP index, the locally configured operator's policies, the allowed NSSAI and the UE context information, including the UE's usage setting, if received during the registration procedure. Definition derived from 3GPP TS 23.501 [8].

**Registered for disaster roaming services:** A UE is considered as "registered for disaster roaming services" when it has successfully completed initial registration or mobility registration for disaster roaming services.

**Registered for emergency services:** A UE is considered as "registered for emergency services" when it has successfully completed initial registration for emergency services.

**Registered for onboarding services in SNPN:** A UE is considered as "registered for onboarding services in SNPN" when it has successfully completed initial registration for onboarding services in SNPN. While registered for onboarding services in SNPN, services other than the onboarding services are not available.

**Registered PLMN**: The PLMN on which the UE performed the last successful registration. The identity of the registered PLMN (MCC and MNC) is provided to the UE within the GUAMI field of the 5G-GUTI.

**Rejected NSSAI:** Rejected NSSAI for the current PLMN or SNPN, rejected NSSAI for the current registration area, rejected NSSAI for the failed or revoked NSSAA or rejected NSSAI for the maximum number of UEs reached.

NOTE 3: Rejected NSSAI for the current PLMN or SNPN, rejected NSSAI for the current registration area or rejected NSSAI for the maximum number of UEs reached contains a set of S-NSSAI(s) associated with a PLMN identity or SNPN identity for the current PLMN or SNPN and in roaming scenarios also contains a set of mapped HPLMN S-NSSAI(s) if available. Rejected NSSAI for the failed or revoked NSSAA only contains a set of S-NSSAI(s) associated with a PLMN identity or SNPN identity for the HPLMN or RSNPN.

**Rejected NSSAI for the current PLMN or SNPN:** A set of S-NSSAI(s) which was included in the requested NSSAI by the UE and is sent by the AMF with the rejection cause "S-NSSAI not available in the current PLMN or SNPN".

**Rejected NSSAI for the current registration area:** A set of S-NSSAI(s) which was included in the requested NSSAI by the UE and is sent by the AMF with the rejection cause "S-NSSAI not available in the current registration area".

**Rejected NSSAI for the failed or revoked NSSAA**: A set of S-NSSAI(s) which is sent by the AMF with the rejection cause "S-NSSAI not available due to the failed or revoked network slice-specific authentication and authorization".

**Rejected NSSAI for the maximum number of UEs reached**: A set of S-NSSAI(s) which was included in the requested NSSAI by the UE and is sent by the AMF with the rejection cause "S-NSSAI not available due to maximum number of UEs reached".

**Local release:** Release of a PDU session without peer-to-peer signalling between the network and the UE.

NOTE 4: Local release can include communication among network entities.

**Removal of eCall only mode restriction:** All the limitations as described in 3GPP TS 22.101 [2] for the eCall only mode do not apply any more.

**SNPN access operation mode**: SNPN access mode or access to SNPN over non-3GPP access.

NOTE 5: The term "non-3GPP access" in an SNPN refers to the case where the UE is accessing SNPN services via a PLMN.

**S-NSSAI** **based congestion control:** Type of congestion control at session management level that is applied to reject session management requests from UEs or release PDU sessions when the associated S-NSSAI and optionally the associated DNN are congested. S-NSSAI based congestion control can be activated at the SMF over session management level and also activated at the AMF over mobility management level.

**Selected core network type information:** A type of core network (EPC or 5GCN) selected by the UE NAS layer in case of an E-UTRA cell connected to both EPC and 5GCN.

**UE supporting UAS services:** A UE which supports an aerial vehicle, such as a drone, with an onboard or built-in USIM and is able to perform UE NAS functionalities specified in this specification. Upper layers of the UE supporting UAS services are responsible for UAS related procedures such as UUAA, C2 authorization, flight authorization, for which the NAS layer of the UE supporting UAS services performs the necessary NAS procedures.

**UE configured for high priority access in selected PLMN:** A UE configured with one or more access identities equal to 1, 2, or 11-15 applicable in the selected PLMN as specified in subclause 4.5.2. Definition derived from 3GPP TS 22.261 [3].

**UE operating in single-registration mode in a network supporting N26 interface:** A UE, supporting both N1 mode and S1 mode. During the last attach, tracking area update (see 3GPP TS 24.301 [15]) or registration procedures, the UE has received either a 5GS network feature support IE with IWK N26 bit set to "interworking without N26 interface not supported" or an EPS network feature support IE with IWK N26 bit set to "interworking without N26 interface not supported".

**UE using 5GS services with control plane CIoT 5GS optimization:** AUE that is registered for 5GS services with the control plane CIOT 5GS optimization accepted by the network.

**User-plane resources:** Resources established between the UE and the UPF. The user-plane resources consist of one of the following:

- user plane radio bearers via the Uu reference point, a tunnel via the N3 reference point and a tunnel via the N9 reference point (if any) for 3GPP access;

- IPsec tunnels via the NWu reference point, a tunnel via the N3 reference point and a tunnel via the N9 reference point (if any) for untrusted non-3GPP access;

- IPsec tunnels via the NWt reference point, a tunnel via the N3 reference point and a tunnel via the N9 reference point (if any) for trusted non-3GPP access used by the UE;

- a layer-2 connection via the Yt reference point, a layer-2 or layer-3 connection via the Yw reference point, a tunnel via the N3 reference point and a tunnel via the N9 reference point (if any) for trusted non-3GPP access used by the N5CW device;

- W-UP resources via Y4 reference point, a tunnel via the N3 reference point and a tunnel via the N9 reference point (if any) for wireline access used by the 5G-RG; and

- L-W-UP resources via Y5 reference point, a tunnel via the N3 reference point and a tunnel via the N9 reference point (if any) for wireline access used by the FN-RG.

**W-AGF acting on behalf of the N5GC device:** A W-AGF that enables an N5GC device behind a 5G-CRG or an FN-CRG to connect to the 5G Core.

For the purposes of the present document, the following terms and definitions given in 3GPP TS 22.261 [3] apply:

**Non-public network**

**Disaster Roaming**

**satellite NG-RAN**

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.003 [4] apply:

**5G-GUTI**

**5G-S-TMSI**

**5G-TMSI**

**Global Line Identifier (GLI)**

**Global Cable Identifier (GCI)**

**GUAMI**

**IMEI**

**IMEISV**

**IMSI**

**PEI**

**SUPI**

**SUCI**

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.122 [5] apply:

**CAG selection**

**Country**

**EHPLMN**

**HPLMN**

**Onboarding services in SNPN**

**Registered SNPN**

**Selected PLMN**

**Selected SNPN**

**Shared network**

**SNPN identity**

**Steering of Roaming (SOR)**

**Steering of roaming connected mode control information (SOR-CMCI)**

**Steering of Roaming information**

**Subscribed SNPN**

**Suitable cell**

**VPLMN**

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.167 [6] apply:

**eCall over IMS**

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.216 [6A] apply:

**SRVCC**

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.401 [7] apply:

**eCall only mode**

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.501 [8] apply:

**5G access network**

**5G core network**

**5G QoS flow**

**5G QoS identifier**

**5G-RG**

**5G-BRG**

**5G-CRG**

**5G System**

**Allowed area**

**Allowed NSSAI**

**AMF region**

**AMF set**

**Closed access group**

**Configured NSSAI**

**Credentials Holder (CH)**

**Default Credentials Server (DCS)**

**IAB-node**

**Local area data network**

**Network identifier (NID)**

**Network slice**

**NG-RAN**

**Non-allowed area**

**Onboarding Standalone Non-Public Network**

**PDU session**

**PDU session type**

**Pending NSSAI**

**Requested NSSAI**

**Routing Indicator**

**Service data flow**

**Service Gap Control**

**Serving PLMN rate control**

**Small data rate control status**

**SNPN access mode**

**SNPN enabled UE**

**Stand-alone Non-Public Network**

**Time Sensitive Communication**

**Time Sensitive Communication and Time Synchronization Function**

**UE-DS-TT residence time**

**UE-Slice-MBR**

**UE presence in LADN service area**

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.503 [10] apply:

**UE local configuration**

For the purposes of the present document, the following terms and definitions given in 3GPP TS 24.008 [12] apply:

**GMM**

**MM**

**A/Gb mode**

**Iu mode**

**GPRS**

**Non-GPRS**

For the purposes of the present document, the following terms and definitions given in 3GPP TS 24.301 [15] apply:

**CIoT EPS optimization**

**Control plane CIoT EPS optimization**

**EENLV**

**EMM**

**EMM-DEREGISTERED**

**EMM-DEREGISTERED-INITIATED**

**EMM-IDLE mode**

**EMM-NULL**

**EMM-REGISTERED**

**EMM-REGISTERED-INITIATED**

**EMM-SERVICE-REQUEST-INITIATED**

**EMM-TRACKING-AREA-UPDATING-INITIATED**

**EPS**

**EPS security context**

**EPS services**

**Lower layer failure**

**Megabit**

**Message header**

**NAS signalling connection recovery**

**Native GUTI**

**NB-S1 mode**

**Non-EPS services**

**S1 mode**

**User plane CIoT EPS optimization**

**WB-S1 mode**

For the purposes of the present document, the following terms and definitions given in 3GPP TS 33.501 [24] apply:

**5G security context**

**5G NAS security context**

**ABBA**

**Current 5G NAS security context**

**Default UE credentials for primary authentication**

**Default UE credentials for secondary authentication**

**Full native 5G NAS security context**

**K'**AME

**K**AMF

**K**ASME

**Mapped 5G NAS security context**

**Mapped security context**

**Native 5G NAS security context**

**NCC**

**Non-current 5G NAS security context**

**Partial native 5G NAS security context**

**RES\***

For the purposes of the present document, the following terms and definitions given in 3GPP TS 38.413 [31] apply:

**NG connection**

**User Location Information**

For the purposes of the present document, the following terms and definitions given in 3GPP TS 24.587 [19B] apply:

**E-UTRA-PC5**

**NR-PC5**

**V2X**

For the purposes of the present document, the following terms and its definitions given in 3GPP TS 23.256 [6AB] apply:

**3GPP UAV ID**

**CAA (Civil Aviation Administration)-Level UAV Identity**

**Command and Control (C2) Communication**

**UAV controller (UAV-C)**

**UAS Services**

**UAS Service Supplier (USS)**

**Uncrewed Aerial System (UAS)**

**USS communication**

**UUAA**

**UUAA-MM**

**UUAA-SM**

For the purposes of the present document, the following terms and definitions given in 3GPP TS 24.554 [19E] apply:

**ProSe**

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.548 [10A] apply:

**Edge Application Server**

**Edge DNS Client**

\*\*\* Next change \*\*\*

### 4.14.2 Stand-alone non-public network

If the UE is not SNPN enabled, the UE is always considered to be not operating in SNPN access operation mode. If the UE is SNPN enabled, the UE can operate in SNPN access operation mode. Details of activation and deactivation of SNPN access operation mode at the SNPN enabled UE are up to UE implementation.

The functions and procedures of NAS described in the present document are applicable to an SNPN and an SNPN enabled UE unless indicated otherwise. The key differences brought by the SNPN to the NAS layer are as follows:

a) instead of the PLMN selection process, the SNPN selection process is performed by a UE operating in SNPN access operation mode (see 3GPP TS 23.122 [5] for further details on the SNPN selection);

b) a "permanently forbidden SNPNs" list and a "temporarily forbidden SNPNs" list are managed per access type independently (i.e. 3GPP access or non-3GPP access) and, if the UE supports access to an SNPN using credentials from a credentials holder, per entry of the "list of subscriber data" or the PLMN subscription, by a UE operating in SNPN access operation mode instead of forbidden PLMN lists. If the UE supports onboarding services in SNPN, an additional "permanently forbidden SNPNs" list for onboarding services and an additional "temporarily forbidden SNPNs" list for onboarding services are managed;

c) inter-system change to and from S1 mode is not supported;

d) void;

e) CAG is not supported in SNPN access operation mode;

f) with respect to the 5GMM cause values:

1) 5GMM cause values #74 "Temporarily not authorized for this SNPN" and #75 "Permanently not authorized for this SNPN" are supported whereas these 5GMM cause values cannot be used in a PLMN; and

2) 5GMM cause values #11 "PLMN not allowed", #31 "Redirection to EPC required", #73 "Serving network not authorized", and #76 "Not authorized for this CAG or authorized for CAG cells only" are not supported whereas these 5GMM cause values can be used in a PLMN;

NOTE 1: The network does not send 5GMM cause value #13 to the UE operating in SNPN access operation mode in this release of specification.

g) a list of "5GS forbidden tracking areas for roaming" and a list of "5GS forbidden tracking areas for regional provision of service" are managed per SNPN and, if the UE supports access to an SNPN using credentials from a credentials holder, entry of the "list of subscriber data" or PLMN subscription (see 3GPP TS 23.122 [5]);

h) when accessing SNPN services via a PLMN using 3GPP access, access to 5GCN of the SNPN is performed using 5GMM procedures for non-3GPP access, 5GMM parameters for non-3GPP access, the UE is performing access to SNPN over non-3GPP access and the UE is not operating in SNPN access mode over 3GPP access. When accessing PLMN services via a SNPN using 3GPP access, access to 5GCN of the PLMN is performed using 5GMM procedures for non-3GPP access, 5GMM parameters for non-3GPP access, the UE is not performing access to SNPN over non-3GPP access, and the UE is operating in SNPN access mode over 3GPP access. From the UE's NAS perspective, accessing PLMN services via an SNPN and accessing SNPN services via a PLMN are treated as untrusted non-3GPP access. If the UE is accessing the PLMN using non-3GPP access, the access to 5GCN of the SNPN via PLMN is not specified in this release of the specification .

Emergency services are not supported in an SNPN when a UE accesses SNPN services via a PLMN;

NOTE 2: The term "non-3GPP access" in an SNPN refers to the case where the UE is accessing SNPN services via a PLMN.

i) when registered to an SNPN, the UE shall use only the UE policies provided by the registered SNPN;

j) equivalent SNPN is not supported;

k) void;

l) void;

m) UE mobility between SNPNs in 5GMM-CONNECTED mode is not supported, UE mobility between SNPNs in 5GMM-IDLE mode is supported when the UE supports access to an SNPN using credentials from a credentials holder, and UE mobility between an SNPN and a PLMN is not supported;

n) CIoT 5GS optimizations are not supported;

o) accessing SNPN services using non-3GPP access is not supported, except when accessing SNPN services via a PLMN using 3GPP access as specified in item h;

p) when registering or registered to an SNPN, the UE shall handle the 5GS mobile identity as described in subclause 5.5.1.2.2;

q) when registering or registered to an SNPN, the UE shall only consider:

1) a last visited registered TAI visited in the same SNPN as an available last visited registered TAI; or

2) a last visited registered TAI visited using the same entry of the "list of subscriber data" or the same PLMN subscription as an available last visited registered TAI, if the UE supports access to an SNPN using credentials from a credentials holder;

NOTE 3: If the last visited registered TAI is assigned by an SNPN other than the current SNPN, the serving AMF can determine the SNPN assigning the last visited registered TAI using the NID provided by the UE.

r) emergency service fallback is not supported;

s) when registering or registered for onboarding services in SNPN, the UE shall not provide the requested NSSAI to the network;

s1) when performing initial registration for onboarding services in SNPN, the UE shall set the 5GS registration type value to "SNPN onboarding registration";

t) when registering or registered for onboarding services in SNPN, the AMF shall not provide the configured NSSAI, the allowed NSSAI or the rejected NSSAI to the UE, shall use the S-NSSAI included in the AMF onboarding configuration data for onboarding services in SNPN and shall not perform NSSAA procedure for S-NSSAI used for onboarding services in SNPN;

u) the UE can access an SNPN indicating that onboarding is allowed using default UE credentials for primary authentication in order for the UE to be configured with one or more entries of the "list of subscriber data";

x) eCall over IMS is not supported in SNPN access operation mode and the UE ignores any USIM configuration for eCall only mode;

y) when registering or registered for onboarding services in SNPN, the AMF shall store in the 5GMM context of the UE an indication that the UE is registered for onboarding services in SNPN;

z) a UE with multiple valid entries of "list of subscriber data", or one or more valid USIMs and one or more valid entries of "list of subscriber data", capable of initiating and maintaining simultaneous separate registration states over 3GPP access with PLMN(s) or SNPN(s), using identities and credentials associated with those entries of "list of subscriber data", or USIMs and entries of "list of subscriber data", and supporting one or more of the N1 NAS signalling connection release, the paging indication for voice services, the reject paging request, the paging restriction and the paging timing collision control may use procedures defined for MUSIM UE, even if the UE does not include multiple valid USIMs; and

za) when the UE is registering or registered for onboarding services in SNPN, the network slice admission control is not performed.

NOTE 4: If the network determines that the UE cannot register to the onboarding SNPN due to lack of resources for the network slice used for onboarding, the AMF can reject the UE with 5GMM cause #22 "congestion".

\*\*\* Next change \*\*\*

### 5.3.2 Permanent identifiers

A globally unique permanent identity, the 5G subscription permanent identifier (SUPI), is allocated to each subscriber for 5GS-based services. The IMSI, the network specific identifier, the GCI and the GLI are valid SUPI types. When the SUPI contains a network specific identifier, a GCI or a GLI, it shall take the form of a network access identifier (NAI). When the UE performs initial registration for onboarding services in SNPN or is registered for onboarding services in SNPN, the SUPI contains the onboarding SUPI derived from the default UE credentials for primary authentication. The UE derives the onboarding SUPI before or during the initial registration for onboarding services in SNPN and uses the derived onboarding SUPI in the initial registration for onboarding services in SNPN and while registered for onboarding services in SNPN.

The structure of the SUPI and its derivatives are specified in 3GPP TS 23.003 [4].

The UE provides the SUPI to the network in concealed form. The SUCI is a privacy preserving identifier containing the concealed SUPI. When the SUPI contains a network specific identifier, a GCI or a GLI, the SUCI shall take the form of a NAI as specified in 3GPP TS 23.003 [4].

A UE supporting N1 mode includes a SUCI:

a) in the REGISTRATION REQUEST message when the UE is attempting initial registration procedure and a valid 5G-GUTI is not available;

b) in the IDENTITY RESPONSE message, if the SUCI is requested by the network during the identification procedure; and

c) in the DEREGISTRATION REQUEST message when the UE initiates a de-registration procedure and a valid 5G-GUTI is not available.

If the UE uses the "null-scheme" as specified in 3GPP TS 33.501 [24] to generate a SUCI, the SUCI contains the unconcealed SUPI.

When:

- not operating in SNPN access operation mode; or

- operating in SNPN access operation mode but not performing initial registration for onboarding services and not registered for onboarding services;

the UE shall use the "null-scheme" if:

a) the home network has not provisioned the public key needed to generate a SUCI;

b) the home network has configured "null-scheme" to be used for the UE;

c) the UE needs to perform a registration procedure for emergency services after the failure of authentication procedure or after reception of a REGISTRATION REJECT message with the 5GMM cause #3 "Illegal UE", or to initiate a de-registration procedure before the registration procedure for emergency services was completed successfully, and the UE does not have a valid 5G-GUTI for the selected PLMN; or

d) the UE receives an identity request for SUCI during a registration procedure for emergency services or during a de-registration procedure that was initiated before the registration procedure for emergency services was completed successfully.

When operating in SNPN access operation mode and:

- performing initial registration for onboarding services; or

- registered for onboarding services;

the UE shall use the "null-scheme" if:

a) the public key needed to generate a SUCI is not configured as part of the default UE credentials for primary authentication; or

b) "null-scheme" usage is configured as part of the default UE credentials for primary authentication.

If:

a) the UE uses the "null-scheme" as specified in 3GPP TS 33.501 [24] to generate a SUCI;

b) the UE operates in SNPN access operation mode and:

1) the UE is not registering or registered for onboarding services in SNPN, and the AAA server of CH acts as EAP server of the EAP based primary authentication and key agreement procedure; or

2) the UE is registering or registered for onboarding services in SNPN and the AAA server of DCS acts as EAP server of the EAP based primary authentication and key agreement procedure;

Editor's note: (WI:eNPN, CR#3847) it is FFS how the UE knows whether the AAA server of CH or DCS acts as EAP server of the EAP based primary authentication and key agreement procedure.

c) the UE does not need to perform a registration procedure for emergency services, or to initiate a de-registration procedure before the registration procedure for emergency services was completed successfully; and

d) the UE does not receive an identity request for SUCI during a registration procedure for emergency services or during a de-registration procedure that was initiated before the registration procedure for emergency services was completed successfully;

then the UE shall use anonymous SUCI as specified in 3GPP TS 23.003 [4].

A W-AGF acting on behalf of an FN-RG shall use the "null-scheme" as specified in 3GPP TS 33.501 [24] to generate a SUCI.

A W-AGF acting on behalf of an N5GC device shall use the "null-scheme" as specified in 3GPP TS 33.501 [24] to generate a SUCI.

If a UE is a Multi-USIM UE, the UE shall use a separate permanent equipment identifier (PEI) for each USIM, if any, and each entry of "list of subscriber data", if any, the UE operates for accessing 5GS-based services; otherwise, a UE contains and uses a permanent equipment identifier (PEI) for accessing 5GS-based services.

In this release of the specification, the IMEI, the IMEISV, the MAC address together with the MAC address usage restriction indication and the EUI-64 are the only PEI formats supported by 5GS. The structure of the PEI and its formats are specified in 3GPP TS 23.003 [4].

Each UE supporting at least one 3GPP access technology (i.e. satellite NG-RAN, NG-RAN, E-UTRAN, UTRAN or GERAN) contains a PEI in the IMEI format and shall be able to provide an IMEI and an IMEISV upon request from the network.

Each UE not supporting any 3GPP access technologies and supporting NAS over untrusted or trusted non-3GPP access shall have a PEI in the form of the Extended Unique Identifier EUI-64 [48] of the access technology the UE uses to connect to the 5GC.

A UE supporting N1 mode includes a PEI:

a) when neither SUPI nor valid 5G-GUTI is available to use for emergency services in the REGISTRATION REQUEST message with 5GS registration type IE set to "emergency registration";

b) when the network requests the PEI by using the identification procedure, in the IDENTITY RESPONSE message; and

c) when the network requests the IMEISV by using the security mode control procedure, in the SECURITY MODE COMPLETE message.

Each 5G-RG supporting only wireline access and each FN-RG shall have a permanent MAC address configured by the manufacturer. For 5G-CRG, the permanent MAC address configured by the manufacturer shall be a cable modem MAC address.

When the 5G-RG contains neither an IMEI nor an IMEISV, the 5G-RG shall use as a PEI the 5G-RG's permanent MAC address configured by the manufacturer and the MAC address usage restriction indication set to "no restrictions".

The W-AGF acting on behalf of the FN-RG shall use as a PEI the MAC address provided by the FN-RG and if the MAC address provided by the FN-RG is not unique or does not correspond to the FN-RG's permanent MAC address according to W-AGF's configuration, the MAC address usage restriction indication set to "MAC address is not usable as an equipment identifier" otherwise the MAC address usage restriction indication set to "no restrictions".

The 5G-RG containing neither an IMEI nor an IMEISV shall include the PEI containing the MAC address together with the MAC address usage restriction indication:

a) when neither SUPI nor valid 5G-GUTI is available to use for emergency services in the REGISTRATION REQUEST message with 5GS registration type IE set to "emergency registration";

b) when the network requests the PEI by using the identification procedure, in the IDENTIFICATION RESPONSE message; and

c) when the network requests the IMEISV by using the security mode control procedure, in the SECURITY MODE COMPLETE message.

NOTE 1: In case c) above, the MAC address is provided even though AMF requests the IMEISV.

The W-AGF acting on behalf of the FN-RG shall include the PEI containing the MAC address together with the MAC address usage restriction indication:

a) when the network requests the PEI by using the identification procedure, in the IDENTIFICATION RESPONSE message; and

b) when the network requests the IMEISV by using the security mode control procedure, in the SECURITY MODE COMPLETE message.

NOTE 2: In case b) above, the MAC address is provided even though AMF requests the IMEISV.

The W-AGF acting on behalf of the N5GC device shall use as a PEI the MAC address provided by the N5GC device and the MAC address usage restriction indication set to "no restrictions". Based on operator policy, the W-AGF acting on behalf of the N5GC device may encode the MAC address of the N5GC device using the EUI-64 format as specified in [48] and use as a PEI the derived EUI-64.

NOTE 3: The MAC address of an N5GC device is universally/globally unique.

The AMF can request the PEI at any time by using the identification procedure.

\*\*\* Next change \*\*\*

5.4.1.2.2.3 UE successfully authenticates network

If a USIM is present and the SNN check is successful, the UE shall handle the EAP-request/AKA'-challenge message as specified in IETF RFC 5448 [40]. The USIM shall derive CK and IK and compute the authentication response (RES) using the 5G authentication challenge data received from the ME, and pass RES to the ME. The ME shall derive CK' and IK' from CK and IK, and if the UE operates in SNPN access operation mode and:

a) the default UE credentials for primary authentication, if the UE is registering or registered for onboarding services in SNPN; or

b) credentials in the USIM, if the UE is not registering or registered for onboarding services in SNPN;

contain an indication to use MSK for derivation of KAUSF after success of primary authentication and key agreement procedure then derive MSK from CK' and IK' otherwise derive EMSK from CK' and IK'.

Furthermore, if the UE operates in SNPN access operation mode and:

a) the default UE credentials for primary authentication, if the UE is registering or registered for onboarding services in SNPN; or

b) credentials in the USIM, if the UE is not registering or registered for onboarding services in SNPN;

contain an indication to use MSK for derivation of KAUSF after success of primary authentication and key agreement procedure then the ME may generate a new KAUSF from the MSK otherwise the ME may generate a new KAUSF from the EMSK.

If the ME generates a new KAUSF, the ME shall generate a new KSEAF from the new KAUSF, and the KAMF from the ABBA received together with the EAP-request/AKA'-challenge message, and the new KSEAF as described in 3GPP TS 33.501 [24], and create a partial native 5G NAS security context identified by the ngKSI value received together with the EAP-request/AKA'-challenge message in subclause 5.4.1.2.4.2 in the volatile memory of the ME. If the KAMF and the partial native 5G NAS security context are created, the ME shall store the KAMF in the created partial native 5G NAS security context, and shall send an EAP-response/AKA'-challenge message as specified in IETF RFC 5448 [40].

NOTE: 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 ME shall not use the new KAUSF in the verification of SOR transparent container and UE parameters update transparent container, if any are received, until receipt of an EAP-success message.

If the EAP-request/AKA'-challenge message contains AT\_RESULT\_IND attribute, the UE may include AT\_RESULT\_IND attribute in the EAP-response/AKA'-challenge message as specified in IETF RFC 5448 [40].

\*\*\* Next change \*\*\*

5.4.1.2.2.8 UE handling EAP-success message

Upon receiving an EAP-success message, the ME shall:

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

b) if the ME has not generated a new KAUSF and a new KSEAF and has not created a partial native 5G NAS security context as described in subclause 5.4.1.2.2.3:

1) if the UE operates in SNPN access operation mode and:

i) the default UE credentials for primary authentication, if the UE is registering or registered for onboarding services in SNPN; or

ii) credentials in the USIM, if the UE is not registering or registered for onboarding services in SNPN;

contain an indication to use MSK for derivation of KAUSF after success of primary authentication and key agreement procedure then generate a new KAUSF from the MSK otherwise generate a new KAUSF from the EMSK;

2) generate a new KSEAF from the new KAUSF, and the KAMF from the ABBA that was received with the EAP-success message, and the new KSEAF as described in 3GPP TS 33.501 [24];

3) create a partial native 5G NAS security context identified by the ngKSI value in the volatile memory of the ME; and

4) store the KAMF in the created partial native 5G NAS security context; and

c) 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.

The UE shall consider the procedure complete.

\*\*\* Next change \*\*\*

5.4.1.2.3.1 General

The UE may support acting as EAP-TLS peer as specified in 3GPP TS 33.501 [24]. The AUSF may support acting as EAP-TLS server as specified in 3GPP TS 33.501 [24]. The AAA server of the CH or the DCS may support acting as EAP server of such EAP method as specified in 3GPP TS 23.501 [8].

The EAP-TLS enables mutual authentication of the UE and the network.

When initiating an EAP based primary authentication and key agreement procedure using EAP-TLS, the network shall select an ngKSI value. If an ngKSI is contained in an initial NAS message during a 5GMM procedure, the network shall select a different ngKSI value. The network shall send the selected ngKSI value to the UE along with each EAP message. The network shall send the ABBA value as described in subclause 9.11.3.10 to the UE along with the EAP-request message and EAP-success message.

When the EAP based primary authentication and key agreement procedure uses EAP-TLS:

a) if the UE operates in SNPN access operation mode and:

1) the default UE credentials for primary authentication, if the UE is registering or registered for onboarding services in SNPN; or

2) credentials in the selected entry of the "list of configuration data", if the UE is not registering or registered for onboarding services in SNPN;

contain an indication to use MSK for derivation of KAUSF after success of primary authentication and key agreement procedure then the ME shall generate MSK as described in 3GPP TS 33.501 [24] otherwise the ME shall generate EMSKas described in 3GPP TS 33.501 [24];

b) if the AUSF acts as the EAP-TLS server, the AUSF shall generate EMSKas described in 3GPP TS 33.501 [24]; and

c) if the AAA server of the CH or the DCS acts as the EAP-TLS server, the AAA server of the CH or the DCS shall generate MSKas described in 3GPP TS 33.501 [24].

When handling of an EAP-request message results into generation of MSK or EMSK, if the UE operates in SNPN access operation mode and:

a) the default UE credentials for primary authentication, if the UE is registering or registered for onboarding services in SNPN; or

b) credentials in the selected entry of the "list of configuration data", if the UE is not registering or registered for onboarding services in SNPN;

contain an indication to use MSK for derivation of KAUSF after success of primary authentication and key agreement procedure , then the ME may generate a new KAUSF from the MSK otherwise the ME may generate a new KAUSF from the EMSK.

If the ME generates a new KAUSF, the ME shall generate a new KSEAF from the new KAUSF, and the KAMF from the ABBA received together with the EAP-request message, and the new KSEAF as described in 3GPP TS 33.501 [24], and create a partial native 5G NAS security context identified by the ngKSI value received together with the EAP-request message in subclause 5.4.1.2.4.2, in the volatile memory of the ME. If the KAMF and the partial native 5G NAS security context are created, the ME shall store the KAMF in the created partial native 5G NAS security context.

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 ME shall not use the new KAUSF in the verification of SOR transparent container and UE parameters update transparent container, if any are received, until receipt of an EAP-success message.

When the AUSF acts as the EAP-TLS server and handling of an EAP response message results into generation of EMSK, the AUSF shall generate the KAUSF from the EMSK, and the KSEAF from the KAUSF as described in 3GPP TS 33.501 [24].

NOTE 2: When the AAA server of the CH or the DCS acts as the EAP-TLS server, the AAA server of the CH or the DCS provides (via the NSSAAF) the MSK to the AUSF. Upon reception of the MSK, the AUSF generates the KAUSF from the MSK, and the KSEAF from the KAUSF as described in 3GPP TS 33.501 [24].

NOTE 3: The AUSF provides the KSEAF to the SEAF. Upon reception of the KSEAF, the SEAF generates the KAMF based on the ABBA and the KSEAF as described in 3GPP TS 33.501 [24], and provides ngKSI and the KAMF to the AMF. Upon reception of the ngKSI and the KAMF, the AMF creates a partial native 5G NAS security context identified by the ngKSI, and stores the KAMF in the created partial native 5G NAS security context.

If the UE does not accept the server certificate of the network, the UE shall start timer T3520 when the AUTHENTICATION RESPONSE message containing the EAP-response message is sent. Furthermore, the UE shall stop any of the retransmission timers that are running (e.g. T3510, T3517 or T3521). Upon receiving an AUTHENTICATION REQUEST message with the EAP message IE containing an EAP-request message from the network, the UE shall stop timer T3520, if running, and then process the EAP-request message as normally.

If the network does not accept the client certificate of the UE, the network handling depends upon the type of identity used by the UE in the initial NAS message, that is:

- if the 5G-GUTI was used; or

- if the SUCI was used.

If the 5G-GUTI was used, the network should transport the EAP-failure message in the AUTHENTICATION RESULT message of the EAP result message transport procedure, initiate an identification procedure to retrieve SUCI from the UE and restart the EAP based primary authentication and key agreement procedure with the received SUCI.

If the SUCI was used for identification in the initial NAS message or in a restarted EAP based primary authentication and key agreement procedure, or the network decides not to initiate the identification procedure to retrieve SUCI from the UE after an unsuccessful the EAP based primary authentication and key agreement procedure, the network should transport the EAP-failure message in an AUTHENTICATION REJECT message of the EAP result message transport procedure.

Depending on local requirements or operator preference for emergency services, if the UE initiates a registration procedure with 5GS registration type IE set to "emergency registration" and the AMF is configured to allow emergency registration without user identity, the AMF needs not follow the procedures specified for transporting the EAP-failure message in the AUTHENTICATION REJECT message of the EAP result message transport procedure in the present subclause. The AMF may include the EAP-failure message in a response of the current 5GMM specific procedure or in the AUTHENTICATION RESULT of the EAP result message transport procedure.

If the EAP-failure message is received in an AUTHENTICATION REJECT message:

a) if the AUTHENTICATION REJECT message has been successfully integrity checked by the NAS:

1) the UE shall set the update status to 5U3 ROAMING NOT ALLOWED, delete the stored 5G-GUTI, TAI list, last visited registered TAI and ngKSI.

In case of PLMN, the USIM shall be considered invalid until switching off the UE or the UICC containing the USIM is removed.

In case of SNPN, if the UE is neither registered for onboarding services in SNPN nor performing initial registration for onboarding services in SNPN and the UE does not support access to an SNPN using credentials from a credentials holder, the entry of the "list of subscriber data" with the SNPN identity of the current SNPN shall be considered invalid until the UE is switched off or the entry is updated;

In case of SNPN, if the UE is neither registered for onboarding services in SNPN nor performing initial registration for onboarding services in SNPN and the UE supports access to an SNPN using credentials from a credentials holder, the UE shall consider the selected entry of the "list of subscriber data" as invalid until the UE is switched off or the entry is updated.

If the UE is registered for onboarding services in SNPN or is performing initial registration for onboarding services in SNPN, the UE shall store the SNPN identity in the "permanently forbidden SNPNs" list for onboarding services, enter state 5GMM-DEREGISTERED.PLMN-SEARCH, and perform an SNPN selection or an SNPN selection for onboarding services according to 3GPP TS 23.122 [5];

2) if the UE is neither registered for onboarding services in SNPN nor performing initial registration for onboarding services in SNPN, the UE shall set:

i) the counter for "SIM/USIM considered invalid for GPRS services" events, the counter for "USIM considered invalid for 5GS services over non-3GPP access" events, and the counter for "SIM/USIM considered invalid for non-GPRS services" events if maintained by the UE, in case of PLMN; or

ii) the counter for "the entry for the current SNPN considered invalid for 3GPP access" events and the counter for "the entry for the current SNPN considered invalid for non-3GPP access" events in case of SNPN;

NOTE 4: The term "non-3GPP access" used in the counter for "the entry for the current SNPN considered invalid for non-3GPP access" events, is used to express access to SNPN services via a PLMN.

to UE implementation-specific maximum value.

If the UE is registered for onboarding services in SNPN or performing initial registration for onboarding services in SNPN, the UE shall set the SNPN-specific attempt counter for the current SNPN to the UE implementation-specific maximum value; and

3) if the UE is operating in single-registration mode, the UE shall handle EMM parameters, 4G-GUTI, last visited registered TAI, TAI list and eKSI as specified in 3GPP TS 24.301 [15] for the case when the authentication procedure is not accepted by the network. The USIM shall be considered as invalid also for non-EPS services until switching off or the UICC containing the USIM is removed; and

b) if the AUTHENTICATION REJECT message is received without integrity protection, the UE shall start timer T3247 with a random value uniformly drawn from the range between 30 minutes and 60 minutes, if the timer is not running (see subclause 5.3.20).

Additionally, if the UE is neither registered for onboarding services in SNPN nor performing initial registration for onboarding services in SNPN, the UE shall:

1) if the AUTHENTICATION REJECT message is received over 3GPP access, and the counter for "SIM/USIM considered invalid for GPRS services" events in case of PLMN or the counter for "the entry for the current SNPN considered invalid for 3GPP access" events in case of SNPN has a value less than a UE implementation-specific maximum value, proceed as specified in subclause 5.3.20, list item 1)-a) of subclause 5.3.20.2 (if the UE is not SNPN enabled or is not operating in SNPN access operation mode) or list item a) 1) of subclause 5.3.20.3 (if the UE is operating in SNPN access operation mode) for the case that the 5GMM cause value received is #3;

2) if the AUTHENTICATION REJECT message is received over non-3GPP access, and the counter for "USIM considered invalid for 5GS services over non-3GPP access" events in case of PLMN or the counter for "the entry for the current SNPN considered invalid for non-3GPP access" events in case of SNPN has a value less than a UE implementation-specific maximum value, proceed as specified in subclause 5.3.20, list item 1)-b) of subclause 5.3.20.2 (if the UE is not operating in SNPN access operation mode) or list item a)-2) of subclause 5.3.20.3 (if the UE is operating in SNPN access operation mode) for the case that the 5GMM cause value received is #3; or

3) otherwise:

i) if the AUTHENTICATION REJECT message is received over 3GPP access:

A) the UE shall set the update status for 3GPP access to 5U3 ROAMING NOT ALLOWED, delete for 3GPP access only the stored 5G-GUTI, TAI list, last visited registered TAI and ngKSI.

In case of PLMN, the UE shall consider the USIM as invalid for 5GS services via 3GPP access and invalid for non-EPS service until switching off the UE or the UICC containing the USIM is removed.

In case of SNPN, if the UE does not support access to an SNPN using credentials from a credentials holder, the UE shall consider the entry of the "list of subscriber data" with the SNPN identity of the current SNPN as invalid for 3GPP access until the UE is switched off or the entry is updated;

In case of SNPN, if the UE supports access to an SNPN using credentials from a credentials holder, the UE shall consider the selected entry of the "list of subscriber data" as invalid for 3GPP access until the UE is switched off or the entry is updated;

B) the UE shall set:

- the counter for "SIM/USIM considered invalid for GPRS services" events and the counter for "SIM/USIM considered invalid for non-GPRS services" events if maintained by the UE, in case of PLMN; or

- the counter for "the entry for the current SNPN considered invalid for 3GPP access" events in case of SNPN;

to UE implementation-specific maximum value; and

C) If the UE is operating in single-registration mode, the UE shall handle 4G-GUTI, TAI list and eKSI as specified in 3GPP TS 24.301 [15] for the case when the authentication procedure is not accepted by the network. The USIM shall be considered as invalid also for non-EPS services until switching off or the UICC containing the USIM is removed; and

ii) if the AUTHENTICATION REJECT message is received over non-3GPP access:

A) the UE shall set the update status for non-3GPP access to 5U3 ROAMING NOT ALLOWED, delete for non-3GPP access only the stored 5G-GUTI, TAI list, last visited registered TAI and ngKSI. In case of PLMN, the USIM shall be considered invalid for 5GS services via non-3GPP access until switching off the UE or the UICC containing the USIM is removed. In case of SNPN, the UE shall consider the entry of the "list of subscriber data" with the SNPN identity of the current SNPN shall be considered invalid for non-3GPP access until the UE is switched off or the entry is updated; and

B) the UE shall set the counter for "USIM considered invalid for 5GS services over non-3GPP access" events in case of PLMN or the counter for "the entry for the current SNPN considered invalid for non-3GPP access" events in case of SNPN to UE implementation-specific maximum value.

If the UE is registered for onboarding services in SNPN or performing initial registration for onboarding services in SNPN, the UE shall:

1) if the SNPN-specific attempt counter for the SNPN sending the AUTHENTICATION REJECT message has a value less than a UE implementation-specific maximum value, increment the SNPN-specific attempt counter for the SNPN; or

2) otherwise, the UE shall set the update status to 5U3.ROAMING NOT ALLOWED, delete the stored 5G-GUTI, TAI list, last visited registered TAI, and ngKSI, store the SNPN identity in the "permanently forbidden SNPNs" list for onboarding services, enter state 5GMM-DEREGISTERED.PLMN-SEARCH, and perform an SNPN selection or an SNPN selection for onboarding services according to 3GPP TS 23.122 [5].

If the AUTHENTICATION REJECT message is received by the UE, the UE shall abort any 5GMM signalling procedure, stop any of the timers T3510, T3517, T3519 or T3521 (if they were running), enter state 5GMM-DEREGISTERED and delete any stored SUCI.

Upon receiving an EAP-success message, the ME shall:

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

b) if the ME has not generated a new KAUSF and a new KSEAF and has not created a partial native 5G NAS security context when handling the EAP-request message which resulted into generation of EMSK or MSK as described above:

1) if the UE operates in SNPN access operation mode and:

i) the default UE credentials for primary authentication, if the UE is registering or registered for onboarding services in SNPN; or

ii) credentials in the selected entry of the "list of configuration data", if the UE is not registering or registered for onboarding services in SNPN;

contain an indication to use MSK for derivation of KAUSF after success of primary authentication and key agreement procedure then generate a new KAUSF from the MSK otherwise generate a new KAUSF from the EMSK;

2) generate a new KSEAF from the new KAUSF, and the KAMF from the ABBA that was received with the EAP-success message, and the new KSEAF as described in 3GPP TS 33.501 [24];

3) create a partial native 5G NAS security context identified by the ngKSI value in the volatile memory of the ME; and

4) store the KAMF in the created partial native 5G NAS security context; and

c) 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, 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.

The UE shall consider the procedure complete.

Upon receiving an EAP-failure message, the UE shall delete the partial native 5G NAS security context and shall delete the new KAUSF and the new KSEAF, if any were created when handling the EAP-request message which resulted into generation of EMSK or MSK as described above.

The UE shall consider the procedure complete.

\*\*\* Next change \*\*\*

5.4.1.2.3A.1 General

This subclause applies when an EAP method:

a) supporting mutual authentication;

b) supporting EMSK or MSK generation; and

c) other than EAP-AKA' and EAP-TLS;

is used for primary authentication and key agreement in an SNPN.

The UE may support acting as EAP peer of such EAP method as specified in 3GPP TS 33.501 [24]. The AUSF may support acting as EAP server of such EAP method as specified in 3GPP TS 33.501 [24]. The AAA server of the CH or the DCS may support acting as EAP server of such EAP method as specified in 3GPP TS 23.501 [8].

When initiating an EAP based primary authentication and key agreement procedure using such EAP method, the network shall select an ngKSI value. If an ngKSI is contained in an initial NAS message during a 5GMM procedure, the network shall select a different ngKSI value. The network shall send the selected ngKSI value to the UE along with each EAP message. The network shall send the ABBA value as described in subclause 9.11.3.10 to the UE along with the EAP-request message and EAP-success message.

When the EAP based primary authentication and key agreement procedure uses such EAP method:

a) if:

1) the default UE credentials for primary authentication, if the UE is registering or registered for onboarding services in SNPN; or

2) credentials in the selected entry of the "list of configuration data", if the UE is not registering or registered for onboarding services in SNPN;

contain an indication to use MSK for derivation of KAUSF after success of primary authentication and key agreement procedure then the ME shall generate MSK as described in 3GPP TS 33.501 [24] otherwise the ME shall generate EMSKas described in 3GPP TS 33.501 [24];

b) if the AUSF acts as the EAP server, the AUSF shall generate EMSK as described in 3GPP TS 33.501 [24]; and

c) if the AAA server of the CH or the DCS acts as the EAP server, the AAA server of the CH or the DCS shall generate MSKas described in 3GPP TS 33.501 [24].

When handling of an EAP-request message results into generation of MSK or EMSK, if:

a) the default UE credentials for primary authentication, if the UE is registering or registered for onboarding services in SNPN; or

b) credentials in the selected entry of the "list of configuration data", if the UE is not registering or registered for onboarding services in SNPN;

contain an indication to use MSK for derivation of KAUSF after success of primary authentication and key agreement procedure then the ME may generate a new KAUSF from the MSK otherwise the ME may generate a new KAUSF from the EMSK.

If the ME generates a new KAUSF, the ME shall generate a new KSEAF from the new KAUSF, and the KAMF from the ABBA received together with the EAP-request message, and the new KSEAF as described in 3GPP TS 33.501 [24], and create a partial native 5G NAS security context identified by the ngKSI value received together with the EAP-request message in subclause 5.4.1.2.4.2, in the volatile memory of the ME. If the KAMF and the partial native 5G NAS security context are created, the ME shall store the KAMF in the created partial native 5G NAS security context.

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 ME shall not use the new KAUSF in the verification of SOR transparent container and UE parameters update transparent container, if any are received, until receipt of an EAP-success message.

When the AUSF acts as the EAP server and handling of an EAP response message results into generation of EMSK, the AUSF shall generate the KAUSF from the EMSK, and the KSEAF from the KAUSF as described in 3GPP TS 33.501 [24].

NOTE 2: When the AAA server of the CH or the DCS acts as the EAP server and handling of an EAP response message results into generation of MSK, the AAA server of the CH or the DCS provides (via the NSSAAF) the MSK to the AUSF. Upon reception of the MSK, the AUSF generates the KAUSF from the MSK, and the KSEAF from the KAUSF as described in 3GPP TS 33.501 [24].

NOTE 3: The AUSF provides the KSEAF to the SEAF. Upon reception of the KSEAF, the SEAF generates the KAMF based on the ABBA and the KSEAF as described in 3GPP TS 33.501 [24], and provides ngKSI and the KAMF to the AMF. Upon reception of the ngKSI and the KAMF, the AMF creates a partial native 5G NAS security context identified by the ngKSI, and stores the KAMF in the created partial native 5G NAS security context.

If the UE fails to authenticate the network, the UE shall start timer T3520 when the AUTHENTICATION RESPONSE message containing the EAP-response message is sent. Furthermore, the UE shall stop any of the retransmission timers that are running (e.g. T3510, T3517 or T3521). Upon receiving an AUTHENTICATION REQUEST message with the EAP message IE containing an EAP-request message from the network, the UE shall stop timer T3520, if running, and then process the EAP-request message as normally.

If the network fails to authenticate the UE, the network handling depends upon the type of identity used by the UE in the initial NAS message, that is:

- if the 5G-GUTI was used; or

- if the SUCI was used.

If the 5G-GUTI was used, the network should transport the EAP-failure message in the AUTHENTICATION RESULT message of the EAP result message transport procedure, initiate an identification procedure to retrieve SUCI from the UE and restart the EAP based primary authentication and key agreement procedure with the received SUCI.

If the SUCI was used for identification in the initial NAS message or in a restarted EAP based primary authentication and key agreement procedure, or the network decides not to initiate the identification procedure to retrieve SUCI from the UE after an unsuccessful the EAP based primary authentication and key agreement procedure, the network should transport the EAP-failure message in an AUTHENTICATION REJECT message of the EAP result message transport procedure.

If the EAP-failure message is received in an AUTHENTICATION REJECT message:

a) if the AUTHENTICATION REJECT message has been successfully integrity checked by the NAS:

1) the UE shall set the update status to 5U3 ROAMING NOT ALLOWED, delete the stored 5G-GUTI, TAI list, last visited registered TAI and ngKSI.

In case of SNPN, if the UE is neither registered for onboarding services in SNPN nor performing initial registration for onboarding services in SNPN and the UE does not support access to an SNPN using credentials from a credentials holder, the entry of the "list of subscriber data" with the SNPN identity of the current SNPN shall be considered invalid until the UE is switched off or the entry is updated;

In case of SNPN, if the UE is neither registered for onboarding services in SNPN nor performing initial registration for onboarding services in SNPN and the UE supports access to an SNPN using credentials from a credentials holder, the UE shall consider the selected entry of the "list of subscriber data" as invalid until the UE is switched off or the entry is updated.

In case of SNPN, if the UE is registered for onboarding services in SNPN or is performing initial registration for onboarding services in SNPN, the UE shall store the SNPN identity in the "permanently forbidden SNPNs" list for onboarding services, enter state 5GMM-DEREGISTERED.PLMN-SEARCH, and perform an SNPN selection or an SNPN selection for onboarding services according to 3GPP TS 23.122 [5]; and

2) if the UE is neither registered for onboarding services in SNPN nor performing initial registration for onboarding services in SNPN, the UE shall set the counter for "the entry for the current SNPN considered invalid for 3GPP access" events and the counter for "the entry for the current SNPN considered invalid for non-3GPP access" events in case of SNPN to UE implementation-specific maximum value.

NOTE 4: The term "non-3GPP access" used in the counter for "the entry for the current SNPN considered invalid for non-3GPP access" events, is used to express access to SNPN services via a PLMN.

If the UE is registered for onboarding services in SNPN or performing initial registration for onboarding services in SNPN, the UE shall set the SNPN-specific attempt counter for the current SNPN to the UE implementation-specific maximum value; and

b) if the AUTHENTICATION REJECT message is received without integrity protection, the UE shall start timer T3247 with a random value uniformly drawn from the range between 30 minutes and 60 minutes, if the timer is not running (see subclause 5.3.20).

Additionally, if the UE is neither registered for onboarding services in SNPN nor performing initial registration for onboarding services in SNPN, the UE shall:

1) if the AUTHENTICATION REJECT message is received over 3GPP access, and the counter for "the entry for the current SNPN considered invalid for 3GPP access" events has a value less than a UE implementation-specific maximum value, proceed as specified in list item a) 1) of subclause 5.3.20.3 for the case that the 5GMM cause value received is #3;

2) if the AUTHENTICATION REJECT message is received over non-3GPP access, and the counter for "the entry for the current SNPN considered invalid for non-3GPP access" events has a value less than a UE implementation-specific maximum value, proceed as specified in list item a)-2) of subclause 5.3.20.3 for the case that the 5GMM cause value received is #3; or

3) otherwise:

i) if the AUTHENTICATION REJECT message is received over 3GPP access:

- the UE shall set the update status for 3GPP access to 5U3 ROAMING NOT ALLOWED, delete for 3GPP access only the stored 5G-GUTI, TAI list, last visited registered TAI and ngKSI;

In case of SNPN, if the UE does not support access to an SNPN using credentials from a credentials holder, the entry of the "list of subscriber data" with the SNPN identity of the current SNPN shall be considered invalid for 3GPP access until the UE is switched off or the entry is updated;

In case of SNPN, if the UE supports access to an SNPN using credentials from a credentials holder, the UE shall consider the selected entry of the "list of subscriber data" as invalid until the UE is switched off or the entry is updated; and

- the UE shall set the counter for "the entry for the current SNPN considered invalid for 3GPP access" events to UE implementation-specific maximum value; and

ii) if the AUTHENTICATION REJECT message is received over non-3GPP access:

- the UE shall set the update status for non-3GPP access to 5U3 ROAMING NOT ALLOWED, delete for non-3GPP access only the stored 5G-GUTI, TAI list, last visited registered TAI and ngKSI. The entry of the "list of subscriber data" with the SNPN identity of the current SNPN shall be considered invalid for non-3GPP access until the UE is switched off or the entry is updated; and

- the UE shall set the counter for "the entry for the current SNPN considered invalid for non-3GPP access" events to UE implementation-specific maximum value.

NOTE 5: The AUTHENTICATION REJECT message "received over non-3GPP access" in this subclause refers to an AUTHENTICATION REJECT message received via a PLMN when the UE attempts to access SNPN services via a PLMN.

If the UE is registered for onboarding services in SNPN or performing initial registration for onboarding services in SNPN, the UE shall:

1) if the SNPN-specific attempt counter for the SNPN sending the AUTHENTICATION REJECT message has a value less than a UE implementation-specific maximum value, increment the SNPN-specific attempt counter for the SNPN; or

2) otherwise, the UE shall set the update status to 5U3.ROAMING NOT ALLOWED, delete the stored 5G-GUTI, TAI list, last visited registered TAI, and ngKSI, store the SNPN identity in the "permanently forbidden SNPNs" list for onboarding services, enter state 5GMM-DEREGISTERED.PLMN-SEARCH, and perform an SNPN selection or an SNPN selection for onboarding services according to 3GPP TS 23.122 [5].

If the AUTHENTICATION REJECT message is received by the UE, the UE shall abort any 5GMM signalling procedure, stop any of the timers T3510, T3517, T3519 or T3521 (if they were running), enter state 5GMM-DEREGISTERED and delete any stored SUCI.

Upon receiving an EAP-success message, the ME shall:

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

b) if the ME has not generated a new KAUSF and a new KSEAF and has not created a partial native 5G NAS security context when handling the EAP-request message which resulted into generation of EMSK as described above:

1) if:

i) the default UE credentials for primary authentication, if the UE is registering or registered for onboarding services in SNPN; or

ii) credentials in the selected entry of the "list of configuration data", if the UE is not registering or registered for onboarding services in SNPN;

contain an indication to use MSK for derivation of KAUSF after success of primary authentication and key agreement procedure then generate a new KAUSF from the MSK otherwise generate a new KAUSF from the EMSK;

2) generate a new KSEAF from the new KAUSF, and the KAMF from the ABBA that was received with the EAP-success message, and the KSEAF as described in 3GPP TS 33.501 [24];

3) create a partial native 5G NAS security context identified by the ngKSI value in the volatile memory of the ME; and

4) store the KAMF in the created partial native 5G NAS security context; and

c) 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, 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.

The UE shall consider the procedure complete.

Upon receiving an EAP-failure message, the UE shall delete the partial native 5G NAS security context and shall delete the new KAUSF and the new KSEAF, if any were created when handling the EAP-request message which resulted into generation of EMSK or MSK as described above.

The UE shall consider the procedure complete.

\*\*\* Next change \*\*\*

5.4.1.2.3A.2 EAP-TTLS with two phases of authentication

The UE may support acting as EAP peer of EAP-TTLS with two phases of authentication as specified in 3GPP TS 33.501 [24] and acting as peer of a legacy authentication protocol as specified in 3GPP TS 33.501 [24]. The AUSF may support acting as EAP server of EAP-TTLS with two phases of authentication as specified in 3GPP TS 33.501 [24]. The AAA server of CH may support acting a server of a legacy authentication protocol as specified in 3GPP TS 33.501 [24].

When EAP-TTLS with two phases of authentication as specified in 3GPP TS 33.501 [24] is used for primary authentication and key agreement in an SNPN:

a) requirements in subclause 5.4.1.2.3A.1 shall apply in addition to requirements specified in 3GPP TS 33.501 [24] annex U.

b) indication to use MSK for derivation of KAUSF after success of primary authentication and key agreement procedure is not included in:

1) the default UE credentials for primary authentication, if the UE is registering or registered for onboarding services in SNPN; or

2) credentials in the selected entry of the "list of configuration data", if the UE is not registering or registered for onboarding services in SNPN.

c) the SUPI of the UE is in the form of a SUPI with the SUPI format "network specific identifier" containing a network-specific identifier.

NOTE: Support of EAP-TTLS with two phases of authentication is based on the informative requirements as specified in 3GPP TS 33.501 [24].

\*\*\* Next change \*\*\*

#### 6.3.1.1 General

The purpose of the PDU session authentication and authorization procedure is to enable the DN:

a) to authenticate the upper layers of the UE, when establishing the PDU session;

b) to authorize the upper layers of the UE, when establishing the PDU session;

c) both of the above; or

d) to re-authenticate the upper layers of the UE after establishment of the PDU session.

The PDU session authentication and authorization procedure can be performed only during or after the UE-requested PDU session procedure establishing a non-emergency PDU session. The PDU session authentication and authorization procedure shall not be performed during or after the UE-requested PDU session establishment procedure establishing an emergency PDU session.

The upper layers store the association between a DNN and corresponding credentials, if any, for the PDU session authentication and authorization.

If the UE is registered for onboarding services in SNPN the SMF may initiate the PDU session authentication and authorization procedure based on local policy with a DCS as specified in 3GPP TS 33.501 [24] clause I.9.2.4.1 or a DN‑AAA server as specified in 3GPP TS 33.501 [24] clause I.9.2.4.2.

If the UE is registered for onboarding services in SNPN and the network initiates the PDU session authentication and authorization procedure, the UE shall use default UE credentials for secondary authentication for the PDU session authentication and authorization procedure.

The network authenticates the UE using the Extensible Authentication Protocol (EAP) as specified in IETF RFC 3748 [34].

EAP has defined four types of EAP messages:

a) an EAP-request message;

b) an EAP-response message;

c) an EAP-success message; and

d) an EAP-failure message.

The EAP-request message is transported from the network to the UE using the PDU SESSION AUTHENTICATION COMMAND message of the PDU EAP message reliable transport procedure.

The EAP-response message to the EAP-request message is transported from the UE to the network using the PDU SESSION AUTHENTICATION COMPLETE message of the PDU EAP message reliable transport procedure.

If the PDU session authentication and authorization procedure is performed during the UE-requested PDU session establishment procedure:

a) and the DN authentication of the UE completes successfully, the EAP-success message is transported from the network to the UE as part of the UE-requested PDU session establishment procedure in the PDU SESSION ESTABLISHMENT ACCEPT message.

b) and the DN authentication of the UE completes unsuccessfully, the EAP-failure message is transported from the network to the UE as part of the UE-requested PDU session establishment procedure in the PDU SESSION ESTABLISHMENT REJECT message.

If the PDU session authentication and authorization procedure is performed after the UE-requested PDU session establishment procedure:

a) and the DN authentication of the UE completes successfully, the EAP-success message is transported from the network to the UE using the PDU SESSION AUTHENTICATION RESULT message of the PDU EAP result message transport procedure.

b) and the DN authentication of the UE completes unsuccessfully, the EAP-failure message is transported from the network to the UE using the PDU SESSION RELEASE COMMAND message of the network-requested PDU session release procedure.

There can be several rounds of exchange of an EAP-request message and a related EAP-response message for the DN to complete the authentication and authorization of the request for a PDU session (see example in figure 6.3.1.1).

The SMF shall set the authenticator retransmission timer specified in IETF RFC 3748 [34] subclause 4.3 to infinite value.

NOTE: The PDU session authentication and authorization procedure provides a reliable transport of EAP messages and therefore retransmissions at the EAP layer of the SMF do not occur.



Figure 6.3.1.1: PDU session authentication and authorization procedure

\*\*\* End of changes \*\*\*