**3GPP TSG-CT WG1 Meeting #131-eC1-21xxxx**

**E-meeting, 19-27 August 2021**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **24.501** | **CR** | **3507** | **rev** | **1** | **Current version:** | **17.3.1** |  |
|  |
| *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 |  |

|  |
| --- |
|  |
| ***Title:***  | Handling of AUTHENTICATION REJECT message in ON-SNPN |
|  |  |
| ***Source to WG:*** |  |
| ***Source to TSG:*** | C1 |
|  |  |
| ***Work item code:*** | eNPN |  | ***Date:*** | 2021-08-25 |
|  |  |  |  |  |
| ***Category:*** | **F** |  | ***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 canbe found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | *Use one of the following releases:Rel-8 (Release 8)Rel-9 (Release 9)Rel-10 (Release 10)Rel-11 (Release 11)...Rel-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)* |
|  |  |
| ***Reason for change:*** | In an ON-SNPN, a UE can receive an AUTHENTICATION REJECT message. How the UE handles the message needs to be clarified. |
|  |  |
| ***Summary of change:*** | The UE update the "list of forbidden ON-SNPNs". |
|  |  |
| ***Consequences if not approved:*** | The UE behavior upon receiving the AUTHENTICATION REJECT message in an ON-SNPN remains unclear. |
|  |  |
| ***Clauses affected:*** | 3.1, 3.2, 5.4.1.2.3.1, 5.4.1.2.3A.1 |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  | **X** |  Other core specifications  | TS/TR ... CR ...  |
| ***affected:*** |  | **X** |  Test specifications | TS/TR ... CR ...  |
| ***(show related CRs)*** |  | **X** |  O&M Specifications | TS/TR ... CR ...  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR's revision history:*** |  |

## 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.

**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.

**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 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.

**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;

h1) rejected NSSAI for the maximum number of UEs reached; 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; and

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

**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 derived by a UE in SNPN access mode, from default UE credentials 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 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.

**UE-DS-TT residence time:** The time taken within the UE and DS-TT to forward a packet between the UE and the DS-TT port.

**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 [2] apply:

**Non-public network**

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**

**Default UE credentials**

**IAB-node**

**Local area data network**

**Multi-USIM UE**

**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**

**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**

**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**

**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**

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)**

**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**

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

## 3.2 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

4G-GUTI 4G-Globally Unique Temporary Identifier

5GCN 5G Core Network

5G-GUTI 5G-Globally Unique Temporary Identifier

5GMM 5GS Mobility Management

5G-RG 5G Residential Gateway

5G-BRG 5G Broadband Residential Gateway

5G-CRG 5G Cable Residential Gateway

5GS 5G System

5GSM 5GS Session Management

5G-S-TMSI 5G S-Temporary Mobile Subscription Identifier

5G-TMSI 5G Temporary Mobile Subscription Identifier

5QI 5G QoS Identifier

ACS Auto-Configuration Server

AKA Authentication and Key Agreement

AKMA Authentication and Key Management for Applications

A-KID AKMA Key Identifier

A-TID AKMA Temporary Identifier

AMBR Aggregate Maximum Bit Rate

AMF Access and Mobility Management Function

APN Access Point Name

ATSSS Access Traffic Steering, Switching and Splitting

AUSF Authentication Server Function

CAG Closed access group

CHAP Challenge Handshake Authentication Protocol

DDX Downlink Data Expected

DL Downlink

DN Data Network

DNN Data Network Name

DNS Domain Name System

eDRX Extended DRX cycle

DS-TT Device-Side TSN Translator

EUI Extended Unique Identifier

E-UTRAN Evolved Universal Terrestrial Radio Access Network

EAC Early Admission Control

EAP-AKA' Improved Extensible Authentication Protocol method for 3rd generation Authentication and Key Agreement

EAS Edge Application Server

EASDF Edge Application Server Discovery Function

ECIES Elliptic Curve Integrated Encryption Scheme

ECS Edge Configuration Server

EEC Edge Enabler Client

EPD Extended Protocol Discriminator

EMM EPS Mobility Management

EPC Evolved Packet Core Network

EPS Evolved Packet System

ESM EPS Session Management

FN-RG Fixed Network RG

FN-BRG Fixed Network Broadband RG

FN-CRG Fixed Network Cable RG

Gbps Gigabits per second

GFBR Guaranteed Flow Bit Rate

GUAMI Globally Unique AMF Identifier

IAB Integrated access and backhaul

IMEI International Mobile station Equipment Identity

IMEISV International Mobile station Equipment Identity and Software Version number

IMSI International Mobile Subscriber Identity

IP-CAN IP-Connectivity Access Network

KSI Key Set Identifier

LADN Local Area Data Network

LCS LoCation Services

LMF Location Management Function

LPP LTE Positioning Protocol

MAC Message Authentication Code

MA PDU Multi-Access PDU

Mbps Megabits per second

MFBR Maximum Flow Bit Rate

MICO Mobile Initiated Connection Only

MUSIM Multi-USIM

N3IWF Non-3GPP Inter-Working Function

N5CW Non-5G-Capable over WLAN

N5GC Non-5G Capable

NAI Network Access Identifier

NITZ Network Identity and Time Zone

NR New Radio

ngKSI Key Set Identifier for Next Generation Radio Access Network

NPN Non-public network

NSAC Network Slice Admission Control

NSACF Network Slice Admission Control FunctionNSSAA Network slice-specific authentication and authorization

NSSAAF NSSAA Function

NSSAI Network Slice Selection Assistance Information

ON-SNPN Onboarding Standalone Non-Public Network

OS Operating System

OS Id OS Identity

PAP Password Authentication Protocol

PCO Protocol Configuration Option

PEI Permanent Equipment Identifier

PNI-NPN Public Network Integrated Non-Public Network

ProSe Proximity based Services

ProSeP 5G ProSe policy

PTI Procedure Transaction Identity

PVS Provisioning Server

QFI QoS Flow Identifier

QoS Quality of Service

QRI QoS Rule Identifier

RACS Radio Capability Signalling Optimisation

(R)AN (Radio) Access Network

RFSP RAT Frequency Selection Priority

RG Residential Gateway

RPLMN Registered PLMN

RQA Reflective QoS Attribute

RQI Reflective QoS Indication

RSNPN Registered SNPN

S-NSSAI Single NSSAI

SA Security Association

SDF Service Data Flow

SMF Session Management Function

SGC Service Gap Control

SNN Serving Network Name

SNPN Stand-alone Non-Public Network

SOR Steering of Roaming

SOR-CMCI Steering of Roaming Connected Mode Control Information

SUCI Subscription Concealed Identifier

SUPI Subscription Permanent Identifier

TA Tracking Area

TAC Tracking Area Code

TAI Tracking Area Identity

Tbps Terabits per second

TNGF Trusted Non-3GPP Gateway Function

TSC Time Sensitive Communication

TWIF Trusted WLAN Interworking Function

TSN Time-Sensitive Networking

UAS Uncrewed Aerial System

UAV Uncrewed Aerial Vehicle

UDM Unified Data Management

UL Uplink

UPDS UE policy delivery service

UPF User Plane Function

UPSC UE Policy Section Code

UPSI UE Policy Section Identifier

URN Uniform Resource Name

URSP UE Route Selection Policy

USS UAS Service Supplier

UUAA USS UAV Authorization/Authentication

V2X Vehicle-to-Everything

V2XP V2X policy

W-AGF Wireline Access Gateway Function

WLAN Wireless Local Area Network

WUS Wake-up signal

\*\*\*\*\* 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 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, the ME and the AUSF shall generate EMSKas described in 3GPP TS 33.501 [24].

When handling of an EAP-request message results into generation of EMSK, the ME may generate a new KAUSF from the EMSK, 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 0: 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 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 1: 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.

 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 "list of forbidden ON-SNPNs";

Editor's note: Detailed handling of the "list of forbidden ON-SNPNs" is FFS.

Editor's note: It is FFS how the UE operates after storing the SNPN identity in the "list of forbidden ON-SNPNs".

2) 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 2: 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; 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

Editor's note: Handling of a non-integrity protected AUTHENTICATION REJECT message by a UE which is registered for onboarding services in SNPN or is performing initial registration for onboarding services in SNPN is FFS.

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, 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 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) generate a new KAUSF from the EMSK, 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];

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

3) 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 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 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].

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, the ME and the AUSF shall generate EMSK as described in 3GPP TS 33.501 [24].

When handling of an EAP-request message results into generation of EMSK, the ME may generate a new KAUSF from the EMSK, 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 0: 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 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 1: 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 "list of forbidden ON-SNPNs"; and

Editor's note: Detailed handling of the "list of forbidden ON-SNPNs" is FFS.

Editor's note: It is FFS how the UE operates after storing the SNPN identity in the "list of forbidden ON-SNPNs".

2) 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; and

NOTE 2: 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.

Editor's note: Handling of a non-integrity protected AUTHENTICATION REJECT message by a UE which is registered for onboarding services in SNPN or is performing initial registration for onboarding services in SNPN is FFS.

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, 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 3: 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 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) generate a new KAUSF from the EMSK, 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];

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

3) 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 as described above.

The UE shall consider the procedure complete.