**3GPP TSG-SA WG2 Meeting #152E (e-meeting)S2-220xxxx**

**17-26 August 2022, Electronic Meeting (revision of S2-22xxxxx)**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **23.502** | **CR** | **DraftCR** | **rev** | **-** | **Current version:** | **17.5.0** |  |
|  |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* |
|  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME | **x** | Radio Access Network |  | Core Network | **x** |

|  |
| --- |
|  |
| ***Title:***  | Untrusted and trusted Non 3GPP Satellite access to 5GC |
|  |  |
| ***Source to WG:*** | Xiaomi |
| ***Source to TSG:*** | SA2 |
|  |  |
| ***Work item code:*** | TEI18\_5GN3SAT |  | ***Date:*** | 2022-08-XX |
|  |  |  |  |  |
| ***Category:*** | **B** |  | ***Release:*** | Rel-18 |
|  | *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 the existing 3GPP defined satellite access in 5GS (before Rel-18), the UE shall support NR(Satellite) to access 3GPP network via satellite, and the satellite NG-RAN is a NG-RAN which uses NR(Satellite) in providing satellite access to UEs.There is a service requirement in Stage1 TS22.261(v18.6.1) ‘Service requirements for the 5G system’:*“A 5G system with satellite access shall support different configurations where the radio access network is either a satellite NG-RAN or a non-3GPP satellite access network, or both.”*How to support satellite access as non-3GPP access network in 5GS needs to be specified in Rel-18 according to the Rel-18 stage1 service requirement. |
|  |  |
| ***Summary of change:*** | §4.12.2.2, 4.12a.2.2- Add RAT Type of untrusted/trusted non-3GPP access with the example of satellite into the registration procedures of untrusted/trusted non-3GPP access to 5GC. |
|  |  |
| ***Consequences if not approved:*** | The stage-1 requirement is not realized in stage-2. |
|  |  |
| ***Clauses affected:*** | 4.12.2.2, 4.12a.2.2 |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  | **x** |  Other core specifications  | TS/TR ... CR ... |
| ***affected:*** |  | **x** |  Test specifications | TS/TR ... CR ...  |
| ***(show related CRs)*** |  | **x** |  O&M Specifications | TS/TR ... CR ...  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR's revision history:*** |  |

\* \* \* \* Start of 1st Change \* \* \* \*

#### 4.12.2.2 Registration procedure for untrusted non-3GPP access

The signalling flow in Figure 4.12.2.2-1 does not show all the details of a registration procedure via untrusted non-3GPP access. It shows primarily the steps executed between the UE and N3IWF. All the details of a registration procedure, including interactions with PCF, UDM, etc. are specified in clause 4.2.2.2.2.



Figure 4.12.2.2-1: Registration via untrusted non-3GPP access

1. The UE connects to an untrusted non-3GPP Access Network with any appropriate authentication procedure and it is assigned an IP address. For example, a non-3GPP authentication method can be used, e.g. no authentication (in the case of a free WLAN), EAP with pre-shared key, username/password, etc. When the UE decides to attach to 5GC network, the UE selects an N3IWF in a 5G PLMN, as described in clause 6.3.6 of TS 23.501 [2].

2. The UE proceeds with the establishment of an IPsec Security Association (SA) with the selected N3IWF by initiating an IKE initial exchange according to RFC 7296 [3]. After step 2, all subsequent IKE messages are encrypted and integrity protected by using the IKE SA established in this step.

3. The UE shall initiate an IKE\_AUTH exchange by sending an IKE\_AUTH request message. The AUTH payload is not included in the IKE\_AUTH request message, which indicates that the IKE\_AUTH exchange shall use EAP signalling (in this case EAP-5G signalling). If the UE supports MOBIKE, it shall include a Notify payload in the IKE\_AUTH request, as specified in RFC 4555 [40], indicating that MOBIKE is supported. In addition, as specified in TS 33.501 [15], if the UE is provisioned with the N3IWF root certificate, it shall include the CERTREQ payload within the IKE\_AUTH request message to request the N3IWF's certificate.

4. The N3IWF responds with an IKE\_AUTH response message, which includes an EAP-Request/5G-Start packet. The EAP-Request/5G-Start packet informs the UE to initiate an EAP-5G session, i.e. to start sending NAS messages encapsulated within EAP-5G packets. If the N3IWF has received a CERTREQ payload from the UE, the N3IWF shall include the CERT payload in the IKE\_AUTH response message containing the N3IWF's certificate. How the UE uses the N3IWF's certificate is specified in TS 33.501 [15].

5. The UE shall send an IKE\_AUTH request, which includes an EAP-Response/5G-NAS packet that contains the Access Network parameters (AN parameters) and a Registration Request message. The AN parameters contain information that is used by the N3IWF for selecting an AMF in the 5G core network. This information includes e.g. the GUAMI, the Selected PLMN ID (or PLMN ID and NID, see clause 5.30 of TS 23.501 [2]), the Requested NSSAI and the Establishment cause. The Establishment cause provides the reason for requesting a signalling connection with 5GC. Whether and how the UE includes the Requested NSSAI as part of the AN parameters is dependent on the value of the Access Stratum Connection Establishment NSSAI Inclusion Mode parameter, as specified in clause 5.15.9 of TS 23.501 [2].

NOTE 1: The N3IWF does not send an EAP-Identity request because the UE includes its identity in the first IKE\_AUTH. This is in line with RFC 7296 [3] clause 3.16.

6. The N3IWF shall select an AMF based on the received AN parameters and local policy, as specified in clause 6.3.5 of TS 23.501 [2]. The N3IWF shall then forward the Registration Request received from the UE to the selected AMF within an N2 message. This message contains N2 parameters that include the Selected PLMN ID, RAT type of the untrusted non-3GPP Access (e.g. Untrusted Non-3GPP Satellite if available) and the Establishment cause.

7. The selected AMF may decide to request the SUCI by sending a NAS Identity Request message to UE. This NAS message and all subsequent NAS messages are sent to UE encapsulated within EAP/5G-NAS packets.

8. The AMF may decide to authenticate the UE by invoking an AUSF. In this case, the AMF shall select an AUSF as specified in clause 6.3.4 of TS 23.501 [2] based on SUPI or SUCI.

 The AUSF executes the authentication of the UE as specified in TS 33.501 [15]. The AUSF selects a UDM as described in clause 6.3.8 of TS 23.501 [2] and gets the authentication data from UDM. The authentication packets are encapsulated within NAS authentication messages and the NAS authentication messages are encapsulated within EAP/5G-NAS packets. After the successful authentication:

- In step 8h, the AUSF shall send the anchor key (SEAF key) to AMF which is used by AMF to derive NAS security keys and a security key for N3IWF (N3IWF key). The UE also derives the anchor key (SEAF key) and from that key it derives the NAS security keys and the security key for N3IWF (N3IWF key). The N3IWF key is used by the UE and N3IWF for establishing the IPsec Security Association (in step 11).

- In step 8h, the AUSF shall also include the SUPI, if in step 8a the AMF provided to AUSF a SUCI.

NOTE 2: EAP-AKA' or 5G-AKA are allowed for the authentication of UE via non-3GPP access, as specified in TS 33.501 [15]. Figure 4.12.2.2-1 only shows authentication flow using EAP-AKA'. Authentication methods other than EAP-AKA' or 5G-AKA are also allowed for UE accessing SNPN services via a PLMN, as specified in TS 33.501 [15], Annex I.

9a. The AMF shall send a NAS Security Mode Command to UE in order to activate NAS security. If an EAP-AKA' authentication was successfully executed in step 8, the AMF shall encapsulate the EAP-Success received from AUSF within the NAS Security Mode Command message.

9b. The N3IWF shall forward the NAS Security Mode Command message to UE within an EAP/5G-NAS packet.

9c. The UE completes the EAP-AKA' authentication (if initiated in step 8), creates a NAS security context and an N3IWF key and sends the NAS Security Mode Complete message within an EAP/5G-NAS packet.

9d. The N3IWF relays the NAS Security Mode Complete message to the AMF.

10a. Upon receiving NAS Security Mode Complete, the AMF shall send an NGAP Initial Context Setup Request message that includes the N3IWF key.

10b. This triggers the N3IWF to send an EAP-Success to UE, which completes the EAP-5G session. No further EAP-5G packets are exchanged.

11. The IPsec SA is established between the UE and N3IWF by using the common N3IWF key that was created in the UE in step 9c and received by the N3IWF in step 10a. This IPsec SA is referred to as the "signalling IPsec SA". After the establishment of the signalling IPsec SA, the N3IWF notifies the AMF that the UE context (including AN security) was created by sending a NGAP Initial Context Setup Response. The signalling IPsec SA shall be configured to operate in tunnel mode and the N3IWF shall assign to UE an "inner" IP address. If the N3IWF has received an indication that the UE supports MOBIKE (see step 3), then the N3IWF shall include a Notify payload in the IKE\_AUTH response message sent in step 11a, indicating that MOBIKE shall be supported, as specified in RFC 4555 [40].

 All subsequent NAS messages exchanged between the UE and N3IWF shall be sent via the signalling IPsec SA and shall be carried over TCP/IP. The UE shall send NAS messages within TCP/IP packets with source address the "inner" IP address of the UE and destination address the NAS\_IP\_ADDRESS that is received in step 11a. The N3IWF shall send NAS messages within TCP/IP packets with source address the NAS\_IP\_ADDRESS and destination address the "inner" IP address of the UE. The TCP connection used for reliable NAS transport between the UE and N3IWF shall be initiated by the UE right after the signalling IPsec SA is established in step 11a. The UE shall send the TCP connection request to the NAS\_IP\_ADDRESS and to the TCP port number specified in TS 24.502 [41].

12. The AMF sends the NAS Registration Accept message to the N3IWF. The N2 Message includes the Allowed NSSAI for the access type for the UE.

13. The N3IWF forwards the NAS Registration Accept message to UE via the established signalling IPsec SA. If the NAS Registration Accept message is received by the N3IWF before the IPsec SA is established, the N3IWF shall store it and forward it to the UE only after the establishment of the signalling IPsec SA.

 The AMF provides the Access Type set to "Non-3GPP access" and RAT Type received in Step 6 to the UDM when it registers with the UDM.

NOTE 3: The Access Type is set to "Non-3GPP access" even when the UE accesses SNPN services via PLMN over 3GPP access.

\* \* \* \* Start of 2nd Change \* \* \* \*

#### 4.12a.2.2 Registration procedure for trusted non-3GPP access

The UE connects to a trusted non-3GPP Access Network (TNAN) and it also registers to 5GC over via this TNAN, by using the EAP-based procedure shown in the figure 4.12a.2.2. This procedure is very similar with the 5GC registration procedure over untrusted non-3GPP access in clause 4.12.2.2. The link between the UE and the TNAN can be any data link (L2) that supports EAP encapsulation, e.g. PPP, PANA, Ethernet, IEEE 802.3, IEEE 802.11, etc. The interface between the TNAP and TNGF is an AAA interface.



Figure 4.12a.2.2-1: Registration via trusted non-3GPP access

0. The UE selects a PLMN and a TNAN for connecting to this PLMN by using the Trusted Non-3GPP Access Network selection procedure specified in clause 6.3.12 of TS 23.501 [2]. During this procedure, the UE discovers the PLMNs with which the TNAN supports trusted connectivity (e.g. "5G connectivity").

NOTE 1: In this Release, it is assumed that when the trusted non-3GPP access is a trusted WLAN access, the UE is configured (e.g. with the WLANSP rules defined in TS 23.503 [20]) to select an SSID associated with a non-3GPP Tracking Area, which supports one or more of the UE's subscribed S-NSSAIs.

1. A layer-2 connection is established between the UE and the TNAP. In the case of IEEE Std 802.11 [48], this step corresponds to an 802.11 Association. In the case of PPP, this step corresponds to a PPP LCP negotiation. In other types of non-3GPP access (e.g. Ethernet), this step may not be required.

2-3. An EAP procedure is initiated. EAP messages are encapsulated into layer-2 packets, e.g. into IEEE 802.3/802.1x packets, into IEEE 802.11/802.1x packets, into PPP packets, etc. The NAI provided by the UE indicates that the UE requests "5G connectivity" to a specific PLMN, e.g. NAI = "<any\_username>@nai.5gc. mnc<MNC>.mcc<MCC>.3gppnetwork.org". This NAI triggers the TNAP to send an AAA request to a TNGF, which operates as an AAA proxy. Between the TNAP and TNGF the EAP packets are encapsulated into AAA messages. The AAA request also include the TNAP identifier, which can be treated as the User Location Information.

NOTE 2: In this Release, it is assumed that when the trusted non-3GPP access is a trusted WLAN access, the TNAP selects a TNGF based on the realm provided by the UE and also based on the SSID selected by the UE. All TNGFs associated with the SSID selected by the UE support the same non-3GPP tracking area.

4-10. An EAP-5G procedure is executed as the one specified in clause 4.12.2.2 for the untrusted non-3GPP access with the following modifications:

- A TNGF key (instead of an N3IWF key) is created in the UE and in the AMF after the successful authentication. The TNGF key is transferred from the AMF to TNGF in step 10a (within the N2 Initial Context Setup Request). The TNGF derives a TNAP key, which is provided to the TNAP. The TNAP key depends on the non-3GPP access technology (e.g. it is a Pairwise Master Key in the case of IEEE Std 802.11 [48]). How these security keys are created, it is specified in TS 33.501 [15].

- In step 5 the UE shall include the Requested NSSAI in the AN parameters only if allowed, according to the conditions defined in clause 5.15.9 of TS 23.501 [2], for the trusted non-3GPP access. The UE shall also include a UE Id in the AN parameters, e.g. a 5G-GUTI if available from a prior registration to the same PLMN.

- In the N2 message sent in step 6b, the TNGF includes a UE Location Information (ULI) that contains a "null" IP address (e.g. 0.0.0.0) because the UE is not yet assigned an IP address. After the UE is assigned an IP address, the TNGF includes this address in subsequent N2 messages. The TNGF sends the RAT type (e.g. Trusted Non-3GPP Satellite if available) to the AMF in the N2 message in step 6b.

- After receiving the TNGF key from AMF in step 10a, the TNGF shall send to UE an EAP-Request/5G-Notification packet containing the "TNGF Contact Info", which includes the IP address of TNGF. After receiving an EAP-Response/5G-Notification packet from the UE in step 10c, the TNGF shall send message 10d containing the EAP-Success packet.

11. The TNAP key is used to establish layer-2 security between the UE and TNAP. In the case of IEEE Std 802.11 [48], a 4-way handshake is executed, which establishes a security context between the WLAN AP and the UE that is used to protect unicast and multicast traffic over the air.

12. The UE receives IP configuration from the TNAN, e.g. with DHCP.

13. At this point, the UE has successfully connected to the TNAN and has obtained IP configuration. The UE sets up a secure NWt connection with the TNGF as follows:

 The UE initiates an IKE\_INIT exchange using the IP address of TNGF received during the EAP-5G signalling, in step 10b. Subsequently, the UE initiates an IKE\_AUTH exchange and provides its identity. The identity provided by the UE in the IKEv2 signalling should be the same as the UE Id included in the AN parameters in step 5. This enables the TNGF to locate the TNGF key that was created before for this UE, during the authentication in step 8. The TNGF key is used for mutual authentication. NULL encryption is negotiated between the UE and the TNGF, as specified in RFC 2410 [49].

 In step 13c, the TNGF provides to UE (a) an "inner" IP address, (b) a NAS\_IP\_ADDRESS and a TCP port number and (c) a DSCP value. After this step, an IPsec SA is established between the UE and TNGF. This is referred to as the "signalling IPsec SA" and operates in Tunnel mode. Operation in Tunnel mode enables the use of MOBIKE [40] for re-establishing the IPsec SAs when the IP address of the UE changes during mobility events. All IP packets exchanged between the UE and TNGF via the "signalling IPsec SA" shall be marked with the above DSCP value. The UE and the TNAP may map the DSCP value to a QoS level (e.g. to an EDCA Access Class [48]) supported by the underlying non-3GPP Access Network. The mapping of a DSCP value to a QoS level of the non-3GPP Access Network is outside the scope of 3GPP.

 Right after the establishment of the "signalling IPsec SA", the UE shall setup a TCP connection with the TNGF by using the NAS\_IP\_ADDRESS and the TCP port number received in step 13c. The UE shall send NAS messages within TCP/IP packets with source address the "inner" IP address of the UE and destination address the NAS\_IP\_ADDRESS. The TNGF shall send NAS messages within TCP/IP packets with source address the NAS\_IP\_ADDRESS and destination address the "inner" IP address of the UE.

 This concludes the setup of the NWt connection between the UE and the TNGF. All subsequent NAS messages between UE and TNGF are carried over this NWt connection (i.e. encapsulated in TCP/IP/ESP).

14. After the NWt connection is successfully established, the TNGF responds to AMF with an N2 Initial Context Setup Response message.

15. Finally, the NAS Registration Accept message is sent by the AMF and is forwarded to UE via the established NWt connection. Now the UE can use the TNAN (a) to transfer non-seamless offload traffic and (b) to establish one or more PDU Sessions.

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