**SA WG2 Meeting #163 S2-2406890**

**27 - 31 May, 2024, Jeju, South Korea (revision of S2-2406244)**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **23.502** | **CR** | **4817** | **rev** | **1** | **Current version:** | **18.5.0** |  |
|  | | | | | | | | |
| *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:*** | Correction about the UE indication of the support of slice based N3IWF/TNGF selection | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Nokia, LG Electronics, Samsung | | | | | | | | | |
| ***Source to TSG:*** | S2 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | 5WWC\_Ph2 | | | | |  | ***Date:*** | | | 2024-05-04 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **F** |  | | | | | ***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 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:*** | | CT1 LS C1-242934 = S2-2405859 that states  TS 23.502 states the following in clause 4.12.2.2:  *Then the AMF triggers the UE PCF to update the UE policies for slice specific N3IWF selection by either indicating the request in Npcf\_UEPolicyControl\_Create or, if a UE policy already exists, by issuing a Npcf\_UEPolicyControl\_Update. (…)*  *NOTE 8: The UE is assumed to inform PCF whether the UE supports Extended Home N3IWF identifier configuration and Slice-specific N3IWF prefix configuration as part of the UE policy update procedure. Details will be specified in Stage 3 specifications.*  Also TS 23.502 states the following in clause 4.12a.2.2:  *Then the AMF triggers the UE PCF to update the UE policies for slice specific trusted access selection by either indicating the request in Npcf\_UEPolicyControl\_Create or, if a UE policy already exists, by issuing a Npcf\_UEPolicyControl\_Update. (…).*  *NOTE 6: The UE is assumed to inform PCF whether the UE supports Extended WLANSP or ANDSP as part of the UE policy update procedure. Details will be specified by CT WG1.*  CT1 […] has the following observations:  As per the current stage 2 requirements, the UE already indicates to the AMF whether it supports the slice-based N3IWF selection and/or the slice-based TNGF selection within the REGISTRATION REQUEST message during the registration procedure, which is in line with the legacy approach.  This uses e.g. Slice-based N3IWFselection support (SBNS) and Slice-based TNGF selection support (SBTS) in 5GMM capability defined in 24.501 § 9.11.3.1    However, as per the above stage 2 NOTEs, the UE also provides separate indications to the PCF about supporting those features. CT1 does not see the reason to step away from the legacy approach in which the AMF indicates to the PCF whether the UE supports slice-based N3IWF selection and/or the slice-based TNGF selection as this is aligned the protocol design defined from Rel-15. CT1 therefore asks SA2 to consider re-using the existing approach. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Removal of NOTE 8 in clause 4.12a.2.2 and of NOTE 6 in in clause 4.12a.2.2.  Clarify that UE report capability on slice-based N3IWF/TNGF selection regarldess of access type the UE registers and the AMF notifies the capability to the PCF if the AMF received the capability indication from the UE. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | SA2 spec is not aligned with CT1 spec.  Unclear how the PCF knows capability of UE on slice-based N3IWF/TNGF selection | | | | | | | | |
|  | |  | | | | | | | | |  |  |  |  |
| ***Clauses affected:*** | | 4.12.2.2 ; 4.12a.2.2 ; 4.16.11.1 .; 4.16.12.1.1 ; 5.2.5.6.2 ; 5.2.5.6.5 | | | | | | | | |  |  |  | Slice-based N3IWF selection not supported |
|  | |  | | | | | | | | |  |  |  | Slice-based N3IWF selection supported |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | |  | **x** | Other core specifications | | | |  | | |
| ***affected:*** | |  | **x** | Test specifications | | | |  | | |
| ***(show related CRs)*** | |  | **x** | O&M Specifications | | | |  | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | | figures | | | | | | | | |

*FIRST 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 not operating in SNPN access mode for NWu interface selects an N3IWF in a 5G PLMN, as described in clause 6.3.6 of TS 23.501 [2]. When the UE decides to attach to 5GC network, the UE operating in SNPN access mode for NWu interface selects an N3IWF in an SNPN, as described in clause 6.3.6.2a of TS 23.501 [2].

NOTE 1: The UE Selection of a N3IWF that supports the S-NSSAIs needed by the UE is enabled based on ANDSP configuration defined in TS 23.501 [2]. The N3IWF selection based on this information is documented in 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. In the case of WLAN access, if the UE has an MPS subscription, the UE shall include a Notify payload in the IKE\_AUTH request indicating its MPS subscription.

NOTE 2: Based on operator policy, the N3IWF can use the MPS subscription indication at this time to handle this UE with priority.

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 and the N3IWF may use the Establishment cause to determine the DSCP value on N2.. 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]. The registration request may contain an indication that the UE supports N3IWF selection based on the slices the UE wishes to use over untrusted non-3GPP access (i.e. that the UE supports Extended Home N3IWF identifier configuration and Slice-specific N3IWF prefix configuration). If at step 1 the UE selects the N3IWF based on Tracking/Location Area of same PLMN as described in clause 6.3.6 of TS 23.501 [2], the UE may include this TA in the last visited TAI in registration request in order to help the AMF to determine the target N3IWF as described in step 17. If the UE in SNPN access mode for NWu interface performs the Registration procedure for UE onboarding, the UE shall include an indication in the AN parameters that the connection request is for onboarding. The Registration Type "SNPN Onboarding" indicates that the UE wants to perform SNPN Onboarding Registration.

NOTE 3: 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 and optionally the Selected NID and the Establishment cause.

NOTE 4: The Selected NID is present when the UE connects to an SNPN via Untrusted non-3GPP access.

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. The AMF may use the Establishment cause to determine the Message Priority header and then the DSCP value for subsequent signalling according to TS 29.500 [17].

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 5: 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, as well as for UE accessing SNPN services directly via Untrusted non-3GPP access.

If the UE in SNPN access mode for NWu interface performs the Registration procedure for UE onboarding, the interaction between AMF and AUSF (step 8a, 8b, 8g and 8h in Figure 4.12.2.2-1) is replaced with step 9-1 or step 9-2 or step 9-3 in Figure 4.2.2.2.4-1, depending on the 5GC architecture that is used for UE onboarding.

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:

a) an "inner" IP address; and

b) a NAS\_IP\_ADDRESS and a TCP port number.

The N3IWF may apply a DSCP value to this signalling IPsec SA, in which case all IP packets exchanged between the UE and N3IWF via the "signalling IPsec SA" shall be marked with this DSCP value. 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].

NOTE 6: The DSCP value is determined by operator policy, and may e.g., be based on the DSCP value on N2.

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 determines the allowed subset of the Requested NSSAI that is allowed by the Subscribed S-NSSAI(s); the AMF may detect that the N3IWF used by the UE is not compatible with this allowed subset and based on operator's policy configured in the AMF, the AMF determines whether a different N3IWF should be used. If the UE supports slice-based N3IWF selection and the AMF determines to use a different N3IWF, then the AMF proceeds with steps 15-19. Otherwise, i.e. if the AMF determines to use the selected N3IWF that supports part of the allowed subset, the AMF proceeds with steps 13 and 14. In this case, steps 15-19 are skipped.

NOTE 7: The AMF considers the subscribed S-NSSAI(s) before determining to trigger the UE PCF to avoid triggering the UE PCF to update the UE policies for Requested S-NSSAIs that the UE is not subscribed for.

13. The AMF sends the NAS Registration Accept message in an N2 message sent to the N3IWF. The N2 Message includes the Allowed NSSAI for the access type for the UE. The Allowed NSSAI is a subset of the slices supported by the selected N3IWF.

14. 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.

14b. If the UE Registration Request contains an indication that the UE supports N3IWF selection based on the slices the UE wishes to use over untrusted non-3GPP access and the AMF is able to select a UE PCF that supports UE policies for slice specific N3IWF selection, the AMF may trigger UE policy association establishment if a suitable UE policy association does not exist yet. The AMF indicates to the PCF that the UE supports N3IWF selection based on the slices the UE wishes to use over untrusted non-3GPP access.

Steps 15 to 19 correspond to the case where the AMF has detected that the N3IWF used by the UE is not compatible with the subset of the requested NSSAI that is allowed by the subscribed S-NSSAI(s).

15. If the UE Registration Request contains an indication that the UE supports N3IWF selection based on the slices the UE wishes to use over untrusted non-3GPP access and the AMF is able to select a UE PCF that supports UE policies for slice specific N3IWF selection, the AMF may trigger UE policy association establishment if a suitable UE policy association does not exist yet. The AMF indicates to the PCF that the UE supports N3IWF selection based on the slices the UE wishes to use over untrusted non-3GPP access.

The AMF triggers the UE PCF to update the UE policies for slice specific N3IWF selection e.

The AMF requests the PCF to receive a notification when the PCF has completed the update of these UE policies.

NOTE 8: Void.

16. The PCF updates the UE policies for slice specific N3IWF selection per the procedure defined in figure 4.2.4.3-1. When the update of these UE policies is completed, the PCF notifies the AMF by invoking Npcf\_UEPolicyControl\_UpdateNotify.

17. The AMF sends via the N3IWF a UE Registration Reject indicating that the UE selected N3IWF was not appropriate for the requested slices that the UE is allowed to access to. The AMF optionally may provide target N3IWF information (FQDN and/or IP address) to the UE within the Registration Reject message.

NOTE 9: The AMF uses locally configured N3IWF information to provide target N3IWF information.

NOTE 10: The AMF may determine a target N3IWF that supports the subset of the requested NSSAI that is allowed by the subscribed S-NSSAI(s) based on the list of supported Tas and the corresponding list of supported slices for each TA obtained in N2 interface management procedures as specified in TS 38.413 [10]. To determine the target N3IWF, the AMF may take into account UE location corresponding to last visited TAI included in Registration Request as described at step 5 when the UE selects N3IWF based on Tracking/Location Area of same PLMN.

18. If supported by the UE and if the UE received target N3IWF information in step 17, the UE connects to the target N3IWF, otherwise the UE may perform N3IWF selection again using the updated N3IWF selection information received in step 16. The UE uses the target N3IWF information in the Registration Reject only for the N3IWF selection directly following the rejected registration and UE shall not store for future use.

The AMF provides the Access Type set to “Non-3GPP access” to the UDM when it registers with the UDM and the RAT type determined as specified in clause 5.3.2.3 of TS 23.501 [2].

NOTE 11: The Access Type and the RAT type are is set to “Untrusted Non-3GPP access” even when the UE accesses SNPN services via PLMN over 3GPP access.

*NEXT CHANGE (2)*

#### 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 which is not operating in SNPN access mode for Yt interface 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”).

The UE operating in SNPN access mode for Yt interface selects an SNPN and a TNAN for connecting to this SNPN by using the Trusted Non-3GPP Access Network selection procedure specified in clause 5.30.2.13 of TS 23.501 [2]. During this procedure, the UE discovers the SNPNs 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 TNAN(SSID and TNGF) 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 not operating in SNPN access mode for Yt interface indicates that the UE requests “5G connectivity” to a specific PLMN (e.g. NAI = “<any\_username>@nai.5gc. mnc<MNC>.mcc<MCC>.3gppnetwork.org”). In the case of WLAN access, if the UE has an MPS subscription, the UE shall also include an indication of its MPS subscription in the username part of the NAI as per TS 23.003 [33]. The NAI provided by the UE operating in SNPN access mode for Yt interface indicates that the UE request “5G connectivity” to a specific SNPN (e.g. NAI = “<any\_username>@nai.5gc. nid<NID>.mnc<MNC>.mcc<MCC>.3gppnetwork.org”). If the WLANSP rule contains information including TNGF ID to use for specific slices and the UE supports such information, the UE builds the realm of NAI taking the TNGF ID into account (e.g. NAI = “<any\_username>@ tngfid<TNGF ID>. 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 defined in clause 5.6.2 of TS 23.501 [2]. In order to support usage of the TNAP identifier defined in TS 23.316 [53], when a 5G-RG acts as a TNAP , the W-5GAN may, as defined in clause 5.6.2 of TS 23.501 [2], provide the 5G RG civic address information in the TNAP identifier.

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 (e.g. MCC, MNC and TNGF ID) provided by the UE and also based on the SSID selected by the UE. In a deployment a TNGF may be reached over different SSID(s) where the TNGF supports a Tracking Area and be associated with a set of slices, or an SSID may provide access to one or more TNGF(s), where each of these TNGF(s) can support a different Tracking Area and a different set of slices.

NOTE 3: Based on operator policy, after receiving the indication of MPS subscription from the UE, the TNAN can treat this UE with priority.

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:

- The registration request may contain an indication that the UE supports TNGF selection based on the slices the UE wishes to use over trusted non-3GPP access (i.e. that the UE supports Extended WLANSP rule).

- 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 or SNPN. If the UE in SNPN access mode for Yt interface performs the Registration procedure for UE onboarding, the UE shall include an indication in the AN parameters that the connection request is for onboarding.

- In the N2 message sent in step 6b, the TNGF includes a UE Location Information (ULI)including the TNAP ID and the UE IP address based on information received in step 3. If the ULI includes the IP address, this is set to a “null” IP address (e.g. 0.0.0.0) because the UE is not yet assigned an IP address. If the TNGF has received the the TNAP ID in step 3 over Ta, the TNGF includes the TNAP ID within UE Location Information (ULI) sent to AMF. After the UE is assigned an IP address, the TNGF includes this address in subsequent N2 messages. This N2 message also includes the Selected PLMN ID and optionally the Selected NID and the Establishment cause.

NOTE 4: The Selected NID is present when the UE connects to an SNPN via Trusted non-3GPP access.

- If the UE in SNPN access mode for Yt interface performs the Registration procedure for UE onboarding, the interaction between AMF and AUSF (step 8a and step 8c in Figure 4.12a.2.2-1) is replaced with step 9-1 or step 9-2 or step 9-3 in Figure 4.2.2.2.4-1, depending on the 5GC architecture that is used for UE onboarding.

- 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. The AMF determines the allowed subset of the Requested NSSAI that is allowed by the Subscribed S-NSSAI(s); the AMF may detect that the TNGF used by the UE is not compatible with this allowed subset and based on operator’s policy configured in the AMF, the AMF determines whether a different TNGF should be used. If the UE supports slice-based TNGF selection and the AMF determines to use a different TNGF, then the AMF proceeds with steps 17-21. Otherwise, i.e. if the AMF determines to use the selected TNGF that supports part of allowed the subset, the AMF proceeds with step 16. In this case, steps 17-21 are skipped.

NOTE 5: The criteria for the AMF to determine that the TNGF used by the UE is not compatible with the subset of the requested NSSAI that is allowed by the subscribed S-NSSAI(s) is based on local AMF policies. For example the AMF can determine that the TNGF used by the UE is compatible as soon as there is one supported slice in common.

16a-16b. 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.

16c. If the UE Registration Request contains an indication that the UE supports TNGF selection based on the slices the UE wishes to use over untrusted non-3GPP access and the AMF is able to select a UE PCF that supports UE policies for slice specific TNGF selection, the AMF may trigger UE policy association establishment if a suitable UE policy association does not exist yet.The AMF indicates to the PCF that the UE supports TNGF selection based on the slices the UE wishes to use over trusted non-3GPP access.

Steps 17 to 21 correspond to the case where the AMF has detected that TNGF used by the UE is not compatible with the subset of the requested NSSAI that is allowed by the subscribed S-NSSAI(s).

17. If the UE Registration Request contains an indication that the UE supports TNGF selection based on the slices the UE wishes to use over trusted non-3GPP access and AMF is able to select a UE PCF that supports UE policies for slice specific trusted access selection, the AMF may trigger UE policy association establishment if a suitable UE policy association does not exist yet. The AMF indicates to the PCF that the UE supports TNGF selection based on the slices the UE wishes to use over trusted non-3GPP access.

The AMF triggers the UE PCF to update the UE policies for slice specific trusted access selection

The AMF requests the PCF to receive a notification when the PCF has completed the update of these UE policies.

NOTE 6: Void.

18. The PCF updates the UE policies for slice specific trusted access selection according to the procedure defined in figure 4.2.4.3-1.

19. When the update of these policies is completed, the PCF notifies the AMF by invoking Npcf\_UEPolicyControl\_UpdateNotify.

20. The AMF sends via the TNGF a UE Registration Reject indicating that the selected TNGF was not appropriate for the requested slices that the UE is allowed to access to. The AMF may provide target TNAN information (SSID, TNGF ID) to the UE within the Registration Reject message indicating the UE to build the NAI based on the TNGF ID.

NOTE 7: The AMF may determine a target TNGF that supports the subset of the requested NSSAI that is allowed by the subscribed S-NSSAI(s) based on the list of supported TAs and the corresponding list of supported slices for each TA obtained in N2 interface management procedures as specified in TS 38.413 [10] and considering UE location.

21. If supported by the UE and if the UE received target TNAN information in step 20, the UE connects to the target TNAN, otherwise the UE may perform TNAN selection again using the updated WLANSP rule received in step 18. If the target TNAN information includes TNGF ID, the UE shall build the NAI based on TNGF ID. The UE uses the target TNAN information in the Registration Reject only for the TNAN selection directly following the rejected registration and UE shall not store it for future use.

*NEXT CHANGE (3)*

#### 4.16.11.1 General

The UE Policy Association Establishment procedure, which may be performed for a UE registered in the same AMF or different AMFs for 3GPP access and non-3GPP access, concerns the following scenarios:

1. UE initial registration with the network.

2. The AMF relocation with PCF change in handover procedure and registration procedure.

3. UE registration with 5GS when the UE moves from EPS to 5GS and there is no existing UE Policy Association between AMF and PCF for this UE.

In Non-roaming case, the H-PCF may interact with the CHF in HPLMN to make a decision about UE Policies based on spending limits.



Figure 4.16.11-1: UE Policy Association Establishment

This procedure concerns both roaming and non-roaming scenarios.

In the non-roaming case the V-PCF is not involved and the role of the H-PCF is performed by the PCF. For the roaming scenarios, the V-PCF interacts with the AMF and the H-PCF interacts with the V-PCF:

1. The AMF establishes UE Policy Association with the (V-)PCF when a UE Policy Container is received from the UE. If a UE Policy Container is not received from the UE, the AMF may establish UE Policy Association with the (V-)PCF based on AMF local configuration.

NOTE 1: In roaming scenario, the AMF local configuration can indicate whether UE Policy delivery is needed based on the roaming agreement with home PLMN of the UE.

2. The AMF sends a Npcf\_UEPolicyControl Create Request with the following information: SUPI, may include Access Type and RAT, PEI, ULI, UE time zone, Serving Network (PLMN ID, or PLMN ID and NID, see clause 5.34 of TS 23.501 [2]), the Internal-Group-ID-list and UE Policy Container (the list of stored PSIs, operating system identifier, Indication of UE support for ANDSP, indication of UE capability of reporting URSP rule enforcement to network, indication of support of URSP delivery in EPS). In roaming scenario, based on operator policies, the AMF may provide to the V-PCF the PCF ID of the selected H-PCF. The V-PCF contacts the H-PCF. In roaming case, steps 3 and 4 are executed, otherwise step 5 follows.

If the AMF, based on configuration, is aware that the UE is accessing over a gNB using satellite backhaul, the AMF includes the Satellite backhaul category as described in clause 5.43 of TS 23.501 [2].

The AMF may indicate to the PCF that the UE supports N3IWF selection based on the slices the UE wishes to use over untrusted non-3GPP access and/or UE support for TNGF selection based on the slices the UE wishes to use over trusted non-3GPP access.

3. The V-PCF forwards the information received from AMF in step 2 to the H-PCF. When a UE Policy Container is received at initial registration, the H-PCF may store the PEI, the OSId, indication of UE capability of reporting URSP rule enforcement to network, indication of support of URSP delivery in EPS or the indication of UE support for ANDSP in the UDR using Nudr\_DM\_Create including DataSet "Policy Data" and Data Subset "UE context policy control data".

The V-PCF may retrieve the Application guidance on URSP Rule for inbound roamers of the PLMN of the SUPI, if not available, using Nudr\_DM\_Query or Nudr\_DM\_Subscribe including the Data Set "Application Data" and Data Subset "Service Specific Information" and DataKey set to "PLMN ID(s) of inbound roamers".

The V-PCF may retrieve the Application guidance on URSP Rule for inbound roamers of the PLMN of the SUPI, if not available, using Nudr\_DM\_Query or Nudr\_DM\_Subscribe including the Data Set "Application.

4. The H-PCF sends a Npcf\_UEPolicyControl Create Response to the V-PCF. The H-PCF may provide the Policy Control Request Trigger parameters in the Npcf\_UEPolicyControl Create Response. Before sending the response, the H-PCF may determine that the decision about UE policy control depends on the status of the policy counters available at the CHF and if such reporting is not established for the subscriber, the H-PCF initiates an Initial Spending Limit Report Retrieval as defined in clause 4.16.8.2. If policy counter status reporting is already established for the subscriber and the H-PCF determines that the status of additional policy counters are required, the H-PCF initiates an Intermediate Spending Limit Report Retrieval as defined in clause 4.16.8.3.

The (H-)PCF in roaming and the PCF in non-roaming may register to the BSF as the PCF serving this UE, if not already registered at the AM Policy Association establishment. This is performed by using the Nbsf\_Management\_Register operation, providing as inputs the UE SUPI/GPSI and the PCF identity.

5. The (V-) PCF sends a Npcf\_UEPolicyControl Create Response to the AMF. The (V-)PCF relays the Policy Control Request Trigger parameters in the Npcf\_UEPolicyControl Create Response.

The (V-)PCF also subscribes to notification of N1 message delivery of policy information to the UE using Namf\_Communication\_N1N2MessageSubscribe service which is not shown in this figure.

6. The (H-)PCF gets policy subscription related information and the latest list of PSIs from the UDR using Nudr\_DM\_Query service operation (SUPI, Policy Data, UE context policy control data, Policy Set Entry) if either or both are not available and makes a policy decision. The (H-)PCF may get the PEI, the OSId, indication of UE capability of reporting URSP rule enforcement to network or the indication of UE support for ANDSP in the UDR using Nudr\_DM\_Query including DataSet "Policy Data" and Data Subset "UE context policy control data" if the AMF relocates and the PCF changes. In the roaming scenario, the H-PCF may provide the indication of UE support for ANDSP to the V-PCF, if the indication was not present in the Npcf\_UEPolicyControl Create request from V-PCF and the H-PCF gets this information from the H-UDR. The (H-)PCF may get the 5G VN group data and 5G VN group membership for each Internal-Group-ID received from the AMF using Nudr\_DM\_Query (Internal-Group-Id, Subscription Data, 5G VN Group Configuration). The (H-)PCF may store the 5G VN group data and 5G VN group membership for later use for other SUPIs that belong to the same Internal-Group-ID. The (H-)PCF may request notifications from the UDR on changes in the subscription information by invoking Nudr\_DM\_Subscribe (Policy Data, SUPI, DNN, S-NSSAI, Notification Target Address (+ Notification Correlation Id), Event Reporting Information (continuous reporting), UE context policy control data) service. The (H-)PCF may request notifications from the UDR on changes in the 5G VN group data or 5G VN group membership associated to each of the Internal-Group-Id provided to the PCF by invoking Nudr\_DM\_Subscribe (Subscription Data, 5G VN Group Configuration, Internal Group ID, Notification Target Address (+ Notification Correlation Id), Event Reporting Information (continuous reporting)) service. The (H-)PCF creates the UE policy container including UE policy information as defined in clause 6.6 of TS 23.503 [20] and in the case of roaming H-PCF provides the UE policy container in the Npcf\_UEPolicyControl UpdateNotify Request. In the non-roaming case, the PCF may subscribe to Analytics from NWDAF as defined in clause 6.1.1.3 of TS 23.503 [20].

7. The V-PCF sends a response to H-PCF using Npcf\_UEPolicyControl UpdateNotify Response.

NOTE 2: Step 6 (and step 7) can be omitted. Then the (H-)PCF creates the UE policy container including UE polices in step 2 (in the case of non-roaming) or step 3 (in the case of roaming). This means that the potential interactions with UDR as in step 6 will have to be executed in step 2 (non-roaming) or step 3 (roaming).

8. The (V-)PCF triggers UE Configuration Update Procedure in clause 4.2.4.3 to sends the UE policy container including UE policy information to the UE. The (V-)PCF checks the size limit as described in clause 6.1.2.2.2 of TS 23.503 [20].

9. If the V-PCF received notification of the reception of the UE Policy container then the V-PCF forwards the notification response of the UE to the H-PCF using Npcf\_UEPolicyControl\_Update Request.

If the V-PCF is notified by the V-UDR about the Service Specific Information applicable to inbound roamers from the HPLMN of the UE as specified in clause 4.15.6.10, the V-PCF provides the Service Parameters to the H-PCF.

10. The H-PCF sends a response to the V-PCF. If the V-PCF received a UE Policy Container step 8 will follow.

*NEXT CHANGE (4)*

##### 4.16.12.1.1 UE Policy Association Modification initiated by the AMF without AMF relocation

This procedure addresses the scenario where a Policy Control Request Trigger condition is met.



Figure 4.16.12.1.1-1: UE Policy Association Modification initiated by the AMF

This procedure concerns both roaming and non-roaming scenarios.

In the non-roaming case the V-PCF is not involved. In the roaming case, the AMF interacts with the V-PCF and the H-PCF interacts with the V-PCF.

1. When a Policy Control Request Trigger condition is met the AMF updates UE Policy Control Association and provides information on the conditions that have changed to the PCF. The AMF sends a Npcf\_UEPolicyControl Update Request with the following information: UE Policy Association ID associated with the SUPI defined in TS 29.525 [58] and the Policy Control Request Trigger met. In roaming scenario, based on operator policies, the AMF may provide to the V-PCF the PCF ID of the selected H-PCF. The V-PCF contacts the H-PCF.

See clause 6.1.2.5 of TS 23.503 [20] and clause 4.2.3.2 of TS 29.525 [58] for more details on Policy Control Request Trigger.

The AMF may indicate to the PCF that the UE supports N3IWF selection based on the slices the UE wishes to use over untrusted non-3GPP access and/or UE support for TNGF selection based on the slices the UE wishes to use over trusted non-3GPP access.

In the roaming case, steps 2 and 3 are executed, otherwise step 4 follows.

2. The V-PCF forwards the information received from AMF in step 1 to the (H-)PCF.

3. The H-PCF replies to the V-PCF. In the non-roaming case, the PCF may subscribe to Analytics from NWDAF as defined in clause 6.1.1.3 of TS 23.503 [20].

4. The (V-) PCF sends a Npcf\_UEPolicyControl Update Response to the AMF.

5. The (H-)PCF may create the UE policy container including UE policy information as defined in clause 6.6 of TS 23.503 [20]. In the case of roaming the H-PCF may include the UE policy container in the Npcf\_UEPolicyControl UpdateNotify Request.

6. The (V-)PCF sends a response to H-PCF using Npcf\_UEPolicyControl UpdateNotify Response.

Steps 7, 8 and 9 are the same as steps 8, 9 and 10 of procedure UE Policy Association Establishment in clause 4.16.11.

*NEXT CHANGE (5)*

##### 5.2.5.6.2 Npcf\_UEPolicyControl\_Create service operation

**Service operation name:** Npcf\_UEPolicyControl\_Create

**Description:** NF Service Consumer can request the creation of a UE Policy Association by providing relevant parameters about the UE context to the PCF.

**Inputs, Required:** Notification endpoint, SUPI.

**Inputs, Optional:** H-PCF ID (if the NF service producer is V-PCF and AMF is NF service consumer), information provided by the AMF as define in clause 6.2.1.2 of TS 23.503 [20], such as Access Type, Permanent Equipment Identifier, GPSI, User Location Information, UE Time Zone, Serving Network (PLMN ID, or PLMN ID and NID, see clause 5.34 of TS 23.501 [2]), RAT type, LBO Information (see clause 6.1.2.2.4 of TS 23.503 [20]), UE policy container including the list of PSIs, OS id, the indication of UE support for ANDSP, UE capability of reporting URSP rule enforcement to network (see clause 6.6.2.4 of TS 23.503 [20]), UE indication of support of URSP delivery in EPS and Internal Group (see TS 23.501 [2]), Satellite backhaul category (see clause 5.43 of TS 23.501 [2]), "5GS to EPS Mobility" indication, request to update the UE policies, request to be notified when updated UE policies have been provided to the UE, the indication of UE support for N3IWF selection based on the slices the UE wishes to use over untrusted non-3GPP access, the indication of UE support for TNGF selection based on the slices the UE wishes to use over trusted non-3GPP access.

**Outputs, Required:** Success or Failure, UE Policy Association ID.

**Outputs, Optional:** Policy Control Request Trigger of UE Policy Association. In the case of H-PCF is producer, UE policy information (see clause 5.2.5.6.1).

*NEXT CHANGE (6)*

##### 5.2.5.6.5 Npcf\_UEPolicyControl\_Update service operation

**Service operation name:** Npcf\_UEPolicyControl\_Update

**Description:** NF Service Consumer, e.g. AMF can request the update of the UE Policy Association to receive updated Policy information for the UE context.

**Inputs, Required:** UE Policy Association ID.

**Inputs, Optional:** Information on the UE policy related Policy Control Request Trigger condition that has been met, as defined in Table 6.1.2.5-1 of TS 23.503 [20], the indication of UE support for N3IWF selection based on the slices the UE wishes to use over untrusted non-3GPP access, the indication of UE support for TNGF selection based on the slices the UE wishes to use over trusted non-3GPP access.

**Outputs, Required:** Success or Failure.

**Outputs, Optional:** Policy Control Request Trigger of UE Policy Association. In the case of H-PCF is producer, UE related policy information.

*END OF CHANGES*