**3GPP TSG-SA3 Meeting #106-e *S3-220398***

**e-meeting, 14 - 25 February 2022**

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

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

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | N5CW and key derivation correction | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** |  | | | | |  | ***Date:*** | | | 2022-02-25 |
|  |  | | | |  | |  | | |  |
| ***Category:*** |  |  | | | | | ***Release:*** | | | Rel-16 |
|  | *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:*** | | Reference to clause that describes how WLAN UEs that do not support 5GC NAS (N5CW) register via trusted non-3GPP access is missing;  KTNAP is derived from KTNGF and not from KTWIF | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Cross-referencing and key derivation correction | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Missing references | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 7A.1, 7A.2.4 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 CHANGES

7A.1 General

Security for trusted non-3GPP access to the 5G Core network is achieved when the UE registers to the 5GC via the TNAN. The UE registers to 5GC and, at the same time, it authenticates with the TNAN by using the EAP-5G procedure, similar to the one used with the registration procedure for untrusted non-3GPP access.

The link between the UE and the TNAN can be any data link (L2) that supports EAP encapsulation. The requirement on the Ta interface between the TNAP and TNGF can be found in clause 4.2.8.3.2 of TS 23.501[2]. The TNGF terminates the EAP-5G signalling andfowards the NAS message to the 5GC when the UE attempts to register to 5GC via the TNAN. The security relies on Layer-2 security between UE and TNAP, which is a trusted entity so that no IPSec encryption would be necessary between UE and TNGF, i.e. NULL encryption is sufficient for the user plane and signalling.

NOTE: The encryption protection over Layer-2 between UE and TNAP is assumed to be enabled.

Separate IPSec SAs may be used for NAS transport and PDU Sessions. At the end of the UE’s registration to 5GC, an IPSec SA (NWt) is established between the UE and TNGF. This is used to protect NAS messages between the UE and TNGF. Later when the UE initiates a PDU session establishment, the TNGF initiates establishment of one or more IPSec child SAs per PDU session. This results in additional IPSec SA’s (NWt) to be setup between the UE and TNGF-UP which are then for user plane transport between the two.

Clause 7A.2.4 describes how WLAN UEs that do not support 5GC NAS (N5CW) register via trusted non-3GPP access. Those N5CW devices are able to authenticate to the network with 3GPP credentials and register with the help of an interworking function (TWIF) that provides the 5GC NAS protocol stack towards the AMF.

As defined in clause 7.1, it is the home operator policy decision if a non-3GPP access network is treated as trusted non-3GPP access network. When all of the security domains in clause 4.1 of the present specification related to the non-3GPP access network are considered sufficiently secure by the home operator, the non-3GPP access may be identified as a trusted non-3GPP access for that operator. However, this policy decision may additionally be based on reasons not related to security feature groups.

NOTE: It is specified in clause 7.1a of the current document how the UE gets the operator policy and how it will behave accordingly.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* NEXT CHANGE

7A.2.4 Authentication for devices that do not support 5GC NAS over WLAN access

A N5CW device is capable to register to 5GC with 3GPP credentials and to establish 5GC connectivity via a trusted WLAN access network. The reference architecture is captured in clause 4.2.8.5.2 of TS 23.501[2]. The 3GPP credentials are stored as defined in clause 6.1.1.1. The Trusted WLAN Interworking Function (TWIF) provides interworking functionality that enables connectivity with 5GC and implements the NAS protocol stack and exchanges NAS messages with the AMF on behalf of the N5CW device. A single EAP-AKA’ authentication procedure is executed for connecting the N5CW device both to the trusted WLAN access network and to the 5G core network.



**Figure 7A.2.4-1: Authentication Procedure for N5CW**

0. The N5CW device selects a PLMN and a trusted WLAN that supports "5G connectivity-without-NAS" to this PLMN by using the procedure specified in TS 23.501 [2] clause 6.3.12a, "Access Network selection for devices that do not support 5GC NAS over WLAN".

Steps 1-10: Initial registration to 5GC.

1. The N5CW device associates with the trusted WLAN network and the EAP-AKA’ authentication procedure is initiated.

2. The N5CW device shall provide its Network Access Identity (NAI) The Trusted WLAN Access Point (TWAP) selects a Trusted WLAN Interworking Function (TWIF), e.g. based on the received realm, and sends an AAA request to the selected TWIF.

If the N5CW device registers to 5GC over 3GPP access for the first time when the above procedure is initiated, then the NAI shall include the SUCI. The SUCI shall be constructed as specified in clause 6.12.2.

If the N5CW device has registered to 5GC over 3GPP access when the above procedure is initiated, then the NAI includes the 5G-GUTI assigned to the N5CW device over 3GPP access. This enables the TWIF in step 4a below to select the same AMF as the one serving the N5CW device over 3GPP access.

3. The TWIF shall create a 5GC Registration Request message on behalf of the N5CW device. The TWIF shall use default values to populate the parameters in the Registration Request message, which are the same for all N5CW device that do not support 5G NAS. The Registration type indicates "Initial Registration".

4. The TWIF shall select an AMF (e.g. by using the 5G-GUTI in the NAI, if provided by the N5CW device) and shall send an N2 message to the AMF including the Registration Request, the User Location and an AN Type.

5. In case the AMF triggers an authentication procedure , it sends a request to AUSF by sending Nausf\_UEAuthentication\_Authenticate Request message. The Nausf\_UEAuthentication\_Authenticate Request message contains SUCI or SUPI (in case of a valid 5G-GUTI is received by the AMF). The request message contains also an indication that the request is from a N5CW device.

6. The AUSF shall send Nudm\_UEAuthentication\_Get Request to the UDM including SUCI or SUPI and the N5CW indication.

7. Upon reception of the Nudm\_UEAuthentication\_Get Request, the UDM shall invoke SIDF if a SUCI is received. SIDF shall de-conceal SUCI to gain SUPI before UDM can process the request. The UDM may select an authentication method based on the "realm" part of the SUPI, the N5CW device indicator, a combination of the "realm" part and the N5CW device indicator, or the UDM local policy.

8. The EAP-AKA’ procedure will be trigged to perform mutual authentication between the N5CW device and the home network as specified in clause 6.1.3.1.

EAP-AKA' takes place between the N5CW device and AUSF. Over the N2 interface, the EAP messages are encapsulated within NAS Authentication messages. The EAP-AKA’ messages exchanged between the N5CW Device and the TWIF shall be encapsulated into the layer-2 packets, e.g. into IEEE 802.3/802.1x packets, into IEEE 802.11/802.1x packets, into PPP packets, etc.

9. The NAS security context is not be required in this scenario. The AMF shall derive an KTWIF key from the received KAMF key as specified in Annex A.9. NAS security between AMF and TWIF is established similar to unauthenticated emergency calls, i.e. with NULL encryption and NULL integrity protection.

10a. The AMF shall send NAS Security Mode Command to the TWIF. The NAS Security Mode Command shall contain the EAP-Success message and the NULL security algorithms.

10b. The TWIF shall not forward the EAP-Success to the N5CW directly, instead, it shall store the EAP-Success message and wait for KTWIF.

10c. The TWIF shall send the NAS Security Mode Complete message to the AMF.

11. The AMF sends an N2 Initial Context Setup Request and provides the KTWIF key to TWIF.

12. The TWIF shall derive a TNAP key, KTNAP, from the KTWIF key as specified in Appendix A.22 and send the TNAP key and the EAP-Success message to the Trusted WLAN Access Point, which forwards the EAP-Success to the N5CW device. The TNAP key corresponds to the PMK (Pairwise Master Key) which is used to secure the WLAN air-interface communication according to IEEE 802.11 [80]. A layer-2 or layer-3 connection is established between the Trusted WLAN Access Point and the TWIF for transporting all user-plane traffic of the N5CW device to TWIF. This connection is later bound to an N3 connection that is created for this N5CW device.

13. The TWIF shall send N2 Initial Context Setup Response message to the AMF.

14. The following steps are captured in clause 4.12b.2 of TS 23.502[8].

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* NEXT CHANGE

# A.22 KTIPSec and KTNAP derivation function

When deriving a KTIPSec from KTNGF and when deriving a KTNAP from Ktwif the following parameters shall be used to form the input S to the KDF.

- FC = 0x84

- P0 = Usage type distinguisher

- L0 = length of Usage type distinguisher (i.e. 0x00 0x01)

The values for the Usage type distinguisher are defined in table A.22-1. The values 0x00 and 0x03 to 0xf0 are reserved for future use, and the values 0xf1 to 0xff are reserved for private use.

The Usage type distinguisher shall be set to the value for IPSec (0x01) when deriving KTIPSec. The Usage type distinguisher shall be set to the value for TNAP (0x02) when deriving KTNAP.

The input key KEY shall be the 256-bit KTNGF or KTWIF.

Table A.22-1: Usage type distinguishers

|  |  |
| --- | --- |
| Usage type distinguisher | Value |
| IPSec | 0x01 |
| TNAP | 0x02 |

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* END OF CHANGES