**3GPP TSG-SA3 Meeting #116 *S3-241816-r1***

Jeju, South Korea, 20th May – 24th May 2024

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  |  | **CR** | **1982** | **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:***  | Clarification in TNGF and N3IWF procedures |
|  |  |
| ***Source to WG:*** | Nokia |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | TEI17 |  | ***Date:*** | 2024-05-10 |
|  |  |  |  |  |
| ***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:*** | * Editorial corrections
* N3IWF Child SA are secure with integrity protection and ciphering however, TNGF Child SA are only integrity protected, but not ciphered. It is not clearly mentioned in the standards.
 |
|  |  |
| ***Summary of change:*** | Editorial changeTNGF Child SA are only integrity protected, but not ciphered. |
|  |  |
| ***Consequences if not approved:*** | Unclear specification  |
|  |  |
| ***Clauses affected:*** | 7.1, 7A.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:*** |  |

**\*\*\*\* START OF CHANGES \*\*\*\***

## 7.1 General

Security for untrusted non-3GPP access to the 5G Core network is achieved by a procedure using IKEv2 as defined in RFC 7296 [25] to set up one or more IPsec ESP [4] security associations. The role of IKE initiator (or client) is taken by the UE, and the role of IKE responder (or server) is taken by the N3IWF.

During this procedure, the AMF delivers a key KN3IWF to the N3IWF. The AMF derives the key KN3IWF from the key KAMF. The key KN3IWF is then used by UE and N3IWF to complete authentication within IKEv2.

Security for trusted non-3GPP access to 5G Core network is defined in clause 7A.

Trusted and untrusted Non-3GPP Access Networks are IP access networks that use access technology whose specification is out of the scope of 3GPP.

Whether a non-3GPP IP access network is trusted or untrusted is not a characteristic of the access network.

In non-roaming scenario it is the HPLMN's operator decision if a non-3GPP IP access network is used as trusted or untrusted non-3GPP access Network. When one or more of the security feature groups provided by the non-3GPP access network are considered not sufficiently secure by the home operator, the non-3GPP access may be identified as an untrusted non-3GPP access for that operator. However, this policy decision may additionally be based on reasons not related to security feature groups.

In roaming scenario, the UDM in HPLMN makes the final decision of whether a non-3GPP IP access network is used as trusted or untrusted non-3GPP access network based on the identities of the access network and the visited network. The UDM may take the VPLMN's policy and capability returned from the AMF or roaming agreement into account

For supporting multiple DNs, the same trust relationship shall apply to all the DNs the UE connects to from a certain non-3GPP access network, i.e. it shall not be possible to access one DN using the non-3GPP access network as trusted, while access to another DN using the same non-3GPP access network as untrusted.

**\*\*\*\* NEXT 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. However, integrity protection would be provided.

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.

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