**3GPP TSG-CT WG1 Meeting #150C1-244275**

**Maastricht, Netherlands, 19-23 August 2024**

|  |
| --- |
| *CR-Form-v12.2* |
| **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 | **X** | Radio Access Network |  | Core Network | **X** |

|  |
| --- |
|  |
| ***Title:***  | Correction for security protection when accessing the network through trusted non-3GPP access |
|  |  |
| ***Source to WG:*** | Nokia |
| ***Source to TSG:*** | C1 |
|  |  |
| ***Work item code:*** | 5GProtoc18-non3GPP |  | ***Date:*** | 2024-07-23 |
|  |  |  |  |  |
| ***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 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-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)Rel-19 (Release 19)* |
|  |  |
| ***Reason for change:*** | Clause 7.3.2.1 in TS 24.502 (the untrusted non-3GPP access case) states the following:*The UE proceeds with the establishment of IKE SA and signalling IPsec SA with the selected N3IWF by initiating an IKE\_SA\_INIT exchange according to IETF RFC 7296 [6]. All the IKE messages following the IKE\_SA\_INIT exchange are* ***encrypted and integrity protected*** *using the cryptographic algorithms and keys negotiated in the IKE\_SA\_INIT exchange as specified in IETF RFC 7296 [6].*It is clear from the above that, when accessing the network through untrusted non-3GPP access, the IKE messages are encrypted and integrity protected. This is aligned with the definition/concept of "**untrusted**" non-3GPP access, where the UE and Network needs to ensure of applying proper encryption of the IKE messages beside the integrity protection.Now, for the trusted non-3GPP access case, clause 7.3A.3.1 in TS 24.502 states the following:*The UE shall establish the secure connection by establishing an IKE SA and signalling IPsec SA (first child SA) by initiating the IKE\_SA\_INIT exchange and then IKE\_AUTH exchange for mutual authentication with the TNGF and* ***NULL encryption*** *as specified in IETF RFC 2410 [34].* It is clear from the above that No encryption (i.e. NULL encryption) is used for IKE messages when accessing the network through trusted non-3GPP access which is also aligned with the definition/concept of "**trusted**" non-3GPP access. **BUT** this statement stays silent about the Integrity protection and whether it shall be applied or not. Actually nothing prevents applying integrity protection in that case and this was actually clarified in TS 33.501 through the agreed CR **S3-242382** which states the following:*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.*Same clarification needs to be reflected in clause 7.3A.3.1 in TS 24.502 in order to emphasize on the usage of Integrity protection in that case. |
|  |  |
| ***Summary of change:*** | Clarifying that Integrity protection is used for the IKE messages when accessing the network through trusted non-3GPP access case.**Backward compatibility analysis:**The CR is backward compatible since it doesn't break or change any existing interfaces between the UE and the TNGF. |
|  |  |
| ***Consequences if not approved:*** | Wrong interpretation that Integrity Protection is not needed/doesn't apply for the trusted non-3GPP access case, specially that Integrity protection is mentioned clearly for the untrusted non-3GPP access case but not mentioned for the trusted non-3GPP access. |
|  |  |
| ***Clauses affected:*** | 7.3A.3.1 |
|  |  |
|  | **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:*** |  |

\*\*\*\*\* First change \*\*\*\*\*

#### 7.3A.3.1 IKE SA and signalling IPsec SA establishment initiation

In a trusted non-3GPP access network, once the EAP- 5G authentication is successfully complete and the UE is configured with a local IP address, the UE shall use the TNGF IP address received in the EAP-Request/5G-Notification message (see clause 7.3A.2.3) to establish a secure connection between the UE and the TNGF over NWt to exchange NAS signalling messages with the AMF. The UE shall establish the secure connection by establishing an IKE SA and signalling IPsec SA (first child SA) by initiating the IKE\_SA\_INIT exchange and then IKE\_AUTH exchange for mutual authentication with the TNGF using integrity protection and NULL encryption as specified in IETF RFC 2410 [34]. The UE shall set the IDi payload of the IKE\_AUTH request message in the IKE\_AUTH exchange (see IETF RFC 7296 [6]) to the NAI format of 5G-GUTI or the NAI format of SUCI as specified in 3GPP TS 23.003 [8], depending on the employed UE identity in the EAP-Response/5G-NAS message at the time of EAP-5G session initiation according to clause 7.3A.2.3.

\*\*\*\*\* End of changes \*\*\*\*\*