**3GPP TSG-CT WG1 Meeting #137-eC1-225098**

**E-Meeting, 18th – 26th Aug 2022 (was C1-224743)**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **.501** | **CR** | **4504** | **rev** | **1** | **Current version:** | **17.7.1** |  |
|  | | | | | | | | |
| *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:*** | Applicability of NULL algorithm upon RAT change | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Apple | | | | | | | | | |
| ***Source to TSG:*** | C1 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | 5GProtoc18 | | | | |  | ***Date:*** | | | 2022-08-20 |
|  |  | | | |  | |  | | |  |
| ***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 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:*** | | If a 5G-EA0 algorithm is configured by a 5G PLMN, the non-cleartext IEs included in the initial NAS are readable and should thus only be sent in the PLMN which has assigned the 5G-EA0.  With current conditions however the comparison is not done against the PLMN which has assigned 5G-EA0, but against the RPLMN.  This will cause problems like this: If the UE has a 5G-EA0 algorithm configured by PLMN-1 on 5G and registers then on 4G on PLMN-2, before returning back to PLMN-1 on 5G, it will detect a PLMN change, i.e. RPLMN PLMN-2, newly selected PLMN PLMN-1 and would thus only include clear text IEs although the PLMN-1 is the PLMN which had configured 5G-EA0.  Rather than to compare the newly selected PLMN against the RPLMN, the UE shall compare the newly selected PLMN against the PLMN by which this selected 5G NAS security algorithm was assigned. With this approach also the case that the UE is already registered on PLMN-1 via non-3GPP and now PLMN-1 is also selected via 3GPP is covered, as now the comparison would detect no PLMN change and thus would not trigger the deletion of the NAS security context.  The Note stating that the "UE deletes the 5G NAS security context only if the UE is not in the connected mode." could be misinterpreted such that the 5G-EA0 condition would also be applicable in CONNECTED mode, which is wrong. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | The UE shall compare the newly selected PLMN against the PLMN which by which this selected 5G NAS security algorithm was assigned, rather than to compare the newly selected PLMN against the RPLMN.  The term "cleartext IEs only" is changed to "only cleartext IEs", as this avoids ambiguities if the term is used before a sub-clause.  Note is deleted to avoid misinterpretation. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Risk that the UE detects a PLMN change by error and in consequence only include clear text IEs although the PLMN-1 is the PLMN which had configured 5G-EA0. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 4.4.6 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 \* \* \* \*

### 4.4.6 Protection of initial NAS signalling messages

The 5GS supports protection of initial NAS messages as specified in 3GPP TS 33.501 [24]. The protection of initial NAS messages applies to the REGISTRATION REQUEST, SERVICE REQUEST and CONTROL PLANE SERVICE REQUEST message, and is achieved as follows:

a) If the UE does not have a valid 5G NAS security context, the UE sends a REGISTRATION REQUEST message including only cleartext IEs. After activating a 5G NAS security context resulting from a security mode control procedure:

1) if the UE needs to send non-cleartext IEs, the UE shall include the entire REGISTRATION REQUEST message (i.e. containing both cleartext IEs and non-cleartext IEs) in the NAS message container IE and shall include the NAS message container IE in the SECURITY MODE COMPLETE message; or

2) if the UE does not need to send non-cleartext IEs, the UE shall include the entire REGISTRATION REQUEST message (i.e. containing only cleartext IEs) in the NAS message container IE and shall include the NAS message container IE in the SECURITY MODE COMPLETE message.

b) If the UE has a valid 5G NAS security context and:

1) the UE needs to send non-cleartext IEs in a REGISTRATION REQUEST or SERVICE REQUEST message, the UE includes the entire REGISTRATION REQUEST or SERVICE REQUEST message (i.e. containing both cleartext IEs and non-cleartext IEs) in the NAS message container IE and shall cipher the value part of the NAS message container IE. The UE shall then send a REGISTRATION REQUEST or SERVICE REQUEST message containing the cleartext IEs and the NAS message container IE;

2) the UE needs to send non-cleartext IEs in a CONTROL PLANE SERVICE REQUEST message:

i) if CIoT small data container IE is the only non-cleartext IE to be sent, the UE shall cipher the value part of the CIoT small data container IE. The UE shall then send a CONTROL PLANE SERVICE REQUEST message containing the cleartext IEs and the CIoT small data container IE;

ii) otherwise, the UE includes non-cleartext IEs in the NAS message container IE and shall cipher the value part of the NAS message container IE. The UE shall then send a CONTROL PLANE SERVICE REQUEST message containing the cleartext IEs and the NAS message container IE;

3) the UE does not need to send non-cleartext IEs in a REGISTRATION REQUEST or SERVICE REQUEST message, the UE sends the REGISTRATION REQUEST or SERVICE REQUEST message without including the NAS message container IE; or

4) the UE does not need to send non-cleartext IEs in a CONTROL PLANE SERVICE REQUEST message, the UE sends the CONTROL PLANE SERVICE REQUEST message without including the NAS message container IE and the CIoT small data container IE.

When the initial NAS message is a REGISTRATION REQUEST message, the cleartext IEs are:

- Extended protocol discriminator;

- Security header type;

- Spare half octet;

- Registration request message identity;

- 5GS registration type;

- ngKSI;

- 5GS mobile identity;

- UE security capability;

- Additional GUTI;

- UE status;

- EPS NAS message container;

- NID; and

- PLMN with disaster condition.

When the initial NAS message is a SERVICE REQUEST message, the cleartext IEs are:

- Extended protocol discriminator;

- Security header type;

- Spare half octet;

- ngKSI;

- Service request message identity;

- Service type; and

- 5G-S-TMSI.

When the initial NAS message is a CONTROL PLANE SERVICE REQUEST message, the cleartext IEs are:

- Extended protocol discriminator;

- Security header type;

- Spare half octet;

- ngKSI;

- Control plane service request message identity; and

- Control plane service type.

When the UE sends a REGISTRATION REQUEST or SERVICE REQUEST or CONTROL PLANE SERVICE REQUEST message that includes a NAS message container IE, the UE shall set the security header type of the initial NAS message to "integrity protected".

When the AMF receives an integrity protected initial NAS message which includes a NAS message container IE, the AMF shall decipher the value part of the NAS message container IE. If the received initial NAS message is a REGISTRATION REQUEST message or a SERVICE REQUEST message, the AMF shall consider the NAS message that is obtained from the NAS message container IE as the initial NAS message that triggered the procedure.

When the AMF receives a CONTROL PLANE SERVICE REQUEST message which includes a CIoT small data container IE, the AMF shall decipher the value part of the CIoT small data container IE and handle the message as specified in subclause 5.6.1.4.2.

When the initial NAS message is a DEREGISTRATION REQUEST message, the UE always sends the NAS message unciphered.

If the UE:

a) has 5G-EA0 as a selected 5G NAS security algorithm; and

b) in 5GMM-IDLE mode selects a PLMN over one access type, other than the PLMN by which this selected 5G NAS security algorithm was assigned , then:

- the UE shall send an initial NAS message including only cleartext IEs via the access type associated with the newly selected PLMN, as described in this subclause for the case when the UE does not have a valid 5G NAS security context; and

- if the UE is not registering or registered via the other access type to a PLMN using this 5G NAS security context, it shall delete the 5G NAS security context.

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