**3GPP TSG-CT WG1 Meeting #136-eC1-21XXX**

**E-meeting, 12-20 May 2022 *was C1-273721***

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **24.501** | **CR** | **4366** | **rev** | **1** | **Current version:** | **17.6.1** |  |
|  |
| *For* [***HELP***](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 |  |

|  |
| --- |
|  |
| ***Title:***  | UE delete NAS security context only when not be used |
|  |  |
| ***Source to WG:*** | Huawei, HiSilicon  |
| ***Source to TSG:*** | C1 |
|  |  |
| ***Work item code:*** | 5GProtoc17 |  | ***Date:*** | 2022-05-17 |
|  |  |  |  |  |
| ***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:*** | As the following text quoted from subclase 6.4.2.2 of TS 33.501 specified, if the UE connects to the same PLMN over two types of access without ciphering, a common 5G NAS security context is shared by these two accesses. *When the UE is registered in a serving network over two types of access (e.g. 3GPP and non-3GPP), then the UE has two active NAS connections with the same AMF. A common 5G NAS security context is created during the registration procedure over the first access type.* Then, suppose the UE switches to another PLMN over one access (e.g., 3GPP) but keeps the connection with the original null cipher PLMN over the other access (e.g., non-3GPP), the “common 5G NAS security context” of course shall be maintained since the UE still needs to use it for non-3GPP.However in the following case described in clause 4.4.6 of TS 24.501, UE directly deletes the 5G NAS security context without considering whether the other access is using the 5G NAS security context.*If the UE:**a) has 5G-EA0 as a selected 5G NAS security algorithm; and**b) selects a PLMN other than Registered PLMN and EPLMN;**the UE shall delete the 5G NAS security context and send an initial NAS message including cleartext IEs only as described in this subclause for the case when the UE does not have a valid 5G NAS security context.*It is proposed to clarify that, UE deletes the 5G NAS security context only when the 5G NAS security context is not used in this case. |
|  |  |
| ***Summary of change:*** | Clarify that when the UE has 5G-EA0 as a selected 5G NAS security algorithm and selects a PLMN other than Registered PLMN and EPLMN over one access, the UE deletes the 5G NAS security context only if the Registered PLMN or EPLMN is not registing or registered over another access |
|  |  |
| ***Consequences if not approved:*** | 5G NAS security context is deleted when the other access is still using it |
|  |  |
| ***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:*** |  |

\*\*\*\*\* start of 1st 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 cleartext IEs only. 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 cleartext IEs only) 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) selects a PLMN other than Registered PLMN and EPLMN over one access;

the UE shall:

1. if the Registered PLMN or EPLMN is not registing or registered over another access, delete the 5G NAS security context; and
2. send an initial NAS message including cleartext IEs only as described in this subclause for the case when the UE does not have a valid 5G NAS security context.

NOTE: UE deletes the 5G NAS security context only if the UE is not in the connected mode.

\*\*\*\*\* end of 1st change \*\*\*\*\*