**3GPP TSG-CT WG1 Meeting #133-eC1-21xxxx**

**E-meeting, 11-19 November 2021 (rev of C1-216617)**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **24.501** | **CR** | **3706** | **rev** | **1** | **Current version:** | **17.4.1** |  |
|  | | | | | | | | |
| *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 |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** |  | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Apple, Nokia, Nokia Shanghai Bell | | | | | | | | | |
| ***Source to TSG:*** | C1 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | 5GProtoc17 | | | | |  | ***Date:*** | | | 2021-11-11 |
|  |  | | | |  | |  | | |  |
| ***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:*** | | Alignment with TS 33.501 (S3-212796, CR #1182):  When the UE is in N1 mode and performs an inter-system change from N1 mode to S1 mode, it will delete any current mapped 5G NAS security context.  According to the CR agreed by SA3, if the UE also has a non-current full native 5G NAS security context, then this context shall become the new current security context. Consequently, if the UE in S1 mode moves to EMM-DEREGISTERED and 5GMM-DEREGISTERED, this native 5G NAS security context will be stored on the USIM or in the non-volatile memory of the UE. So it can be re-used during a future initial registration.  With this optimization, a new primary authentication procedure and NAS security mode control procedure can be avoided.  (Note: Currently, if the UE also has a non-current full native 5G NAS security context at inter-system change, then this context will **remain** a **non-current** security context. As a consequence, if the UE in S1 mode moves to EMM-DEREGISTERED and 5GMM-DEREGISTERED, this native 5G NAS security context will not be stored on the USIM or in the non-volatile memory of the UE, but will be deleted.) | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Add the requirement in bullet h) that if the UE also has a non-current full native 5G NAS security context, then this context shall become the new current security context. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | A UE in S1 mode will unnecessarily delete a non-current native 5G NAS security context when moving to EMM-/5GMM-DEREGISTERED. This will cause an unnecessary delay during a subsequent initial registration when the network performs a new 5G primary authentication and NAS security mode control procedure. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 4.4.2.1 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

### 4.4.2 Handling of 5G NAS security contexts

#### 4.4.2.1 General

The security parameters for authentication, integrity protection and ciphering are tied together in a 5G NAS security context and identified by a key set identifier (ngKSI). The relationship between the security parameters is defined in 3GPP TS 33.501 [24].

Before security can be activated, the AMF and the UE need to establish a 5G NAS security context. Usually, the 5G NAS security context is created as the result of a primary authentication and key agreement procedure between the AMF and the UE. A new 5G NAS security context may also be created during an N1 mode to N1 mode handover. Alternatively, during inter-system change from S1 mode to N1 mode, the AMF not supporting interworking without N26 and the UE operating in single-registration mode may derive a mapped 5G NAS security context from an EPS security context that has been established while the UE was in S1 mode.

The 5G NAS security context is taken into use by the UE and the AMF, when the AMF initiates a security mode control procedure, during an N1 mode to N1 mode handover, or during the inter-system change procedure from S1 mode to N1 mode. The 5G NAS security context which has been taken into use by the network most recently is called current 5G NAS security context. This current 5G NAS security context can be of type native or mapped, i.e. originating from a native 5G NAS security context or mapped 5G NAS security context.

The key set identifier ngKSI is assigned by the AMF either during the primary authentication and key agreement procedure or, for the mapped 5G NAS security context, during the inter-system change. The ngKSI consists of a value and a type of security context parameter indicating whether a 5G NAS security context is a native 5G NAS security context or a mapped 5G NAS security context. When the 5G NAS security context is a native 5G NAS security context, the ngKSI has the value of KSIAMF, and when the current 5G NAS security context is of type mapped, the ngKSI has the value of KSIASME.

The 5G NAS security context which is indicated by an ngKSI can be taken into use to establish the secure exchange of NAS messages when a new N1 NAS signalling connection is established without executing a new primary authentication and key agreement procedure (see subclause 5.4.1) or when the AMF initiates a security mode control procedure. For this purpose, the initial NAS messages (i.e. REGISTRATION REQUEST, DEREGISTRATION REQUEST, SERVICE REQUEST and CONTROL PLANE SERVICE REQUEST) and the SECURITY MODE COMMAND message contain an ngKSI in the ngKSI IE indicating the current 5G NAS security context used to integrity protect the NAS message.

In the present document, when the UE is required to delete an ngKSI, the UE shall set the ngKSI to the value "no key is available" and consider also the associated keys KAMF or K'AMF, 5G NAS ciphering key and 5G NAS integrity key invalid (i.e. the 5G NAS security context associated with the ngKSI as no longer valid). In the initial registration procedure, when the key KAUSF, is invalid, the UE shall delete the ngKSI.

NOTE: In some specifications the term ciphering key sequence number might be used instead of the term key set identifier (KSI).

As described in subclause 4.8 in order to interwork with E-UTRAN connected to EPC, the UE supporting both S1 mode and N1 mode can operate in either single-registration mode or dual-registration mode. A UE operating in dual-registration mode shall independently maintain and use both EPS security context (see 3GPP TS 24.301 [15]) and 5G NAS security context. When the UE operating in dual-registration mode performs an EPS attach procedure, it shall take into use an EPS security context and follow the handling of this security context as specified in 3GPP TS 24.301 [15]. However, when the UE operating in dual-registration mode performs an initial registration procedure, it shall take into use a 5G NAS security context and follow the handling of this security context as described in the present specification.

The UE and the AMF need to be able to maintain two 5G NAS security contexts simultaneously, i.e. a current 5G NAS security context and a non-current 5G NAS security context, since:

a) after a 5G re-authentication, the UE and the AMF can have both a current 5G NAS security context and a non-current 5G NAS security context which has not yet been taken into use (i.e. a partial native 5G NAS security context); and

b) after an inter-system change from S1 mode to N1 mode, the UE and the AMF can have both a mapped 5G NAS security context, which is the current 5G NAS security context, and a non-current native 5G NAS security context that was created during a previous access in N1 mode.

The number of 5G NAS security contexts that need to be maintained simultaneously by the UE and the AMF is limited by the following requirements:

a) after a successful 5G (re-)authentication, which creates a new partial native 5G NAS security context, the AMF and the UE shall delete the non-current 5G NAS security context, if any;

b) when a partial native 5G NAS security context is taken into use through a security mode control procedure, the AMF shall delete the previously current 5G NAS security context. If the UE does not support multiple records of NAS security context storage for multiple registration (see 3GPP TS 31.102 [22]), the UE shall delete the previously current 5G NAS security context. If the UE supports multiple records of NAS security context storage for multiple registration, the UE shall:

1) replace the previously current 5G NAS security context stored in the first 5G security context of that access (see 3GPP TS 31.102 [22]) with the new 5G security context (taken into use through a security mode control procedure), when the UE activates the new 5G security context for the same PLMN and access; or

2) store the previously current 5G NAS security context in the second 5G security context of that access (see 3GPP TS 31.102 [22]) and store the new 5G security context (taken into use through a security mode control procedure) in the first 5G security context, when the UE activates the new 5G security context for a different PLMN over that access but the previously current 5G NAS security context is associated with the 5G-GUTI of the other access;

c) when the AMF and the UE create a 5G NAS security context using "null integrity protection algorithm" and "null ciphering algorithm" during an initial registration procedure for emergency services, or a registration procedure for mobility and periodic registration update for a UE that has an emergency PDU session (see subclause 5.4.2.2), the AMF and the UE shall delete the previous current 5G NAS security context;

d) when a new mapped 5G NAS security context or 5G NAS security context created using "null integrity protection algorithm" and "null ciphering algorithm" is taken into use during the inter-system change from S1 mode to N1 mode, the AMF and the UE shall not delete the previously current native 5G NAS security context, if any. Instead, the previously current native 5G NAS security context shall become a non-current native 5G NAS security context, and the AMF and the UE shall delete any partial native 5G NAS security context;

If no previously current native 5G NAS security context exists, the AMF and the UE shall not delete the partial native 5G NAS security context, if any;

e) when the AMF and the UE derive a new mapped 5G NAS security context during inter-system change from S1 mode to N1 mode, the AMF and the UE shall delete any existing current mapped 5G NAS security context;

f) when a non-current full native 5G NAS security context is taken into use by a security mode control procedure, then the AMF and the UE shall delete the previously current mapped 5G NAS security context;

g) when the UE or the AMF moves from 5GMM-REGISTERED to 5GMM-DEREGISTERED state, if the current 5G NAS security context is a mapped 5G NAS security context and a non-current full native 5G NAS security context exists, then the non-current 5G NAS security context shall become the current 5G NAS security context. Furthermore, the UE and the AMF shall delete any mapped 5G NAS security context or partial native 5G NAS security context.

h) when the UE operating in single-registration mode in a network supporting N26 interface performs an inter-system change from N1 mode to S1 mode:

1) if the UE has a mapped 5G NAS security context and the inter-system change is performed in:

i) 5GMM-IDLE mode, the UE shall delete the mapped 5G NAS security context after the successful completion of the tracking area update procedure or attach procedure (see 3GPP TS 24.301 [15]); or

ii) 5GMM-CONNECTED mode, the UE shall delete the mapped 5G NAS security context after the completion of the inter-system change.

After deletion of the mapped 5G NAS security context, if the UE has a non-current full native 5G NAS security context, then the non-current full native 5G NAS security context shall become the current full native 5G NAS security context; and

i) when the UE operating in single-registration mode in a network supporting N26 interface performs an inter-system change from S1 mode to N1 mode in 5GMM-IDLE mode, if the UE has a non-current full native 5G NAS security context, then the UE shall make the non-current full native 5G NAS security context as the current native 5G NAS security context. The UE shall delete the mapped 5G NAS security context, if any.

If the UE is capable of registration over both 3GPP access and non-3GPP access, the UE in the state 5GMM-DEREGISTERED over both 3GPP access and non-3GPP access shall mark the 5G NAS security contexts of the 3GPP access and the non-3GPP access on the USIM or in the non-volatile memory as invalid when the UE initiates an initial registration procedure over either 3GPP access or non-3GPP access as described in subclause 5.5.1.2 or when the UE leaves state 5GMM-DEREGISTERED for any other state except 5GMM-NULL over either 3GPP access or non-3GPP access. Otherwise, the UE shall mark the 5G NAS security context on the USIM or in the non-volatile memory as invalid when the UE initiates an initial registration procedure as described in subclause 5.5.1.2 or when the UE leaves state 5GMM-DEREGISTERED for any other state except 5GMM-NULL.

If the UE is capable of registration over both 3GPP access and non-3GPP access, the UE shall store the current native 5G NAS security contexts of the 3GPP access and the non-3GPP access as specified in annex C and mark them as valid only when the UE enters state 5GMM-DEREGISTERED from any other state except 5GMM-NULL over both the 3GPP access and non-3GPP access or only when the UE aborts the initial registration procedure without having left 5GMM-DEREGISTERED over both the 3GPP access and non-3GPP access. Otherwise, the UE shall store the current native 5G NAS security context as specified in annex C and mark it as valid only when the UE enters state 5GMM-DEREGISTERED from any other state except 5GMM-NULL or when the UE aborts the initial registration procedure without having left 5GMM-DEREGISTERED.