**3GPP TSG-SA3 Meeting #101-e *S3-202889***

**E-meeting, 09 - 20 November 2020** Revision of S3-xxxxxx

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** | 961 | **rev** |  | **Current version:** | 16.4.0 |  |
|  | | | | | | | | |
| *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 | **X** | ME | **X** | Radio Access Network |  | Core Network | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Storage of 5G security context for each access type during multiple PLMN registration | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell, | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | TEI-16 | | | | |  | ***Date:*** | | | 10-26-2020 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | F |  | | | | | ***Release:*** | | | Rel-16 |
|  | *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-12 (Release 12)* *Rel-13 (Release 13) Rel-14 (Release 14) Rel-15 (Release 15) Rel-16 (Release 16)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | 1) TS 33.501 clause ‘6.4.2.1 Multiple active NAS connections with different PLMNs’ it is not explicitly clear that when the UE registers in two PLMNs, UE shall store full 5G parameter storage for 3GPP and non-3GPP access types per PLMN. Without such a storage of the full 5G parameters, in different mobility scenarios of the UE, mix up of NAS COUNTS are possible between the PLMNs and their corresponding access types.  2) Because of the lack of explicit text in TS 33.501, the parameter storage file description in TS 31.102 clause 4.4.11.4 EF5GS3GPPNSC (5GS 3GPP Access NAS Security Context) and clause 4.4.11.5 EF5GSN3GPPNSC (5GS non-3GPP Access NAS Security Context) is organized per access type only. This misses the full context storage for both access types per PLMN.  Therefore, in rare corner cases, i.e. when UE is attached to two PLMNs over different access types, then switches off, back on, and then tries to reattach to the same PLMN reusing the security context stored on UICC, there is a risk of a NAS replay attack over the air towards the UE. This risk is considered low enough to not warrant backporting into R15.  Please note that there are no new requirements added here, but clarifying existing requirements. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Add an explicit requirement in TS 33.501 clause 6.4.2.1 to say that “The 5G security context maintained by the UE shall contain full set of 5G parameters, including NAS context parameters for 3GPP and non-3GPP access types per PLMN “  Clarification in 6.3.2.2 Multiple registrations in the same PLMN The AMF and the UE shall also parameters specific to each NAS connection in the common NAS security context including two sets of NAS COUNTs for each access (i.e. 3GPP access and non-3GPP access)  3) Typos in 6.3.2.1, 6.3.2.2, 6.4.2.1, 6.4.2.2 | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Unclear specifications resulting in gap between TS 33.501 and CT6 TS 31.102, wrong UE behavior during inter PLMN mobility. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 6.3.2.1, 6.3.2.2, 6.4.2.1, 6.4.2.2 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 second Change \*\*\*\*\*\***

6.3 Security contexts

6.3.1 Distribution of security contexts

6.3.1.1 General

The present clause focuses on the security contexts themselves; the handling of security contexts in mobility procedures is described in clause 6.9.

6.3.1.2 Distribution of subscriber identities and security data within one 5G serving network domain

The transmission of the following subscriber identities and security data is permitted between 5G core network entities of the same serving network domain:

- SUPI in the clear

- 5G security contexts, as described in clause 6.9

A 5G authentication vector shall not be transmitted between SEAFs.

Once the subscriber identities and security data have been transmitted from an old to a new network entity the old network entity shall delete the data.

6.3.1.3 Distribution of subscriber identities and security data between 5G serving network domains

The transmission of the following subscriber identities and security data is permitted between 5G core network entities of different serving network domains:

- SUPI in the clear

- 5G security contexts, as described in clause 6.9, if the security policy of the transmitting 5G serving network domain allows this.

A 5G authentication vector or non-current 5G security contexts shall not be transmitted to a different 5G serving network domain.

6.3.1.4 Distribution of subscriber identities and security data between 5G and EPS serving network domains

NOTE 1: No direct interworking between 5G networks and network of generations prior to EPS are foreseen. Therefore, only the interaction between 5G and EPS serving network domains is addressed here.

The transmission of the SUPI in the clear is permitted between 5G and EPS core network entities if it has the form of an IMSI.

The transmission of any unmodified 5G security contexts to a EPS core network entity is not permitted. Details of security context transfer between EPS and 5G core network entities can be found in clause 8.

The transmission of a 5G authentication vector to an EPS core network entity is not permitted. The transmission of any unused EPS authentication vectors to a 5G core network entity is not permitted. If SEAF receives any unused authentication vectors (e.g. in mobility scenarios from legacy MME) they shall be dropped without any processing.

NOTE 2: The rules above differ from the corresponding rules in 3GPP TS 33.401, clause 6.1.6: The latter allows forwarding of UMTS authentication vectors from an SGSN to an MME and back to the same SGSN under certain conditions. But this feature goes against a strict security separation of EPS and 5G domains. As its performance advantage is questionable it was not copied into 5G.

NOTE 3: Security context mapping between EPS and 5G serving networks is allowed, according to clause 8.

6.3.2 Multiple registrations in same or different serving networks

6.3.2.0 General

There are two cases where the UE can be multiple registered in different PLMN's serving networks or in the same PLMN's serving networks. The first case is when the UE is registered in one PLMN serving network over a certain type of access (e.g. 3GPP) and is registered to another PLMN serving network over the other type of access (e.g. non-3GPP). The second case is where the UE is registered in the same AMF in the same PLMN serving network over both 3GPP and non-3GPP accesses. The UE will establish two NAS connections with the network in both cases.

NOTE: The UE uses the same subscription credential(s) for multiple registrations in the same or different serving networks.

6.3.2.1 Multiple registrations in different PLMNs

The UE shall independently maintain and use two different 5G security contexts, one per PLMN's serving network. Each security context shall be established separately via a successful primary authentication procedure with the Home PLMN.

The ME shall store the two different 5G security contexts on the USIM if the USIM supports the 5G parameters storage. If the USIM does not support the 5G parameters storage, then the ME shall store the two different 5G security contexts in the ME non-volatile memory. Both of the two different 5G security contexts are current 5G security context.

6.3.2.2 Multiple registrations in the same PLMN

When the UE is registered in the same AMF in the same PLMN serving network over both 3GPP and non-3GPP accesses, the UE shall establish two NAS connections with the network. Upon receiving the registration request message, the AMF should check whether the UE is authenticated by the network. The AMF may decide to skip a new authentication run in case there is an available 5G security context for this UE by means of 5G-GUTI, e.g. when the UE successfully registered to 3GPP access.

If the UE registers to the same AMF via non-3GPP access, the AMF can decide not to run a new authentication if it has an available security context to use. In this case, the UE shall directly take into use the available common 5G NAS security context and use it to protect the registration over the non-3GPP access. If there are stored NAS counts for the non-3GPP access for the PLMN in the UE, then the stored NAS counts for the non-3GPP access for the PLMN shall be used to protect the registration over the non-3GPP access. Otherwise, the common 5G NAS security context is taken into use for the first time (partial) over non-3GPP access. In this case, the UL NAS COUNT value and DL NAS COUNT value for the non-3GPP access needs to be set to zero by the UE before the UE is taking the 5G NAS security context into use over non 3GPP access.

The AMF and the UE shall establish a common NAS security context consisting of a single set of NAS keys and algorithm at the time of first registration over any access. The AMF and the UE shall also store parameters specific to each NAS connection in the common NAS security context including two pairs of NAS COUNTs for each access (i.e. 3GPP access and non-3GPP access). The connection specific parameters are specified in clause 6.4.2.2 of the present document.

## 6.4 NAS security mechanisms

### 6.4.1 General

This sub-clause describes the security mechanisms for the protection of NAS signalling and data between the UE and the AMF over the N1 reference point. This protection involves both integrity and confidentiality protection. The security parameters for NAS protection are part of the 5G security context described in sub-clause 6.3 of the present document.

### 6.4.2 Security for multiple NAS connections

#### 6.4.2.1 Multiple active NAS connections with different PLMNs

TS 23.501 [2] has a scenario when the UE is registered to a VPLMN's serving network via 3GPP access and to another VPLMN's or HPLMN's serving network via non-3GPP access at the same time. When the UE is registered in one PLMN's serving network over a certain type of access (e.g. 3GPP) and is registered to another PLMN's serving network over another type of access (e.g. non-3GPP), then the UE has two active NAS connections with different AMF's in different PLMNs. As described in clause 6.3.2.1, the UE shall independently maintain and use two different 5G security contexts, one per PLMN serving network. The 5G security context maintained by the UE shall contain the full set of 5G parameters, including NAS context parameters for 3GPP and non-3GPP access types per PLMN. In case of connection to two different PLMNs, it is necessary to maintain a complete 5G NAS security context for each PLMNs independently, each with all associated parameters (such as two pairs of NAS COUNTs, i.e. one pair for 3GPP access and one pair for non-3GPP access).  Each security context shall be established separately via a successful primary authentication procedure with the Home PLMN. All the NAS and AS security mechanisms defined for single registration mode are applicable independently on each access using the corresponding 5G security context.

NOTE: The UE belongs to a single HPLMN.

#### 6.4.2.2 Multiple active NAS connections in the same PLMN's serving network

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.

In order to realize cryptographic separation and replay protection, the common NAS security-context shall have parameters specific to each NAS connection. The connection specific parameters include a pair of NAS COUNTs for uplink and downlink and unique NAS connection identifier. The value of the unique NAS connection identifier shall be set to "0x01" for 3GPP access and set to "0x02" for non-3GPP access. All other parameters as e.g. algorithm identifiers in the common NAS security context are common to multiple NAS connections.

In non-mobility cases, when the UE is simultaneously registered over both types of accesses, and if NAS key re-keying as described in clause 6.9.4.2 or if NAS key refresh as described in clause 6.9.4.3 takes place over one of the accesses (say access A):

1) If the other access (access B) is in CM-CONNECTED state, then the new NAS security context shall only be activated over that access (access A). The UE and the AMF shall not change the NAS security context in use on the other access (say access B). In order to activate the new NAS security context over the other access (access B), the AMF shall trigger a NAS SMC run over that access either in the current running procedure or a subsequent NAS procedure. During the second NAS SMC run (on access B), the AMF shall include the same ngKSI associated with the new NAS security context and the same algorithm choices as for the first access. After a successful second NAS SMC procedure over the other access (access B), both the UE and the AMF shall delete the old NAS security context.

2) Whenever the AMF sends a NAS SMC over access (access A) and AMF considers the UE to not be in CM-CONNECTED state on the other access (access B), the AMF shall additionally activate (if not already in use on the other access) the security context that is active on the other accesses. Similarly, whenever the UE receives a NAS SMC over the access (access A) and UE is not in CM-CONNECTED state on the other access (access B), the UE additionally activates (if not already in use on the other access) the security context on the other access.

In case of 3GPP access mobility or interworking with EPS, the following procedures apply:

1) If the UE is in CM-CONNECTED state on the non-3GPP access, then:

a) if the AMF does not have the security context the UE is using on the non-3GPP access (e.g. KAMF change on 3GPP access when the AMF changes), then in order to activate the same NAS security context that is in use over the 3GPP access the AMF shall run a NAS SMC procedure on the non-3GPP access; or

b) in the case of handover from EPS, then a mapped context will be in use on the 3GPP access and a different security context will be active on the non-3GPP access. To align the security contexts in use over both accesses, the AMF shall run a NAS SMC procedure over one access to take into use on that access the security context that is in use on the other access. In the case that a native security context is in use on the non-3GPP access, then the NAS SMC procedure shall be on the 3GPP access to take the native security context into use.

2) Whenever the AMF sends a Registration Accept over the 3GPP access and AMF considers the UE to not be in CM-CONNECTED state on the non-3GPP access, the AMF shall activate (if not already in use on the non-3GPP access) the security context that is in use on the 3GPP access on the non-3GPP access. The AMF shall keep a native security context that was in use on non-3GPP access if the security context in use on the 3GPP access is a mapped security context. In order to take this native security context into use, the AMF shall run a NAS SMC procedure.

Similarly, whenever the UE receives a Registration Accept over the 3GPP access and UE is not in CM-CONNECTED state on the non-3GPP access, the UE activates (if not already in use on the non-3GPP access) the security context that is in use on the 3GPP access on the non-3GPP access. The UE shall keep a native security context that was in use on non-3GPP access if the security context in use on the 3GPP access is a mapped security context.

To recover from a failure to align the NAS security contexts due to a state mis-match between AMF and UE, the AMF can align the security contexts in use on the 3GPP and non-3GPP access using the a NAS SMC procedure during a subsequent registration procedure (that was either initiated by the UE or sent in response to a Service Reject if the UE sends a Service Request).

**\*\*\*\* END of CHANGE \*\*\*\***