**3GPP TSG-SA3 Meeting #106-e *S3-220415-r3***

**e-meeting, 14 - 25 February 2022**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.501** | **CR** | 1345 | **rev** | **1** | **Current version:** | 17.4.2 |  |
|  | | | | | | | | |
| *For* [***HE***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)***LP*** *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:*** | CR to 33.501 to protect additional SoR information (CPSOR-CMCI) (future proof alternative) | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | NTT DOCOMO | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | eCPSOR\_CON | | | | |  | ***Date:*** | | | 2022-02-07 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | C |  | | | | | ***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:*** | | In TS 23.122 Annex C, additional optional parameters were introduced in the SOR information, namely the SOR-CMCI and the "Store the SOR-CMCI in the ME" indicator. This information needs to be protected as well. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | This CR implements CT4's recommendation, i.e. a mechanism to protect all octets located after the "PLMN ID and access technology list" in Figure 9.11.3.51.2A of TS 24.501. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Unprotected information elements. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 6.14.2.1, 6.14.2.2, A.17 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | | Implementing CT1's request, alternative implementing non-future proof version is in S3-220416 | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | |  | | | | | | | | |

++++++++++++++++++++++++++++++++ Begin Changes ++++++++++++++++++++++++++++++

#### 6.14.2.1 Procedure for steering of UE in VPLMN during registration

The security procedure for the case where the UE registers with VPLMN AMF is described below in figure 6.14.2.1-1:



Figure 6.14.2.1-1: Procedure for providing list of preferred PLMN/access technology combinations during registration in VPLMN

1) The UE initiates registration by sending Registration Request message to the VPLMN AMF.

2-3) The VPLMN AMF executes the registration procedure as defined in sub-clause 4.2.2.2.2 of 3GPP TS 23.502 [8]. As part of the registration procedure, the VPLMN AMF executes primary authentication of the UE and then initiates the NAS SMC procedure, after the authentication is successful.

4-5) The VPLMN AMF invokes the Nudm\_UECM\_Registration message to the UDM and registers access with the UDM as per step 14a in sub-clause 4.2.2.2.2 of 3GPP TS 23.502[8].

6) The VPLMN AMF invokes Nudm\_SDM\_Get service operation message to the UDM to get amongst other information the Access and Mobility Subscription data for the UE (see step 14b in sub-clause 4.2.2.2.2 of 3GPP TS 23.502 [8]).

7) The UDM decides to send the Steering of Roaming Information, and obtains a list of preferred PLMN/access technology combinations and optional additional SoR information (e.g. SOR-CMCI and the "Store the SOR-CMCI in the ME" indicator) , or a secured packet list as described in TS 23.122 [53].

NOTE X: Additional SoR information (e.g. SOR-CMCI and the "Store the SOR-CMCI in the ME" indicator) can only be added when the AMF supports SoR transparent container.

If the UDM determines that the UE is configured to not expect to receive Steering of Roaming Information at initial registration and if the UDM determines that no change of the "Operator Controlled PLMN Selector with Access Technology" list or additional SoR information , stored in the UE is needed, then the UDM may not piggyback Steering of Roaming Information at all in the Nudm\_SDM\_Get response and hence the following steps are omitted.

8-9) The UDM shall invoke Nausf\_SoRProtection service operation message to the AUSF to get SoR-MAC-IAUSF and CounterSoR as specified in sub-clause 14.1.3 of this document. The UDM shall select the AUSF that holds the latest KAUSF of the UE.

If the HPLMN decides that the UE is to acknowledge the successful security check of the received Steering of Roaming Information, then the UDM shall set accordingly the ACK Indication included in the Nausf\_SoRProtection service operation message to signal that it also needs the expected SoR-XMAC-IUE, as specified in sub-clause 14.1.3 of this document.

NOTE Y: At reception of Nausf\_SoRProtection\_Protect request from the UDM, if the SoR header is not included in the request, the AUSF constructs the SOR header, as described in clause 9.11.3.51 of TS 24.501 [35], based on the information received from the UDM, i.e. ACK Indication and list of preferred PLMN/access technology combinations or secured packet (if provided); otherwise, if the SoR header is contained in the request, the AUSF uses the received SoR header in the calculation of SoR-MAC-IAUSF..

The details of the CounterSoR are specified in sub-clause 6.14.2.3 of this document. The inclusion of the Steering List and the SoR header in the calculation of SoR-MAC-IAUSF allows the UE to verify that the received Steering of Roaming Information is not tampered with or removed by the VPLMN. The expected SoR-XMAC-IUE allows the UDM to verify that the UE received the Steering of Roaming Information.

10) The UDM responds to the Nudm\_SDM\_Get service operation to the VPLMN AMF, which shall include the SoR transparent container as specified in clause 6.1.6.3.2 of TS 29.503 [93] if the VPLMN AMF support SoR transparent container, or shall include individual IEs comprising the ACK Indication, the list of preferred PLMN/access technology combinations or secured packet (if provided), SoR-MAC-IAUSF and CounterSoR within the Access and Mobility Subscription data. If the UDM requests an acknowledgement, it shall temporarily store the expected SoR-XMAC-IUE.

11) If the SoR transparent container is received from the UDM, the VPLMN AMF shall include the received SoR transparent container in the Registration Accept message and send it to the UE. If the individual IEs are received from the UDM, the VPLMN AMF shall construct the SOR header based on the ACK Indication and the list of preferred PLMN/access technology combinations or secured packet (if provided) received from the UDM and include it in the SOR transparent container as specified in clause 9.11.3.51 of TS 24.501 [35]. The vPLMN shall also include SoR-MAC-IAUSFand CounterSoR(both also received from the UDM) in the constructed SoR transparent container, and convey the constructed SoR transparent container to the UE in the Registration Accept message.

12) On receiving the Registration Accept message with the SoR transparent container from the AMF the UE shall calculate the SoR-MAC-IAUSF in the same way as the AUSF (as specified in Annex A.17) on the SoR transparent container, including the CounterSoR and the SoR header, and verifies whether it matches the SoR-MAC-IAUSF value received in the Registration Accept message. Based on the SoR-MAC-IAUSF verification outcome, the behaviour of the UE is specified in TS 23.122 [53].

13) If the UDM has requested an acknowledgement from the UE and the UE verified that the SoR transparent container received in step 12 has been provided by the HPLMN, then the UE shall send the Registration Complete message to the serving AMF. The UE shall generate the SoR-MAC-IUE as specified in Annex A.18 and includes the generated SoR-MAC-IUE in a SOR transparent container in the Registration Complete message.

14) The AMF sends a Nudm\_SDM\_Info request message to the UDM. If a transparent container with the SoR-MAC-IUE was received in the Registration Complete message, then if the AMF supports SoR transparent container, the AMF shall include the received SoR transparent container in SoR transparent container in the Nudm\_SDM\_Info request message, otherwise, the AMF shall include the SoR-MAC-IUE  in the received SoR transparent container in the Nudm\_SDM\_Info request message.

15) If the HPLMN indicated that the UE is to acknowledge the successful security check of the received Steering of Roaming Information in step 10, then the UDM shall compare the received SoR-MAC-IUE with the expected SoR-XMAC-IUE that the UDM stored temporarily in step 10.

### 

++++++++++++++++++++++++++++++++ Next Change ++++++++++++++++++++++++++++++

#### 6.14.2.2 Procedure for steering of UE in VPLMN or HPLMN after registration

The security procedure for the steering of UE in VPLMN after registration is described below in figure 6.14.2.2-1:



Figure 6.14.2.2-1: Procedure for providing list of preferred PLMN/access technology combinations after registration

1) The UDM decides to notify the UE of the changes to the Steering of Roaming Information by the means of invoking Nudm\_SDM\_Notification service operation.

2-3) The UDM shall invoke Nausf\_SoRProtection service operation message by including the ACK Indication and optionally the list of preferred PLMN/access technology combinations or secured packet or SoR transparent container (only if transparent container is supported by the AMF) to the AUSF to get SoR-MAC-IAUSF and CounterSoR as specified in sub-clause 14.1.3 of this document. The UDM shall select the AUSF that holds the latest KAUSF of the UE.

If the HPLMN decided that the UE is to acknowledge the successful security check of the received Steering of Roaming Information, then the UDM shall set accordingly the ACK Indication included in the Nausf\_SoRProtection service operation message to signal that it also needs the expected SoR-XMAC-IUE, as specified in sub-clause 14.1.3 of this document.

NOTE: At reception of Nausf\_SoRProtection\_Protect request from the UDM, if the SoR header is not included in the request, the AUSF constructs the SOR header, as described in clause 9.11.3.51 of TS 24.501 [35], based on the information received from the UDM, i.e. ACK Indication, optionally the list of preferred PLMN/access technology combinationsor secured packet; otherwise, if the SoR header in contained in the request, the AUSF uses the received SoR header in the calculation of SoR-MAC-IAUSF..

The details of the CounterSoR are specified in sub-clause 6.14.2.3 of this document. The inclusion of the Steering List and the SOR header in the calculation of SoR-MAC-IAUSF allows the UE to verify that the Steering of Roaming Information received is not tampered with or removed by the VPLMN. The inclusion of these information in the calculation of the expected SoR-XMAC-IUE allows the UDM to verify that the UE received the Steering of Roaming Information.

4) The UDM shall invoke Nudm\_SDM\_Notification service operation, which contains the SoR transaprent container as specified in clause 6.1.6.3.2 of TS 29.503 [93] if the VPMN AMF support SOR transparent container, or contains individual IEs including an optional the list of preferred PLMN/access technology combinations or secured packet, the ACK Indication, SoR-MAC-IAUSF, and CounterSoR within the Access and Mobility Subscription data. If the UDM requests an acknowledgement, it shall temporarily store the expected SoR-XMAC-IUE.

5) Upon receiving the Nudm\_SDM\_Notification message, if the SoR transparent container is included in the message, the AMF shall send a DL NAS Transport message to the served UE. including the received SoR transparent container; otherwise, the AMF shallconstruct the SOR transparent container (including the SOR header) as specified in clause 9.11.3.51 of 3GPP TS 24.501 [35] based on the ACK Indication, the Steering List, SoR-MAC-IAUSF and CounterSoR received from the UDM, and send the constructed SoR transparent container included to the served UE in a DL NAS Transport message.

6) On receiving the DL NAS Transport message, the UE shall calculate the SoR-MAC-IAUSF in the same way as the AUSF (as specified in Annex A.17) on the received SoR transparent container, including the CounterSoR and the SoR header and verify whether it matches the SoR-MAC-IAUSF value received in the DL NAS Transport message.

7) If the UDM has requested an acknowledgement from the UE and the UE verified that the Steering Information has been provided by the HPLMN, then the UE shall send the UL NAS Transport message to the serving AMF. The UE shall generate the SoR-MAC-IUE as specified in Annex A.18 and includes the generated SoR-MAC-IUE in a SOR transparent container in the UL NAS Transport message.

8) The AMF shall send a Nudm\_SDM\_Info request message to the UDM. If a SOR transparent container with the SoR-MAC-IUE was received in the UL NAS Transport message, the AMF shall include the received SoR transparent container in the Nudm\_SDM\_Info request message if the AMF supports SoR transparent container, otherwise, the AMF shall include the SoR-MAC-IUE in the Nudm\_SDM\_Info request message.

9) If the HPLMN indicated that the UE is to acknowledge the successful security check of the received Steering of Roaming Information, then the UDM shall compare the received SoR-MAC-IUE with the expected SoR-XMAC-IUE that the UDM stored temporarily in step 4.

++++++++++++++++++++++++++++++++ Next Change ++++++++++++++++++++++++++++++

### 14.1.3 Nausf\_SoRProtection service

The following table illustrates the security related services for SoR that AUSF provides.

Table 14.1.3-1: NF services for SoR provided by AUSF

|  |  |  |  |
| --- | --- | --- | --- |
| Service Name | Service Operations | Operation Semantics | Example Consumer(s) |
| Nausf\_SoRProtection | Protect | Request/Response | UDM |

**Service operation name:** Nausf\_SoRProtection.

**Description:** The AUSF calculates the SoR-MAC-IAUSF as specified in the Annex A.17 of this document using UE specific home key (KAUSF), the Steering Information List and ACK Indication received from the requester NF and delivers the SoR-MAC-IAUSF and CounterSoR to the requester NF. If the ACK Indication input is set to indicate that the acknowledgement is requested, then the AUSF shall compute the SoR-XMAC-IUE and return it in the response.

NOTE: At reception of Nausf\_SoRProtection\_Protect request from the UDM, the AUSF constructs the SOR header, as described in clause 9.11.3.51 of TS 24.501 [35], based on the information received from the requester NF, i.e. ACK Indication and list of preferred PLMN/access technology combinations or a secured packet (if provided).

**Input, Required:** Requester ID, SUPI, service name, ACK Indication.

**Input, Optional:** list of preferred PLMN/access technology combinations or secured packet or SoR transparent container.

**Output, Required:** SoR-MAC-IAUSF, CounterSoR or error (counter\_wrap).

**Output, Optional:** SoR-XMAC-IUE (if the ACK Indication input is set to indicate that the acknowledgement is requested, then the SoR-XMAC-IUE shall be computed and returned).

++++++++++++++++++++++++++++++++ Next Change ++++++++++++++++++++++++++++++

# A.17 SoR-MAC-IAUSF generation function

When deriving a SoR-MAC-IAUSF from KAUSF, the following parameters shall be used to form the input S to the KDF.

- FC = 0x77,

- P0 = SoR header,

- L0 = length of SoR header,

- P1 = CounterSoR,

- L1 = length of CounterSoR,

- P2 = list of preferred PLMN/access technology combinations or secured packet or SoR transparent container,

- L2 = length of list data included in P2

-

The input key KEY shall be KAUSF.

The selection of parameters included in P2 (list of preferred PLMN/access technology combinations or secured packet parameter or SoR Transparent container) shall be the same as the selection of input to the Nausf\_SoRProtection service operation. If none of these parameters are included in Nausf\_SoRProtection service operation, P2 and L2 are not included for SoR-MAC-IAUSF generation.

The SOR header is either received from the requester NF (e.g UDM), or constructed by the AUSF, as described in clause 9.11.3.51 of TS 24.501 [35], based on the information received from the requester NF (e.g. UDM), i.e. ACK Indication and List of preferred PLMN/access technology combinations or secured packet (if provided).

The SoR-MAC-IAUSF is identified with the 128 least significant bits of the output of the KDF.

++++++++++++++++++++++++++ End of Changes ++++++++++++++++++++++++++++++