**3GPP TSG-SA3 Meeting #100e *S3-202050-r1***

**e-meeting, 17 – 21 August 2020**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** | **0944** | **rev** | 1 | **Current version:** |  |  |
|  | | | | | | | | |
| *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 |  | Radio Access Network |  | Core Network | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Clarifications to SoR integrity protection mechanism | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Orange, Ericsson, Samsung | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | 5GS\_Ph1-SEC | | | | |  | ***Date:*** | | | 28 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | A |  | | | | | ***Release:*** | | | 6 |
|  | *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:*** | | There are currently some misalignments between stage 2 and stage 3 specifications with regards to SoR integrity protection mechanism:   * CT4 specified in 3GPP°TS°29.509 the input parameters to the Nausf\_SoRProtection\_Protect procedure as composed of the ACK indication (Mandatory) attribute and the steeringContainer (Conditional) attribute (i.e. "Steering List" to reuse the wording of TS°33.501). It does not specify the SOR header as an input parameter. Therefore, TS°33.501 should be updated accordingly to align with what was defined in stage 3. It is worth noting that changing stage 3 specifications to align with stage 2 would generate backwards incompatible changes, not only to Rel-16 but also to Rel-15 specifications, which is to be avoided. * This also means that it is the AUSF that should construct the SOR header, as specified in TS°24.501 and based on the information provided by the UDM (i.e. ACK indication, format of the steeringContainer / Steering List to determine whether it contains a secured packet or a list of preferred PLMN/access technology combinations), before applying integrity protection measures. The UDM does not perform this task. * Idem for the interaction between the UDM and the AMF, i.e. it is the AMF that should construct the SOR header, as specified in TS°24.501 and based on the information provided by the UDM, that goes into the SOR transparent container. * Clarification of the meaning of the wordings "Steering List" and “Steering of Roaming Information” to align with TS°23.122. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | The proposed changes are summarized hereinafter:   * Clarify the input parameters to the Nausf\_SoRProtection service operation as explained above. Clarify accordingly the description text and the figures in clauses 6.14.1, 6.14.2, 14.1.3, A.17 and A.18. * Clarify the role of each NF with regards to the SoR integrity protection mechanism. Add a NOTE to indicate that it is the AUSF that constructs the SOR header as specified in TS°24.501 and based on the information provided by the UDM. Idem for the UDM – AMF interaction. * Add clarification text and a NOTE to clarif the meanings of the wordings "Steering List" and "SoR Information" in order to avoid any confusions and align with CT1 specifications. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Misalignements between the various stage 2 and stage 3 specifications related to 5G SoR. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 6.14.1, 6.14.2.1, 6.14.2.2, 14.1.3, Annex A.17, Annex A.18 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | | Rev 1: Merged with S3-201920, S3-201976 | | | | | | | | |

\* \* \* First Change \* \* \* \*

6.14 Steering of roaming security mechanism

6.14.1 General

This clause describes the security functions necessary to support steering of the UE in the VPLMN during registration procedure and also after registration as described in TS 23.122 [53] Annex C. The security functions are described in the context of the functions supporting the control plane solution for steering of roaming in 5GS.

If the control plane solution for Steering of Roaming is supported by the HPLMN, the AUSF shall store the KAUSF after the completion of the primary authentication.

The content of the Steering List as well as the conditions for sending it to the UE are described in TS 23.122 [53] Annex C. The Steering List includes either a list of preferred PLMN/access technology combinations, a secured packet or the HPLMN indication that 'no change of the "Operator Controlled PLMN Selector with Access Technology" list stored in the UE is needed and thus no list of preferred PLMN/access technology combinations is provided'.

NOTE: The Steering of Roaming Information is defined in clause 1.2 of 3GPP TS 23.122 [53]. It contains thus the ACK indication, the Steering List and the integrity protection information.

\* \* \* Next Change \* \* \* \*

6.14.2 Security mechanisms

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 or a secured packet as described in TS 23.122 [53].

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 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. 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: At reception of Nausf\_SoRProtection\_Protect request from the UDM, the AUSF shall construct the SOR header, as described in clause 9.11.3.51 of 3GPP 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).

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 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) 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 3GPP TS 24.501 [35]. The resulting Steering of Roaming Information, also including SoR-MAC-IAUSFand CounterSoR (both also received from the UDM), is conveyed to the UE in the Registration Accept message;

12) On receiving the Registration Accept message with Steering of Roaming Information the UE shall calculate the SoR-MAC-IAUSF in the same way as the AUSF (as specified in Annex A.17) on the received Steering of Roaming Information, 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 3GPP TS 23.122 [53].

13) If the UDM has requested an acknowledgement from the UE and the UE verified that the Steering of Roaming Information received in step 11 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, the AMF shall include the SoR-MAC-IUEin 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.

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 packetto the AUSF to get SoR-MAC-IAUSF and CounterSoR as specified in sub-clause 14.1.3 of this document. 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 accodingly 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, the AUSF shall construct the SOR header, as described in clause 9.11.3.51 of 3GPP TS 24.501 [35], based on the information received from the UDM, i.e. ACK Indication and optionally the list of preferred PLMN/access technology combinations or secured packet.

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 optionally 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, the AMF shall send a DL NAS Transport message to the served UE. The AMF shall include in the DL NAS Transport message the SOR transparent container (including the SOR header) constructed 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.

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 Steering of Roaming Information, 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 of Roaming 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 include 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 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 shall construct the SOR header, as described in clause 9.11.3.51 of 3GPP 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.

**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,

- L2 = length of list of preferred PLMN/access technology combinations or secured packet.

The input key KEY shall be KAUSF.

List of preferred PLMN/access technology combinations or secured packet parameter is included for SoR-MAC-IAUSF generation only if it is included in the Nausf\_SoRProtection service operation message, otherwise P2 and L2 are not included.

The SOR header is constructed by the AUSF, as described in clause 9.11.3.51 of 3GPP 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.

\* \* \* Next Change \* \* \* \*

A.18 SoR-MAC-IUE generation function

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

- FC = 0x78,

- P0 = 0x01 (SoR Acknowledgement: Verified the Steering of Roaming Information successfully),

- L0 = length of SoR Acknowledgement (i.e. 0x00 0x01),

- P1 = CounterSoR,

- L1 = length of CounterSoR.

The input key KEY shall be KAUSF.

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

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