**3GPP TSG-SA3 Meeting #104-e *S3-212738***

**e-meeting, 16 – 27 August 2021**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **33.501** | **CR** | **1173** | **rev** | **-** | **Current version:** | **17.2.1** |  |
|  |
| *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 | **X** |

|  |
| --- |
|  |
| ***Title:***  | Protection of “ME support of SOR-CMCI” indication |
|  |  |
| ***Source to WG:*** | Ericsson |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | TEI17 |  | ***Date:*** | 2021-08-09 |
|  |  |  |  |  |
| ***Category:*** |  B |  | ***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:*** | In LS from CT1 [S3-211440](https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_103e/Docs/S3-211440.zip), SA3 is informed that CT1 defined the need for the UE to include additional fields (i.e. "ME support of SOR-CMCI") in SOR transparent container carrying SOR acknowledgement between the UE and the HN and asks SA3 whether it is required to integrity protect this information and if so make the necessary updates in the security mechanism to allow that. DP S3-213736 justifies the need for protection of this type of information provided by the UE in the context of SoR and UPU procedures and recommends that the “ME support of SOR-CMCI” indicator is used as input for the generation of the SoR-MAC-Iue.  |
|  |  |
| ***Summary of change:*** | “ME support of SOR-CMCI” indicator is used as input for the generation of the SoR-MAC-Iue.This requires the UDM to request a new SoR-MAC-Iue to the AUSF over a new service operation with AUSF.  |
|  |  |
| ***Consequences if not approved:*** | “ME support of SOR-CMCI” is not integrity protected over SoR acknowledgement responses. AMF can tamper of discard the “ME support of SOR-CMCI” in SoR acknowledgement responses. |
|  |  |
| ***Clauses affected:*** | 6.14; 14.1.3; 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:*** |  |

\*\*\*\*\* 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 latest KAUSF after the completion of the latest 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 TS 23.122 [53]. It contains thus the ACK indication, the Steering List, the “ME support of SOR-CMCI” indication and the integrity protection information.

### 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 list 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. 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.

If the HPLMN decides that the UE is to send a SoR-CMCI indicator, and if the AMF has support for transparent container, then the UDM that supports the SoR-CMCI feature shall set accordingly the SoR-CMCI Indication included in the Nausf\_SoRProtection service operation message to be able to include this value in the generation of the SoR-MAC\_IUE.

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 UDM, i.e. ACK Indication and list of preferred PLMN/access technology combinations or secured packet (if provided) and SoR-CMCI indication.

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 and the received CounterSOR.

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-IAUSF and 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. If a SoR-CMCI indicator was received and the UE supports the SOR-CMCI feature, the UE shall set the "ME support of SOR-CMCI" indicator in the header of the SOR transparent container and shall generate the SoR-MAC-IUE\_Data as specified in Annex A.XX and include the generated SoR-MAC-IUE\_Data in a SOR transparent container in the Registration Complete message. If no SoR-CMCI indicator was received, the UE shall generate the MAC-IUE as specified in Annex A.18 and include it 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 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.

NOTE: In step 8-9 above the UDM needs to verify that AMF has support for transparent container before sending the SoR-CMCI indication to the UE to avoid that transparent container with MAC-IUE\_Data is lost.

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, and the "ME support of SOR-CMCI" indicator in the header of the SOR transparent container is not set, then the UDM shall compare the received SoR-MAC-IUE with the expected SoR-XMAC-IUE that the UDM stored temporarily in step 10.

If the "ME support of SOR-CMCI" in the header of the SOR transparent container is set, then the UDM shall request the AUSF to generate a new SOR-MAC-IUE\_Data that considers the "ME support of SOR-CMCI" indicator as set by the UE. The UDM shall invoke the Nausf\_SORProtection\_ProtectACK service operation as specified in sub-clause 14.1.3.X of this document by including the content of the SOR transparent container received from the UE except for the SOR-MAC-IUE and the CounterSOR (temporarily stored by UDM in step 10) to the AUSF. The AUSF shall use the received CounterSOR when calculating a new SOR-XMAC-IUE. The UDM shall verify the received SoR-MAC-IUE based on the new SOR-XMAC-IUE and store the "ME support of SOR-CMCI" indicator upon successful verification.

#### 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, optionally including the SoR-CMCI indication and optionally the list of preferred PLMN/access technology combinations or secured packet 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, 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 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 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 and the received CounterSOR.

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. If a SoR-CMCI indicator was received, the UE shall set the "ME support of SOR-CMCI" indicator in the header of the SOR transparent container and shall generate the SoR-MAC-IUE\_Data as specified in Annex A.XX and include the generated SoR-MAC-IUE\_Data in a SOR transparent container. If no SoR-CMCI indicator was received, 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 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.

NOTE: In step 2-3 above the UDM needs to verify that AMF has support for transparent container before sending the SoR-CMCI indication to the UE to avoid that transparent container with MAC-IUE\_Data is lost.

9) If the HPLMN indicated that the UE is to acknowledge the successful security check of the received Steering of Roaming Information, and the "ME support of SOR-CMCI" indicator in the header of the SOR transparent container is not set then the UDM shall compare the received SoR-MAC-IUE with the expected SoR-XMAC-IUE that the UDM stored temporarily in step 4.

#### If the "ME support of SOR-CMCI" indicator in the header of the SOR transparent container is set, then the UDM shall request the AUSF to generate a new SOR-MAC-IUE\_Data that considers the "ME support of SOR-CMCI" indicator as set by the UE. The UDM shall invoke the Nausf\_SORProtection\_ProtectACK service operation as specified in sub-clause 14.1.3.X of this document by including the content of the SOR transparent container received from the UE except for the SOR-MAC-IUE and the CounterSOR (temporarily stored by UDM in step 10) to the AUSF. The AUSF shall use the received CounterSOR when calculating a new SOR-XMAC-IUE.6.14.2.3 SoR Counter

The AUSF and the UE shall associate a 16-bit counter, CounterSoR, with the key KAUSF.

The UE shall initialize the CounterSoR to 0x00 0x00 when the newly derived KAUSF is stored (see clause 6.2.2.2). The UE shall store the SoR counter. If the USIM supports both 5G parameters storage and 5G parameters extended storage, then CounterSoR shall be stored in the USIM. Otherwise, CounterSoR shall be stored in the non-volatile memory of the ME

To generate the SoR-MAC-IAUSF, the AUSF shall use the CounterSoR. The CounterSoR shall be incremented by the AUSF for every new computation of the SoR-MAC-IAUSF. The CounterSoR is used as freshness input into SoR-MAC-IAUSF and SoR-MAC-IUE derivations as described in the Annex A.17 and Annex A.18 respectively, to mitigate the replay attack. The AUSF shall send the value of the CounterSoR (used to generate the SoR-MAC-IAUSF) along with the SoR-MAC-IAUSF to the UE. The UE shall only accept CounterSoR value that is greater than stored CounterSoR value. The UE shall store the received CounterSoR, onlyif the verification of the received SoR-MAC-IAUSF is successful. The UE shall use the stored CounterSoR received from the HPLMN, when deriving the SoR-MAC-IUE for the SoR acknowledgement.

To generate the SOR-XMAC-IUE the AUSF uses the same CounterSOR used for the generation of the SOR-MAC-IAUSF (i.e. at reception of a Nausf\_SORProtection\_Protect Request) or the CounterSOR provided by the UDM (i.e. at reception of a Nausf\_SORProtection\_ProtectACK Request).

The AUSF and the UE shall maintain the CounterSoR for lifetime of the KAUSF.

The AUSF that supports the control plane solution for steering of roaming shall initialize the CounterSoR to 0x00 0x01 when the newly derived KAUSF is stored (see clause 6.2.2.1). The AUSF shall set the CounterSoR to 0x00 0x02 after the first calculated SoR-MAC-IAUSF, and monotonically increment it for each additional calculated SoR-MAC-IAUSF. The SoR Counter value of 0x00 0x00 shall not be used to calculate the SoR-MAC-IAUSF and SoR-MAC-IUE.

The AUSF shall suspend the SoR protection service for the UE, if the CounterSoR associated with the KAUSF of the UE, is about to wrap around. When a fresh KAUSF is generated for the UE, the CounterSoR at the AUSF is reset to 0x00 0x01 as defined above and the AUSF shall resume the SoR protection service for the UE.

\*\*\*\*\* Next change \*\*\*\*\*

### 14.1.3 Nausf\_SoRProtection service

#### 14.1.3.1 General

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 |
| ProtectACK | Request/Response | UDM |

#### 14.1.3.2 Nausf\_SORProtection\_Protect service operation

**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.

**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).

#### 14.1.3.3 Nausf\_SORProtection\_ProtectACK service operation

**Service operation name:** Nausf\_SORProtection\_ProtectACK.

**Description:** The AUSF calculates a SOR-MAC-IUE\_Data as specified in the Annex A.XX of this document using UE specific home key (KAUSF) along with the CounterSOR and the content of the SOR Acknowledgement (see clause A.20) and delivers the SOR-MAC-IUE to the requester NF.

NOTE: The AUSF uses the CounterSOR received from the requester NF.

**Input, Required:** Requester ID, SUPI, service name, SOR Acknowledgement, CounterSOR

**Input, Optional:** -

**Output, Required:** SOR-MAC-IUE

**Output, Optional: -**

\*\*\*\*\* Next change \*\*\*\*\*

# A.18 SoR-MAC-IUE\_Data generation function

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

- FC = 0xTBD,

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

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

- P1 = UE Provided Data in SoR ack,

- L1 = length of UE Provided Data in SoR ack

- P2 = CounterSoR,

- L2 = length of CounterSoR.

The input key KEY shall be KAUSF.

The UE Provided Data in SoR ack includes the content of the UE ack including header and any data provided in the SoR transparent ack container.

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

\*\*\*\*\* End of changes \*\*\*

##