**3GPP TSG-CT WG1 Meeting #136-eC1-22xxxx**

**E-Meeting, 12th – 20th May 2022 *was C1-223584***

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **23.122** | **CR** | **0936** | **rev** | **1** | **Current version:** | **17.6.0** |  |
|  |
| *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 |  | ME | **X** | Radio Access Network |  | Core Network |  |

|  |
| --- |
|  |
| ***Title:***  | Release N1 NAS signalling connection when security check fails |
|  |  |
| ***Source to WG:*** | Huawei, HiSilicon |
| ***Source to TSG:*** | C1 |
|  |  |
| ***Work item code:*** | 5GProtoc17 |  | ***Date:*** | 2022-05-01 |
|  |  |  |  |  |
| ***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 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:*** | If the security check is not successful on the received SOR information after registration, and UE has no configured SOR-CMCI in the non-volatile memory of the ME, the UE shall wait the network to release N1 NAS signalling connection. See below:*If the selected PLMN is a VPLMN, the security check is not successful and the UE is in automatic network selection mode, then:**- if the UE has a SOR-CMCI stored in the non-volatile memory of the ME, the current PLMN is considered as lowest priority and the UE shall apply the actions in clause C.4.2;**- otherwise, the UE shall wait until it moves to idle mode or 5GMM-CONNECTED mode with RRC inactive indication (see 3GPP TS 24.501 [64]) before attempting to obtain service on a higher priority PLMN as specified in clause 4.4.3.3 by acting as if timer T that controls periodic attempts has expired, with an exception that the current PLMN is considered as lowest priority. If the selected PLMN is a VPLMN and the UE has an established emergency PDU session, then the UE shall attempt to perform the PLMN selection after the emergency PDU session is released.*If there are ongoing PDU sessions or services, there is no problem that the UE shall wait for the network to release the NAS signaling. However, if there are no ongoing PDU sessions or services, it may take a long time to wait the network to release the NAS signalling. Hence, it proposes that if thers is no ongoing PDU sessions or services, the UE shall release the current N1 NAS signalling connection locally. |
|  |  |
| ***Summary of change:*** | If thers is no ongoing PDU sessions or services, the UE shall immediately release the current N1 NAS signalling connection locally. |
|  |  |
| ***Consequences if not approved:*** | it may take a long time to wait for the network to release the NAS signalling. |
|  |  |
| ***Clauses affected:*** | C.3 |
|  |  |
|  | **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 \*\*\*\*\*

## C.3 Stage-2 flow for steering of UE in HPLMN or VPLMN after registration

The stage-2 flow for the steering of UE in HPLMN or VPLMN after registration is indicated in figure C.3.1. The selected PLMN can be the HPLMN or a VPLMN. The AMF is located in the selected PLMN. In this procedure, the SOR-CMCI, if any, is sent together with the list of preferred PLMN/access technology combinations in plain text or is sent within the secured packet.

The procedure is triggered:

- If the HPLMN UDM supports obtaining a list of preferred PLMN/access technology combinations and SOR-CMCI, if any, or a secured packet from the SOR-AF, the HPLMN policy for the SOR-AF invocation is present in the HPLMN UDM and the SOR-AF provides the HPLMN UDM with a new list of preferred PLMN/access technology combinations or a secured packet for a UE identified by SUPI. If the ME supports the SOR-CMCI, the SOR-AF may provide the SOR-CMCI and optionally provides the "Store SOR-CMCI in ME" indicator otherwise the SOR-AF shall provide neither the SOR-CMCI nor the "Store SOR-CMCI in ME" indicator.

 The secured packet provided by the SOR-AF may include SOR-CMCI only if the SOR-AF has determined that the ME supports the SOR-CMCI and the USIM of the indicated SUPI supports SOR-CMCI. Otherwise if only the "ME support of SOR-CMCI" indicator is stored for the UE, then the SOR-AF shall not include the SOR-CMCI, if any, in the secured packet; or

NOTE 1: The SOR-AF can determine that the ME supports the SOR-CMCI if the Nsoraf\_SoR\_Info service operation has returned the "ME support of SOR-CMCI" indicator. How the SOR-AF determines that the USIM for the indicated SUPI supports SOR-CMCI is implementation specific.

- When a new list of preferred PLMN/access technology combinations or a secured packet becomes available in the HPLMN UDM (i.e. retrieved from the UDR).

 If the "ME support of SOR-CMCI" indicator is stored for the UE and the new list of preferred PLMN/access technology combinations becomes available in the HPLMN UDM (i.e. retrieved from the UDR), the HPLMN UDM shall obtain the SOR-CMCI and the "Store SOR-CMCI in ME" indicator, if available, otherwise the HPLMN UDM shall obtain neither the SOR-CMCI nor the "Store SOR-CMCI in ME" indicator.

NOTE 3: Based on operator deployment and policy, if the UDM receives the list of preferred PLMN/access technology combinations, SOR-CMCI, if any, the "Store SOR-CMCI in ME" indicator, if any, and the USIM of the indicated SUPI supports SOR-CMCI from the UDR, and the UDM supports communication with the SP-AF, the UDM can send this list and SOR-CMCI to the SP-AF requesting it to provide this information in a secured packet as defined in 3GPP TS 29.544 [71].

NOTE 4: Before providing the HPLMN UDM with a new list of preferred PLMN/access technology combinations or a secured packet for a UE identified by SUPI, the SOR-AF, based on operator policies or criteria, can obtain the user location information by triggering the unified location service exposure procedure as defined in 3GPP TS 23.273 [70] clause 6.5, or additionally based on implementation specific criteria, by requesting the UE location information from other application function using implementation specific method. This user location information can then be used in the SOR-AF algorithms.

NOTE 5: The secured packet obtained by the UDM can include SOR-CMCI only if the "ME support of SOR-CMCI" indicator is stored for the UE and the USIM of the indicated SUPI supports SOR-CMCI. Otherwise if only the "ME support of SOR-CMCI" indicator is stored for the UE, then the SOR-CMCI, if any, cannot be included in the secured packet.

Figure C.3.1: Procedure for providing list of preferred PLMN/access technology combinations and the SOR-CMCI, if any, or secured packet after registration

For the steps below, security protection is described in 3GPP TS 33.501 [24].

1) The SOR-AF to the HPLMN UDM: Nudm\_ParameterProvision\_Update request is sent to the HPLMN UDM to trigger the update of the UE with the new list of preferred PLMN/access technology combinations, the SOR-CMCI, if any, and the "Store SOR-CMCI in ME" indicator, if any, or a secured packet for a UE identified by SUPI.

2) The HPLMN UDM to the AMF: The UDM notifies the changes of the user profile to the affected AMF by the means of invoking Nudm\_SDM\_Notification service operation. The Nudm\_SDM\_Notification service operation contains the steering of roaming information that needs to be delivered transparently to the UE over NAS within the Access and Mobility Subscription data. If the HPLMN decided that the UE is to acknowledge successful security check of the received steering of roaming information, the Nudm\_SDM\_Notification service operation also contains an indication that the UDM requests an acknowledgement from the UE as part of the steering of roaming information. If the SOR-CMCI was obtained, the HPLMN UDM shall include the SOR-CMCI into the steering of roaming information. If the "Store SOR-CMCI in ME" indicator was obtained, the HPLMN UDM shall include the "Store SOR-CMCI in ME" indicator; otherwise, the HPLMN UDM shall include the "Store SOR-CMCI in ME" indicator set to "Do not store SOR-CMCI in ME";

NOTE 6: The UDM cannot provide the SOR-CMCI, if any, to the VPLMN AMF which does not support receiving SoR transparent container (see 3GPP TS 29.503 [78]).

3) The AMF to the UE: the AMF sends a DL NAS TRANSPORT message to the served UE. The AMF includes in the DL NAS TRANSPORT message the steering of roaming information received from the UDM.

4) Upon receiving the steering of roaming information, the UE shall perform a security check on the steering of roaming information included in the DL NAS TRANSPORT message to verify that the steering of roaming information is provided by HPLMN, and:

- if the security check is successful and:

a) if the steering of roaming information contains a secured packet (see 3GPP TS 31.115 [67]):

- if the service "data download via SMS Point-to-point" is allocated and activated in the USIM Service Table (see 3GPP TS 31.102 [40]), the ME shall upload the secured packet to the USIM using procedures in 3GPP TS 31.111 [41].

 If the UDM has requested an acknowledgement from the UE in the DL NAS TRANSPORT message and the ME receives UICC responses indicating that the UICC has received the secured packet successfully, then the UE sends an UL NAS TRANSPORT message to the serving AMF with an SOR transparent container including the UE acknowledgement and the UE shall set the "ME support of SOR-CMCI" indicator in the header of the SOR transparent container to "supported"; and

NOTE 7: How the ME handles UICC responses that do not indicate that the UICC has received the secured packet successfully and failures in communication between the ME and UICC is implementation specific and out of scope of this release of the specification.

- when the ME receives a USAT REFRESH command qualifier (see 3GPP TS 31.111 [41]) of type "Steering of Roaming" and neither a SOR-CMCI is included, nor the UE is configured with the SOR-CMCI, it performs the procedure for steering of roaming in clause 4.4.6 with an exception that if the UE is in automatic network selection mode, then the UE shall wait until it moves to idle mode or 5GMM-CONNECTED mode with RRC inactive indication (see 3GPP TS 24.501 [64]) before attempting to obtain service on a higher priority PLMN (specified in clause 4.4.6 bullet d); or

- when the ME receives a USAT REFRESH with command qualifier (see 3GPP TS 31.111 [41]) of type "Steering of Roaming" and either a SOR-CMCI is included, or the UE is configured with the SOR-CMCI, the UE shall perform items a), b) and c) of the procedure for steering of roaming in clause 4.4.6. If the UE is in automatic network selection mode it shall apply the actions in clause C.4.2;

b) if the steering of roaming information contains the list of preferred PLMN/access technology combinations, the ME shall replace the highest priority entries in the "Operator Controlled PLMN Selector with Access Technology" list stored in the ME with the received list of preferred PLMN/access technology combinations, and delete the PLMNs identified by the list of preferred PLMN/access technology combinations from the Forbidden PLMN list and from the Forbidden PLMNs for GPRS service list, if they are present in these lists.

 If the UDM has requested an acknowledgement from the UE in the DL NAS TRANSPORT message, the UE sends an UL NAS TRANSPORT message to the serving AMF with an SOR transparent container including the UE acknowledgement and the UE shall set the "ME support of SOR-CMCI" indicator to "supported".

 If the UE is in automatic network selection mode and the selected PLMN is a VPLMN, then:

- if the UE has a SOR-CMCI stored in the non-volatile memory of the ME or received the SOR-CMCI over N1 NAS signalling, the UE shall apply the actions in clause C.4; or

- the UE shall wait until it moves to idle mode or 5GMM-CONNECTED mode with RRC inactive indication (see 3GPP TS 24.501 [64]) before attempting to obtain service on a higher priority PLMN as specified in clause 4.4.3.3 by acting as if timer T that controls periodic attempts has expired.

 If the selected PLMN is a VPLMN and the UE has an established emergency PDU session then the UE shall attempt to perform the PLMN selection subsequently after the emergency PDU session is released, if the UE is in automatic network selection mode.

 If the UDM has not requested an acknowledgement from the UE, then step 5 is skipped; and

- If the selected PLMN is a VPLMN, the security check is not successful and the UE is in automatic network selection mode, then:

- if the UE has a SOR-CMCI stored in the non-volatile memory of the ME, the current PLMN is considered as lowest priority and the UE shall apply the actions in clause C.4.2; or

- if the UE does not have a SOR-CMCI stored in the non-volatile memory of the ME, and:

- if there are ongoing PDU sessions or services, the UE shall wait until it moves to idle mode or 5GMM-CONNECTED mode with RRC inactive indication (see 3GPP TS 24.501 [64]) before attempting to obtain service on a higher priority PLMN as specified in clause 4.4.3.3 by acting as if timer T that controls periodic attempts has expired, with an exception that the current PLMN is considered as lowest priority. If the selected PLMN is a VPLMN and the UE has an established emergency PDU session, then the UE shall attempt to perform the PLMN selection after the emergency PDU session is released; or

- if there are no ongoing PDU sessions or services, the UE shall release the current N1 NAS signalling connection locally and attempt to obtain service on a higher priority PLMN as specified in clause 4.4.3.3 by acting as if timer T that controls periodic attempts has expired, with an exception that the current PLMN is considered as lowest priority.

 Step 5 is skipped;

NOTE 8: When the UE is in the manual mode of operation or the current chosen VPLMN is part of the "User Controlled PLMN Selector with Access Technology" list, the UE stays on the VPLMN.

5) The AMF to the HPLMN UDM: If the UL NAS TRANSPORT message with an SOR transparent container is received, the AMF uses the Nudm\_SDM\_Info service operation to provide the received SOR transparent container to the UDM. If the HPLMN decided that the UE is to acknowledge successful security check of the received steering of roaming information in step 1, the UDM verifies that the acknowledgement is provided by the UE. If the "ME support of SOR-CMCI" indicator in the header of the SOR transparent container is set to "supported", then the HPLMN UDM shall store the "ME support of SOR-CMCI" indicator, otherwise the HPLMN UDM shall delete the stored "ME support of SOR-CMCI" indicator, if any; and

6) The HPLMN UDM to the SOR-AF: Nsoraf\_SoR\_Info (SUPI of the UE, successful delivery, "ME support of SOR-CMCI" indicator, if any). If the HPLMN policy for the SOR-AF invocation is present and the HPLMN UDM received and verified the UE acknowledgement in step 5, then the HPLMN UDM informs the SOR-AF about successful delivery of the list of preferred PLMN/access technology combinations, SOR-CMCI, if any, or of the secured packet to the UE. If the "ME support of SOR-CMCI" indicator is stored for the UE, the HPLMN UDM shall include the "ME support of SOR-CMCI" indicator.

If the selected PLMN is a VPLMN and:

- the UE in manual mode of operation encounters security check failure of SOR information in DL NAS TRANSPORT message; and

- upon switching to automatic network selection mode, the UE remembers that it is still registered on the PLMN where the security check failure of SOR information was encountered;

the UE shall wait until it moves to idle mode or 5GMM-CONNECTED mode with RRC inactive indication (see 3GPP TS 24.501 [64]) before attempting to obtain service on a higher priority PLMN as specified in clause 4.4.3.3, by acting as if timer T that controls periodic attempts has expired, with an exception that the current registered PLMN is considered as lowest priority. If the selected PLMN is a VPLMN and the UE has an established emergency PDU session, then the UE shall attempt to perform the PLMN selection after the emergency PDU session is released.

NOTE 9: The receipt of the steering of roaming information by itself does not trigger the release of the emergency PDU session.

NOTE 10: If the selected PLMN is the HPLMN, regardless whether the UE is in automatic network selection mode or manual network selection mode, regardless whether the UE has an established emergency PDU session or not, and regardless whether the security check is successful or not successful, the UE is not required to perform the PLMN selection.

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