**3GPP TSG-CT WG1 Meeting #123-eC1-20vxxx**

**Electronic meeting, 16-24 April 2020**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **23.122** | **CR** | **0511** | **rev** | **1** | **Current version:** | **16.5.0** |  |
|  | | | | | | | | |
| *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:*** | Management of forbidden SNPNs list upon receipt of a non-integrity protected reject message | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell | | | | | | | | | |
| ***Source to TSG:*** | C1 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | Vertical\_LAN | | | | |  | ***Date:*** | | | 2020-04-05 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **C** |  | | | | | ***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:*** | | Currently , there are three different types of UE behaviours in terms of forbidden network list handling upon receipt of a non-integrity protected reject message including a 5GMM cause value indicating that the UE is not allowed to access the network (i.e. #11, #73, #74, #75)   1. **#11/73 (E)HPLMN type** The (E)HPLMN ID is never added in the forbidden list. Instead, the TAI is added and then (upon T3247 expiry) removed from the forbidden TAI list. 2. **#11/73 VPLMN type** Before the network-specific attempt counter reaches the maximum value, the network ID is added and then (upon T3247 expiry) removed from the forbidden network list. After the network-specific attempt counter reaches the maximum value, the network ID is included in the forbidden network list. 3. **#74/75 type** Before the network-specific attempt counter reaches the maximum value, the TAI is added and then (upon T3247 expiry) removed from the forbidden TAI list. After the network-specific attempt counter reaches the maximum value, the network ID is included in the forbidden network list.   Our preference is to align c) to b) because:   * there is no SNPN-specific requirement on handling of non-integrity protected reject messages; * the UE can have multiple entries in the "list of subscriber data". It is better to let the UE perform SNPN selection than keeping the UE in the same SNPN because the SNPN can be anyways selected again after T3247 expiry; and * even though there will be no SNPN to select for a UE with a single entry in the “list of subscriber data" when the UE receives a single non-integrity protected reject message with #74 or #75, this is temporary (until T3247 expires). And taking into account that one of the key operations of T3247 is to temporarily include a network ID in a list until the UE estimates that the non-integrity protected message is coming from a genuine network (i.e. an attempt counter reaches the maximum value), this temporary inclusion is not something that should be avoided. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | To align c) with b) (see Reason for change for b) and c)). | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | As long as management of forbidden SNPNs list upon receipt of a non-integrity protected reject message is concerned, other entries in the "list of subscriber data" are ignored. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 4.9.3.0 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

#### 4.9.3.0 General

The registration on the selected SNPN and the LR are only necessary if the MS is capable of services which require registration. Otherwise, the SNPN selection procedures are performed without registration.

The ME is configured with a "list of subscriber data" containing zero or more entries. Each entry of the "list of subscriber data" consists of:

a) a subscriber identifier in the form of a SUPI containing a network-specific identifier or an IMSI except when the SNPN uses:

1) the EAP based primary authentication and key agreement procedure using the EAP-AKA'; or

2) the 5G AKA based primary authentication and key agreement procedure;

NOTE 1: A subscriber identifier in the form of a SUPI containing a network-specific identifier or an IMSI is available in USIM if the SNPN uses the EAP based primary authentication and key agreement procedure using the EAP-AKA' or the 5G AKA based primary authentication and key agreement procedure.

b) credentials except when the SNPN uses:

1) the EAP based primary authentication and key agreement procedure using the EAP-AKA'; or

2) the 5G AKA based primary authentication and key agreement procedure;

NOTE 2: Credentials are available in USIM if the SNPN uses the EAP based primary authentication and key agreement procedure using the EAP-AKA' or the 5G AKA based primary authentication and key agreement procedure.

c) an SNPN identity; and

d) optionally, the unified access control configuration indicating for which access identities (see 3GPP TS 24.501 [64]) the ME is configured in the SNPN.

NOTE 3: How the ME is configured with the "list of subscriber data" is out of scope of 3GPP in this release of the specification.

NOTE 4: Multiple entries can include the same subscriber identifier and credentials.

NOTE 5: Handling of more than one entry with the same SNPN identity is left up to MS implementation.

NOTE 6: Handling of the case when the SNPN uses the EAP based primary authentication and key agreement procedure using the EAP-AKA' or the 5G AKA based primary authentication and key agreement procedure and the MS has multiple valid USIMs (3GPP TS 31.102 [40]) is left up to MS implementation.

The MS shall maintain a list of "temporarily forbidden SNPNs" and a list of "permanently forbidden SNPNs" in the ME. Each entry of those lists consists of an SNPN identity.

The MS shall add an SNPN to the list of "temporarily forbidden SNPNs", if a message with cause value #74 "Temporarily not authorized for this SNPN" (see 3GPP TS 24.501 [64]) is received by the MS in response to an LR request from the SNPN. In addition:

- if:

1) the message is integrity-protected; or

2) the message is not integrity-protected, and the value of the SNPN-specific attempt counter for that SNPN is equal to the MS implementation specific maximum value as defined in 3GPP TS 24.501 [64];

then the MS shall start an MS implementation specific timer not shorter than 60 minutes.

- if tthe message is not integrity-protected, and the value of the SNPN-specific attempt counter for that SNPN is less than the MS implementation specific maximum value as defined in 3GPP TS 24.501 [64], then the MS shall start timer T3247.

The MS shall remove an SNPN from the list of "temporarily forbidden SNPNs", if:

a) there is a successful LR after a subsequent manual selection of the SNPN;

b) the MS implementation specific timer not shorter than 60 minutes expires;

c) the timer T3247 expires;

d) the MS is switched off; or

e) an entry of the "list of subscriber data" with the SNPN identity of the SNPN is updated or the USIM is removed if:

- EAP based primary authentication and key agreement procedure using EAP-AKA'; or

- 5G AKA based primary authentication and key agreement procedure;

was performed in the selected SNPN.

If an SNPN is removed from the list of "temporarily forbidden SNPNs" list, the MS shall stop the MS implementation specific timer not shorter than 60 minutes, if running.

The MS shall add an SNPN to the list of "permanently forbidden SNPNs", if a message with cause value #75 "Permanently not authorized for this SNPN" (see 3GPP TS 24.501 [64]) is received by the MS in response to an LR request from the SNPN. In addition, if the message is not integrity-protected, and the value of the SNPN-specific attempt counter for that SNPN is less than the MS implementation specific maximum value as defined in 3GPP TS 24.501 [64], then the MS shall start timer T3247.

The MS shall remove an SNPN from the list of "permanently forbidden SNPNs", if:

a) there is a successful LR after a subsequent manual selection of the SNPN;

b) the timer T3247 expires; or

c) an entry of the "list of subscriber data" with the SNPN identity of the SNPN is updated or the USIM is removed if:

- EAP based primary authentication and key agreement procedure using EAP-AKA'; or

- 5G AKA based primary authentication and key agreement procedure;

was performed in the selected SNPN.

When the MS reselects to a cell in a shared network, and the cell is a suitable cell for multiple SNPN identities received in the broadcast information as specified in 3GPP TS 36.331 [42] and 3GPP TS 38.331 [65], the AS indicates these multiple SNPN identities to the NAS according to 3GPP TS 36.304 [43] and 3GPP TS 38.304 [61]. The MS shall select one of these SNPNs. If the registered SNPN is available among these SNPNs, the MS shall not select a different SNPN.

The MS operating in SNPN access mode shall maintain one or more lists of "5GS forbidden tracking areas for roaming", each associated with an SNPN. The MS shall use the list of "5GS forbidden tracking areas for roaming" associated with the selected SNPN. If the MS selects a new SNPN, the MS shall keep the list of "5GS forbidden tracking areas for roaming" associated with the previously selected SNPN. If the number of the lists to be kept is higher than supported, the MS shall delete the oldest stored list of "5GS forbidden tracking areas for roaming". The MS shall delete all lists of "5GS forbidden tracking areas for roaming", when the MS is switched off and periodically (with period in the range 12 to 24 hours). The MS shall delete the list of "5GS forbidden tracking areas for roaming" associated with an SNPN, when the entry of the SNPN in the list of subscriber data" is updated or when the USIM is removed if:

- the EAP based primary authentication and key agreement procedure using the EAP-AKA'; or

- the 5G AKA based primary authentication and key agreement procedure;

was performed in the selected SNPN.

NOTE 7: The number of the lists of "5GS forbidden tracking areas for roaming" supported by the MS is MS implementation specific.

If a message with cause value #15 (see 3GPP TS 24.501 [64]) is received by an MS operating in SNPN access mode, the TA is added to the list of "5GS forbidden tracking areas for roaming" of the selected SNPN. The MS shall then search for a suitable cell in the same SNPN but belonging to a TA which is not in the "5GS forbidden tracking areas for roaming" list of the selected SNPN.

The MS should maintain a list of SNPNs for which the N1 mode capability was disabled due to receipt of a reject from the network with 5GMM cause #27 "N1 mode not allowed". When the MS disables its N1 mode capability due to receipt of a reject from an SNPN with 5GMM cause #27 "N1 mode not allowed":

- the MS should add the SNPN identity of the SNPN which sent a reject with 5GMM cause #27 "N1 mode not allowed" to the list of SNPNs for which the N1 mode capability was disabled and should start timer TG if timer TG is not already running. The number of SNPNs for which N1 mode was not allowed that the MS can store is implementation specific, but it shall be at least one. The value of timer TG is MS implementation specific;

- in automatic SNPN selection, the MS shall not select an SNPN for which the N1 mode capability was disabled as SNPN selection candidates, unless no other SNPN is available; and

- the MS shall delete stored information on SNPNs for which the N1 mode capability was disabled when the MS is switched off, the USIM is removed, the entries of the "list of subscriber data" for the SNPNs are updated, or timer TG expires.