**3GPP TSG-Meeting # *draft\_***-r1

**, , -**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** |  | **rev** |  | **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 changeaffects:*** | UICC apps |  | ME |  | Radio Access Network |  | Core Network | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** |  | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** |  | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** |  | | | | |  | ***Date:*** | | |  |
|  |  | | | |  | |  | | |  |
| ***Category:*** |  |  | | | | | ***Release:*** | | |  |
|  | *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:*** | | TS 33.501 specifies security handling in registration with AMF reallocation via direct NAS route in its clause 6.9.6. According to the currently defined security handling, the target AMF always sends protected NAS message to the UE (when the KAMF is not horizontally derived) or initiates NAS SMC (when the KAMF is horizontally derived). But protecting the subsequent messages to the UE or initiate NAS SMC is not necessary if the initial AMF has not activated security with the UE. It leads to waste of signalling and poor system performance. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Detail of message of initial AMF to Target AMF and handling in Target AMF. The reroute message includes an indication of security activation (i.e., SecActivatedInd) if security is activated between the UE and the initial AMF. Upon receiving the reroute message, if the target AMF receives the indication of security activation (i.e., SecActivatedInd), it shall further check the indication of horizontal KAMF derivation (i.e., keyAmfHDevirationInd). | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Incompleted specification. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | Clause 6.9.6. | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*start of change\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

6.9.6 Security handling in registration with AMF reallocation via direct NAS reroute

In registration with AMF reallocation via direct NAS reroute, the initial AMF sends a reroute message to the target AMF. It includes an indication of security activation (i.e., SecActivatedInd) in the message if security is activated between the UE and the initial AMF. The initial AMF shall use its local policy to determine whether to perform horizontal KAMF derivation on current KAMF. The initial AMF includes an indication of horizontal KAMF derivation (i.e., keyAmfHDerivationInd) in the message if the horizontal KAMF derivation is performed.

Upon receiving the reroute message, if the target AMF receives the indication of security activation (i.e., SecActivatedInd), it shall further check the indication of horizontal KAMF derivation (i.e., keyAmfHDevirationInd). If the target AMF receives the indication of horizontal KAMF derivation (i.e., keyAmfHDerivationInd) from the initial AMF, it shall initiate NAS SMC. If the target AMF does not receive keyAmfHDerivationInd, the target AMF shall use the received security context and send protected NAS message including protected authentication request message if the target AMF decides to perform authentication.

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*end of change\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***