**3GPP TSG-SA3 Meeting #106-e *draft S3-220379-r6***

**e-meeting, 14 - 25 February 2022**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** | **0012** | **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 change affects:*** | UICC apps |  | ME |  | Radio Access Network |  | Core Network | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | TR 33.847 Updates to conclusions for KI 2 and KI 3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | MITRE | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | FS\_5G\_ProSe\_Sec | | | | |  | ***Date:*** | | | 2022-02-14 |
|  |  | | | |  | |  | | |  |
| ***Category:*** |  |  | | | | | ***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 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-15 (Release 15) Rel-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | This contribution proposes updates to TR 33.847 conclusions for key issue #2: Keys in ProSe discovery scenario to cover the case of ProSe discovery in public safety cases. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Group Member Discovery is applicable in both commercial and public safety cases. For commercial use cases, either the 5G DDNMF or 5G PKMF manages discovery keying material, for both group member discovery and UE to Network relay discovery (e.g., #35). For public safety use cases, the 5G PKMF manages discovery keying material, for both group member discovery and UE to network relay discovery (e.g. sol#37). | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | The conclusions regarding what Network Function will manage discovery keys for group member discovery and UE to Network relay discovery in public safety cases are not specified. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | Clause 7.2 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* 1st Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

7.2 Key Issue #2: Keys in ProSe discovery scenario

The conclusions for direct discovery are as follows:

The discovery keys include a cipher key, an integrity key, and a scrambling key.

For open discovery, only the integrity key will be assigned by the 5G DDNMF and will be used to provide integrity protection of the announce message.

For restricted discovery, 5G DDNMF will assign the discovery key(s) based on the requirement of the Prose Service.

For Group Member discovery and UE-to-Network Relay discovery, assignment of keys and other security material is described in TS 23.304 clause 5.12 and 5.1.4 respectively. Which NF is responsible for provisioning security material will be decided in normative phase.

In user plane based solutions, the discovery keys are managed by PKMF (e.g., in public safety cases solution #37 is used as a baseline)

The same types of discovery keys are assigned for both public safety and commercial use cases. Multiple sets of keys might be assigned to allow for out of coverage operation.

Security of mission critical public safety over ProSe is defined in 33.180.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of 1st Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*