**3GPP TSG-SA3 Meeting #106-e *draft S3-220379-r2***

**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 and key issue #3: Security of UE-to-Network Relay, 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).  This contribution proposes to transfer discovery keying provisioning from KI 3 conclusions to KI 2 conclusions. | | | | | | | | |
|  | |  | | | | | | | | |
| ***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 & Clause 7.3 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* 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-Relay discovery, assignment of keys and other security material follows the conclusion for restricted discovery in commercial use cases.

In public safety use cases, keys and other security material are assigned by the 5G PKMF.

The same types of discovery keys are assigned for both public safety and commercial use cases, with the difference that for public safety, multiple sets can be assigned to allow for out of coverage operation.\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of 1st Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* 2nd Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

7.3 Key Issue #3: Security of UE-to-Network Relay

Note: Further conclusions is not addressed in the present document.

The solutions for U2N Relay authorization and security can be classified as user-plane (UP) or controlled-plane (CP) based solutions. The UP based solutions use a UP connection to an AF (PKMF) while CP based solutions use the primary authentication for PC5 keys establishment.

It is concluded that both control plane and user plane solutions are supported for L3 U2N relay.

The following text is taken as conclusions for UE-to-Network Relay solution:

- For the control plane solution, the following conclusion is made:

- For PC5 link security, PC5 keys are derived using keys derived from the primary authentication (e.g., sol#1, #10, #15, #30). The security of the communication between UE-to-Network relay and remote UE is established based on a shared key which is derived and distributed with the assistance of the network. A root credential is configured in the remote UE and the network. The shared key is individually derived from the root credential by the remote UE and the network. The shared key is distributed by the AMF to the UE-to-Network relay.

- AUSF derives the PC5 anchor key (e.g., sol#1, sol#15, sol#30, sol#39) used for PC5 keys derivation.

NOTE1: The detailed procedure to enable the PC5 link security and the details of the PC5 key hierarchy will be determined accordingly during the normative phase.

- For the user-plane solution, the following is concluded for security in U2N relay:

- the approach of using the user plane for key management of security keys used for PC5 communication, between the Remote UE and the UE-to-network relay, is adopted as the basis for normative work.

- a new 5G PKMF function, for commercial services, internal to PLMN, is supporting the key management of security keys used for PC5 communication (between the Remote UE and the UE-to-network relay), which is accessed in the user plane, is adopted as the basis for normative work.

- the user-plane solutions including Solution #18 and Solution #29 are selected as the basis of normative work.

The following text is taken as the conclusion for the L3 UE-to-Network Relay solution:

- In addition to PC5 link security above, support of end-to-end security requirements when required by Remote UE services using N3IWF as described in solution #19 is taken as a baseline for normative work.

The following text is taken as the conclusion for the L2 UE-to-Network Relay solution:

- It is concluded that the high-level procedure defined in the Solution #14 is taken as the baseline for the normative work. The details of AS security establishment between the Remote UE and the NG-RAN is to be discussed and defined in the normative phase.

- For end-to-end security, the existing NAS/AS security and UP security mechanisms defined in 33.501 [14] are to be reused.

For user-plane solutions, the followings are concluded for both commercial and public safety use cases:

- All security materials for ProSe U2N relay are provided to the UE by PKMF.

- PC5 keys are managed by PKMF.

- PCF and/or 5G DDNMF provides the PKMF address to the UE.

NOTE2: if PKMF address is configured by both PCF and DDNMF, which one takes precedence will be determined in normative phase in coordination with SA2.

- For commercial use cases, PKMF can be collocated with 5G DDNMF.

- For commercial use cases, the PC3 connection between UE and DDNMF (or Ua) can be reused to deliver both the discovery security materials and the PC5 keys (i.e., PRUK and PRUK ID).

- Both remote UE and relay UE are only required to communicate with the PKMF of their own HPLMN for commercial use cases.

- For the public safety use case, PKMF may be managed by a public safety operator and located outside of the 3GPP network.

- Authorization information is stored at UDM (and is made available to 5G DDNMF and PKMF) for commercial use cases and at the PKMF for the Public Safety use case.

- When the remote UE has been provided with the PC5 security materials by the PKMF, the PRUK ID (or PC5 key ID) is included in the DCR as a UE ID and other UE IDs and/or UE Info are not sent in clear over the air.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of 2nd Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*