**3GPP TSG-SA3 Meeting #108-e *draft\_S3-221910-r1***

**e-meeting, 22 August - 26 August 2022**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.503** | **CR** | **0011** | **rev** |  | **Current version:** | **17.0.1** |  |
|  | | | | | | | | |
| *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 | **X** | Core Network | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Clarifications of general description to Restricted 5G ProSe Direct Discovery | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Ericsson | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | 5G\_ProSe | | | | |  | ***Date:*** | | | 2022-08-15 |
|  |  | | | |  | |  | | |  |
| ***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:*** | | Clarifications of general description | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Some editorial changes for better understanding | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Misunderstanding of the general description | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 6.1.3.2.1 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

\*\*\* BEGIN OF CHANGES \*\*\*

#### 6.1.3.2 Restricted 5G ProSe Direct Discovery

##### 6.1.3.2.1 General

The security for both models of restricted 5G ProSe Direct Discovery is similar to that of open 5G ProSe Direct Discovery described in clause 6.1.3.1. Both models also use a UTC-based counter (see step 9 in clause 6.1.3.1) to provide freshness for the protection of the restricted 5G ProSe Direct Discovery message on the PC5 interface. The parameters CURRENT\_TIME and MAX\_OFFSET are also provided to the UE from the 5G DDNMF in its HPLMN to ensure that the obtained UTC-based counter is sufficiently close to real time to protect against replays.

The major differences are that restricted 5G ProSe Direct Discovery requires confidentiality protection of the discovery messages (e.g., to ensure a UE’s privacy is not disclosed to unauthorized parties or tracked due to constantly sending the same ProSe Restricted/Response Code in the clear) and that the MIC checking may be performed by the receiving UE (if allowed by the 5G DDNMF).

The security parameters needed by a sending UE to protect a discovery message (i.e., in Model A the Announcing UE and in Model B the Discoverer UE sending the ProSe Query Code and the Discoveree UE sending the ProSe Response Code) are provided in the Code-Sending Security Parameters. Similarly, the security parameters needed by a UE receiving a discovery message (i.e., in Model A the Monitoring UE and in Model B the Discoverer UE receiving a ProSe Response Code and the Discoveree receiving a ProSe Query Code) are provided in the Code-Receiving Security Parameters.

In addition to clause 6.1.3.4.1 in TS 33.303 [4], 5G Prose introduced two new features:

- During the discovery request procedure, 5G DDNMF may optionally provide the PC5 security policies to the UEs.

- A ciphering algorithm for message-specific confidentiality is configured at the UE during the Discovery Request procedure.

5G ProSe UE-to-Network Relay discovery is different from 5G ProSe Restricted Direct Discovery. In 5G ProSe UE-to-Network Relay discovery, the discovery security materials are provided by the PKMF in case of user-plane based security procedure (as specified in clause 6.3.3.2), and by the DDNMF or the PCF in case of control-plane based security procedure . The 5G ProSe UE-to-Network Relay discovery procedures described in clause 6.1.3.2.2.1 and clause 6.1.3.2.2.2 apply with adjustment when 5G DDNMF or 5G PKMF is used for 5G ProSe UE-to-Network Relay discovery.