**3GPP TSG-SA3 Meeting #108e *draft\_S3-222002-r1***

**e-meeting, 22nd – 26th August, 2022**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.303** | **CR** | **0136** | **rev** |  | **Current version:** | **15.0.0** |  |
|  | | | | | | | | |
| *For* ***[HE](http://www.3gpp.org/3G_Specs/CRs.htm" \l "_blank)******[LP](http://www.3gpp.org/3G_Specs/CRs.htm" \l "_blank)*** *on using this form: comprehensive instructions can be found at  <http://www.3gpp.org/Change-Requests>.* | | | | | | | | |
|  | | | | | | | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME |  | Radio Access Network |  | Core Network | **x** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Correction figure in ProSe discovery in TS33.303(R15) | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | ChinaTelecom | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | 5GS\_Ph1-SEC | | | | |  | ***Date:*** | | | 2022-08-22 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | F |  | | | | | ***Release:*** | | | Rel-15 |
|  | *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:*** | | The proposed CR aims to correct the mistakes in the flow chart related to ProSe Discovery which is Figure 6.1.3.4.2.2-1.  The ‘Discoverer’ in “VPLMN of Discoveree ProSe Function” which is in model B figure is missing based on the procedure. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Changing the mistake in Figure 6.1.3.4.2.2-1. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Mistaken in specification flow chart is misunderstanding. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 6.1.3.4.2.2 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

\*\*\*\*\*\*\*\*\*\*\*\* START OF CHANGES

###### 6.1.3.4.2.2 Model B security flows

This subclause contains the message flows for the protection of a model B restricted discovery. The flows show how a particular discovery is protected. The exact details of the actual protection to be applied to a discovery message are given in subclause 6.1.3.4.3. The message flows apply when both the UEs are roaming or when one or both are in their HPLMN. If either of the UEs is not roaming some steps in the flows are omitted as detailed in the flows.

The flows are broken down into 4 boxed stages to better to relate to the procedures given in TS 23.303 [2]. The first, second and fourth stage correspond to subclause 5.3.3A.3, 5.3.3A.5 and 5.3.4A.2 of TS 23.303 [2] respectively. The interaction between the ProSe Function(s) and HSS is omitted for simplicity.



Figure 6.1.3.4.2.2-1: Flows for securing model B restricted discovery

Steps 1-4 refer to a Discoveree UE.

1. Discoveree UE sends a Discovery Request message containing the RPAUID to the ProSe Function in its HPLMN in order to get the ProSe Code to announce and associated security material. The command indicates that this is for ProSe Response (Model B) operation, i.e. for a Discoveree UE.

2. The ProSe Function may check for the announce authorization with the ProSe Application Server depending on ProSe Function configuration.

3. The ProSe Functions in the HPLMN and VPLMN of the Discoveree UE exchange Announce Auth. messages. If the Discoveree UE is not roaming, these steps do not take place.

4. The ProSe Function in the HPLMN of the Discoveree UE returns the ProSe Response Code and the Code-Sending Security Parameters, Discovery Query Filter(s) and their Code-Receiving Security Parameters corresponding to each discovery filter along with the CURRENT\_TIME and MAX\_OFFSET parameters. The Code-Sending Security Parameters provide the necessary information for the Discoveree UE to protect the transmission of the ProSe Response Code (see subclause 6.1.3.4.3.2) and are stored with the ProSe Response Code. The Code-Receiving Security Parameters provide the information needed by the Discoveree UE to undo the protection applied to the ProSe Query Code by the Discoverer UE (see subclause 6.1.3.4.3.3). The Code-Receiving Security Parameters shall indicate a Match Report will not be used for MIC checking. The UE stores each Discovery Filter with its associated Code-Receiving Security Parameters. The Discoveree UE takes the same actions with CURRENT\_TIME and MAX\_OFFSET as described for the Announcing UE in step 4 of subclause 6.1.3.3.1 of the current specification.

Steps 5-10 refer to a Discoverer UE

5. The Discoverer UE sends a Discovery Request message containing the RPAUID to the ProSe Function in its HPLMN in order to be allowed to discover one or more Restricted ProSe Application IDs.

6. The ProSe Function in the HPLMN of the Discoverer UE sends an authorization request to the ProSe Application Server. If, based on the permission settings, the RPAUID is allowed to discover at least one of the Target RPAUIDs contained in the Application Level Container, the ProSe Application Server returns an authorization response.

7. If the Discovery Request is authorized, and the PLMN ID in the Target RPAUID indicates a different PLMN, the ProSe Function in the HPLMN of the Discoverer UE contacts the indicated PLMN’s ProSe Function i.e. the ProSe Function in the HPLMN of the Discoveree UE, by sending a Discovery Request message.

8. The ProSe Function in the HPLMN of the Discoveree UE may exchange authorization messages with the ProSe Application Server.

9. The ProSe Function in the HPLMN of the Discoveree UE responds to the ProSe Function in the HPLMN of the Discoverer UE with a Discovery Response message including the ProSe Query Code(s) and their associated Code-Sending Security Parameters, ProSe Response Code and its associated Code-Receiving Security Parameters (see subclause 6.1.3.4.3.3), and an optional Discovery User Integrity Key (DUIK) for the ProSe Response Code. The Code-Receiving Security Parameters provide the information needed by the Discoverer UE to undo the protection applied by the Discoveree UE. The DUIK shall be included as a separate parameter if the Code-Receiving Security Parameters indicate that the Discoverer UE shall use Match Reports for MIC checking. The ProSe Function in the HPLMN of the Discoverer UE stores the ProSe Response Code and the Discovery User Integrity Key (if it received one outside of the Code-Receiving Security Parameters). The Code-Sending Security Parameters provide the information needed by the Discoverer UE to protect the ProSe Query Code (see subclause 6.1.3.4.3.2)

NOTE 1: There are two configurations possible for integrity checking, namely, MIC checked by the ProSe Function, and MIC checked at the UE side; this is decided by the ProSe Function that assigned the ProSe Code being monitored, and signalled to the Monitoring UE in the Code-Receiving Security Parameters.

10. The ProSe Functions in the HPLMN and VPLMN of the Discoverer UE exchange Announce Auth. messages. If the Discoverer UE is not roaming, these steps do not take place.

11. The ProSe Function in the HPLMN of the Discoverer UE returns the Discovery Response Filter and the Code-Receiving Security Parameters, the ProSe Query Code and the Code-Sending Security Parameters along with the CURRENT\_TIME and MAX\_OFFSET parameters. The Discoverer UE takes the same actions with CURRENT\_TIME and MAX\_OFFSET as described for the Monitoring UE in step 9 of subclause 6.1.3.3.1 of the current specification. The UE stores the Discovery Response Filter and its Code-Receiving Security Parameters and the ProSe Query Code and its Code-Sending Security Parameters.

Steps 12 to 14 occur over PC5.

12. The Discoverer UE sends the ProSe Query Code and also listens for a response message, if the UTC-based counter provided by the system associated with the discovery slot is within the MAX\_OFFSET of the announcing UE's ProSe clock and if the Validity Timer has not expired. The Discoverer UE forms the discovery message and protects it as described in 6.1.3.4.3.2. The four least significant bits of UTC-based counter are transmitted along with the protected discovery message.

13a. The Discoveree UE listens for a discovery message that satisfies its Discovery Filter, if the UTC-based counter associated with that discovery slot is within the MAX\_OFFSET of the Discoverer UE's ProSe clock. In order to find such a matching message, it processes the message as described in 6.1.3.4.3.3.

NOTE 1a: Match Reports are not used for the MIC checking of ProSe Query Codes.

13b. The Discoveree sends the ProSe Response Code associated with the discovered ProSe Query Code. The Discoveree UE forms the discovery message and protects it as described in 6.1.3.4.3.2. The four least significant bits of UTC-based counter are transmitted along with the protected discovery message.

14. The Discoverer UE listens for a discovery message that satisfies its Discovery Filter. In order to find such a matching message, it processes the message as described in 6.1.3.4.3.3. If the Discoverer UE was not asked to send Match Reports for MIC checking, it stops at this step from a security perspective. Otherwise it proceeds to step 15.

NOTE 2: The UE checking the integrity of the discovery message on its own does not prevent the UE from sending a Match Report due to requirements in TS 23. 303 [2]. If such a Match Report is sent, then there is no security functionality involved.

Steps 15-18 refer to a Discoverer UE that has encountered a match.

15. If the Discoverer UE has either not had the ProSe Function check the MIC for the discovered ProSe Response Code previously or the ProSe Function has checked a MIC for the ProSe Response Code and the associated Match Report refresh timer (see step 17 for details of this timer) has expired, then the Discoverer UE sends a Match Report message to the ProSe Function in the HPLMN of the Discoverer UE. The Match Report contains the UTC-based counter value with four least significant bits equal to four least significant bits received along with discovery message and nearest to the monitoring UE’s UTC-based counter associated with the discovery slot where it heard the announcement, and other discovery message parameters including the ProSe Response Code and MIC. The ProSe Function checks the MIC.

16. The ProSe Function in the HPLMN of the Discoverer UE may exchange an Auth Req/Auth Resp with the ProSe App Server to ensure that Discoverer UE is authorised to discover the Discoveree UE.

17. The ProSe Function in the HPLMN of the Discoverer UE returns to the Discoverer UE an acknowledgement that the integrity check passed. It also provides the CURRENT\_TIME parameter, by which the UE (re)sets its ProSe clock. The ProSe Function in the HPLMN of the Discoverer UE shall include the Match Report refresh timer in the message to the Discoverer UE. The Match Report refresh timer indicates how long the UE will wait before sending a new Match Report for the ProSe Response Code.

18. The Prose Function in the HPLMN of the Discoverer UE may send a Match Report Info message to the ProSe Function in the HPLMN of the Discoveree UE.

\*\*\*\*\*\*\*\*\*\*\*\* END OF CHANGES