**3GPP TSG-SA3 Meeting #116 *S3-242409***

**Jeju, Korea, 20th – 24th May 2024** revision of *S3-242076*

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.503** | **CR** | **0178** | **rev** | **-** | **Current version:** | **18.2.0** |  |
|  | | | | | | | | |
| *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 | **X** | Radio Access Network |  | Core Network |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Clarification related to U2U discovery model B | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | China Telecom, Xiaomi | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | 5G\_ProSe\_Ph2 | | | | |  | ***Date:*** | | | 2024-05-20 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **F** |  | | | | | ***Release:*** | | | Rel-18 |
|  | *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:*** | | In Model B discovery, there are two roles, discoverer UE and discoveree UE, the direct discovery procedure between two UEs uses the security material obtained from HPLMN of discoveree UE. There are three UE and two discovery procedures related RSC in U2U scene, from the text, it is hard to determine whether the security material obtained from U2U Relay together or HPLMN of discoveree UE and U2U Relay seprately for these two discovery procedure. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | * Add a Note to clarify the relationship among discoveree 5G ProSe End UE, discoverer 5G ProSe End UE and UE-to-UE Relay during the discovery procedure. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | The reused implement of UE-to-UE Relay Discovery procedure based the text are not clear. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 6.1.3.3.3.2 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 \*\*\***

###### 6.1.3.3.3.2 Security procedure for 5G ProSe UE-to-UE Relay Discovery with Model B

The security procedure for 5G ProSe UE-to-UE Discovery with Model B is shown in Figure 6.1.3.3.3.2-1.



Figure 6.1.3.3.3.2-1: Security procedure for 5G ProSe UE-to-UE Relay Discovery with Model B

0. The discoverer 5G ProSe End UE and discoveree 5G ProSe End UE are provisioned with the discovery security materials associated with a 5G ProSe Direct Discovery service based on the discovery security materials provisioning procedure for Restricted 5G ProSe Direct Discovery, as specified defined in clause 6.1.3.2.2.2.

1. The discoverer 5G ProSe End UE, discoveree 5G ProSe End UE and 5G ProSe UE-to-UE Relay are provisioned with the discovery security materials associated with an RSC based on the discovery security materials provisioning procedure for UE-to-Network Relay Discovery, as specified in clause 6.1.3.2.2.2. For the discovery procedure between 5G ProSe End UE and 5G ProSe UE-to-UE Relay, 5G ProSe End UE plays the role of 5G ProSe Remote UE and the 5G ProSe UE-to-UE Relay plays the role of a 5G ProSe UE-to-Network Relay. The discoverer 5G ProSe End UE shall construct a direct discovery set that contains two End UE discovery infos.Each End UE discovery info is protected using the discovery security materials associated with the 5G ProSe Direct Discovery service as specified in clause 6.1.3.2.3. The first protected End UE discovery info shall include User Info ID of the discoverer 5G ProSe End UE, the UTC-based counter LSB parameter, and a MIC IE. The second protected End UE discovery info shall include the and User Info ID of the discoveree 5G ProSe End UE, the UTC-based counter LSB parameter, and a MIC IE. Then, the discoverer 5G ProSe End UE shall include the direct discovery set in the Solicitation message and protect the Solicitation message using the discovery security materials associated with the RSC as specified in clause 6.1.3.2.3. The solicitation message is sent to the 5G ProSe UE-to-UE Relay.

2. On receiving the 5G ProSe UE-to-UE Relay Discovery Solicitation message from the discoverer 5G ProSe End UE, the 5G ProSe UE-to-UE Relay shall process the received UE-to-UE Relay Discovery Solicitation message using the discovery security materials associated with the RSC as specified in clause 6.1.3.2.3.

If the verification is successful, the 5G ProSe UE-to-UE Relay shall modify the UE-to-UE Relay Discovery Solicitation message to include User Info ID of the 5G ProSe UE-to-UE Relay.

The 5G ProSe UE-to-UE Relay Discovery Solicitation message is protected using the security materials associated with the RSC as specified in clause 6.1.3.2.3.

Then, 5G ProSe UE-to-UE Relay sends the message to the discoveree 5G ProSe End UE.

3. The discoveree 5G ProSe End UE shall process the received UE-to-UE Relay Discovery Solicitation message using the discovery security materials associated with the RSC as specified in clause 6.1.3.2.3.

If the verification is successful, the discoveree 5G ProSe End UE shall extract the protected direct discovery set from the message and process the protected End UE discovery infos using the discovery security materials associated with the 5G ProSe Direct Discovery service as specified in clause 6.1.3.2.3. If the verification of the second End UE discovery info is successful and the User Info ID of the discoveree matches, the discoveree 5G ProSe End UE processes the first End UE discovery info.

The discoveree 5G ProSe End UE shall construct a direct discovery set that contains two End UE discovery infos. Each End UE discovery info is protected using the discovery security materials associated with the 5G ProSe Direct Discovery service as specified in clause 6.1.3.2.3. The first protected End UE discovery info shall include User Info ID of the discoverer 5G ProSe End UE, the UTC-based counter LSB parameter, and a MIC IE. The second protected End UE discovery info shall include the User Info ID of the discoveree 5G ProSe End UE, the UTC-based counter LSB parameter, and a MIC IE. Then, the discoveree 5G ProSe End UE shall include the direct discovery set in the UE-to-UE Relay Discovery Response message and protect the UE-to-UE Relay Discovery Response message using the discovery security materials associated with the RSC as specified in clause 6.1.3.2.3. The discoveree 5G ProSe End UE replies to the 5G ProSe UE-to-UE Relay with the UE-to-UE Relay Discovery Response message.

4. On receiving the UE-to-UE Relay Discovery Response message from the discoveree 5G ProSe End UE, the 5G ProSe UE-to-UE Relay shall process the received UE-to-UE Relay Discovery Response message using the discovery security materials associated with the RSC as specified in clause 6.1.3.2.3.

If the verification is successful, the 5G ProSe UE-to-UE Relay shall modify the UE-to-UE Relay Discovery Response message to include User Info ID of 5G ProSe UE-to-UE Relay.

The UE-to-UE Relay Discovery Response message is protected using the security materials associated with the RSC as specified in clause 6.1.3.2.3. Then, 5G ProSe UE-to-UE Relay sends the UE-to-UE Relay Discovery Response message to the discoverer 5G ProSe End UE.

On receiving the UE-to-UE Relay Discovery Response message, the discoverer 5G ProSe End UE shall process the UE-to-UE Relay Discovery Response message using the discovery security materials associated with the RSC as specified in clause 6.1.3.2.3.

If the verification is successful, the discoverer 5G ProSe End UE shall extract the protected direct discovery set from the UE-to-UE Relay Discovery Response message and process the protected End UE discovery infos using the discovery security materials associated with the 5G ProSe Direct Discovery service as specified in clause 6.1.3.2.3. If the verification of the first End UE discovery info is successful and the User Info ID of the discoverer matches, the discoverer 5G ProSe End UE processes the second End UE discovery info.

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