**3GPP TSG-SA3 Meeting #115 *draft\_S3-240732-r1***

Athens, Greece, 26th February - 1st March 2024

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  |  | **CR** |  | **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 | **X** | Radio Access Network |  | Core Network |  |

|  |
| --- |
|  |
| ***Title:***  | Rel18 ProSe – Clarification on direct discovery set protection in U2U relay discovery with model A |
|  |  |
| ***Source to WG:*** | Qualcomm Incorporated |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | 5G\_ProSe\_Ph2 |  | ***Date:*** | 2024-02-16 |
|  |  |  |  |  |
| ***Category:*** |  |  | ***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 canbe 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:*** | According to clause 6.3.2.4 of TS 23.304, a 5G ProSe UE-to-UE Relay can store direct discovery sets from the discovery messages during 5G ProSe UE-to-UE Relay Discovery with Model B. If the 5G ProSe UE-to-UE Relay is also authorized to be a relay for 5G ProSe UE-to-UE Relay Discovery with Model A, it can announce the retrieved direct discovery sets. In addition, during 5G ProSe UE-to-UE Relay Discovery with Model B, the 5G ProSe End UEs indicate if they allow announcing their User Info ID by including Announce Prohibited Indication in the discovery message.If either the discoverer UE or discoveree UE only allows announcing its User Info ID, the 5G ProSe UE-to-UE Relay has to store only allowed User Info ID in the direct discovery set. This is because the direct discovery set contains both the discoverer UE and discoveree UE’s User Info ID in case of 5G ProSe UE-to-UE Relay Discovery with Model B. However, based on the security procedure for 5G ProSe UE-to-UE Relay Discovery with Model B specified in clause 6.1.3.3.3.2 of TS 33.503, the entire direct discovey set is protected by the 5G ProSe End UEs, and the 5G ProSe UE-to-UE Relay does not process the protected direct discovery set. This means the 5G ProSe UE-to-UE Relay cannot process the protected direct discovery set to only include the allowed User Info ID of the 5G ProSe End UE.  |
|  |  |
| ***Summary of change:*** | User info ID of Discoverer UE and User info ID of Discoveree UE in the direct discovery set are protected separately. |
|  |  |
| ***Consequences if not approved:*** | Lack of description on how the security procedure for 5G ProSe UE-to-UE Relay Disocvery with Model B works |
|  |  |
| ***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 1st CHANGE\*\*\*\*\*\*\*

###### 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.X.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.

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.

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 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 direct discovery set using the discovery security materials associated with the 5G ProSe Direct Discovery service as specified in clause 6.1.3.2.3.

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 direct discovery set using the discovery security materials associated with the 5G ProSe Direct Discovery service as specified in clause 6.1.3.2.3.

\*\*\*\*\*\*\*\*\*\*\*\* END OF 1st CHANGE\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\* START OF 2nd CHANGE\*\*\*\*\*\*

#### 6.1.3.3 5G ProSe UE-to-UE Relay Discovery

##### 6.1.3.3.1 General

This clause describes the security requirements and the procedures for 5G ProSe UE-to-UE Relay Discovery defined in TS 23.304 [2].

Two sets of discovery security materials are used for UE-to-UE Relay discovery message protection. Direct Discovery security materials are used by 5G ProSe End UEs to protect a direct discovery set that is an end-to-end data element between 5G ProSe End UEs and is not processed by the 5G ProSe UE-to-UE Relay. UE-to-UE Relay Discovery security materials are used by 5G ProSe UE-to-UE Relay and 5G ProSe End UEs to protect 5G ProSe UE-to-UE Relay Discovery messages. The 5G ProSe UE-to-UE Relay Discovery message includes the protected direct discovery set.

Provisioning of the Direct Discovery security materials reuses the security materials provisioning mechanism for Restricted 5G ProSe Direct Discovery as specified in clause 6.1.3.2.

Provisioning of the UE-to-UE Relay Discovery security materials reuses the security materials provisioning mechanism for 5G ProSe UE-to-Network Relay discovery as specified in clause 6.1.3.2.

The protection of 5G ProSe UE-to-UE Relay Discovery message and direct discovery set is configurable based on the provisioned discovery security materials.

NOTE 1: For a 5G ProSe UE-to-UE Relay to announce the direct discovery sets obtained from prior 5G ProSe UE-to-UE Relay Discovery with Model B, the same Direct Discovery security materials used for 5G ProSe UE-to-UE Relay Discovery with Mode B need to be used for 5G ProSe UE-to-UE Relay Discovery with Model A.

\*\*\*\*\*\*\*\*\*\*\*\* END OF 2nd CHANGE\*\*\*\*\*\*\*