**3GPP TSG-SA3 Meeting #119 *Draft\_S3-24xxxxr1***

Orlando, USA 11 - 15 November 2024

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **33.503** | **CR** | **0210** | **rev** | **-** | **Current version:** | **18.4.0** |  |
|  |
| *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:***  | Support cleartext HPLMN ID in PC5 U2U relay discovery |
|  |  |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | 5G\_ProSe\_Ph2 |  | ***Date:*** | 2024-11-04 |
|  |  |  |  |  |
| ***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 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:*** | Adding the HPLMN ID in the PC5 discovery messages for 5G ProSe U2N relay assists the 5G ProSe U2N remote UE to know the exact security parameters that were used in protecting the PC5 discovery message. For the discovery messages sent over PC5 interface, the following is specified for 5G ProSe UE-to-Network relay in clause 6.1.3.2.2 of TS 33.503 ().*For 5G ProSe UE-to-Network Relay discovery, RSC is used instead of ProSe Response Code and the announcing message also includes the HPLMN ID in cleartext to identify the discovery security materials.**For 5G ProSe UE-to-Network Relay discovery, RSC is used instead of ProSe Response Code and the discovery message also includes the HPLMN ID in cleartext to identify the discovery security materials.*Similar requirements are needed for 5G ProSe U2U relay in order to stay consistent in the whole design and optimize the 5G ProSe U2U relay discovery procedure.In clause 6.1.3.3.3 (Security flows of 5G ProSe UE-to-UE Relay Discovery) of 33.503, the discovery security materials provisioning procedure for U2N Relay Discovery is reused to get security materials by ProSe End UEs and ProSe U2U relay, e.g. in step 1b of 6.1.3.3.3.1 and step 0 of 6.1.3.3.3.2 However, the ProSe U2U relay discovery security flows doesn’t refer to 6.1.3.2.2 for discovery procedure over PC5, instead, the discovery procedure over PC5 is explicitly described in step 2-4 of 6.1.3.3.3.1 and step 1-3 of 6.1.3.3.3.2 |
|  |  |
| ***Summary of change:*** | Update 6.1.3.3.3 to include cleartext HPLMN ID in the announcing/discover message over PC5 in 5G ProSe UE-to-UE Relay Discovery procedure. Also fix editorial errors in step 1 of 6.1.3.3.3.1. |
|  |  |
| ***Consequences if not approved:*** | PC5 discovery procedure is inconsistent, and ProSe U2U relay discovery is inefficient. |
|  |  |
| ***Clauses affected:*** | 6.1.3.3.3 |
|  |  |
|  | **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:*** |  |

################### Start the 1st change ##################

##### 6.1.3.3.3 Security flows

###### 6.1.3.3.3.1 Security procedure for 5G ProSe UE-to-UE Relay Discovery with Model A

The security procedure for 5G ProSe UE-to-UE Relay Discovery with Model A is described as follows.



Figure 6.1.3.3.3.1-1: Security procedure for 5G ProSe UE-to-UE Relay Discovery with Model A

NOTE 1: The protection of direct discovery set and Announcement message reuses the protection mechanism specified in clause 6.1.3.2.3 of the present document.

1a. The monitoring 5G ProSe End UE and announcing 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 in clause 6.1.3.2.2.1 of the present document.

1b. The monitoring 5G ProSe End UE, announcing 5G ProSe End UE, and 5G ProSe UE-to-UE Relay are provisioned with 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 6.1.3.2.2.1 of the present document.

2. The announcing 5G ProSe End UE shall protect 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 of the present document. The protected direct discovery set shall include the application layer ID of the announcing 5G ProSe End UE, the UTC-based counter LSB parameter, and a MIC IE. The 5G ProSe UE-to-UE Relay obtains the RSC and protected direct discovery set from the announcing 5G ProSe End UE in proximity (e.g., via a previous 5G ProSe UE-to-UE Relay Discovery procedure as specified in clause 6.3.2.4.2 of TS 23.304 [2] or via secure PC5 unicast link between 5G ProSe UE-to-UE Relay and 5G ProSe End UE). When 5G ProSe UE-to-UE Relay Discovery is used to deliver the direct discovery set, the announcing 5G ProSe End UE shall include the RSC and protected direct discovery set in a discovery message that is protected using the discovery security materials associated with the RSC as specified in clause 6.1.3.2.3 of the present document. When 5G ProSe UE-to-UE Relay Communication is used to deliver the direct discovery set, the announcing 5G ProSe End UE shall use the secure PC5 unicast link with the 5G ProSe UE-to-UE Relay to send the RSC and protected direct discovery set. The 5G ProSe UE-to-UE Relay shall store the valid protected direct discovery set along with its validity time. A protected discovery set shall be removed once its validity time has expired. The validity time is determined from the UTC-based counter associated to the received direct discovery set that works as a timestamp.

NOTE 2: The protected direct discovery set remains valid as long as the 5G ProSe UE-to-UE Relay and Monitoring 5G ProSe End UE estimates the same UTC-based counter used by the Announcing ProSe End UE.

3. When broadcasting the Announcement message, the 5G ProSe UE-to-UE Relay shall include the HPLMN ID in cleartext and the list of valid protected direct discovery sets in the Announcement message and protect the Announcement message using the discovery security materials associated with the RSC as specified in clause 6.1.3.2.3 of the present document. Then, the 5G ProSe UE-to-UE Relay sends the Announcement message.

4. On receiving the Announcement message from the 5G ProSe UE-to-UE Relay, the monitoring 5G ProSe End UE shall process the received Announcement message using the discovery security materials associated with the RSC as specified in clause 6.1.3.2.3 of the present document. The 5G ProSe End UE decides the discovery security materials to process the announcing message based on the HPLMN ID in the announcing message. If the verification is successful, the monitoring 5G ProSe End UE shall extract the direct discovery set(s) from the Announcement message, and process the direct discovery set(s) using the discovery security materials associated with the 5G ProSe Direct Discovery service as specified in clause 6.1.3.2.3 of the present document.

###### 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 security materials provisioning procedure for the discoverer 5G ProSe End UE and 5G ProSe UE-to-UE Relay, discoverer 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 the application layer ID of the discoveree 5G ProSe End UE, the UTC-based counter LSB parameter, and a MIC IE. The second protected End UE discovery info shall include the application layer ID of the discoverer 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 application layer 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 the application layer ID of the discoveree 5G ProSe End UE, the UTC-based counter LSB parameter, and a MIC IE. The second protected End UE discovery info shall include the application layer ID of the discoverer 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 the HPLMN ID in cleartext and 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. The discoverer 5G ProSe End UE decides the discovery security materials to process the Discovery Response message based on the HPLMN ID in the message.

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 second End UE discovery info is successful and the application layer ID of the discoverer matches, the discoverer 5G ProSe End UE processes the first End UE discovery info.

################### End the change ##################