**3GPP TSG-SA3 Meeting #115 *S3-230340-r4***

**Athens, Greece, 26 Feb - 01 March 2024**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** | **0157** | **rev** | **4** | **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:*** | Protection of the direct discovery set - clarification | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Philips International B.V. | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | 5G\_ProSe | | | | |  | ***Date:*** | | | 2023-02-19 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **B** |  | | | | | ***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:*** | | The security procedures to protect the direct discovery set is specified to be similar to the security procedures used to protect ProSe discovery messages, although the direct discovery set is structured differently. Hence, changes are introduced to section 6.1.3.2.3 to capture the difference in security procedures applied to protect the direct discovery set. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | * The scrambling operation of the direct discovery set to take into account the length of the direct discovery set such that it is ensured that the UTC-based counter is not scrambled. * Partial matching after unscrambling operation to be performed against the Discoveree End UE’s User Info ID during UE-to-UE relay discovery with model B. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | * Direct discovery set may not be protected adequately thus making it irretrievable at the receiving end. * End UE to waste ressources on decryption and/or integrity verification of direct discovery set(s) that aren’t intended for it. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 6.1.3.2.3, Annex A.7 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 \*\*\***

##### 6.1.3.2.3 Protection of discovery messages over PC5 interface

There are three types of security that are used to protect the restricted 5G ProSe Direct Discovery messages over the PC5 interface: integrity protection, scrambling protection, and message-specific confidentiality which are defined in clause 6.1.3.4.3 in TS 33.303 [4]. The protection mechanisms specified in TS 33.303 [4] are reused with the following changes:

- Input parameters to integrity protection algorithm as specified in clause A.6 in the present document.

- Message-specific confidentiality mechanisms as specified in clause A.7 in the present document.

- In A.5 of TS 33.303 [4], the time-hash-bitsequence keystream is set to L least significant bits of the output of the KDF, where L is the bit length of the discovery message to be scrambled and set to Min (the length of discovery message - 16, 256).

- Step 3 of clause 6.1.3.4.3.5 of TS 33.303 [4] becomes:

XOR (0xFFFF || time-hash-bitsequence) with the most significant (L + 16) bits of discovery message.

NOTE 1: 16 is the size of Message Type and UTC-based counter LSB in bit length.

NOTE 2: The maximum length of the discovery message to be scrambled is limited to 256 bits.

- Step 2 of clause 6.1.3.4.3.2 of TS 33.303 [4] becomes:

Calculate MIC if a DUIK was provided, otherwise set MIC to a 32-bit random string. Then, set the MIC IE to the MIC.

- Step 4 of clause 6.1.3.4.3.2 of TS 33.303 [4] is not processed.

NOTE 3: Protection for the discovery messages between the ProSe UEs is provided at the ProSe layer.

In 5G ProSe UE-to-UE Relay discovery, the End UE discovery infos to be included in the direct discovery set are protected using the protection mechanism described above with the following changes:

- Message-specific confidentiality mechanisms as specified in clause A.7 in the present document with the following changes:

- discovery message is replaced by End UE discovery info

- The length of Message Type is set to zero

- In A.5 of TS 33.303 [4], the time-hash-bitsequence keystream is set to L least significant bits of the output of the KDF, where L is the bit length of the End UE discovery info to be scrambled and set to Min (the length of End UE discovery info - 8, 256).

- Step 3 of clause 6.1.3.4.3.5 of TS 33.303 [4] becomes:

If L is set to 256:

XOR the time-hash-bitsequence with the most significant L bits of the End UE discovery info.

Otherwise:

XOR (time-hash-bitsequence || 0xFF) with the most significant (L + 8) bits of the End UE discovery info.

NOTE 4: 8 is the size of the UTC-based counter LSB field in bit length.

**\*\*\* 2nd 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.

1. The discoverer 5G ProSe End UE shall protect a 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 protected direct discovery set shall include User Info ID of the discoverer 5G ProSe End UE 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 protected 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 protect a 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. Then, the discoveree 5G ProSe End UE shall include the protected 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 \*\*\***