**3GPP TSG-SA3 Meeting #116 *S3-242412-r1***

Jeju, South Korea, 20th - 24th May 2024

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **33.503** | **CR** | **0182** | **rev** | **1** | **Current version:** | **18.2.0** |  |
|  |
| *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:***  | Correction on the scrambing mechanism for U2U relay discovery |
|  |  |
| ***Source to WG:*** | Xiaomi, Philips International B.V. |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | 5G\_Prose\_Ph2 |  | ***Date:*** | 2024-05-13 |
|  |  |  |  |  |
| ***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:*** | As specified in TS 24.554, the UTC-based counter LSB is located on bits 1 to 4 of End UE discovery info, which should not be scrambled in the scrambling mechanism.However, as specified in clause 6.1.3.2.3, the time-hash-bitsequence || 0xFF is used for scrambling. As a result, the UTC-based counter LSB will be scrambled. |
|  |  |
| ***Summary of change:*** | Update the scrambling mechanism for UE-to-UE relay discovery. |
|  |  |
| ***Consequences if not approved:*** | The UTC-based counter LSB will be scrambled.  |
|  |  |
| ***Clauses affected:*** | 6.1.3.2.3 |
|  |  |
|  | **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 of the 1st Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

##### 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 - 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 the End UE discovery info.

NOTE 4: 16 is the size of the length field, spare field and UTC-based counter LSB field in bit length.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of the Changes \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*