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

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

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.503** | **CR** | **0157** | **rev** | **-** | **Current version:** | **18.1.0** |  |
|  | | | | | | | | |
| *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:*** | 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:

* 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 set to be scrambled and set to Min (the length of direct discovery set - 8, 256).
* Step 3 of clause 6.1.3.4.3.5 of TS 33.303 [4] becomes:

If L is set to 256bits:

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.

In 5G ProSe UE-to-UE Model B Relay discovery, the processing of the protected discoverer end UE discovery info shall only be performed if the received discoveree end UE user info, upon being processed, matches the discoveree end UE's User Info ID.

**\*\*\* 2nd CHANGE \*\*\***

# A.7 Message-specific confidentiality mechanisms for discovery

Message-specific confidentiality protection is provided by ProSe layer between ProSe UEs.

The use and mode of operation of the ciphering algorithms are specified in Annex D in TS 33.501 [3].

The input parameters to the ciphering algorithms as described in Annex D in TS 33.501 [3] are:

- KEY: 128 least significant bits of the output of the KDF (DUCK, UTC-based counter, MIC)

- COUNT: UTC-based counter

- BEARER: 0x00

- DIRECTION: 0x00

- LENGTH: LEN(discovery message) - (LEN(Message Type) + LEN(UTC-based counter LSB) + LEN(MIC)), where LEN(x) is the length of x in number of bits

KEY is set to as such to generate message-specific keystream as in TS 33.303 [4].

For the direct discovery set message specific confidentiality protection, LEN(discovery message) becomes LEN(end UE discovery info), and LEN(Message Type) is omitted.

The output keystream of the ciphering algorithm (output\_keystream) is then masked with the Encrytped\_bits\_mask to produce the final keystream for the message-specific confidentiality protection (KEYSTREAM):

KEYSTREAM = output\_keystream AND (Encrypted\_bits\_mask || 0xFF..FF)

The KEYSTREAM is XORed with the discovery message for message-specific confidentiality protection.

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