**3GPP TSG-SA3 Meeting #116 *S3-242130***

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

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.533** | **CR** |  | **rev** | **-** | **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 | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | PC5-U integrity protection policy for Ranging/SL positioning service | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Xiaomi | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | Ranging\_SL\_Sec | | | | |  | ***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 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:*** | | For Ranging/SL positioning services, RSPP signalling messages over PC5-U is protected via PC5 security policy configuration. Only when the integrity protection policy of PC5-U is configured to “REQUIRED”, the RSPP signalling messages can be protected. This is currently missing in TS 33.533.  If RSPP signalling messages are not integrity protected, not only the SL positioning operations between UEs can be manipulated by attackers, but also the other security mechanisms (e.g. authorization procedures defined in clause 6.3.6 and 6.3.7) relying on supplementary RSPP signalling messages lost its fundamental protection and become ineffective.  Hence it is proposed to add SR5 signalling integrity protection policy configuration for Ranging/SL positioning services. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Added the integrity protection policy on SR5 interface which transfers RSPP signalling messages for Ranging/SL positioning services, including SLPP signalling and supplementary RSPP signalling messages. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Security mechanisms relying on supplementary RSPP signalling messages become ineffective. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 6.4.2 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 the Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### 6.4.2 Security requirements

The 5G system shall support mutually authentication between the UEs during unicast direct communication establishment for Ranging/SL Positioning control over RSPP.

The 5G system shall support integrity, confidentiality and anti-replay protection for the information transferred during unicast direct communication for Ranging/SL Positioning control over RSPP.

The 5G system shall support cryptographic separation for each SR5 interface and for each peer UE during unicast direct communication for Ranging/SL Positioning control over RSPP.

The 5G system shall support integrity, confidentiality and anti-replay protection for the information transferred during unicast communication for Ranging/SL Positioning control over the protocol between the UE and LMF.

The 5G system shall support a means to configure PC5 security policies to the UE for Ranging/SL positioning services.

SR5 signalling integrity protection policy is configured to "REQUIRED" for Ranging/SL positioning services.

The 5G system shall support a means to provide confidentiality, integrity and anti-replay protection of SL positioning signalling during broadcast/groupcast communication for Ranging/SL positioning.

The 5G system shall provide a means to mitigate trackability and linkability attacks of the UE during broadcast/ groupcast communication for Ranging/SL positioning.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of the Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*