**3GPP TSG-SA3 Meeting #116 *draft\_S3-242468-r1***

Jeju, South Korea, 20th - 24th May 2024 revision of S3-242131

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

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** |  | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Xiaomi | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | \_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:*** | | According to the note in clause 6.4.1 of TS 33.533, RSPP messages includes SLPP signalling messages, supplementary service messages and supplementary RSPP signalling messages. The security requirements on broadcast/ groupcast communication over RSPP in 6.4.2 were originally defined for SLPP broadcast/groupcast signalling messages discussed in RAN2, but not for supplementary service messages and supplementary RSPP signalling messages. Hence the current wording of broadcast/ groupcast communication over RSPP in 6.4.2 and 6.4.4 is not accurate and needs to be updated.  In addition, according to the Revised WID on Expanded and Improved NR Positioning in RP-232670 approved at RAN#101, RAN specification on the protocol and procedures for SL positioning between UEs (SLPP) is restricted to unicast session-based signalling procedure only in Release 18. It means that SLPP broadcast and groupcast signalling procedures are not supported in Release 18.  However, security requirements and procedures for SLPP broadcast and groupcast signalling procedures have already been specified in current release of TS 33.533. In order to align with the updated scope of features supported by RAN WGs, it is proposed to add notes in the corresponding clauses of TS 33.533 indicating that security for SLPP broadcast and groupcast signalling procedures is not applicable in this release of the specification. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Updated the wording of broadcast/groupcast communication over RSPP in 6.4.2 and 6.4.4.  Added the notes in clauses 6.4.2 and 6.4.4.1 indicating that security for SL Positioning broadcast/groupcast signalling is not applicable in this release of the specification. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Applicability of the security requirements is not completely correct.  Security requrements and procedures are specified for the features not supported in Release 18. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 6.4.2, 6.4.4, 6.4.4.1, 6.4.4.2, 6.4.4.3.1, 6.4.4.4 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### 6.4.2 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 provide confidentiality, integrity and anti-replay protection of SL positioning broadcast/groupcast signalling.

The 5G system shall provide a means to mitigate trackability and linkability attacks of the UE during SL Positioning broadcast/ groupcast signalling procedures.

NOTE: SL Positioning broadcast/groupcast signalling procedures are not supported in this release.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of the 2nd Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### 6.4.4 Security procedure for SL Positioning broadcast/groupcast signalling protection

#### 6.4.4.1 General

This clause describes the security mechanism for protecting SL Positioning broadcast/groupcast signalling messages.

NOTE: SL Positioning broadcast/groupcast signalling procedures are not supported in this release. Hence the security mechanism for protecting SL Positioning broadcast/groupcast signalling is not applicable in this release of the specification.

#### 6.4.4.2 Security flows for broadcast/groupcast communication



Figure 6.4.4.2-1: Security flows for broadcast/groupcast communication

0a and 0b. Both sending and receiving UEs shall be provisioned with the parameters/policy for Ranging/SL positioning service as specified in clause 5.1 of TS 23.586 [2].

1a. The sending UE shall establish a secure connection with the Sidelink Positioning Key Management Function (SLPKMF) based on the security procedures specified in clause 5.2.5 of TS 33.503 [6]. The sending UE sends a Key Request message to Sidelink Positioning Key Management Function (SLPKMF) including the Ranging/SL positioning application identifier provisioned in step 0a, and UE security capabilities.

1b. The SLPKMF shall reply with the Key Response message containing the Sidelink Positioning Group Key (SLPGK), the Sidelink Positioning Group Key ID (SLPGK ID), the validity time, and the chosen ciphering and integrity algorithms. The SLPKMF may be locally configured with the UE's authorization information. Otherwise, the SLPKMF interacts with the UDM of the UE to retrieve the UE's authorization information. The chosen ciphering and integrity algorithms are determined by SLPKMF based on the received UE security capabilities in step 1a. The Key Response message may include multiple SLPGK and SLPGK ID pairs with different validity times. Group member ID shall be assigned by the SLPKMF which is included in the Key Response message. As an alternative, the sending UE may generate a Group member ID randomly.

NOTE 1: For V2X capable UEs, the security materials (e.g. SLPGK, SLPGK ID, validity time) and the ciphering and integrity algorithms used for broadcast/groupcast communication are provisioned at the application, which is out of the scope of the present document.

NOTE 2: In case the SLPKMF of a receiving UE is different from the SLPKMF of a sending UE, the provisioning of security materials as specified in clause 6.1.3.2 in TS 33.503 [6] is reused.

NOTE 3: Sidelink Positioning Group refers to a specific Ranging/SL positioning service. Accordingly, Group member ID refers to the identifier of the UE that is authorized to use the Ranging/SL positioning service.

2. The receiving UE shall perform a Key Request procedure to get security materials from the SLPKMF as described in step 1. This may happen any time before step 5.

3. The sending UE shall derive the Sidelink Positioning Traffic Key (SLPTK) from SLPGK using Group member ID, and SLPTK ID as specified in Annex A.3 of present document. SLPTK ID is a counter set to a unique value in the sending UE that has not been previously used together with the same SLPGK and the associated SLPGK ID. The UE shall use a new SLPGK and SLPGK ID pair based on step 1 before the SLPTK ID wraps around. The UE shall calculate the Sidelink Positioning Encryption Key (SLPEK) and Sidelink Positioning Integrity Key (SLPIK) from SLPTK using the chosen ciphering and integrity algorithms, respectively as specified in Annex A.4 of present document.

4. The sending UE shall protect the message as described in clause 6.4.4.3.1 and send the message.

5. Upon receiving the message matching the SLPGK ID, the receiving UE shall calculate SLPTK, SLPEK and SLPIK if it has not calculated them. The receiving UE derives security keys as in step 3 using the SLPGK ID, SLPTK ID and Group member ID (if it is included) in the received message. Then, the UE shall decrypt the message and verifies the integrity of the message as described in clause 6.4.4.3.2.

#### 6.4.4.3 Protection of messages between UEs

##### 6.4.4.3.1 Message processing in the sending UE

The UE sending a message shall construct the message as follows:

1) Form message header that contains Group member ID, SLPGK ID, SLPTK ID, and a counter. Then, append the Payload to it as illustrated in figure 6.4.4.3.1-1. The counter is used in combination with the selected ciphering algorithm and integrity algorithm.

NOTE 1: The counter can be a time counter.

2. If the chosen integrity algorithm is not the NULL algorithm, calculate MAC of the message header and the Payload based on the chosen integrity algorithm. If the chosen algorithm is the NULL algorithm, then the sending UE shall set the MAC to a 32-bit random string or all zeros in the message header. The use and mode of operation of the chosen integrity algorithm are specified in Annex D of TS 33.501 [11].

3. If the chosen ciphering algorithm is not the NULL algorithm, encrypt the Payload and MAC based on the chosen ciphering algorithm. The use and mode of operation of the chosen ciphering algorithm are specified in Annex D of TS 33.501 [11].

In case the Group member ID is provided by the SLPKMF, multiple Group member IDs can be provisioned for privacy. If multiple Group member IDs are provisioned by the SLPKMF or Group member IDs are self-generated, the sending UE shall change its Group member ID according to its policy.

NOTE 2: Additional procedures to mitigate trackability/linkability attacks may apply to Group member ID, SLPGK ID, SLPTK ID, and Counter.



Figure 6.4.4.3.1-1: Message format for Sidelink Positioning  
broadcast/groupcast communication

##### 6.4.4.3.2 Protected message processing in the receiving UE

The UE receiving a message shall do the following steps:

1. If the chosen ciphering algorithm is not the NULL algorithm, undo confidentiality protection based on the chosen ciphering algorithm.

2. If the chosen integrity algorithm is not the NULL algorithm, verify the integrity of the received message by checking MAC based on the chosen integrity algorithm. The message with MAC part filled with all zeroes is discarded.

NOTE: Freshness verification may be required.

#### 6.4.4.4 Key hierarchy for broadcast/groupcast signalling protection

The key hierarchy for broadcast/groupcast communication follows the key hierarchy for one-to-many ProSe direct communication as specified in TS 33.303 [9]. The different layers of keys (see figure 6.4.4.4-1) are the following:



Figure 6.4.4.4-1: Key hierarchy for broadcast/groupcast signalling protection

- SLPGK: SL Positioning Group Key is a 256-bit root key specific to a Ranging/SL positioning application (for broadcast) or group (for groupcast) provisioned with an expiry time. Each SLPGK has an SLPGK ID to identify it. This allows several SLPGKs to be held simultaneously for one Ranging/SL positioning application (for broadcast) or Ranging/SL positioning group (for groupcast). SLPGK may either be provisioned by the SLPKMF to the UE or be derived by the UE from locally configured long-term credentials.

- SLPTK: SL Positioning Traffic Key is a 256-bit intermediate key derived by the UE from SLPGK. It is unique per UE to ensure that each UE generates unique SLPTKs for protecting the messages it sends. Each SLPTK has a 16-bit SLPTK ID to identify it. SLPTK ID is a counter in the UE set to a unique value that has not been previously used together with the same SLPGK and associated SLPGK ID. Every time a new SLPTK needs to be derived, the SLPTK ID counter is incremented.

- SLPEK and SLPIK: The SL Positioning Encryption Key (SLPEK) and SL Positioning Integrity Key (SLPIK) are derived by the UE from SLPTK and used as broadcast/groupcast keys to protect the integrity and confidentiality of messages for Sidelink Positioning broadcast/groupcast communication respectively.

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