**3GPP TSG-SA3 Meeting #115 *S3-240866-r1\_was\_804***

Athens, Greece, 26th February - 1st March 2024

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.533** | **CR** | **0066** | **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 | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Clean up of TS 33.533 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Xiaomi, OPPO, ZTE | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | Ranging\_SL | | | | |  | ***Date:*** | | | 2024-02-19 |
|  |  | | | |  | |  | | |  |
| ***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:*** | | In current version of TS 33.533, there are some more abbreviations to be added. Some implementation errors need to be corrected. Some imcomplete sentences need to be completed. A typo needs to be corrected.  Therefore, it is proposed to make a clean up of TS 33.533. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Added some more abbreviations used in the specification.  Corrected some implementation errors.  Completed some imcomplete sentences.  Corrected one typo. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Errors and imcompleteness in the specification. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 3.3, 6.3.5, 6.4.3.3, 6.4.4.2 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 1st Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [1].

AKMA Authentication and Key Management for Applications

DCR Direct Communication Request

GBA Generic Bootstrapping Architecture

LCS Location Service

LMF Location Management Function

ProSe Proximity based Service

RSPP Ranging/SL Positioning Protocol

SLP Sidelink Positioning

SLPEK Sidelink Positioning Encryption Key

SLPGK Sidelink Positioning Group Key

SLPIK Sidelink Positioning Integrity Key

SLPK SideLink Positioning Key

SLPKMF SideLink Positioning Key Management Function

SLPP SideLink Positioning Protocol

SLPTK Sidelink Positioning Traffic Key

UTC Universal Time Coordinated

V2X Vehicle-to-Everything

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

### 6.3.5 Procedures for authorization of AF/5GC NF/LCS Client for Ranging/SL positioning service exposure

For the authorization of the AF, 5GC NF or LCS client for Ranging/SL Positioning service exposure, the SL-MT-LR procedure specified in TS 23.273 [3] is taken as the baseline. The authorization shall be performed towards all the n UEs (n ≥ 2), i.e. UE1, UE2, ..., UEn in the request message. If all of the UEs grant permission for Ranging/SL Positioning exposure, the GMLC shall forward the service request from the AF/5GC NF to the AMF. If none of the UEs grants permission for Ranging/SL Positioning exposure, the GMLC shall reject the service request. If part of the UEs grant and part of the UEs don't grant permission for Ranging/SL Positioning exposure, the GMLC shall decide to proceed with or reject the service request from the AF/5GC NF/LCS client based on the privacy check results of the n UEs and a criterion up to implementation, e.g. a local rule configured by the network operator. If the GMLC decides to accept the service request, it shall only include the identities of the UEs granting permission in the service request forwarded to the AMF.

When receiving the Ranging/SL Positioning service request from the AF, 5GC NF or LCS client, the GMLC interacts with the UDM to check the UE privacy profile. The UE LCS Privacy Profile defined in clause 5.4.2 of TS 23.273 [3] is taken as the baseline for the UE privacy profile for Ranging/SL positioning services.

NOTE: The details of the UE privacy profile for Ranging/SL positioning services needs to be align with SA2.

The GMLC interacts with the AMF to request the ranging/SL positioning result of UEs, which may include an indication of a privacy related action. If the indicator of privacy check related action indicates that the UE must either be notified or notified with privacy verification, a notification invoke message is sent to the UE if NAS connection is established. However, if the Ranging/SL Positioning service is disallowed by the UE, or NAS connection establishment fails and UE notification (including UE notification with privacy verification) is required, the AMF shall provide failure response to the GMLC.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of the 3rd Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

#### 6.4.3.3 Unicast direct communication for Ranging/SL Positioning services provided by network

For Ranging/SL Positioning services provided by network operators, the network shall support key provisioning and management for unicast direct communication. The security procedures defined for 5G ProSe UE-to-Network Relay communication in clause 6.3.3.2 of TS 33.503 [6] are reused with the following modifications:

- The SLPKMF instead of 5G PKMF is used to generate and provision the key materials for secure unicast direct communication of Ranging/SL Positioning services.

- UE SLP Key Request/Response are used instead of ProSe Remote User Key Request/Response.

- Ranging/SL Positioning Application Identifier is used instead of RSC.

- SLPK and SLPK ID are used instead of UP-PRUK and UP-PRUK ID.

- SLP Key Request/Response are used instead of Key Request/Response.

- KSLP is used instead of KNRP.

- KDF of KSLP as defined in A.2 uses Ranging/SL Positioning Application Identifier as input instead of RSC.

NOTE: This procedure does not apply to V2X capable UEs.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of the 4th Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

#### 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.

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