**3GPP TSG-SA3 Meeting #110 *Adhoc-e*** ***S3-231823***

**Online, 17 - 21 April 2023**

**Source: Philips International B.V.**

**Title:** **New solution: secure groupcast/broadcast of SL positioning data**

**Document for: Approval**

**Agenda Item: 5.19**

# 1 Decision/action requested

***This contribution proposes a new solution addressing KI#5.***

# 2 References

# 3 Rationale

This solution addresses KI#5 and proposes to protect the groupcast/broadcast of SL positioning data, in particular, SL positioning capability and SL positioning assistance data, by adapting the communication flow and security mechanisms in TS 38305 (Clause 7.5) and TS 37.355 (Clause 7.5) used for the protection of positioning assistance data.

# 4 Detailed proposal

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of Changes \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

6.Y New Solution: secure groupcast/broadcast of SL positioning data

### 6.Y.1 Introduction

This solution addresses KI#5.

This solution proposes to protect the groupcast/broadcast of SL positioning data, in particular, SL positioning capability and SL positioning assistance data, by adapting the communication flow and security mechanisms in TS 38.305 (Clause 7.5) and TS 37.355 (Clause 7.5) used for the protection of positioning assistance data.

### 6.Y.2 Solution details



**Figure 6.Y.2-1 Message flow for secure broadcast/groupcast**

The overall message flow proposed by this solution is as follows:

* Step 1: UE1 (and UE2) send a request to join a ranging service.
* Step 2: UE 1 (and UE2) are configured with the corresponding security information as applicable to the ranging service, if the UEs are authorized.

Editor’s Note: it is ffs which entity handles the keys, how UEs are identified and authorized by the CN, and how the ranging service request is protected.

* Step 3: UE 1 / UE 2 determine a ranging trigger that requires the distribution of SL ranging data when in in-coverage (IC) or partial coverage (PC).
* Step 4: UE2 sends a ranging request to retrieve SL positioning data.
* Step 5: CN, e.g., LMF, determines suitable SL positioning data, and protects it as in TS 37.355.
* Step 6: Protected SL positioning data is transferred to UE2 in charge of local groupcast/broadcast.
* Step 7: Optionally, UE2 verifies received SL positioning data before broadcast/groupcast.
* Step 8: UE 1 / UE 2 determine a ranging trigger that requires the distribution of SL positioning data when out of 3GPP coverage.
* Step 9: Optionally, UE2 adds further protection (e.g., scrambling/integrity protection) to SL positioning data.
* Step 10: Protected SL positioning data is sent by means of groupcast/broadcast.

NOTE: message fields required for data protection are left for ffs in normative phase.

In Step 2, UEs may be configured:

* with keys as in TS 37.355 for confidentiality protection when Ues are IC/PC.
* with keys as in TS 37.355 for usage when Ues are OOC. In this case, UE2 uses its key (e.g., as in step 9) for confidentiality protection of SL positioning data.
* With keys for the computation of a MIC that allows e.g., UE1 to verify SL positioning data transmitted in groupcast/broadcast.
* With keys for the scrambling of SL positioning data transmitted in groupcast/broadcast to prevent privacy threats.

If devices are out of 3GPP coverage, Steps 3-7 are not applicable. Instead, the UE (e.g., UE2) may implement the functionality of server UE thus replacing LMF functionality.

If devices are in-coverage / partial coverage, it is preferable to use Steps 3-7, although these steps may be skipped based on a policy/configuration.

Message in Step 6 may be securely transferred, e.g., as a NAS message.

Protection in Step 9 can be based on TS 37.355 for confidentiality and may include further protection (e.g., integrity protection and/or scrambling protection).

NOTE: The choice of specific security algorithms/keys is left to normative phase.

### 6.Y.3 Evaluation

TBD

|  |
| --- |
| \*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of the Changes \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* |