**3GPP TSG-SA3 Meeting #109AdHoc-e *draft\_S3-230273-r1***

**Electronic meeting, 16 - 20 January 2023**

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

**Title: Update Key Issue #1: privacy risks of exposing positioning reference signals**

**Document for: Approval**

**Agenda Item: 5.19**

# 1 Decision/action requested

***This contribution proposes to add a description and a potential security requirement regarding the potential privacy risks of exposing positioning reference signals for ranging/sidelink positioning.***

# 2 References

[1] 3GPP TS 38.211: "NR; Physical channels and modulation".

[2] 3GPP TS 38.214: "NR; Physical layer procedures for data".

# 3 Rationale

*The goal of ranging and sidelink-based positioning is to determine the range to or the position of a target UE. To this end, a target UE needs to receive or transmit reference signals from/to, e.g., a reference UE or an assistant UE, e.g., PRS and SRS [1], in a similar way as it is done in current positioning techniques, e.g., as in [2, Clause 9]. Malicious UEs might use/monitor the reference signals transmitted by the UE to determine the UE position or track the UE. For instance, if a UE keeps broadcasting the same PRS during a long period of time while moving, then tracking of the user carrying the UE is feasible.*

**

*Fig. 3-1*

*To illustrate this threat we refer to one of the multiple documents describing how ranging and sidelink-based positioning may be performed. For instance, R2-2208126 describes multiple approaches for ranging and sidelink-based positioning in which sidelink PRS are used. A particular approach in R2-2208126 that is easy to understand due to its simplicity is a SLPP session-less model between UEs 1, 2, and 3 as shown in Fig. 3-1. This approach includes a phase (2. Transmit and measure PRS) in which PRS are exchanged between UEs. A potential design option is to assign a fixed PRS, e.g., to UE2 where UE2 might be a UE requiring the ranging service and UE2 might be carried by a user. If this occurs, tracking of user by tracking the PRS broadcasted by UE2 is feasible.*

*Tdoc S3-230272 describes how such a SLPP session-less model could be protected.*

# 4 Detailed proposal

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

## 5.1 Key issue #1: Privacy protection for Ranging/SL Positioning services

### 5.1.1 Key issue details

As the information of almost all Ranging/Sidelink Positioning services is related to location, all the UEs participating in Ranging/Sidelink Positioning, including the reference UE, target UE, assistant UE, etc., may need to disclose its location information to others. If such privacy sensitive information is not well protected, the UE’s privacy could be compromised. Among the requirements defined for Ranging services in clause 6.37.2 of TS 22.261 [7], there are following requirements concerning privacy protection for Ranging services:

*The 5G system shall be able to protect privacy of a UE and its user, ensuring that no identifiable information can be tracked by undesired entities during ranging.*

*The 5G system shall be able to ensure that user privacy is not violated during ranging, e.g., subject to regional or national regulatory requirements.*

Privacy protection is also raised in clause 4.1 of TR 23.700-86 [2] as one of the architecture assumptions for Ranging/SL Positioning services and is tasked for SA3 to study. In multiple solutions (e.g. solutions #6, #9, #13, #18, #21, #23, #24, #25) of TR 23.700-86 [2], privacy is considered as an issue to be addressed, either during discovery, or during Ranging/SL positioning procedure, or for service exposure.

### 5.1.2 Security threats

When UE’s identifiable information is disclosed to undesired/malicious UEs during discovery or during communication for Ranging/SL positioning, the UE’s behaviour will become trackable to others. Hence the UE’s privacy could be violated.

The goal of ranging and sidelink-based positioning is to determine the range to or the position of a target UE. To this end, a target UE needs to receive or transmit reference signals from/to, e.g., a reference UE or an assistant UE, e.g., PRS and SRS [1], in a similar way as it is done in current positioning techniques, e.g., as in [2, Clause 9]. Malicious UEs might use/monitor the reference signals transmitted by the UE to determine the UE position or track the UE. For instance, if a UE keeps broadcasting the same PRS during a long period of time while moving, then tracking of the user carrying the UE is feasible.

When the UE’s Ranging/SL positioning information (e.g. distance measurement, direction measurement, or both, or assistant data) and/or the associated UE’s identity are disclosed to undesired/malicious UEs or undesired network functions during communication for Ranging/SL positioning, the UE’s whereabouts and/or movements will become traceable to others. Hence the UE’s privacy could be violated.

### 5.1.3 Potential security requirements

The 5G Ranging/SL Positioning system shall provide means to mitigate trackability and linkability attacks of the UE during PRS exchange.

The 5G Ranging/SL Positioning system shall provide means to mitigate trackability and linkability attacks of the UE during discovery for Ranging/SL positioning.

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

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Next Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TR 23.700-86: "Study on Architecture Enhancement to support Ranging based services and sidelink positioning"

[3] 3GPP TS 23.287: "Architecture enhancements for 5G System (5GS) to support Vehicle-to-Everything (V2X) services".

[4] 3GPP TS 23.304: "Proximity based Services (ProSe) in the 5G System (5GS)".

[5] 3GPP TS 33.536: "Security aspects of 3GPP support for advanced Vehicle-to-Everything (V2X) services".

[6] 3GPP TS 33.503: "Security Aspects of Proximity based Services (ProSe) in the 5G System (5GS)".

[7] 3GPP TS 22.261: "Service requirements for the 5G system".

[x] 3GPP TS 38.211: "NR; Physical channels and modulation".

[y] 3GPP TS 38.214: "NR; Physical layer procedures for data".

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