**3GPP TSG-SA3 Meeting #108e *draft\_S3-221973-r1***

**e-meeting, 22nd – 26th August, 2022** Revision of S3-22xxxx

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

**Title: Update Key Issue #3: source authenticity verification**

**Document for: Approval**

**Agenda Item: 5.19**

# 1 Decision/action requested

***This contribution proposes to add a potential security requirement***

***for source authenticity verification in Key Issue #3.***

# 2 References

# 3 Rationale

As described in TR 33.893 V0.1.0:

* “…when a UE discovers another UE for Ranging/SL Positioning service, both UE needs to know its own role and the role of the UE to be discovered.”
* “…if the authenticity of the discovery message cannot be verified, an attacker can impersonate the reference UE or target UE or assistant UE or Network assisted UE, or even the network function triggering the discovery. ”

These aspects imply that the source authenticity of the messages and/or involved UEs needs to be verified.

Thus, the following requirement is requested to be added: “*The 5G Ranging/SL Positioning system should be able to provide a means of source authenticity verification during discovery.*”

# 4 Detailed proposal

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

## 5.3 Key issue #3: Protection of discovery procedure

### 5.3.1 Key issue details

As per TR 23.700-86 [2], for discovery related aspects, the architecture and solutions defined for V2X and ProSe will be reused as much as possible. This provides the basis for reusing the direct discovery security defined for ProSe in TS 33.503 [6] to protect the direct discovery for Ranging/ SL Positioning services, which supports either Model A or Model B discovery.

For discovery of ProSe/V2X, the UEs can successfully discover each other if both UEs support the same ProSe/V2X service or the discovery filters provisioned to both UEs match and support the same ProSe/V2X service. Different from ProSe/V2X discovery, the discovery for Ranging/SL Positioning services needs to take the role of the UE (i.e. reference UE or target UE or assistant UE) into consideration. This means that when a UE discovers another UE for Ranging/SL Positioning service, both UE needs to know its own role and the role of the UE to be discovered.

In addition to the discovery initiated by the UE, in solutions #18 and #20 of TR 23.700-86 [2], the discovery for Ranging/SL positioning can also be triggered by the network (e.g. LMF) for discovering the Network assisted UE.

Another difference between ProSe/V2X discovery and Ranging/SL Positioning discovery is that, for ProSe/V2X, the discovery message initiated by the announcing/discoverer UE only includes its own identity. While for Ranging/SL positioning, when a UE or the network starts to initiate a discovery procedure, it may already know which UE is to be discovered for Ranging and hence may include the identity of both UEs (the identity of the initiating UE and the identity of the UE to be discovered) in the discovery message.

### 5.3.2 Security threats

During discovery, if the authenticity of the discovery message cannot be verified, an attacker can impersonate the reference UE or target UE or assistant UE or Network assisted UE, or even the network function triggering the discovery.

If the discovery messages are not integrity protected and anti-replay protected, the discovery parameters can be removed, intercepted, modified, or replayed by an attacker. Consequently, the UE may connect with a UE with an unexpected role (e.g. a reference UE connects with a reference UE) hence fails the Ranging/SL positioning service; or the UE may not connect with any UE, which is a form of DoS attack; or the UE may connect with a malicious UE which could launch more severe attacks.

If the discovery messages are not confidentiality protected, the privacy sensitive parameters (e.g. the identity of the initiating UE, the identity of the UE to be discovered) can be leaked to other irrelevant parties, hence the privacy of the UE(s) may be violated.

### 5.3.3 Potential security requirements

The 5G Ranging/SL Positioning system should be able to support integrity protection and anti-replay protection of discovery messages.

The 5G Ranging/SL Positioning system should be able to support confidentiality protection of discovery messages.

The 5G Ranging/SL Positioning system should be able to provide a means of source authenticity verification during discovery.

NOTE: Existing solutions and procedures should be reused as much as possible.

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