**3GPP TSG-SA3 Meeting #124 draft\_S3-253178-r1**

**Wuhan, China, 13th - 17th October 2025**

**Source: ZTE, Xiaomi(?)**

**Title: New key issue on Security protection for sensing result exposure**

**Document for: Approval**

**Agenda item: 5.2.7**

**Spec: 3GPP TR 33.777**

**Version: 0.1.0**

**Work Item: FS\_Sensing\_SEC**

**Comments**

This contribution proposes a new key issue about security of sensing result exposure.

**Proposed Changes**

\* \* \* First Change \* \* \* \*

## 5.1 Key Issue #1: Security of authorization for sensing service invocation and revocation and sensing result exposure

### 5.1.1 Key issue details

In TR 23.700-14 [2], architecture for sensing services is studied to enable the 3GPP network to support sensing service invocation and revocation from the service consumer, and sensing result exposure to the service consumer.

Solutions addressing the KI#2 in TR 23.700-14 [2] of authorization and revocation for particular sensing services are developed, which focus on service request authorization or revocation based on the information of the service level agreement. Security aspects need to be discussed for the above mentioned procedures.

NOTE: Security aspects of sensing service revocation triggered by sensing service consumer is addressed in this key issue.

In addition, KI#5 in TR 23.700-14 [X] addresses the type of sensing result to be exposed and the method for the network to expose the sensing result to the service consumer. Security aspect of the exposure procedure also needs to be investigated.

This key issue is related to KI#2 and KI#5 of TR 23.700-14 [2] and addresses the security aspects for sensing service invocation, revocation, and sensing result exposure procedures between the network and sensing service consumer.

### 5.1.2 Security threats

Without proper authentication and authorization for sensing service, unauthorized party may be able to access to sensing service.

If the connection between sensing service consumer and NEF/SF is not protected, the attacker can tamper, inject, sniff or replay messages related to sensing service invocation, revocation and sensing result exposure.

### 5.1.3 Potential security requirements

The 5G system shall be able to support mutual authentication between sensing service consumer and NEF/SF.

The 5G system shall be able to support integrity protection, confidentiality protection and replay protection for the communication between sensing service consumer and NEF/SF.

The 5G system shall be able to authorize sensing service request from a sensing service consumer.

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