**3GPP TSG-SA3 Meeting #123 draft\_S3-252858-r1**

**Goteborg, Sweden, 25 – 29 August 2025 merger of S3-252858, S3-252622, S3-252674, S3-252881, S3-252568, S3-252694, S3-252742**

**Source: Xiaomi, InterDigital, Huawei, HiSilicon, ZTE, Nokia, Nokia Shanghai Bell, vivo, ChinaTelecom, OPPO**

**Title: Key Issue on Security Aspects of Authorization for Sensing Service Invocation Revocation and Exposure**

**Document for: Endorsement**

**Agenda item: 6.1.8**

**Spec: 3GPP TS/TR <TS/TR number>**

**Version: <TS version>**

**Work Item: <Work Item>**

**Comments**

This paper proposes to add a new key issue for ISAC security study on security aspects of authorization for sensing service invocation, revocation and exposure.

\* \* \* First 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".

[X] 3GPP TR 23.700-14: "Study on Integrated Sensing and Communication; Stage 2".

…\* \* \* Second Change \* \* \* \*

## 5.X Key Issue #X: Security aspects of sensing service request authorization and result exposure

### 5.X.1 Key issue details

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

On the one hand, solutions addressing the KI#2 in TR 23.700-14 [X] 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 about for the above mentioned procedures.

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

On the other hand, 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 addresses the security aspects for sensing service innovation, revocation and sensing data/result exposure procedures between the network and sensing service consumer.

### 5.X.2 Security threats

Without proper authentication and authorization for sensing service, unauthorized party may be able to access to sensing service, and illegally collect sensing information, that may impact normal 5G communication or other services, and also imply incompliance with regulatory requirements.

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 data/result exposure.

### 5.X.1 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 anti-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 \* \* \* \*