**3GPP TSG-SA3 Meeting #123 draft\_S3-252859-r1**

**Goteborg, Sweden, 25 – 29 August 2025 merger of S3-252859, S3-252673, and S3-252743**

**Source: Xiaomi, InterDigital, Huawei, HiSilicon, OPPO, vivo, China Telecom**

**Title: Key Issue on Security Protection for Sensing Service Operations**

**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 on security protection for sensing service operations for ISAC security study.

\* \* \* 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 (Release 20)"

…\* \* \* Second Change \* \* \* \*

## 5.X Key Issue #X: Security protection for sensing service operations

### 5.X.1 Key issue details

According to TR 23.700-14 [X], after the sensing service request from the service consumer is authorized by the network, sensing service operations will be triggered and performed by the relevant network functions, which communicate with each other to obtain the sensing result.

In TR 23.700-14 [X], there are multiple solutions proposing sensing service operation procedures supported by sensing entities and different sensing related network functions (e.g. NEF, SF, sensing management function, sensing control function, sensing processing function). The NEF needs to discover and select the SF to trigger sensing service operation. The SF needs to discover and select proper sensing entity to collect sensing data in a specific sensing mode. To support the discovery and selection by the SF, sensing entities need to register themselves in the network with their profiles. After sensing data is collected by the selected sensing entities, the data needs to be transported to the SF to be processed for sensing result generation. When any of the service conditions of a sensing service is no longer met, an ongoing sensing service can be revoked by the network. The security aspects of all these sensing operations and procedures are to be addressed in this key issue.

NOTE x: Security aspects of service operation revocation triggered by sensing functions is addressed in this key issue, as it can be viewed as one type of sensing service operations.

### 5.X.2 Security threats

As the sensing service operations are performed between sensing functions and between sensing entity and sensing function, if the sensing functions and sensing entities are not authenticated for participating in the operations, an attacker is able to impersonate a sensing function or sensing entity to join in and manipulate (e.g. maliciously revoke) any of the sensing operations.

As the sensing service operations are performed between sensing functions and between sensing entity and sensing function, if the sensing functions and sensing entities are not authorized for participating in the operations, misbehaving network function or sensing entity can access/revoke any of the sensing operations which are not allowed to be accessed/revoked.

If the connections between sensing related network functions are not securely established (e.g. between the NEF and SF), an attacker is able to tamper or inject or replay sensing operation messages and the sensing result to be exposed, or sniff the sensing result.

If the connection between sensing entity and sensing related network function is not securely established, an attacker is able to tamper or inject or replay sensing control messages and sensing data, or sniff the collected sensing data.

### 5.X.1 Potential security requirements

The 5G system shall be able to support mutual authentication between SFs and between the sensing entity and SF.

The 5G system shall be able to support authorization for sensing service operations.

The 5G system shall be able to support integrity protection, confidentiality protection and anti-replay protection for the connections between SFs and between sensing entity and SF.

NOTE y: If there is no interaction between SFs based on architecture defined in SA2, the security requirements between SFs are not needed.

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