**3GPP TSG-SA3 Meeting #124 draft\_S3-253751-r2**

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

**Source: Huawei, HiSilicon**

**Title: New Solution to secure the connection between Sensing Entity and SF**

**Document for: Approval**

**Agenda item: 5.2.7**

**Spec: 3GPP TR 33.777**

**Version: 0.0.0**

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

**Comments**

This contribution aims to provide solution to address the connection security between Sensing Entity and SF, by reusing existing mechanisms.

Was S3-253394.

\* \* \* 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".

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

[3] 3GPP TS 22.137: "Service requirements for Integrated Sensing and Communication; Stage 1".

[4] 3GPP TR 22.837: "Feasibility Study on Integrated Sensing and Communication".

[5] 3GPP TS 33.501: "Security architecture and procedures for 5G system".

\* \* \* Second Change \* \* \* \*

## 6.0 Mapping of solutions to key issues

Editor's Note: This clause contains a table mapping between key issues and solutions.

Table 6.1-1: Mapping of solutions to key issues

|  |  |  |  |
| --- | --- | --- | --- |
| Solutions | KI#1 | KI#2 | KI#Z |
| 2.X |  | X |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

\* \* \* Third Change \* \* \* \*

## 6.2 Solutions to KI#2

### 6.2.X Solution #2.X: Security of the connection between Sensing Entity and SF

#### 6.2.X.1 Introduction

This solution aims to address the following security requirement as listed in Key Issue #2 Security protection for sensing service operations:

*‘The 5G system shall be able to support integrity protection, confidentiality protection and replay protection for the connection between sensing entity and SF.’*

This solution to secure the connection between Sensing Entity and Sensing Function (SF). SF is responsible for to handle both sensing service control and sensing data processing.

Editor’s Note: the architecture of SF needs to further align with SA WG2.

#### 6.2.X.2 Solution details

The SF supports a direct interface (e.g. Nx interface) to send the sensing service control signalling to sensing entity, and the sensing entity uses the same interface to reply the sensing data to the SF.

In this architecture, the security mechanisms for non-service based interfaces as specified in clause 9.2 of [5] are reused to offer the integrity protection, confidentiality protection and replay protection for the connection between sensing entity and SF.

Editor’s Note: Whether using direct connection between SF and sensing entity needs to align with SA WG2.

Editor’s Note: the architecture of SF needs to further align with SA WG2 and the security is FFS.

#### 6.2.X.3 Evaluation

TBD.

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