**3GPP TSG-SA3 Meeting #123 draft\_S3-253012-r2**

**Goteborg, Sweden, 25 – 29 August 2025**

**Source: Huawei, HiSilicon, Xiaomi**

**Title: Adding scope of Sensing**

**Document for: Approval**

**Agenda item: 6.1.8**

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

**Version: <TS version>**

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

**Comments**

Based on the agreement in RAN (RP-251861), the scope of Integrated Sensing and Communication (ISAC) in Rel-20 focuses on the gNB-based mono-static sensing mode for UAV sensing target use case. The scope of the architecture study (SP-250833) also aligns with above agreement with considering the aspects of architecture enhancement and end-to-end operations procedures to support sensing services, and the architecture enhancement study of Sensing has been initiated in TR 23.700-14.

As a highly architecture dependency topic, the security and privacy scopes of Sensing are limited due to the limited scenario in both RAN and SA2. In SA1, all the potential use cases in the UAV scenario serve either the purpose of public safety, or as requested by the management entity (UAV management department, USS or UTM), without the necessity to identify the object. This contribution aims to provide the scope of the Sensing study based on the above observations.

Was S3-252675, merger of S3-252870.

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

# 1 Scope

The present document investigates and identifies the security threats, requirements and potential solution for Integrated Sensing and Communication (ISAC). Based on the architecture and system level enhancements studied in TR 23.700-14 [a1], this document focuses on the security aspects of gNB-based mono-static sensing mode for UAV sensing target use cases.

The UAV sensing target uses cases defined by TS 22.137 [a2] and TR 22.837 [a3] serve either the purpose of public safety, or as requested by the management entity (UAV management department, USS or UTM), without the necessity to identify the object.

Specifically, the present document covers the following:

- The identified key issues, threats, potential requirements and solutions for security protection during the service operations and procedures supporting Sensing services;

- The identified key issues, threats, potential requirements and solutions for protecting privacy for sensing data collection, sensing data processing, and sensing data exposure.

\* \* \* Second 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".

 [a1] 3GPP TR 23.700-14: "Study on Integrated Sensing and Communication; Stage 2".[a2] 3GPP TS 22.137: "Service requirements for Integrated Sensing and Communication; Stage 1".

[a3] 3GPP TR 22.837: "Feasibility Study on Integrated Sensing and Communication".

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