**3GPP TSG-SA3 Meeting #123 draft\_S3-252860-r2**

**Goteborg, Sweden, 25 – 29 August 2025 merger of S3-252860, S3-252623, and S3-252764**

**Source: Xiaomi, InterDigital, NTT DOCOMO, ZTE**

**Title: Key Issue on Privacy Protection for Sensing Services**

**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 privacy protection for sensing services 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".

…\* \* \* Second Change \* \* \* \*

## 5.X Key Issue #X: Privacy protection for sensing services

### 5.X.1 Key issue details

Sensing technology enables the detection of objects and activities without requiring a direct line of sight, such as around corners, through walls, and behind closed doors. This capability can intrude upon areas once considered private, including apartments, other living spaces, and even more specific locations like the interiors of bags, boxes, or clothing.

Importantly, individuals being sensed do not need to have any business relationship with the entities performing the sensing and may not even carry a 3GPP defined device.

According to TR 23.700-14 [X], integration of sensing and communication requires 3GPP network to support the following sensing data handling procedures: sensing data collection, sensing data processing, and sensing result exposure. If the sensing data or sensing result for a sensing service contain privacy sensitive information, the privacy aspect of the sensing service needs to be investigated.

### 5.X.2 Security threats

The threat to the service is that non-adherence to privacy requirements will make it illegal to deploy sensing.

Threats to individuals being sensed include loss of control of personal data and loss of privacy.

In some use cases, sensing data or result may contain privacy sensitive information. If such sensitive information is leaked out during the transmission of the sensing data or result, the privacy may be violated.

### 5.X.1 Potential security requirements

The sensing system shall ensure privacy of individuals subjected to sensing, including privacy sensitive information, even if they are not subscribers of the sensing operator.

The sensing system shall ensure privacy in locations where sensing is not allowed.

NOTE 1: The locations include non-public places, places of national security relevance.

NOTE 2: The security requirements do not require 3GPP to provide mechanism(s), as this may be addressed by out-of-3GPP, e.g., Regulations.

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