**3GPP TSG-SA3 Meeting #124 draft\_S3-253744-r1**

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

**Source: ZTE**

**Title: New solution on authorization for sensing service request from AF**

**Document for: Approval**

**Agenda item: 5.2.7**

**Spec: 3GPP TR 33.777**

**Version: 0.1.0**

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

**Comments**

The contribution proposes to add a new solution for key issue #1.

**Proposed Changes**

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

## 6.Y Solution #Y: Authorization for sensing service request from AF

### 6.Y.1 Introduction

This solution addresses Key Issue #1: Security of authorization for sensing service invocation and revocation.

In this solution, the sensing service consumer is assumed to be an external AF. The NEF performs the access authorization by verifying the AF's identity, and the SF performs the service authorization by validating the feasibility and policy compliance of the specific sensing request parameters against network capabilities and operator rules.

Editor’s Note: Whether this solution is applicable only for external AF is FFS.

### 6.Y.2 Solution details

This solution proposes mutual certificate-based authentication between the NEF and the external AF/sensing service consumer using TLS. Certificate based authentication follows the profiles given in 3GPP TS 33.310 [x], clause 6.1.3a. The identities in the end entity certificates is used for authentication and policy checks.

For the protection of communication between AF/sensing service consumer and NEF, TLS is used to provide integrity protection, replay protection and confidentiality protection for the interface between the NEF and the AF/sensing service consumer. Security profiles for TLS implementation and usage follow the provisions given in clause 6.2 of TS 33.210 [y].

After the authentication, the following procedures are used for authorizing sensing service request.



Figure 6.Y.2-1: Procedure for sensing service authorization

1. The AF sends sensing service request message to the NEF. The message includes AF ID, OAuth 2.0 token, and sensing service related parameters (e.g., target sensing area, sensing time, sensing accuracy, etc).

Editor’s note: Details of the sensing service related parameters are FFS.

1. NEF performs the authorization check for the sensing service request. This includes:

- validating the OAuth 2.0 token presented by the AF; and

- checking the AF's subscription profile to verify that the AF is entitled to request the sensing service.

If the check fails, the NEF rejects the request with a failure cause.

1. If the AF is authorized by the NEF to request for sensing service, the NEF discovers and selects the SF, and sends the Sensing service request message to the SF. This message includes sensing service related parameters.
2. The SF performs sensing service authorization based on the sensing service related parameters. Specifically, this includes:

- validating the sensing service related parameters against operator-defined service policies (e.g., restricted zones, restricted time); and

- checking if the network has available resources to fulfill the request.

If the authorization fails, the SF rejects the request with a failure cause. The reject message is sent to AF via NEF.

Editor’s note: Other validations performed by SF for sensing service authorization are FFS.

1. After successful authorization, the SF proceeds to execute the sensing service.

6-7. The SF provides sensing results in sensing service response to the AF via NEF.

Editor’s note: Details of the procedures are to be aligned with TR 23.700-14 [x].

### 6.Y.3 Evaluation

TBD

\* \* \* End of First Change \* \* \* \*

\* \* \* 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".

[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 TR 33.501: "Security architecture and procedures for 5G system".

[x] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

[y] 3GPP TS 33.210 :”3G security; Network Domain Security (NDS); IP network layer security”.

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