**3GPP TSG-SA3 Meeting #124 S3-253746r3**

**Wuhan, China, 13 – 17 October 2025** revision of S3-253514

**Source: Nokia, Nokia Shanghai Bell**

**Title: new solution on authorization of sensing service request**

**Document for: Approval**

**Agenda item: 5.2.7**

**Spec: 3GPP TR 33.777**

**Version: 0.1.0**

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

**Comments**

New solution to address KI#1: authorization for sensing service invocation and revocation

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

<all content is new>

## 6.X Solutions to KI#X

### 6.X.Y Solution #X.Y: authorize sensing service request using OAuth-based authorization mechanism

#### 6.X.Y.1 Introduction

The solution addresses KI#1 to authorize sensing service request from the sensing service consumer

Key issues related to System Architecture to Support Sensing, Authorization and Revocation to Support Sensing Service, and Sensing Result Exposure are studied in TR 23.700-14. Based on solutions for those KIs, a sensing service consumer may access sensing service from sensing function indirectly via NEF. For example, if the sensing service consumer is external AF, it accesses the sensing function through NEF. The sensing service request may trigger operation or revocation of sensing on specific object in specific area at specific accuracy level during specific time, or subscribe to specific sensing result. Sensing service authorization polices are defined in some solutions, and local policies-based authorization is also discussed in some solutions.

If the sensing service consumer is external AF, as specified in clause 12 of TS 33.501, the NEF shall authorize the requests from AF using OAuth-based authorization mechanism, the specific authorization mechanisms shall follow the provisions given in RFC 6749 [43]. When the NEF supports CAPIF for external exposure as specified in clause 6.2.5.1 in TS 23.501[2], then CAPIF core function shall choose the appropriate CAPIF-2e security method as defined in the sub-clause 6.5.2 in TS 33.122[53] for mutual authentication and protection of the NEF – AF interface.

In general, OAuth 2.0 based authorization can be reused to authorize sensing service request from sensing service consumer.

Editor’s Note: As sensing architecture and procedures, and sensing authorization policies are still under discussion in TR 23.700-14, where to retrieve sensing authorization policies, which network function and how to authorize the content of sensing service request by using OAuth 2.0 based authorization is FFS.

Editor’s Note: the architecture and workflow need to inline to SA2

#### 6.X.Y.3 Evaluation

Editor’s Note: Each solution should motivate how the potential security requirements of the key issues being addressed are fulfilled.

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