**3GPP TSG-SA3 Meeting #124 draft\_S3-253748-r2**

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

**Source: Ericsson**

**Title: Reusing existing mechanism for security of authorization of sensing service operation**

**Document for: Approval**

**Agenda item:** **5.2.7**

**Spec:** **3GPP TR 33.777**

**Version:** **0.1.0**

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

**Comments**

This document proposes a solution reusing existing mechanism for Key Issue #1 (security of authorization for sensing service invocation and revocation) in TR 33.777.

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

## 6.X Solutions to KI#1

### 6.X.Y Solution #X.Y: Reusing existing mechanism for security of authorization of sensing service

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

This solution addresses the Key Issue #1 (security of authorization for sensing service invocation and revocation). Authentication, communication security, and authorization aspects for NEF and AF interaction have already been specified in Clause 12 of TS 33.501 [5]. The interface between the sensing service consumer acting as an AF and the NEF, is the same interface whose security is addressed in Clause 12 of TS 33.501 [5].

Editor’s Note: The architecture and workflow needs to inline with SA2.

#### 6.X.Y.2 Solution details

The security mechanism, specified in Clause 12 of TS 33.501 [5], is reused to address the security requirements of mutual authentication, integrity protection, confidentiality protection, replay protection, authorization for the communication between sensing service consumer and NEF.

Editor’s Note: The authorization of the content of the Sensing Service Request is FFS

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

TBD

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