**3GPP TSG-SA3 Meeting #124 draft\_S3-253395-r1**

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

**Source: Huawei, HiSilicon**

**Title: New Solution to secure the connection to the Sensing service consumer**

**Document for: Approval**

**Agenda item: 5.2.7**

**Spec: 3GPP TR 33.777**

**Version: 0.0.0**

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

**Comments**

This contribution aims to use existing security mechanism to address security requirements of KI#1.

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

## 6.0 Mapping of solutions to key issues

Editor's Note: This clause contains a table mapping between key issues and solutions.

Table 6.1-1: Mapping of solutions to key issues

|  |  |  |  |
| --- | --- | --- | --- |
| Solutions | KI#1 | KI#2 | KI#Z |
| 2.X | X |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

\* \* \* Second Change \* \* \* \*

## 6.1 Solutions to KI#1

### 6.1.X Solution #1.X: Security of the connection to the Sensing service consumer

#### 6.1.X.1 Introduction

This solution aims to address the security requirements in Key Issue #2. In TR 23.700-14 [2], architecture for sensing services is studied to enable the 3GPP network to support sensing service invocation and revocation from the service consumer.

#### 6.1.X.2 Solution details

The Sensing service consumer acts as external Application Function (AF) to interact with the network.

If the Sensing service consumer acting as external AF then it only interacts with network via NEF. In this case the security mechanisms in clauses 12 of [5] are reused to provide mutual authentication, authorisation, integrity protection, confidentiality protection and replay protection between Sensing service consumer and the NEF.

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

#### 6.1.X.3 Evaluation

TBD.

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