**3GPP TSG-SA3 Meeting #115 *S3-240474-r2***

**Athens, Greece, 26 February – 01 March 2023**

**Source: IIT Delhi, Samsung, IIT Bhilai, IIT Jodhpur, Lenovo, DoT, IIT Bombay**

**Title: Key issue on SUPI privacy issue in PLMN hosting NPN scenario**

**Document for: Approval**

**Agenda Item: 5.3**

# 1 Decision/action requested

***It is proposed to approve this Key issue to study potential solutions.***

# 2 References

[1] 3GPP TS 22.261 Service requirements for the 5G system

[2] 3GPP TS 33.501 Security architecture and procedures for 5G system

# 3 Rationale

It is proposed to approve this key issue.

# 4 Detailed proposal

\*\*\* BEGIN OF 1st CHANGE \*\*\*

## 5.X Key issue #X: SUPI privacy issue in PLMN hosting NPN scenario

### 5.X.1 Key issue details

SA1 has captured the scenario for NPN security considerations in clause 8.2 of TS 22.261 [1], which is:

|  |
| --- |
| *The 5G system shall enable a PLMN to host an NPN without compromising the security of that PLMN.*  *NOTE: Dedicated network entities of NPN can be deployed in customer premises that are outside the control of the PLMN operator.* |

When NPN is hosted by a PLMN, there are two possible deployment scenarios as below:

- For scenario 1, dedicated UPF is deployed in customer premises, with N4 interface (non-SBA interface) with the operator premises.

- For scenario 2, dedicated UPF and part of CP functions are deployed in customer premises with SBA interface with operator premises.

Considering primary authentication and authorization procedure specified in clause in TS 33.501 [2], if a Subscription Permanent Identifier (SUPI) is available in clear text to the NFs in customer premises then it may potentially lead to security threats, privacy breach, UE location tracking and targeted attacks.

Further, with the evolution of the roaming architectures (Roaming Hub) and Core network (NPN, Edge computing), distributed CN (multi-site CN), as there is no direct trust relationship between HN and SN/VPLMN/Edge network (i.e., between the different security domains), in this case HN need to consider exposing of permanent and/or sensitive identifiers/ parameter to the NFs in different security domain.

The privacy sensitive SUPI is the home network operator provided identifier used exclusively to identify its subscribers and related subscription information to handle the related services.

This key issue is to study how to avoid exposure of the sensitive parameters (specifically, permanent identifier) to the entities outside the MNO premises (in other security domains).

### 5.X.2 Security Threats

An attacker can compromise NFs in customer premise and can retrieve the SUPI to launch targeted attacks.

A NFs can be compromised in customer premises, then Subscription Permanent Identifier (SUPI) is available to the attacker, it can potentially lead to security threats, like privacy breach, UE location tracking, mapping of the user to the identifiers and targeted DoS.

### 5.X.3 Potential security requirements

The 5G system shall support a mechanism to ensure protection of the sensitive parameters against the risk caused by PLMN hosting NPN and vice versa

\*\*\* END OF 1nd CHANGE \*\*\*