**3GPP TSG-SA3 Meeting #116 *S3-241983***

Jeju, Republic of Korea, 20th – 24th May 2024

**Source: Huawei, HiSilicon**

**Title: Using 3GPP security context to derive authentication pre-shared key for NIN3A**

**Document for: Approval**

**Agenda Item: 5.15**

# 1 Decision/action requested

***Approve the pCR to*** ***TR 33.754[1].***

# 2 References

[1] 3GPP TR 33.754: "Study on security aspects for Multi-Access (DualSteer + ATSSS Ph-4) ".

# 3 Rationale

This contribution proposes a new solution about using 3GPP security context to derive authentication key for non-3GPP in ATSSS over Non-Integrated Non-3GPP Access (NIN3A).

# 4 Detailed proposal

\*\*\* Start of 1st Change \*\*\*

## 6.Y Solution #Y: Using 3GPP security context to derive authentication pre-shared key for NIN3A

### 6.Y.1 Introduction

This solution addresses key issue #1.

This solution gives the key architecture for ATSSS-Lite scenario and lists some options about how to derive and obtain the authentication key used for non-3GPP access between UE and UPF.

### 6.Y.2 Solution details

In simplified ATSSS architecture, there is an assumption that UE will establishe connection with network and establish PDU session using 3GPP access. Considering UE and network already generated shared security context during the registration procedure via 3GPP acess. A sub-level shared key can be generated, and be used as a pre-shared key for IKEv2 procedure.

The key hierarchy defined in TS 33.501[3] for this scenario can be extended as follows:



Figure 6.Y.2.1 Key hierarchy generation for ATSSS-lite scenario

A new key KUPF is derived from KAMF as depicted in Figure 6. Y.2.1. AMF derives the KUPF from KAMF during the PDU session establishment procedure over 3GPP access as showing in clause 6.Y.2 of S3-241982.

Reagrding with when SMF gets the KUPF in the case the SMF needs to transfer the KUPF, there are severl options:

Option 1: AMF sends KUPF to SMF in the CreateSMContext Request message, SMF selects the UPF and sends the key KUPF to UPF.

Option 2: SMF requests the key from AMF and based on the reply, the SMF further sends it to UPF during the PDU session establishment procedure.

Reagrding with when UPF gets the KUPF, there are severl options as well:

Option 1: UPF requests the key from SMF based on the request from the UE via NIN3A.

Option 2: SMF sends the key to the UPF during the PDU session establishment procedure.

Option 3: SMF requests the key from AMF and AMF sends the key to UPF during the PDU session establishment procedure.

Editor’s Note: the details of KUPF derivation from KAMF can be FFS.

### 6.Y.3 Evaluation

TBD

There is no direct interface between UPF and AMF, AMF directly sends KUPF to UPF has 5G system impact.

\*\*\* End of 1st Change \*\*\*