**3GPP TSG-SA3 Meeting #116 *S3-242575***

Jeju, Republic of Korea, 20th – 24th May 2024 is the revision of S3-241982

**Source: Huawei, HiSilicon**

**Title: IPsec solution between UE and UPF**

**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 IPsec to authenticate UE in ATSSS over Non-Integrated Non-3GPP (NIN3A) Access.

# 4 Detailed proposal

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

## 6.Y Solution #Y: Using IPsec to authenticate UE and UPF for non-3GPP access

### 6.Y.1 Introduction

This solution addresses key issue #1.

 The authentication of UE during the IKEv2 procedure can be optimized by using the 3GPP security context for the same UE.

### 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. In that case, before UE connects to UPF through NIN3A, UE and network already shared security context for 3GPP access. So, the authentication method of IKEv2 protocol for non-3GPP access can utilise pre-shared key between UE and UPF instead of EAP-5G method. The specific procedure is as follows:

 

**Figure 6.Y.2.1 ATSSS-lite authentication procedure over NIN3A**

1. 3GPP registration procedure is executed between UE and network through 3GPP access.

2. UE sends PDU session request to AMF through 3GPP access which carries an ATSSS-Lite indication.

3-4. AMF selects ATSSS-lite enabled SMF and forwards PDU session request to SMF.

5. SMF selects ATSSS-lite enabled UPF and obtains an authentication key KUPF for the direct connection between the UE and the UPF. Then the SMF initiates the N4 Session Establishment procedure with the selected UPF and sends the KUPF to UPF.

6. The UPF allocates the IP address for the IPSec functionality of the UPF and responds to the SMF the N4 Session Establishment Accept message including the UPF IP address which is to be used for establishment of the IPSec tunnel with the UE.

Editor’s Note: The UPF IP address to establish IPsec tunnel, is a dynamic IP address allocated per UE and PDU session is FFS.7. UPF IP address is sent to UE along with the PDU session accept message.

8. UE derives the key KUPF used for authentication between UE and UPF.

9. Data Link Layer L2 is connected.

10.The UE starts the IPSec Tunnel Establishment procedure to the UPF indicated by the UPF IP address received in PDU Session Establishment Accept message via 3GPP access, and exchanges the first pair of messages known as IKE\_SA\_INIT.

11.UE sends the IKE\_AUTH\_request to the UPF with the Authentication Method “Shared Key Message Integrity Code” (i.e. the value of authentication method is “2”), and the MAC value (MAC1) carried in the AUTH payload is constructed using the derived key KUPF in step 8.

12.The UPF will check the validity of MAC value carried in AUTH payload using the KUPF as described in step 5. If the verification is passed, UPF constructs AUTH payload as in step 11 (with authentication method is “2”, and MAC2 constructed from KUPF) and sends it to UE.

Editor’s Note: The message name is FFS.

UE checks the validity of AUTH payload using the KUPF and if the verification passed the authentication of UPF to UE is also passed.

13. UE and UPF run the CREAT\_CHILD\_SA procedure and establish the IPsec security tunnel.

### 6.Y.3 Evaluation

TBD

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