**3GPP TSG-SA3 Meeting #108Adhoc-e draft\_S3-222516-r2**

**e-meeting, 10th – 14th October, 2022**

**Source:**  **Huawei, HiSilicon**

**Title:** **Solution on PINE authentication**

**Document for: Approval**

**Agenda Item: 5.10**

# 1 Decision/action requested

***It is proposed to approve the change described in this document.***

# 2 References

[1] 3GPP TR 33.882: " Study on personal IoT networks security aspects".

# 3 Rationale

If the PINE without 3GPP creditial, it’s proposed to use PIN authentication to authorize PINE.

# 4 Detailed proposal

\*\*\* 1st CHANGE \*\*\*

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TR 23.700-88: "Study on Personal IoT Networks"

[Y] 3GPP TS 33.501: " Security architecture and procedures for 5G system"

\*\*\* END OF 1st CHANGE\*\*\*

\*\*\* 2nd CHANGE \*\*\*

## 6.X Solution #X: PINE authentication and authorization

### 6.X.1 Introduction

This solution addresses the requirement in KI#1 on authentication and authorization for PINE.

This solution provides a method to ensure that the PINE can be authenticated and authorized by a AF before the connectivity for PINE is enabled. The authentication may be triggered by the SMF during the PDU session modification procedure. The authorization is performed based on authentication results.

### 6.X.2 Solution details



Figure 6.X.2-1 call flow of authentication and authorization for PINE

As show in the Figure 6.X.2-1, the details of authentication and authorization for PINE is summarized as following:

1. PEGC registates to the 5GS and joins into the PIN.

2. A PINE requests to access the PEGC for traffic relay to 5GS.

NOTE: the transport mechanism used to send the access request from PINE to PEGC is out of 3GPP scope.

3. The PEGC initiates PDU Session modification procedure with the PINE information sent to the SMF via NAS signalling. PINE information includes at least PINE ID.

4. The SMF determines whether authentication is required for the PINE. Authentication for PINE shall only be triggered if the PEGC has provided PINE ID. The SMF triggers the authentication procedure and send a message to AF via NEF. The authentication messages are included in a transparent container and conveyed between the PINE and the AF via 5GC. AF provides authentication result to SMF. In this case, authorization is performed based on authentication results.

NOTE: Multiple round-trip messages may be needed as required by the authentication method used by the AF. The method used to authenticate the UE (e.g. whether over EAP or not) and the content of Authentication Messages (e.g. EAP packets) to support that method are out of scope of 3GPP.

Editor’s Note: How does 5GC/SMF identify PINE is FFS.

5. The SMF updates the PCF with the PINE information in SM Policy Association Modification if PINE is authorized.

6. The QoS flow for the PINE communication with 5GS is established via PDU session modification procedure.

7. The PEGC sends a response to the PINE.

8. The application traffic of the PINE is relayed to the AF via the PEGC and 5GS.

### 6.X.3 Evaluation

TBD

Editor’s Note: The impact to 5GC is FFS.

\*\*\* END OF 2nd CHANGE\*\*\*