|  |  |
| --- | --- |
| 3GPP TR 33.882 V0.3.0 (2022-10) | |
| Technical Report | |
| 3rd Generation Partnership Project;  Technical Specification Group Services and System Aspects;  Study on personal IoT networks security aspects  (Release 18) | |
|  | |
|  | 3GPP-logo_web |
|  | |
| The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP. The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented. This Specification is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification. Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices. | |

|  |
| --- |
|  |
| ***3GPP***  Postal address  3GPP support office address  650 Route des Lucioles - Sophia Antipolis  Valbonne - FRANCE  Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16  Internet  http://www.3gpp.org |
| ***Copyright Notification***  No part may be reproduced except as authorized by written permission. The copyright and the foregoing restriction extend to reproduction in all media.  © 2022, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).  All rights reserved.  UMTS™ is a Trade Mark of ETSI registered for the benefit of its members  3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners LTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners  GSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 4

1 Scope 6

2 References 6

3 Definitions of terms and abbreviations 6

3.1 Terms 6

3.2 Abbreviations 7

4 Assumptions 7

5 Key issues 7

5.1 Key Issue #1: Authentication and authorization for PINE 7

5.1.1 Key issue details 7

5.1.2 Security threats 7

5.1.3 Potential security requirements 7

5.2 Key Issue #2: Authorization of PIN capabilities 8

5.2.1 Key issue details 8

5.2.2 Security threats 8

5.2.3 Potential security requirements 8

6 Proposed solutions 8

6.1 Mapping of solutions to key issues 8

6.2 Solution #1: PINE authentication and authorization 8

6.2.1 Introduction 8

6.2.2 Solution details 9

6.2.3 Evaluation 9

6.3 Solution #2: Authentication and authorization for PINE 10

6.3.1 Introduction 10

6.3.2 Solution details 10

6.3.3 Evaluation 11

6.4 Solution #3: Authentication for PIN elements involving SMF 11

6.4.1 Introduction 11

6.4.2 Solution details 11

6.4.3 Evaluation 13

6.5 Solution #4: PEGC/PEMC and PINE Authentication and Authorization 13

6.5.1 Introduction 13

6.5.2 Solution details 13

6.5.2.1 General 13

6.5.2.2 PEGC/PEMC authentication and/or authorization procedure 13

6.5.2.2 PINE authentication and/or authorization procedure 14

6.5.3 Evaluation 14

6.6 Solution #5: EAP-based PINE authentication 15

6.6.1 Introduction 15

6.6.2 Solution details 15

6.6.3 Evaluation 16

7 Conclusions 16

Annex A (informative): Change history 16

# Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

In the present document, modal verbs have the following meanings:

**shall** indicates a mandatory requirement to do something

**shall not** indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

**should** indicates a recommendation to do something

**should not** indicates a recommendation not to do something

**may** indicates permission to do something

**need not** indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

**can** indicates that something is possible

**cannot** indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

**will** indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**will not** indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**might** indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

**might not** indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

**is** (or any other verb in the indicative mood) indicates a statement of fact

**is not** (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

# 1 Scope

The present document studies how 5G security architecture and procedures can be enhanced to support Personal IoT Network. The aim of this document is to study the security aspects of Personal IoT Networks for any potential enhancements in alignment with the outcome of SA2 study in TR 23.700-88 [2]. The study will look at the following aspects, performing gap analysis where necessary:

1) Study potential security enhancements for authentications required to secure Personal IoT Networks.

2) Study the security protection and access control for communications required to secure Personal IoT Networks.

3) Study the security enhancements for privacy required to secure Personal IoT Networks.

4) Other security aspects for any potential enhancements in alignment with the outcome of SA2 study in TR 23.700-88 [2].

# 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"

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

# 3 Definitions of terms and abbreviations

## 3.1 Terms

For the purposes of the present document, the terms given in 3GPP TR 21.905 [1], 3GPP TR 23.700-88 [2], and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

For the purposes of the present document, the following terms and definitions given in TR 23.700-88 [2] apply:

**Personal IoT Network:** A configured and managed group of PIN Element that are able to communicate each other directly or via PIN Elements with Gateway Capability (PEGC), communicate with 5G network via at least one PEGC, and managed by at least one PIN Element with Management Capability (PEMC).

**PIN Element:** A UE or non-3GPP device that can communicate within a PIN (via PIN direct connection, via PEGC, or via PEGC and 5GC), or outside the PIN via a PEGC and 5GC.

**PIN Element with Gateway Capability:** A PIN Element with the ability to provide connectivity to and from the 5G network for other PIN Elements, or to provide relay for the communication between PIN Elements.

## 3.2 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1], 3GPP TR 23.700-88 [2], and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

PIN Personal IoT Networks

PINE PIN Element

PEGC PIN Elements with Gateway Capability

PSP PIN Service Provider

AF Application Function

API Application Programming Interface

DN Data Network

NEF Network Exposure Function

QoS Quality of Service

URSP UE Route Selection Policy

# 4 Assumptions

Editor's note: This clause includes the architectural and security assumptions applicable for the study.

If sidelink is used for the direct communication between PEMC and PEGC, reuse security procedures defined for 5G ProSe Direct Communication without introducing new features to sidelink.

# 5 Key issues

## 5.1 Key Issue #1: Authentication and authorization for PINE

### 5.1.1 Key issue details

A key aspect of the planned support of the 5G system for PIN is the ability of a UE (referred to as PEGC) to act as a gateway for PIN elements (PINEs), which are not acting as 5G UEs, to connect to 5GC.

According to TR 23.700-88 [2], a PINE without 3GPP capability cannot directly connect to the 5GC, but through the PEGC. Whether the PINE without 3GPP capability needs to be known by the 5GC and how to identify the PINE needs to be studied, e.g., for controlling access of the PINE to connecting 5G data networks, differentiating the PINE for policy provisioning, authorizing the PINE for traffic relay, etc.

### 5.1.2 Security threats

5GS supports the policy and QoS differentiation for the traffic between a PINE and 5GS. The network resource may be misused by the malicious, unauthenticated, and unauthorized PINE.

### 5.1.3 Potential security requirements

The PINE in a Personal IoT network shall be authenticated.

The PINE in a Personal IoT network shall be authorized.

Editor’s note: Further requirements might be added if found.

## 5.2 Key Issue #2: Authorization of PIN capabilities

### 5.2.1 Key issue details

Some aspects of a PIN network might be configurable by an Application Function through the 5G NEF, for instance (depending on details defined in the SA3 study on PIN [2]) QoS of a PIN Element or URSP rules related to a PIN Element.

From a security point of view the scope of access granted to an AF needs to be restricted to the level of certain PEGCs or PINs and needs to be subject to permissions and consent granted by resource owners.

So far TS 33.501 [3] defines authorization of exposure capabilities on a rather general level in Clause 12. That is, authorization is based on operator policies using the identity of the AF (clause 12.2 in TS 33.501 [3]) as well as the OAuth authorization mechanism (Clause 12.4 in TS 33.501 [3]). No details about handling of permissions or providing consent to a specific application function are defined.

In case of PIN the requirements for API security might be especially demanding, since on the one hand a PIN network might consist of several UEs and on the other hand a single UE might contribute to several PINs.

Therefore, aspects related to ownership and possible operation models of PINs shall be included in the analysis of the key issue.

### 5.2.2 Security threats

An application function associated with one PIN might use the NEF API to manipulate another PIN.

An application function associated with a PIN might use the NEF API to manipulate resources not assigned to the PIN.

### 5.2.3 Potential security requirements

The 5GS shall be able to restrict resource request from an Application Function associated with a PIN to the resources associated with the PIN.

Application functions associated with a PIN shall be able to use APIs for accessing resource only with authorization from the resource owner.

# 6 Proposed solutions

## 6.1 Mapping of solutions to key issues

Table 6.1-1: Mapping of solutions to key issues

|  |  |  |
| --- | --- | --- |
| Solutions | KI#1 | KI#2 |
| Solution #1: PINE authentication and authorization | X |  |
| Solution #2: Authentication and authorization for PINE | X |  |
| Solution #3: Authentication for PIN elements involving SMF | X |  |
| Solution #4: PEGC/PEMC and PINE Authentication and Authorization | X |  |
| Solution #5: EAP-based PINE authentication | X |  |

## 6.2 Solution #1: PINE authentication and authorization

### 6.2.1 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.

### 6.2.2 Solution details

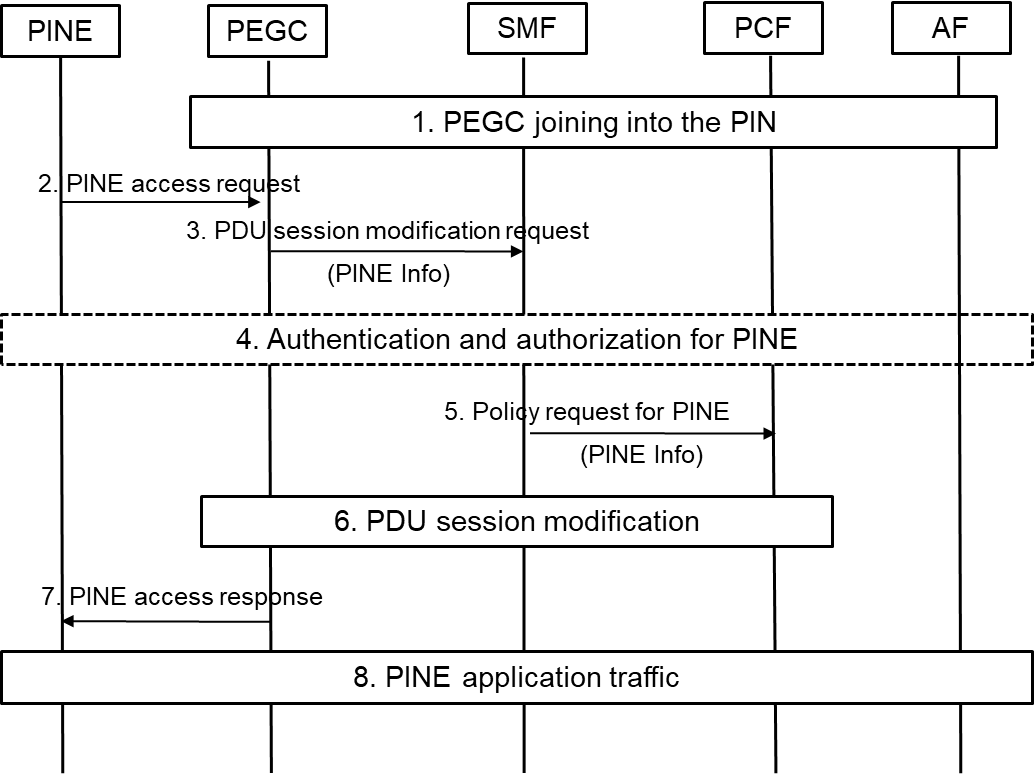


Figure 6.2.2-1 call flow of authentication and authorization for PINE

As show in the Figure 6.2.2-1, the details of authentication and authorization for PINE is summarized as following:

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

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

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.

Editor’s Note: How does PEGC trigger PDU session modification request with PINE info is FFS.

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.

### 6.2.3 Evaluation

TBD

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

## 6.3 Solution #2: Authentication and authorization for PINE

### 6.3.1 Introduction

This solution addresses the KI#1 "Authentication and authorization for PINE".

### 6.3.2 Solution details

The procedure describes how 5GC requests the authentication and authorization for a PINE.

****

**Figure 6.3.2-1: Authentication and authorization for PINE**

1. The PINE initially connects to the PEGC, the PEGC indicates to the PEMC of the connection. The PEMC authorizes the PINE connecting to the PEGC based on local configuration, e.g., whether a device with the MAC address is allowed to connect to the PEGC. If success, the PEMC indicates the PEGC that the PINE needs authentication and authorization based on local configuration, e.g., whether the device is a sensitive property and is able to be authenticated.

2. [Optional] The PINE may disconnect the PEGC and sometime reconnect the PEGC again. In this case, if the PEGC still holds the configuration of the PINE, the PEGC may not indicates to the PEMC for authorization, this can avoid to frequently disturb the PEMC, or the PINE can still access the PIN when PEMC is not reachable.

The PEGC may report the IP address of the PINE to the SMF.

3. If the PINE needs authentication and authorization, the PEGC sends PDU Session Modification Request to the SMF corresponding to the PDU Session related to the PIN.

Editor's note: How the PEGC determines a PINE needs AA is FFS.

4. The SMF may request identity from PINE using EAP messages over NAS same as described in steps 9-10 of clause 11.1.2 in TS 23.501 [X], the PEGC forwards the EAP messages between the SMF and the PINE.

5. The SMF sends the EAP message to the external DN-AAA, then the external DN-AAA and the PINE exchange EAP messages via the SMF, UPF, and the PEGC same as described in steps 11-13 of clause 11.1.2 in TS 33.501 [X] with following difference:

- The PEGC exchanges the EAP messages with the PINE.

6. If the authentication succeeds, the same as described in steps 14 of clause 11.1.2 in TS 33.501 [X] is performed.

7. The SMF authorizes the PINE based on the information received from external AAA.

8. The SMF sends PDU Session Modification Ack to the PEGC.

9. The PEGC authorize the PINE connecting to the PEGC.

Editor's note: Whether AA context needs to be stored and where to store is FFS.

### 6.3.3 Evaluation

TBD.

## 6.4 Solution #3: Authentication for PIN elements involving SMF

### 6.4.1 Introduction

This solution addresses the authentication of PIN elements as described in KI#1 by utilizing a procedure similar to Data Network specific secondary authentication.

In case of Data Network specific secondary authentication as currently defined in TS 33.501 [3] a UE is authenticating itself towards an external AAA server to obtain access to a specific Data Network.

This concept is extended in the proposed solution to the case of PIN networks.

The AAA server and the Data Network are typically operated by the same third party referred to as PIN Service Provider (PSP). The PECG is relaying EAP messages to and from a PINE.

### 6.4.2 Solution details

Figure 6.4.2-1 shows the procedure for authentication of a PINE.



**Figure 6.4.2-1 Authentication procedure for PINE using DN specific secondary authentication**

PINE acts as an EAP client, SMF acts as an EAP Authenticator and PSP DN-AAA server acts as an EAP server.

The individual steps are described below.

PINE requesting connectivity via PEGC/UE:

Step 1a. When a PINE wants to connect to the PSP (PIN application Service Provider) Data Network, PINE request for connection towards PEGC/UE.

Step 1b. If the PEGC/UE is not yet registered with the 5GS, it performs primary authentication using PEGC/UE USIM credentials.

Step 1c. The PEGC/UE request for PDU session establishment towards the PSP DN via 5GS.

Step 1d. The SMF obtains the subscription information from the UDM and verifies if the PEGC/UE request for PSP DN is allowed or not.

Step 1e. If the PEGC/UE is allowed to connect to the requested PSP DN, then SMF initiates the EAP authentication.

Secondary Authentication between PINE and PSP DN:

Step 2a. The SMF request for EAP identity towards PINE and PINE responds with EAP identity response. The PEGC/UE will start relaying the messages to/from PINE and SMF.

Step 2b. If there is no existing N4 session, SMF selects a UPF and establishes a N4 Session with the selected UPF.

Step 2c. The SMF forwards the EAP-Response with identity (received from PINE) towards PSP DN-AAA server.

Step 2d. Further EAP message exchanges between PINE and DN-AAA server of PSP.

Step 2e. The PSP DN-AAA server verifies if the PINE is authorized or not.

Editor's Note: Detailed threat analysis is FFS, i.e., how to ensure that only authorized PEGCs are used within a PIN.

Step 2f. Depending upon the verification, the EAP-Success / EAP-Failure message is sent to the SMF.

Step 2g. This completes the EAP authentication procedure for the PINE at the SMF.

Step 2h. Rest of the procedures for PDU establishment is executed as described in TS 33.501[3] figure 11.1.2-1 step 16a to step 18.

Step 2i. The PDU session establishment accept message is sent with EAP-Success towards PEGC/UE.

Step 2j. The communication between PINE and PSP application server can take place.

Editor's note: How 5GC/SMF identifies PINE is FFS.

### 6.4.3 Evaluation

TBD

## 6.5 Solution #4: PEGC/PEMC and PINE Authentication and Authorization

### 6.5.1 Introduction

This solution addresses KI#1 and proposes two procedures:

- The first procedure aims at authenticating/authorizing a PEGC/PEMC to manage or act as a gateway in a PIN,

- The second procedure aims at authenticating/authorizing a PINE to make use of the PIN resources.

### 6.5.2 Solution details

#### 6.5.2.1 General

****

**Figure 6.5.2.1-1 PEGC/PEMC and PINE Authentication and Authorization**

Figure 6.5.2.1-1 depicts the main steps of this solution that can be divided into two main procedures: (1) PEGC/PEMC authentication and/or authorization procedure and (2) PINE authentication and/or authorization procedure

#### 6.5.2.2 PEGC/PEMC authentication and/or authorization procedure

In reference to Figure 6.5.2.1-1:

- In Step 1, primary authentication is performed between UE and CN where the UE aims at becoming (PEGC/PEMC) in a PIN;

- In Step 2, the UE (or an application on it) requests PIN access to the CN or to an AF through the CN. This may be through AKMA (TS 33.535).

- In Step 3, the UE and AF perform an authentication and authorization step. This step maybe based on the AKMA keys distributed in Step 2.

- In Step 4a, the AF informs the CN about the outcome of Step 3 and provides the CN with a configuration. This configuration includes information about: PIN, PIN elements, communication requirements such as QoS, allowed interactions between PINE, etc. In Step 4b, the CN stores the configuration, e.g., in the UDR or in the AnPF.

- In Step 5a, the CN informs the UE about the outcome of Step 4 and provides the UE with a configuration. This configuration includes information about: PIN, PIN elements, communication requirements such as QoS, allowed interactions between PINE, etc. This configuration includes rules to enable an authentication and authorization procedure for a PINE (e.g., as required in Step 7c). This configuration may already include one or more "authorization tokens" for one or more PINEs. In Step 5b, the UE stores this configuration.

NOTE: With “authorization token” it is meant some type of keys/authorization tokens that can be used to authenticate/authorize the access to the PIN.

Editor’s Note: The details of the generation, distribution and use of “authorization token” are FFS.

- In Step 6, the AF informs the UE about the outcome of Step 4 and provides the UE with a configuration. This configuration received from the AF relates to application-related aspects assigned to the PIN by the AF.

#### 6.5.2.2 PINE authentication and/or authorization procedure

In reference to Figure 6.4.2.1-1:

- In Step 7a, the PINE and PEGC/PEMC setup a secure communication channel, e.g., based on a non 3GPP protocol. In Step 7b, the PINE may send a PIN access request to the PEGC/PEMC. In Step 7c, the PEGC/PEMC may grant either temporary or full access, e.g., based on information received in Step 5a. If full access is granted, then the PINE communicates as in Step 11. If temporary access is granted, then PINE proceeds to Step 8.

- In Step 8, PINE and AF perform an authentication and authorization step.

Editor’s Note: The impact/requirement of step 8 on 5GS is FFS.

- In Step 9a, the AF informs the CN about the outcome of Step 8 and provides the CN with a configuration related to the PINE. In Step 9b, the CN stores the configuration. In Step 9c, the CN informs the PEGC/PEMC about the outcome of Step 8 and provides the PEGC/PEMC with a configuration for the PINE. In Step 9d, the PEGC/PEMC stores the configuration. This configuration received from the CN may relate to communication parameters assigned to the PINE.

- In Step 10, the PINE and PEGC/PEMC receive an “authorization token” from the CN. The PINE may receive it through a secure channel established with the AF. The goal of this “authorization token” is to ensure that only authenticated/authorized PINEs can communicated with / through the PEGC/PEMC.

- In Step 11, data may be exchanged between PINE/PEGC/PEMC authenticated and/or authorized with said “authentication token”.

Editor’s Note: Security details of the solution in Steps 7a, 8 and 11 is FFS.

Editor’s Note: the need in the CN of configuration from AF (e.g. steps 4b, 9b) and the associated impacts are FFS.

### 6.5.3 Evaluation

TBD.

## 6.6 Solution #5: EAP-based PINE authentication

### 6.6.1 Introduction

This solution addresses KI #1 in terms of PINE authentication.

EAP-based authentication mechanisms are employed to enable 5GS to authenticate the PINEs.

### 6.6.2 Solution details

It is also assumed that PIN AS has provisioned the PINE ID, authenticated EAP identity and PINE related policies to the UDR.

PIN AS can be the AAA server.

It is assumed that SMF and PCF are aware of PINE ID and EAP identity.



**Figure 6.6.2-1: EAP-based PINE authentication**

1. PDU Session is established for PEGC.

2. Application layer signalling is exchanged between the PEGC and the PIN AS. A list of PINEs authorized to access the PEGC are provisioned to the PEGC.

3. A PINE requests to access the PEGC for traffic relay to 5GS. The request includes identities of PINE, external AAA server address (optional). The identities of PINE could be EAP identity of PINE or PINE ID of PINE. EAP identity of PINE can contains information about PINE ID, MAC Address, PEI, device ID.

4. The PEGC authenticates and authorizes the access of the PINE, and allocates IP address for the PINE. This procedure is realized based on non-3GPP access, which is out of scope of 3GPP.

5. PEGC sends PDU Session modification to the SMF. The PEGC sends EAP identity of PINE, address of the external AAA server (optional), PINE ID, IP address and allocated port number of the PINE to SMF via the modification message.

6-8. The SMF can select the AAA server based on the AAA server address provided by the PINE. The SMF sends the EAP identity of PINE to the external AAA server to trigger EAP-based authentication mechanism. The external AAA server sends the successfully authenticated EAP identity of PINE to the SMF. The SMF terminates the procedure if the authentication is failed.

9. The SMF updates the PCF with the PINE ID and authenticated EAP identity of PINE in SM Policy Association Modification.

10. The PCF queries the UDR for PIN Specific Service Parameters PINE ID and authenticated EAP identity, and receives the QoS requirement of the PINE communication.

The PCF derives the PCC rules for the PINE according to the QoS requirement received from the UDR and IP address/port number of the PINE from the SMF.

11. The PDU Session Modification procedures is triggered.

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

Editor’s Note: The need to involve the 5GC and the impacts to 5GC are FFS.

Editor’s Note: How does PEGC trigger PDU session modification request with PINE info is FFS.

### 6.6.3 Evaluation

TBD.

# 7 Conclusions

Editor's Note: This clause contains the agreed conclusions that will form the basis for any normative work.

Annex A (informative):  
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2022-06 | SA3#107-e-Ad Hoc | S3-221502 |  |  |  | Skeleton | 0.0.0 |
| 2022-06 | SA3#107-e-Ad Hoc | S3-221504 |  |  |  | Scope of TR 33.882 | 0.1.0 |
| 2022-06 | SA3#107-e-Ad Hoc | S3-221676 |  |  |  | KI on Authentication and authorization for PINE | 0.1.0 |
| 2022-08 | SA3#108-e | S3-221892 |  |  |  | Add terms and abbreviations | 0.2.0 |
| 2022-08 | SA3#108-e | S3-222343 |  |  |  | New Ki related to authorization of exposed PIN capabilities | 0.2.0 |
| 2022-08 | SA3#108-e | S3-222374 |  |  |  | Add threat and requirement to PINE authentication | 0.2.0 |
| 2022-10 | SA3#108adhoc-e | S3-223108 |  |  |  | Solution on PINE authentication | 0.3.0 |
| 2022-10 | SA3#108adhoc-e | S3-223012 |  |  |  | New solution for authentication and authorization of PINE | 0.3.0 |
| 2022-10 | SA3#108adhoc-e | S3-223056 |  |  |  | New solution to KI#1: Using secondary authentication for PIN elements | 0.3.0 |
| 2022-10 | SA3#108adhoc-e | S3-222949 |  |  |  | PIN - New solution KI#1 | 0.3.0 |
| 2022-10 | SA3#108adhoc-e | S3-222974 |  |  |  | KI 1, New Sol on EAP-based PINE authentication | 0.3.0 |
| 2022-10 | SA3#108adhoc-e | S3-222645 |  |  |  | Add some context to assumptions to TR 33.882 | 0.3.0 |
| 2022-10 | SA3#108adhoc-e | S3-222648 |  |  |  | Clean up to TR 33.882 | 0.3.0 |