|  |
| --- |
| 3GPP TR 33.882 V0.6.0 (2023-02) |
| 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 address3GPP support office address650 Route des Lucioles - Sophia AntipolisValbonne - FRANCETel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16Internethttp://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 members3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersLTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersGSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 5

1 Scope 7

2 References 7

3 Definitions of terms and abbreviations 7

3.1 Terms 7

3.2 Abbreviations 8

4 Assumptions 8

5 Key issues 8

5.1 Key Issue #1: Authentication and authorization for PINE 8

5.1.1 Key issue details 8

5.1.2 Security threats 8

5.1.3 Potential security requirements 8

5.2 Key Issue #2: Authorization of PIN capabilities 9

5.2.1 Key issue details 9

5.2.2 Security threats 9

5.2.3 Potential security requirements 9

6 Proposed solutions 9

6.1 Mapping of solutions to key issues 9

6.2 Solution #1: PINE authentication and authorization 10

6.2.1 Introduction 10

6.2.2 Solution details 10

6.2.3 Evaluation 11

6.3 Solution #2: PINE authentication by AAA over 5G CP 11

6.3.1 Introduction 11

6.3.2 Solution details 11

6.3.3 Evaluation 12

6.4 Solution #3: Authentication for PIN elements involving SMF 13

6.4.1 Introduction 13

6.4.2 Solution details 13

6.4.3 Evaluation 14

6.5 Solution #4: PEGC/PEMC and PINE Authentication and Authorization 15

6.5.1 Introduction 15

6.5.2 Solution details 15

6.5.2.1 General 15

6.5.2.2 PEGC/PEMC authentication and/or authorization procedure 15

6.5.2.3 PINE authentication and/or authorization procedure 16

6.5.3 Evaluation 16

6.6 Solution #5: EAP-based PINE authentication 17

6.6.1 Introduction 17

6.6.2 Solution details 17

6.6.3 Evaluation 19

6.7 Solution #6: Authorization on AF manipulating PIN 19

6.7.1 Introduction 19

6.7.2 Solution details 19

6.7.3 Evaluation 19

6.8 Solution #7: Authentication and Authorization of PINE Elements 19

6.8.1 Introduction 19

6.8.2 Solution details 20

6.8.3. Evaluation 21

6.9 Solution #8: AF authorization in PIN scenarios 21

6.9.1 Introduction 21

6.9.2 Solution details 21

6.9.3 Evaluation 21

6.10 Solution #9: PIN AF authorization for accessing the UDR 21

6.10.1 Introduction 21

6.10.2 Solution details 21

6.10.3 Evaluation 22

6.11.1 Introduction 22

6.11.2 Solution details 22

6.11.2.1 Architecture 22

6.11.2.2 Procedures 24

6.11.3 Evaluation 25

7 Conclusions 25

Annex A (informative): Change history 26

# 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"

[4] Connectivity Security Alliance: "Matter Specification Version 1.0"

# 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].

EAP Extensible Authentication Protocol

MSK Master Session Key

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 |  |
| Solution #6: Authorization on AF manipulating PIN |  | X |
| Solution #7: Authentication and Authorization of PINE Elements | X |  |
| Solution #8: AF authorization in PIN scenarios |  | X |
| Solution #9: PIN AF authorization for accessing the UDR |  | X |
| Solution #10: Local Authentication and Authorization of PINE | 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 an 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. The criteria for triggering PDU Session modification request can be based on existing mechanism or implementation.

4. The SMF determines whether authentication is required for the PINE with PINE information. 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 EAP method used to authenticate the UE and the content of Authentication Messages to support that method are out of scope of 3GPP.

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

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

In 5GC, SMF determines to trigger the authentication procedure during the PDU session modification procedure. The authorization is performed based on authentication results. Therefore, the solution has impact on 5GC.

The authentication messages are included in a transparent container and conveyed between the PINE and the AF via 5GC.

Editor’s note: Alignment with SA2 conclusion is FFS.

Editor’s note: Impact of 5GS managing credentials should be evaluated.

## 6.3 Solution #2: PINE authentication by AAA over 5G CP

### 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 supports the PINE authentication and authorization by AAA over control plane.

****

**Figure 6.3.2-1: PINE authentication by AAA over 5G CP**

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.

3. When the PINE accessing the PIN requests PINE authentication with external DN-AAA, e.g., the PINE is preconfigured with credential and sends indication to PEGC, the PEGC sends PDU Session Establishment/Modification Request with a flag for PINE authentication to the SMF corresponding to the PDU Session related to the PIN. The PDU Session Establishment/Modification Request may include the PINE ID. If the PDU Session associated with the PIN has been established, PDU Session Modification Request is used, otherwise PDU Session Establishment Request is used.

The SMF performes following steps 4-9 based on whether the flag for PINE authentication is received or not.

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 and PINE uses PIN Auth message for encapsulating the EAP messages transferred between the SMF and the PINE.

5. The SMF determines whether the external DN-AAA (derived from PINE ID) is allowed to perform PINE authentication, which may be per PIN and the configuration of allowed/disallowed external DN-AAA is out of scope. If allowed, the SMF sends the PINE ID to the external DN-AAA via UPF, e.g., using RADIUS protocol or Diameter protocol, 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 over PIN Auth message.

6. If the PINE authentication succeeds, the same as described in steps 14 of clause 11.1.2 in TS 33.501 [3] is performed with the following difference:

- The DN authorization data described in clause 5.6.6 of TS 23.501 [3] only include a DN Authorization Profile Index.

7. The SMF sends PDU Session Establishment Ack or PDU Session Modification Ack/Reject to the PEGC based on the result of the PINE authentication. If EAP-failure is received from the external DN-AAA, the SMF sends a cause value to the PEGC to indicate the failure of PINE authentication.

8. If PINE authentication succeeds, the PEGC allows the PINE connecting to the PEGC for accessing the PIN, and sends PIN message (PIN ID, EAP Success) to the PINE. The PIN ID is determined based on information configured by PEMC, which is out of 3GPP scope.

If PINE authentication fails, the PEGC closes the connection with the PINE.

### 6.3.3 Evaluation

This solution is suitable for the case that PINE is preconfigured with credential that is able to be authenticated by external DN-AAA.

This solution does not require that the PEGC acts as authenticator, i.e., the SMF acts as authenticator, and does not require 5G UP resources for PINE authentication.

This solution requires SMF to support triggering secondary authentication and authorization during PDU Session Establishment and UE initiated PDU Session Modification procedure.

This solution requires SMF to authorize which AAA is allowed or disallowed to authenticate PINE.

Editor’s note: Further evaluation is for FFS.

Editor’s note: Alignment with SA2 conclusion is FFS.

## 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.

If several PINs are using the same AAA server, potential attacks result from the circumstance that the PEGC, which is relaying EAP messages between EAP client (PINE), and EAP authenticator (SMF) and PINE might belong to different entities. An attacker might deploy a potentially malicious PEGC with aim to connect a victims' PINEs to this PEGC. Alternatively, an attacker might try to connect potentially malicious PINEs to a victim's PEGC. These attacks are possible, if the AAA server can not verify that PINE and PEGC are both authorized to be part of a PIN.

Therefore, this solution introduces an authorization code, which is used by the AAA server to authorize PEGCs together with 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.

The request contains the identity of the PEGC and a PECG specific authorization code. The authorization code is a secret, which is prehsared between the 5GS and the AAA server in an initial configuration step.

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.

The authorization step includes the verification of the PEGC identity and the authorization code. That is, the AAA server verifies that the authorization code configured for the PECG is identical to the authorization code received in step 2c.

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

The identiy of the PINE is provided by the AAA server to the SMF together with the EAP-Success message.

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.

### 6.4.3 Evaluation

This solution proposes combining PINE authentication and authorization with PDU session management, In this way, the authentication and authorization can happen outside of the 5G core (i.e., executed by a central external AAA server), but the5G system can be aware of each individual authentication and authorization decision and of the identity of the authenticated PINE.

The solution also consists of a mechanism based on authorization code, which prevents potential attacks stemming from the fact that a PEGC and PINE might be operated by different entities.

3GPP TR 23.700-88 [2] has concluded not to specify the PINE authentication and authorization.

Whether PDU Session Establishment or PDU Session Modification messages are used and potential modifications to SMF can be aligned with SA2.

## 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 a PEGC and/or a 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 may be 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. This is a required configuration to fulfil the PINE authentication and authorization requirement to guarantee, e.g., a certain QoS to a certain PINE. In Step 4b, the CN stores the configuration, e.g., in the UDR.

- In Step 5a, the CN informs the UE about the outcome of Step 4 and provides the UE with a configuration. This configuration (provisioned information) 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 include one or more "authorization values" for one or more PINEs. In Step 5b, the UE stores this configuration.

NOTE: With “authorization values” it is meant some type of authorization tokens that can be used to authenticate/authorize the access to the PIN during operation. For instance, the authorization values might be used by PINE/PEGC to protect/verify the traffic. These authorization values may be generated and handled by the AF and provided to the CN/PEGC to ensure that only authorized devices can exchange data.

- 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 includes application-related aspects assigned to the PIN by the AF. Parameters such as PIN element identities or allowed interactions between PINEs may also be provided to PEGC/PEMC by the AF, if not supported in Steps 4 and 5. Some parameters may also be entered by the user by means of the UE e.g., password.

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

In reference to Figure 6.4.2.1-1:

- In Step 7a, the PINE and PEGC/PEMC may 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 the provisioned information received in Step 5a. If full access is granted (local authorization), 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 end-to-end authentication and authorization step. The details of this procedure are out-of-scope of 3GPP and this procedure is just executed over the 5GS in user plane.

- 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. This configuration may include further information about: PIN, PIN elements, communication requirements such as QoS, allowed interactions, etc. 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. Parameters such as PIN element identities or allowed interactions between PINEs may also be provided to PEGC/PEMC by the AF, if not supported in this step. Some parameters may also be entered by the user by means of the UE e.g., password.

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

- In Step 11, data may be exchanged between PINE/PEGC/PEMC authenticated and/or authorized with said “authorization values”. For instance, the authorization values might be used by PINE to protect the uplink traffic in Step 11a. In Step 11b, the PEGC can verify the incoming traffic from the PINE. If the verification is successful, then the PEGC forwards the traffic further towards the AF in Step 11c. Downlink traffic can be protected in a similar way.

### 6.5.3 Evaluation

This solution addresses KI#1 and involves two phases: a first phase to authenticate/authorize the PEGC/PEMC and a second phase to authenticate/authorize a PINE.

After the first phase (authentication/authorization of the PEGC/PEMC), the 5GC and PEGC/PEMC are provided with configuration information to facilitate the second phase.

The proposed solution aims at reusing existing procedures and supports performing PINE authentication/authorization either locally or end-to-end (with an AF) at application layer.

* Performing the end-to-end authentication/authorization over the 5GS has certain impacts such as:Step 7c, providing initial access to perform such end-to-end authentication/authorization.
* Step 9a, informing the 5GS about the result and/or updating provisioned parameters.
* Step 9c, 5GC informing PEGC/PEMC about the result and/or updated provisioned parameters.

The provisioning of information, e.g., in Steps 4, 5, and/or 9, are not fully aligned with SA2 conclusions including, e.g.:

* Storage and retrieval of PIN related policy and QoS parameters
* Provisioning of the policy and parameters to PEGC by 5GC.

Thus, the solution impacts the 5GC

This provisioned information is used for local PINE authorization at the PEGC.

NOTE: The solution may require additional work on security related details. Non-3GPP aspects are outside the scope of the study and normative work.

Editor’s note: Further evaluation is FFS.

## 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 EAP identity of PINE.

**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: The need to involve the 5GC and the impacts to 5GC are FFS.

### 6.6.3 Evaluation

The SMF can select the AAA server based on the AAA server address provided by the PINE.

PINE is authenticated by AAA server with EAP-based mechanism.

The PCF queries the UDR with authenticated EAP identity, and receives the QoS requirement of the PINE communication.

Editor's Note: Further evaluation is FFS.

## 6.7 Solution #6: Authorization on AF manipulating PIN

### 6.7.1 Introduction

This solution addresses the KI#2 "Authorization of PIN capabilities".

### 6.7.2 Solution details

When the AF requests 5GC to setup resources for a PIN via NEF, the NEF shall assign a randomized unique ID to the AF, which could be the PIN Session ID, and associates the ID with the AF.

When the AF requests to query, update, or delete the information related to the PIN, the AF shall provide the NEF assigned ID to the NEF, and the NEF shall authorize whether the ID is associated with the AF.

The NEF may change the ID and provide the updated ID to the AF when the AF interacts with the NEF.

This randomized unique ID is working like a token, which is sent only to the AF which is authorized to manipulate the PIN.

### 6.7.3 Evaluation

TBD.

## 6.8 Solution #7: Authentication and Authorization of PINE Elements

### 6.8.1 Introduction

This solution addresses KI#1.

As per KI#1, the PIN Elements in a Personal IoT Network need to be authenticated and authorized. According to the conclusions of TR 23.700-88 [2] the PIN Elements are authorized locally by the PEMC, which is a UE belonging to the PIN and having PIN management capability. Furthermore, the PIN Elements are allowed or disallowed to join the network by the PEGC, which is a UE belonging to the PIN and having PIN gateway capability. The PEMC and PEGC are authenticated and authorized as 5G UEs by the 5GC using existing procedures. Application-level authentication and authorization can use existing specifications e.g., CSA Matter [4].

### 6.8.2 Solution details



**Figure 6.8.2-1: PINE Authentication and Authorization**

Figure 6.8.2-1 depicts the main steps of this solution.

In reference to Figure 6.8.2-1:

1. Authentication and authorization are performed between UEs (PEMC and PEGC) and the 5GC using existing 5G UE authentication and authorization procedures.
2. The AF provisions the policy and other necessary parameters to the 5GC, PEMC and PEGC using application layer provisioning procedures. Step 2 can also be performed prior to step 1.

NOTE: Steps 1 and 2 is not specific to PINE authentication.

1. PIN Element establishes connection to the PEMC and PEGC using the local interface e.g., PC5, WLAN or Bluetooth, and performs authentication with PEMC and PEGC using security mechanisms specific to the local interface. Upon successful authentication with PEMC, PIN Element is authorized by the PEMC to join the PIN. PEMC and PEGC can be either the same or separate UEs.

The actual security mechanism used over the local interface is outside the scope of this solution, as they are defined elsewhere. For example, in case of WLAN, for PINE authentication WPA defined by WFA can be reused, where PINE acts as a supplicant and PEMC or PEGC (depending on with which entity PIN Element establishes the local connection) acts as an authenticator. Depending on the WPA mode (personal/enterprise) an authentication server, local to the PIN, can be used. In particular, the WPA enterprise mode requires an authentication server, while the personal mode doesn’t. The authorization is performed by PEMC or PEGC after successful authentication of PINE based on local authorization policy or configuration. The authentication server can be implemented as a part of the PEMC/PEGC or separately. The choice of authentication method is left to the decision of the PIN owner.

1. After being authorized by the PEMC to join the PIN, the PIN Element requests data transfer to the PEGC. This request uses transport and/or application layer messages and is implementation specific.
2. [Optional] The data transfer request from step 4 triggers the establishment of data connection between the PEGC and 5GC. If the data connection already exists and can be reused for PIN traffic, then Step 5 is not needed.
3. The PEGC accepts/rejects the PIN Element request for data transfer from step 4. Similarly, to step 4, step 6 uses transport and/or application layer messages and is implementation specific.
4. The PIN Element uses the application layer mechanisms (including security mechanisms) to establish secure communication with other entities in the PIN (such as other PIN Elements, the PEMC, PEGC or AF). Step 7 uses procedures of existing standards such as e.g., CSA Matter [4]. Initial packets of step 7 can be transmitted concurrently with steps 4,5 and 6. However, these initial packets will not be forwarded by PEGC/PEMC to the AF until the acceptance from step 6.

### 6.8.3. Evaluation

In this solution, the security of PINE authentication and authorization is dependent on the authentication method chosen by the PIN owner.

Editor’s Note: Further evaluation is FFS.

## 6.9 Solution #8: AF authorization in PIN scenarios

### 6.9.1 Introduction

This solution addresses part of KI #2 "Authorization of PIN capabilities", i.e. the 5GS shall be able to restrict resource request from an Application Function associated with a PIN to the resources associated with the PIN.

This solution reuses the OAuth 2.0 to authorize the AF to manage a specific PIN.

### 6.9.2 Solution details

This solution reuses the OAuth 2.0, which is already captured in clause 12 and clause 13 of TS 33.501 [3], to authorize the AF to manage a specific PIN.To authorize the AF to manage a specific PIN, the access token sent to the AF includes PIN identity.

### 6.9.3 Evaluation

This solution reuses the OAuth 2.0 to authorize the AF to manage a specific PIN.To authorize the AF to manage a specific PIN, the access token sent to the AF includes PIN identity.

## 6.10 Solution #9: PIN AF authorization for accessing the UDR

### 6.10.1 Introduction

This solution addresses KI#2 by using normal authorization/authentication procedure with CCA and taking into account the PIN ID in the additional scope.

### 6.10.2 Solution details

The solution is based on 13.4.1.3 “Service access authorization in indirect communication scenarios” of TS 33.501 [3], with the PIN AF taking the role of the NF Service Consumer, the NEF the role as the SCP, the UDR the role as the NF Service Producer. The PIN AF includes the PIN ID in the additional scope which is then taken into account by the NRF for the authorization and access token generation.

### 6.10.3 Evaluation

The PIN ID should be taken into account when authorizing the PIN AF for accessing the UDR for modifying data related to that specific PIN ID.

Editor’s note: Further evaluation is FFS

6.11 Solution #10: Local Authentication and Authorization of PINE

### 6.11.1 Introduction

This solution addresses KI#1. Based on architectural proposals and preliminary conclusions in the TR 23.700-88 [2], this solution proposes an authentication and authorization architecture, which involves PEGC and PEMC.

The solution proposes to use EAP protocol between a PINE and PEMC, with the PINE acting as EAP client, the PEMC acting as EAP server, and the PEGC as EAP authenticator.

That is, authentication and authorization happen locally within the domain of the non 3GPP network of the PIN.

This solution requires that PINEs support EAP.

This solution does not exclude coexistence with other authentication methods, which are not relying on EAP.

### 6.11.2 Solution details

#### 6.11.2.1 Architecture

The architecture, which the solution is based on is shown in Figure 6.11.2.1-1. This architecture figure is closely following the architecture proposed in Solution #0D in [2] including the labelling of the reference points.

P1 and P2 are the reference points, which are based on a non-cellular short-range communication protocol (typically defined outside the scope of 3GPP), and which are used for communicating between the PEGC and the PINEs and PEGC and PEMC, respectively. The part of the network, which is using the non-cellular network for communication, is referred to as PIN domain.

Since both PEMC and PEGC are UEs, they can use cellular connectivity to connect via the 5G user plane to application in a Data Network. The P3 reference point is used between PEMC and PIN AF to exchange information related to the management of the PIN, whereas P4 is used by the PEGC to provide PINEs with connectivity with the actual PIN application (which can be part of the PIN AF or not).

 **Figure 6.11.2.1-1 Architecture assumed by the solution**

In general, a PIN consists of several PIN domains. Each PIN domain consists of one or several PEGCs and is represented by a PEMC. The PEMCs of all PIN domains constituting the PIN are connected to the same PIN AF. This architecture is visualized in Figure 6.11.2.1-2. The PIN Management Protocol between PEMC and PIN AF as well as the functionality of the PIN AF are out of scope of this solution.

PINE authentication and authorization is executed locally within a PIN domain. For this purpose, EAP is used between the PINE and the (local) PEMC. The PEGC is acting as EAP authenticator and in this role is relaying EAP messages between PINE and PEMC. The EAP messages are carried on top of the non-cellular communication protocol which is used for communication within a PIN domain.

Each PEMC is using credential information from a local database for the authentication and authorization of the PINE. The provisioning of this information (e.g., using the PIN Management Protocol) is out of scope of this solution. The type of credential information depends on the used EAP protocol. Definition of the EAP protocol and of the credential information is out of scope of this solution.



**Figure 6.11.2.1-2 PIN Authentication and Authorization Architecture**

#### 6.11.2.2 Procedures



**Figure 6.11.2.2-1 Local Authentication and authorization flow**

The actual procedure used for local authentication and authorization of a PINE is shown in Figure 6.11.2.2.1-1. The PINE is acting as EAP Client, the PEGC as EAP Authenticator and the PEMC as EAP Server.

As defined by SA2 [2], the communication between PINE and PEGC as well as the communication between PEGC and PEMC is executed using the non-cellular short range communication protocol.

The individual steps are described in more detail below.

Step 1: PINE sends a connection request to PEGC.

Step 2: The PEGC sends EAP Identity Request to the PINE, if the PINE identity is not included in the message sent in step 1, and fetches the PIN Identity in Identity response message.

Step 3: The PEGC sends Access Request to the PEMC, which includes the EAP identity of PINE.

 Existing protocol suites, like RADIUS or Diameter can be used to convey the Access Request to the PEMC.

Step 4: The PEMC and the PINE exchanges several EAP messages, as required by the EAP method.

Step 5: The PEMC verifies the PINE request based on provisioned information.

 This step also includes the authorization of the PINE using the provisioned information.

Step 6: After successful completion of the authentication procedure, the PEMC sends EAP success message to the PEGC. This message may contain a secret which was derived as part of the execution of the EAP message exchange, e.g., a Master Session Key (MSK). The exact way, how the MSK is calculated on the PINE and on the PEMC, is up to the EAP method.

 The same protocol as in step 3, e.g., RADIUS or Diameter, can be used to convey this message to the PEMC.

Step 7: The EAP Success message sent to the PINE completes the authentication procedure.

Step 8: A further PIN specific handshake takes place to establish secure communication within the PIN. As part of this handshake PEGC and PINE can derive further communication keys from the MSK.

Specification of the protocol between PEMC and PIN AF is out of scope of the solution.

### 6.11.3 Evaluation

This solution proposes a local mechanism for authentication and authorization of PINEs.

The solution proposes to use EAP, but the solution might exist with other solutions, which are not relying on EAP.

Editor's Note: Further evaluation is ffs.

# 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 |
| 2022-11 | SA3#109 | S3-223307 |  |  |  | Sol#3 Resolution of EN on identification of PINE | 0.4.0 |
| 2022-11 | SA3#109 | S3-224059 |  |  |  | PIN - Addressing EN#2 in Solution #4 | 0.4.0 |
| 2022-11 | SA3#109 | S3-224060 |  |  |  | PIN - Addressing EN#4 in Solution #4 | 0.4.0 |
| 2022-11 | SA3#109 | S3-224062 |  |  |  | Sol#3 Adding Evaluation | 0.4.0 |
| 2022-11 | SA3#109 | S3-224063 |  |  |  | Addressing the ENs in solution 1 | 0.4.0 |
| 2022-11 | SA3#109 | S3-224064 |  |  |  | New solution for AF manipulate PIN | 0.4.0 |
| 2022-11 | SA3#109 | S3-224067 |  |  |  | Solution for KI#1: Authentication and Authorization of PINE | 0.4.0 |
| 2022-11 | SA3#109 | S3-224073 |  |  |  | PIN - Addressing EN#1 in Solution #4 | 0.4.0 |
| 2022-11 | SA3#109 | S3-224074 |  |  |  | PIN - Addressing EN#3 in Solution #4 | 0.4.0 |
| 2022-11 | SA3#109 | S3-224088 |  |  |  | Sol#3 Resolution of EN on authorization of PEGC | 0.4.0 |
| 2023-01 | SA3#109 Adhoc-e | S3-230386 |  |  |  | KI #2, new Sol on AF authorization in PIN scenarios | 0.5.0 |
| 2023-01 | SA3#109 Adhoc-e | S3-230482 |  |  |  | Update solution for PINE authentication and authorization over 5G CP | 0.5.0 |
| 2023-01 | SA3#109 Adhoc-e | S3-230469 |  |  |  | Addressing the editor's note in solution 1 | 0.5.0 |
| 2023-01 | SA3#109 Adhoc-e | S3-230531 |  |  |  | Resolve ENs for sol #5 | 0.5.0 |
| 2023-02 | SA3#110 | S3-230778 |  |  |  | Sol#1 Updating Evaluation | 0.6.0 |
| 2023-02 | SA3#110 | S3-230820 |  |  |  | Resolution of EN#2 in Solution#7 for KI#1 | 0.6.0 |
| 2023-02 | SA3#110 | S3-231345 |  |  |  | Solution for KI#2 | 0.6.0 |
| 2023-02 | SA3#110 | S3‑231539 |  |  |  | PIN - Evaluation Solution #4 | 0.6.0 |
| 2023-02 | SA3#110 | S3‑231540 |  |  |  | Resolution of EN#1 in Solution#7 for KI#1 | 0.6.0 |
| 2023-02 | SA3#110 | S3‑231541 |  |  |  | KI#1 New Sol for local PINE authentication | 0.6.0 |
| 2023-02 | SA3#110 | S3‑231596 |  |  |  | Sol#3 Removal of EN | 0.6.0 |