|  |  |
| --- | --- |
| 3GPP TR 23.700-88 V0.2.0 (2022-04) | |
| Technical Report | |
| 3rd Generation Partnership Project;  Technical Specification Group Services and System Aspects;  Study on architecture enhancements for Personal IoT Network (PIN)  (Release 18) | |
|  | |
|  |  |
|  | |
| 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 6

1 Scope 8

2 References 8

3 Definitions of terms and abbreviations 8

3.1 Terms 8

3.2 Abbreviations 9

4 Architectural requirements and assumptions 9

4.1 Architectural Requirements 9

4.2 Architectural Assumptions 9

5 Key issues 10

5.1 Key Issue #1: 5GC architecture enhancements to support PIN 10

5.1.1 Description 10

5.2 Key Issue #2: PIN and PIN Element discovery and selection 10

5.2.1 Description 10

5.3 Key Issue #3: Management of PIN and PIN Elements 10

5.3.1 Description 10

5.4 Key Issue #4: Communication of PIN 11

5.4.1 Description 11

5.5 Key Issue #5: Authorization for PIN 11

5.5.1 Description 11

5.6 Key Issue #6: Policy and parameters provisioning for PIN 12

5.6.1 Description 12

6 Solutions 12

6.0 Mapping of Solutions to Key Issues 12

6.1 Solution #1: PIN and PIN element discovery and selection 13

6.1.1 Description 13

6.1.2 Procedures 13

6.1.2.1 PIN Discovery and Selection 13

6.1.2.2 Discoverability by other PIN elements 15

6.1.2.3 Discovery and Selection of PEGC 15

6.1.3 Impacts on Existing Nodes and Functionality 16

6.2 Solution #2: PIN and PINE discovery and selection 17

6.2.1 Description 17

6.2.1.1 Overall architecture 17

6.2.1.2 PIN and PIN element discovery and selection 18

6.2.2 Procedures 19

6.2.3 Impacts on services, entities and interfaces 19

6.3 Solution #3: Solution for PIN and PIN Elements discovery and selection 19

6.3.1 Description 19

6.3.2 Procedures 20

6.3.3 Impacts on Existing Nodes and Functionality 21

6.4a Solution #4a: PIN and PIN Element discovery by A PINE 21

6.4a.1 Description 21

6.4a.2 Procedures 21

6.4a.3 Impacts on Existing Nodes and Functionality 22

6.4b Solution #4b: PIN Elements with Gateway Capabilities (PEGC) discovery and selection by PEMC 22

6.4b.1 Description 22

6.4b.1.1 Introduction 22

6.4b.1.2 Functional Description 22

6.4b.2 Procedures 23

6.4b.3 Impacts on Existing Nodes and Functionality 23

6.5 Solution #5: Solution for authorization and management of PIN and PIN Elements 23

6.5.1 Description 23

6.5.1.1 Registration management of PEMC, PEGC and PINE 23

6.5.1.2 Management of PIN and PINE Elements 24

6.5.2 Procedures 25

6.5.2.1 PIN Elements registration and PIN management 25

6.5.2.2 PINE accessing to 5GC via PEGC 26

6.5.3 Impacts on Existing Nodes and Functionality 26

6.6 Solution #6: Management of PIN and PIN Elements 27

6.6.1 Description 27

6.6.2 Procedures 31

6.6.2.1 PIN creation 31

6.6.2.2 PINE authentication and registration 33

6.6.3 Impacts on services, entities, and interfaces 34

6.7 Solution #7: PIN Management by 5GS. 34

6.7.1 Description 34

6.7.2 Procedures 35

6.7.3 Impacts on services, entities and interfaces 36

6.8 Solution #8: Management of PIN and PIN Elements 36

6.8.1 Description 36

6.8.1.1 Architecture reference model for application level 36

6.8.1.2 Architecture reference model for 5GS level 37

6.8.1.3 Reference points 37

6.8.2 Procedures 38

6.8.2.1 Management of PIN 38

6.8.2.2 Management of PEGC and PINE 38

6.8.2.3 Management of association between PEGC and PINE 40

6.8.2.4 Parameters provisioned to PEMC 40

6.8.2.5 Parameters provisioned to PINE 41

6.8.2.6 Parameters provisioned to PEGC 41

6.8.3 Impacts on Existing Nodes and Functionality 42

6.9 Solution #X: PIN management and PINE management 42

6.9.1 Description 42

6.9.2 Procedures 43

6.9.2.1 An authorized UE to create a PIN 43

6.9.2.2 A device joins a PIN 44

6.9.3 Impacts on Existing Nodes and Functionality 45

6.10 Solution #10: Management of PIN and PIN Elements 46

6.10.1 Description 46

6.10.1.1 Overall architecture 46

6.10.1.2 Management of PIN and PIN Elements 47

6.10.2 Procedures 48

6.10.3 Impacts on services, entities and interfaces 48

6.11 Solution #11: Differentiated QoS between a PINE and 5GS when a PEGC is used for the relay 49

6.11.1 Description 49

6.11.1.1 Introduction 49

6.11.1.2 Solution principles 49

6.11.2 Procedures 49

6.11.3 Impacts on Existing Nodes and Functionality 50

6.12 Solution #12: Communication of PIN 50

6.12.1 Description 50

6.12.2 Procedures 51

6.12.2.1 Management of relay path 51

6.12.2.2 Management of communication via 5GC 53

6.12.2.3 Management of communication via PEGC 54

6.12.2.4 Mobile termination procedure for PINE 55

6.12.3 Impacts on Existing Nodes and Functionality 56

6.13 Solution #13: Communication of PIN 57

6.13.1 Description 57

6.13.1.1 Communication between PINE and 5GS via PEGC 57

6.13.1.2 Communication between PIN elements within PIN 58

6.13.2 Procedures 58

6.13.3 Impacts on services, entities and interfaces 59

6.X Solution #X: <Solution Title> 59

6.X.1 Description 59

6.X.2 Procedures 59

6.X.3 Impacts on Existing Nodes and Functionality 59

7 Evaluation 59

8 Conclusions 60

# 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 scope of this Technical Report is to study the enhancement of 5G System to support Personal IoT Network (PIN). The study addresses the service requirements documented in TS 22.261 [5] for the Personal IoT Networks. The following aspects needs to be studied:

- Architecture enhancement:

- To study the potential architectural enhancements for supporting management of PIN, access of PIN via PIN Element with Gateway Capability (PEGC), and communication of PIN (e.g. PIN Element communicates with other PIN Elements directly or via PEGC or via PEGC and 5GS).

- To study the potential architecture enhancements for supporting identifying PIN and the PIN Elements.

- Security related:

NOTE: The study may need cooperation with SA3. If solutions are related to security impact, they will be studied in SA WG3.

- To study how to identify PIN and the PIN Elements in the PIN at 5GC level to serve for authentication/authorization.

- Management as well as policy and routing control enforcement:

- To study the management of a PIN.

- To study the procedures for PIN discovery, PIN Element discovery.

# 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 TS 23.501: "System Architecture for the 5G System; Stage 2".

[3] 3GPP TS 23.502: "Procedures for the 5G system, Stage 2".

[4] 3GPP TS 23.503: "Policy and Charging Control Framework for the 5G System".

[5] 3GPP TS 22.261: " Service requirements for the 5G system; Stage 1".

# 3 Definitions of terms and abbreviations

## 3.1 Terms

For the purposes of the present document, the terms given in TR 21.905 [1], in TS 23.501 [2] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1] or in TS 23.501 [2].

**Personal IoT Network:** A configured and managed group of at least one PIN Element with Gateway Capability and one or more PIN Elements that are able to communicate each other and with 5G network via PIN Element with Gateway Capability.

**PIN Element:** A device that can communicate within a PIN (via PIN direct connection or via PEGC), or outside the PIN via a PEGC.

**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 provide relay for the communication between PIN Elements.

**PIN Element with Management Capability:** A PIN Element with capability to manage the PIN.

NOTE: A PIN Element can have both PIN Management Capability and Gateway Capability.

**PIN direct connection:** the connection between two PIN Elements without any 3GPP RAN or core network entity in the middle.

## 3.2 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1], in TS 23.501 [2] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [1] or in TS 23.501 [2].

PIN Personal IoT Networks

PINE PIN Element

PEGC PIN Elements with Gateway Capability

PEMC PIN Elements with Management Capability

# 4 Architectural requirements and assumptions

## 4.1 Architectural Requirements

This study has following architectural requirements:

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

- There shall be no change to underlying non-3GPP access (e.g. WIFI, Bluetooth) standards.

## 4.2 Architectural Assumptions

This study has following architectural assumptions:

- Only a 3GPP UE can act as PEGC and/or PEMC.

- There are one or more PEGCs in a PIN.

- There are one or more PEMCs in a PIN.

- The PIN Elements assumes to use non-3GPP access (e.g. WIFI, Bluetooth) for direct communication, the PEMC can use 5G ProSe Direct Communication for direct communication with PEGC.

NOTE: In this release the 5G-RG is considered outside the scope of the study and consequently not part of PIN.

Editor's note: It is FFS whether data traffic of PINE over control plane is in scope of this study.

# 5 Key issues

## 5.1 Key Issue #1: 5GC architecture enhancements to support PIN

### 5.1.1 Description

It is required that at least one PEGC is in a PIN, which is able to relay the traffic between 5GS and PINEs that are behind the PEGC. A PINE may be a non-3GPP device, or can be a UE. There are one or more PEMCs for a PIN, at any point of time one of which is able to control the PIN, e.g., create/delete a PIN, add/remove a PINE for the PIN, etc.

The following aspects will be studied:

- Whether additional 5GC function(s) and/or interface(s) are needed for supporting identification of PIN and PIN Elements, management of PIN, access of PIN via PEGC and communication of PIN.

- Define the architecture of the Personal IoT Network.

NOTE: If new function(s) or new interface(s) are introduced in solution proposals addressed to other key issues, the architecture proposal needs to be addressed in this key issue, and those solutions needs to indicate the architecture proposal addressed to this key issue.

## 5.2 Key Issue #2: PIN and PIN Element discovery and selection

### 5.2.1 Description

The PIN discovery is used for a device to discover a PIN. PINE discovery is used for device to discover the PIN Elements (i.e. PINE, PEGC, and PEMC).

Following issues need to be addressed in this key issue:

- How to discover and select a PIN.

- How to discover and select PIN Elements with Gateway Capability (PEGC) and with Management Capability (PEMC)

- How to discover PIN Elements in a PIN based on criteria's, for example, the capability, availability, reachability and services (e.g. printer).

- How to enable and manage the discovery for all possible case, for example, whether a PIN Element is discoverable by devices that are not members of the PIN or by other PIN Elements of the same PIN.

## 5.3 Key Issue #3: Management of PIN and PIN Elements

### 5.3.1 Description

This key issue intends to support the management of the PIN, including the management of different types of PIN Elements and the configuration of the PIN. Both the network operator and authorized 3rd party, i.e. PIN Element with Management Capability (PEMC) could create and configure the PIN and its elements.

After a PIN has been created, PEMC can add a PEGC into the PIN, or remove a PEGC from the PIN, as well as add a PIN Element into the PIN and associate it to some PEGCs that have already been added into the PIN, or remove a PIN Element from the PIN.

The Key Issue is to study the following aspects in the 5GS:

- How to support mechanisms for network operator or authorized 3rd party (e.g., a PEMC) for PIN management, e.g. create/modify/delete/activate/deactivate a PIN, etc.

- How to support for the management of PIN Elements, including to add/remove the PIN Elements, as well as the association between PEGC and other PIN Elements.

- How to support establishing and enforcing the validity duration and the time validity of a PIN (e.g. the PIN is valid for 30 minutes, the PIN is valid from 15:00 UTC to 23:00 UTC) and of the PIN Elements in a PIN (e.g. the PINE will be member of PIN for 1 hour, the PIN element will be member of PIN from 16:00 UTC to 17:00 UTC).

## 5.4 Key Issue #4: Communication of PIN

### 5.4.1 Description

The PIN connectivity supports communications between PIN Elements, communications between PIN Elements and 5GS.

The PINE behind the PEGC may run an application with different QoS requirement, which may need the PEGC to have a corresponding QoS flow for relaying the traffic.

Following issues need to be addressed in this key issue:

- How to support communications between PIN Elements within a PIN.

- How to enable a PIN Element to use a PIN Element with Gateway Capability to communicate (PEGC) with the 5GS.

- Whether and how 5GS supports relay path management for a PINE when a PEGC is used for the relay, e.g. including setup and release.

- How to select communication path for communication between PIN Elements, e.g. direct communication, via PEGC, via 5GS.

- Whether and how 5GS supports the policy and QoS differentiation for the traffic relayed between a PINE and 5GS when a PEGC is used for the relay.

## 5.5 Key Issue #5: Authorization for PIN

### 5.5.1 Description

The owner of a PIN may configure authorization information for the PIN, e.g., whether a PINE can communicate with other PINEs or with a specific data network, whether a UE is allowed to act as a PEMC and/or a PEGC, etc.

The following aspects will be studied:

- How to support authorization in a PIN, including following aspects:

- How to authorize/deauthorize a PIN Element to access 5GS service.

- How to authorize/de-authorize PIN Elements with Management Capability (PEMC) to manage the PIN.

- How to authorize/de-authorize PIN Elements with Gateway Capability (PEGC) to provide connectivity to and from the 5G network for other PIN Elements that is not capable to access the 5G network, considering the case when there are multiple PEGC capable UEs present in a specific PIN.

- How to enforce the authorization result for a PIN.

## 5.6 Key Issue #6: Policy and parameters provisioning for PIN

### 5.6.1 Description

In order to support the necessary procedures regarding to PIN, e.g., communication between PINEs, PINE/PEGC/PEMC discovery, authorization for PINE/PEGC/PEMC, etc., necessary policy/parameters configuration are needed.

The following aspects will be studied:

- Whether and How the PIN related policy and parameter(s) identified in the other KIs for PIN discovery, PINE discovery, authentication/authorization for PINE and PIN communication are configured to the PEMC, PEGC and PINE.

- Whether and how 5GC supports provisioning of configuration information to PEGC for access control.

5.7 Key Issue #7: Identification of PIN and PIN Elements

5.7.1 Description

The key issue focuses on potential enhancements needed to support identification of PIN and PIN Elements. The following aspects will be studied as part of the key issue:

- How to identify a PIN and who manages the PIN identity. Whether and what characteristics of a PIN shall be known to the 3GPP network (e.g. type of PIN (wearable, home automation, factory etc.), max of PIN elements in the PIN, etc.).

- How to support identifying PINE, PEGC and PEMC, and whether and how the 5GS manages the identifier.

# 6 Solutions

## 6.0 Mapping of Solutions to Key Issues

Table 6.0-1: Mapping of Solutions to Key Issues

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Key Issues | | | | | | |
| Solutions | 1  5GC architecture enhancements to support PIN | 2  PIN and PIN Element discovery and selection | 3  Management of PIN and PIN Elements | 4  Communication of PIN | 5  Authorization for PIN | 6  Policy and parameters provisioning for PIN | 7  Identification of PIN and PIN Elements |
| 1 |  | X |  |  |  |  |  |
| 2 |  | X |  |  |  |  |  |
| 3 |  | X |  |  |  |  |  |
| 4a |  | X |  |  |  |  |  |
| 4b |  | X |  |  |  |  |  |
| 5 |  |  | X |  | X |  |  |
| 6 |  | X | X |  |  |  |  |
| 7 |  |  | X |  |  |  |  |
| 8 | X |  | X |  | X | X |  |
| 9 |  |  | X |  |  |  |  |
| 10 |  | X |  |  |  |  |  |
| 11 |  |  |  | X |  |  |  |
| 12 |  |  |  | X |  | X | X |
| 13 |  |  |  | X |  |  |  |

## 6.1 Solution #1: PIN and PIN element discovery and selection

### 6.1.1 Description

This solution addresses the Key Issue#2 PIN and PIN element discovery and selection. The solution proposes method for PIN element discovery and PIN selection, PEGC discovery in a PIN, discoverability of PIN elements in a PIN.

The following are the key aspects of the solution

- PIN elements discover a Personal IoT Network either by listening to announcements from a PEMC or by querying for a PIN by its services.

- A PIN could be configured to support either an open or a restricted discovery.

- A PIN element could set its discoverability level within a PIN.

- A PEGC assignment is performed by PEMC.

### 6.1.2 Procedures

#### 6.1.2.1 PIN Discovery and Selection

**PIN Setup with PIN elements**

A PIN element offers one or more of PIN Services (these are corresponding to the functionality offered by the PIN element, some examples are audio output device, printer device, display device etc). A PIN might be configured to support only specific services.

There are two methods by which PIN elements discover and join a PIN.

Both methods are running on top of Non-3GPP (Bluetooth or WiFi) connections or on top of NR PC5 Direct Communication:

NOTE: NR PC5 applies only for PIN elements with Gateway Capability and PIN elements with Management Capability.



**Figure 6.1.2.1‑1 PIN Element function**

The first step is to discover PIN element functions on devices that are connected using any of these methods. The following call flow explains the two methods of PIN element (PIN E) discovery.

Alt 2 - PIN Element queries PEMC

Alt 1 - PEMC Announce

**PEMC**

**U**

**E**

**PI**

**N**

**E2**

**PI**

**N**

**E1**

PEMC authorized for PIN establishment  
UE has been provisioned with PIN policy parameters

PIN-Announce (List of Services, PIN Class, Time Window)

PIN Join Request (Service, Visibility)

PIN Join Accept (PIN Element Identifier)

PIN Join Request (Service, Visibility)

PIN Join Accept (PIN Element Identifier)

PIN Query (Service(s) in the PIN)

PIN Announce (List of Services or Open to All)

PEMC monitors for PIN Query from PIN elements

**Figure 6.1.2.1‑2 PIN Discovery**

**Method 1:**

In this method, PEMC periodically sends PIN related information and waits for a response within a time window. The announced information includes PIN identifier, PIN services offered (including services over 5GS), PIN Class (open to all or restricted), time window within which PEMC expects join requests from PIN elements.

A PIN is created by PEMC. PEMC periodically announces PIN parameters. This could be transmissions on multiple connections (Bluetooth links) or broadcast (WiFi, PC5)

PIN elements receive the announcement from PEMC and depending on their local configurations decide whether to join the PIN or wait for another PEMC broadcast. For joining the PIN, a PIN element sends PIN Join Request. This contains the services the PIN element offers in the PIN and also whether PIN element can be discovered by other PIN elements within the PIN or externally. The PIN Join request can also carry security credentials which enables PEMC to successfully validate a PIN element and adds it to the PIN.

A PIN Join Accept is sent by the PEMC through which the PIN element is informed of its PIN Element Identifier. The PIN Join Accept also include PIN Element Identifier for PEGC applicable for this PIN element.

**Method 2:**

In the second method, a PEMC, after it has been authorized by 5GC for PIN operation, begins to monitor incoming queries for PIN services. A PIN element sends out a query and waits for response. PEMC announces PIN related information. This includes PIN identity, PIN services, PIN status (open to all or restricted), time window within which PEMC expects “PIN Join” requests from PIN elements. PIN element then sends a PIN Join request as described for Method 1.

Editor’s note: Whether the protocol of the PIN layer is defined by 3GPP or it uses IETF protocols or part of Prose signalling is FFS.

**Open and Restricted PIN Discovery**

There are three broad classes of PIN:

1. Private PIN (e.g., home network)

2. Public PIN (e.g., shopping mall)

3. Personal Body area PIN (e.g., smart watch, smart glasses)

PIN supports two types of discovery - open and restricted discovery. In an open discovery any PIN element can attempt to join the PIN. The restricted discovery allows only PIN elements which have been configured with the PIN information to join. This configuration could be based on user input or local configuration in devices.

#### 6.1.2.2 Discoverability by other PIN elements

A PEMC offers a lookup service, where in a PIN element (either a member of the PIN or one that has not yet joined the PIN) is able to query for a PIN element identifier corresponding to a service.

A PIN element can set its visibility when joining a PIN. PIN elements can also indicate whether they want to share their information to other elements by PEMC. PIN element visibility can be set to {Private = PIN element cannot be looked up by other PIN elements}, {Restricted = PIN element can be discovered by other members of the PIN}, {Public= PIN element can be discovered by anyone querying for it, irrespective of whether they are a member of the PIN or not}.

Alt 2 - PIN element visibility to °Public”

Alt 2 - PIN element visibility to °within PIN”

**PEMC**

**U**

**E**

**PI**

**N**

**E2**

**PI**

**N**

**E1**

PEMC authorized for PIN establishment  
UE has been provisioned with PIN policy parameters

PINE1 has joined the PIN with visibility set to “Public”

PINE2 has not yet joined the PIN

PIN Element Query (PIN Elements offering services)

PIN Response (PIN identifiers matching queried service)

PINE1 has joined the PIN with visibility set to °Within PIN”

PINE2 has not yet joined the PIN

PIN Element Query (PIN Elements offering services)

PIN Response (No information)

PINE2 joins the PIN

PIN Element Query (PIN Elements offering services)

PIN Response (PIN Identifier for PINE1)

**Figure 6.1.2.2‑1 PIN Element Discovery**

#### 6.1.2.3 Discovery and Selection of PEGC

A UE capable of PEGC functionality is authorized for PIN operation by the 5GC.

A PEGC joins a PIN as a PIN element using either of the above methods. Along with the services, it also indicates in the PIN Join request that it is capable of functioning as a PIN Gateway.

**PEMC**

**U**

**E**

**UE (with PEGC capability)**

PEMC authorized for PIN establishment

UE has been pr

ovisioned with PIN policy parameters

PEGC is authorized by the MNO for

participating in a PIN as Gateway

PIN element discovery   
PEGC joins the PIN as a normal PIN element  
(indicates PEGC capability as a service offered)

Based on the PIN capabilities and other  
 local configurations, PEMC selects the PEGC

PEGC Assign Request

If UE accepts PEGC assignment, it responds with 3GPP UE identifier

[Optional] URSP Policy provisioning for PEGC by 5GC

PDU Session Establishment/Modification (PIN identifier, PEGC)

,

PEGC Assign Accept

**Figure 6.1.2.3‑1 PEGC Selection**

A PEMC selects a PEGC depending on whether it is trusted by PEMC. This could be from pre-configurations. A PEMC can be pre-configured with certain UE identifiers for potentially suitable PEGC (3GPP identifiers e.g., SUCI or GPSI are used to identify trusted PEGCs). A PEMC can also query within a PIN to find any pre-configured UE that can function as PEGC in the PIN.

PEMC assigns the role of PEGC by sending PEGC Assign Request to a PIN element capable of Gateway function. Once the PIN element accepts the PEGC assignment, it responds with PEGC Assign Accept. PEGC informs the membership of a PIN to the 5GC in PDU Session Establishment/Modification by including the PIN identifier for which it is acting as a PIN Gateway.

A PEGC can also indicate to the PEMC that it wants to stop functioning as a Gateway. This could be due to power consumption limitations or moving out of coverage of cellular network. In this case, PEGC sends a PEGC Release Request to PEMC. The PEMC will run the PEGC selection procedure again and confirms the role change to the former PEGC with PEGC Release Confirm.

### 6.1.3 Impacts on Existing Nodes and Functionality

Editor's Note: This clause captures impacts on existing 3GPP nodes and functional elements.

UE: implements the PIN Element Function protocol.

## 6.2 Solution #2: PIN and PINE discovery and selection

### 6.2.1 Description

#### 6.2.1.1 Overall architecture

Service Request

PINE/PEGC

PEMC

PINE

Producer

Consumer

Broker

Authentication/Service Registration

Authentication/Service Discovery

**Figure 6.2.1-1: SBA Architecture for PIN discovery and selection**

This solution addresses KI#2 and describes the architecture of the PIN, PINE services discovery and selecting PEMC, PEGC and PINE functionality in the PIN network.

We propose Service Based Architecture (SBA) for PIN discovery, selection and communication in the Personal IoT Network. In this SBA, we use consumer, producer and broker model for the PINE to register and provide its services to other PINE and discover services of other PINE in the PIN as shown in Figure 6.2.1-1. The PINE in the PIN, communicates among each other using Request-Response and subscribe-notify mechanism.

We assume that the PIN Elements in a PIN network are reachable via a wireless link such as WiFi, Bluetooth, WiGi etc., and the procedure to form a reachable PIN network at wireless link is out of scope of this document. PEMC acts as a broker in the service and producer model with PINE/PEGC service repository function. Higher layer protocol such as http is used for internal PIN communication and 5G NAS signalling is used to communicate with 5G systems such as PIN registration. A device will discover a PEMC using Request-Response broadcast message and register its services with the PEMC of the appropriate PIN network. PINE with PEGC capability will register itself with the DNN and then discover PEMC to register its gateway and other services.

Security and authentication of the PINE with the PEMC is described in the solution for KI#5. PEMC will maintain a repository of the PIN elements services and its FQDN or IP address. A PINE in the PIN will discovery other PINE services and reachability from the PEMC for eg., A PINE such as printer or a UE with gateway functionality will register its FQDN and its services with the PEMC. The PINE would query the PEMC for the printer or gateway functionality and based on the management policies the appropriate FQDN and its services of the printer and gateway is sent to the PINE. Management and configuring policies are described in the solution for KI#3 and KI#6.

#### 6.2.1.2 PIN and PIN element discovery and selection

PINE1

PINE2

PINEn

PINE3

Personal IoT Network (PIN)

PEMC/PEGC

5G System

http based “Authentication/Service Discovery”

http based PIN/PEMC discovery msg

PEMC (Broker)

PINE (Consumer)

http based “Auth/List of Service and access token”

http based “Service Request”

HTTP Broadcast based PIN/PEMC discovery

HTTP based Service Discovery

HTTP based Service Request/Response

PINE/PEGC (Producer)

http based “Service Ack”

http based PIN/PEMC response

**(a)**

**(b)**

**Figure 6.2.1-2: SBA Architecture for PIN discovery and selection**

We assume that the PIN elements are connected to a wireless LAN/ PAN network and each element are reachable via the wireless link. The procedure to connect to the wireless network and assign IP address is out of the scope of this document.

**PEMC Identification:** A NAS capable UE will register with the 5GS with “PIN capable” in the initial registration message to be authorized to form the PIN. 5GC architecture enhancements to support PIN are described in the solution for KI#1. Based on the “PIN control function” policies, the 5G core will authorize/deny the PIN formation. PIN element is identified as PEMC either by the 5GC policies or by 3rd party configuration. A PIN element with management capability (PEMC) can form a PIN and it can name the PIN based on the configuration. PEMC of the PIN will act as a broker in the proposed SBA architecture and respond to the PIN discovery query by the PINE or PEGC as shown in Figure 6.2.1-2 (a). PEMC will be NAS capable, and the policies and its capabilities are configured by the 5G core network. Policy and Provisioning for PIN are described in solution for KI#5.

**PEMC Discovery:** We assume that the PIN Elements in a PIN network are reachable via a wireless link such as WiFi, Bluetooth, WiGi etc., A device intending to join a PIN network will broadcast an http message for PIN discovery, and PEMC, when active, will respond to the query with PIN name and its capabilities as shown in Figure 6.2.1-2 (b). Once a device discovers the PIN networks and decides to join the PIN network based on the PINE local configuration. The device will authorize and register its services with the PEMC as described in solutions to KI#5.

**PEMC discovery Broadcast message:** We use IP broadcast message to discover PEMC. Unlike conventional http over TCP, we propose to send an Http discovery message over UDP + IP broadcast address, so that all the devices connected wirelessly get the http-based broadcast message. PIN elements can discover PEMC by broadcasting this http discovery broadcast message and the appropriate all PEMC of different PIN will respond to the queries. Similarly, PEMC will periodically and upon successful PIN registration will send http-based discovery message to all the wirelessly connected devices.

**PIN Elements Discovery:** The registered PINE can discover other PINE using the PINE discovery query to the PEMC (broker) as shown in Figure 6.2.1-2 (b). The PEMC will respond to the query with the list of all the devices, services and its FQDN or IP address. PIN elements can subscribe-notify for an event with the PEMC for example if a PINE wants to be notified when a PEGC or PINE with certain capabilities such as printer, scanner etc., joins the PIN.

**PEGC Selection and Discovery:** UE capable of NAS will register itself with the 5GC using registration procedure given in 23.501[X]. The UE will then discover the PIN using the PIN discovery query, will authenticate and register its gateway services with the PEMC. The PEMC will notify the subscribed PIN elements and it will include PEGC producer in the all the future PINE discovery queries. PEMC will assign PEGC to appropriate PINE based on the policies and notify both PINE and PEGC about their association.

Editor’s Note: The scenario of PEGC and PEMC not in same location is FFS

### 6.2.2 Procedures

Editor's note: Detailed Procedure is FFS.

### 6.2.3 Impacts on services, entities and interfaces

The solution largely re-uses existing functionality

The solution has the following impacts:

Impact to the UE (PEMC):

- Ability to support http broadcast messages, http request-response and http based subscribe-notify features

- Ability to maintain a list of all the PINE and its supported services

Impact to the UE (PINE/PEGC):

- Ability to support http broadcast messages, http request-response and http based subscribe-notify features

Impact to the 5G System:

- Add new Network Function (PINCTL) to the NAS in 5GS

- Add new fields to the Registration request such as “PIN capable”

- Add new fields to the Registration Accept message such as “PIN allowable”, “PIN Name”

## 6.3 Solution #3: Solution for PIN and PIN Elements discovery and selection

### 6.3.1 Description

This solution assumes the PINE is configured with basic information to select the PEMC as part of KI#6. Thus, PINE is able to select the PEMC and send the PIN\_join request to join the PIN.

The PIN\_join message contains the PIN Information as described in the clause 6.3.3.

Based on the PIN information and available subscription information with PEMC, the PEMC decides whether to add the PINE into the PIN, in response PEMC may provide PEGC\_name to the PIN in PIN\_join\_response command, if PINE has to be added to the PIN.

Whether the PINE is authorised to join the PIN is decided by a solution to KI#5, and how the PINE is joined into the PIN is described using the solution to KI#3.

### 6.3.2 Procedures



**Figure 6.3.2-1: PIN and PIN Elements discovery and selection**

0) The PINE is configured with PIN information (see below) either by 5GC (as part of KI#6), or by the authroised user. The PINE is configured with PEMC\_name (e.g. FQDN or address, in general the identifier of the PEMC) either by the 5GC or the authorised user.

1) PINE sends PIN\_join message to the PEMC including the PIN information (see below) to the PEMC.

2a) PEMC based on the PIN information decides whether to add the PINE in the respective PIN. If authorization of the PINE is successful following the solution selected as part of the KI#5, the PINE is added to the PIN by the PEMC, in this case PEMC may provide PEGC\_name to the PINE as part of the PIN\_join\_accept message. The solution selected as part of the KI#3 will describe how to add the PINE by the PEMC to the PIN.

If PINE is added to the PIN then PEMC stores the PIN information e.g. Supported service/device type part of the PIN information to identify that PIN supports particular service for e.g. Printer. The discoverability criteria based on which this PINE is discoverable to other PINE in the PIN.

2b) Based on PIN information if the PEMC is not able to select the PIN for example the respective service is not supported by any of the PINs or the PIN for respective group ID is not yet active then PIN\_join\_reject message is sent to the PINE. The PINE should not request for same PIN information for implementation dependent time.

The PIN information is at least one of the following:

a) Supported Service/device type (e.g. IOT, printer): Indicate particular service supported by the PINE.

b) Requested Service/device type (e.g. IOT, Printer): Indicate the requested service which the PIN should support in which this PINE has to be added.

c) Group ID (also called as PIN ID): The group ID configured by the authorised user or the 5GC, indicates the request to join the PIN which supports a particular group.

d) User defined name: This is a plain string configured by authorized user or the 5GC in the PINE. Based on this plain string PEMC identifies which PIN the PINE should be added. This plain string can be any configurable text for example it can be an ID or PIN\_NAME or PIN\_DISCOVERY name etc.

e) Discoverability criteria: The PINE is allowed to be discovered if requested for:

1) a specific service.

2) a specific group ID.

3) a specific user defined name.

4) a specific time for e.g. time slot.

### 6.3.3 Impacts on Existing Nodes and Functionality

Editor's note: This clause captures impacts on existing 3GPP nodes and functional elements.

## 6.4a Solution #4a: PIN and PIN Element discovery by A PINE

### 6.4a.1 Description

This solution resolves aspects of Key Issue #2: PIN and PIN Element discovery and selection that relate to how to discover PIN Elements in a PIN.

In this solution, connections between PINEs depends on lower layer (e.g. WIFI, Bluetooth), which is out of 3GPP scope. The PINEs (including PEMC and PEGC) communicates each other for PIN discovery via established connections.

### 6.4a.2 Procedures



**Figure 6.4a.2-1: PIN and PIN Element discovery**

0. Connections have been established between PEMC and other PINEs (including PEGC). How to establish connection depends on lower layer (e.g. WiFi, Bluetooth), which is out of 3GPP scope.

1. PEMC provides PIN discovery policy configuration to PINEs via established connections in step 0. The PIN discovery policy includes enable/disable discovery, PIN ID used for PIN discovery, PIN information (PIN Elements list, capability, availability, reachability and services).

2. PINEs (including PEGC) broadcast PIN announcement based on received PIN discovery policy. The PIN announcement includes PIN ID.

NOTE: How to broadcast PIN announcement depends on lower layer, for example, PIN ID may be broadcasted as SSID in WiFi access.

3. A PINE receives PIN announcement from a PINE (including PEMC or PEGC). The PINE selects PIN based on received PIN ID in PIN announcement and establish connection with the PINE. How to establish connection depends on lower layer (e.g. WiFi, Bluetooth), which is out of 3GPP scope.

4. The PINE sends PIN Solicitation Request, which indicates selected PIN ID and PIN information to be requested, e.g. PINEs in the PIN and corresponding capability, availability, reachability and services.

5. The PINE, which received the PIN Solicitation Request, sends PIN Solicitation response to the PINE, which includes PIN information requested by the PIN element.

### 6.4a.3 Impacts on Existing Nodes and Functionality

Editor's note: This clause captures impacts on existing 3GPP nodes and functional elements.

## 6.4b Solution #4b: PIN Elements with Gateway Capabilities (PEGC) discovery and selection by PEMC

### 6.4b.1 Description

#### 6.4b.1.1 Introduction

The aspect of the key issue #2 under that is addressed by this solution is how to discover and select PIN Elements with Gateway Capability (PEGC).

A typical PIN would consist of different PINEs (sensors, AR/VR, smart TV etc.) and these PINEs have different requirements and as such it could be possible that they require access to different 5G core networks services. This may mean that they need to use different PEGC’s to communicate with the different core networks to access required services.

A PEMC which does the management of the PINEs, would take into consideration PIN element types, connectivity & QoS requirements and accordingly, select a PEGC to ensure PINEs are connected to their respective core networks and meet required QoS requirements.

The solution addresses the above aspect and explains how a PEMC (PIN element with management capability) could be configured with the policy parameters and other information for PEGC selection.

In this solution, connections between PINEs depends on lower layer (e.g., WIFI, Bluetooth), which is out of 3GPP scope. The PINEs (including PEMC and PEGC) communicate each other for PIN discovery via established connections.

#### 6.4b.1.2 Functional Description

A PIN may have several PINEs with different characteristics such as wearable devices, home automation devices, in the office or smart industrial automation devices, having different requirements and roles in terms of size, weight, power consumption, mission critical, high bandwidth and so forth. Users may create a network of all or subset of these devices (PIN) and for each PIN there can be one or more PEGCs available.

To make selection of most appropriate PEGC, the PEMC can consider PINEs characteritics (PIN Types supported, CN Connectivity, Power source, QoS support, network slice ) or PIN type (Sensor Type, AR/VR, smart light, plug, UE etc.). The PEMC could be configured with the identities, capabilities, and prioritization information for PEGCs as follows.

1. The PEMC device could be configured by the application layer/user interface with required information for PEGC selection. This could be something as “user defined prioritized list of PEGCs” along with the PEGC capabilities i.e., PEGC ID, PIN Type supported, QoS Support, 5G CN Identigier , Network slice etc.

2. The PEGC selection parameters could be received by the PEMC during the registration procedure with the 5G core network, based on the provided PEMC capabilities in the registration request procedure. PEMC could request or receive data from active PINEs to learn PINEs characteristics before requesting 5G core network for parameters for PEGC selection.

### 6.4b.2 Procedures

In this option PEMC could request the 5G core network for PEGC selection information.



**Figure 6.4b.2-1: PEGC selection information during initial registration procedure**

1. PEMC has successfully established connection with the PINEs via lower layers (i.e., WiFi, Bluetooth), which is out of 3GPP scope, determines the PIN type and PIN characteristics (PIN Type, size, QoS requirements etc.) and will accordingly request PEGC selection information from the 5G core network.

2. The UE sends registration request messages and indicates its support as PEMC in the 5GMM Capability information element and provides PEMC capabilities (PIN Type, size, QoS requirements etc.).

3. The AMF sends a registration accept message including “network provided prioritized list of PEGCs” list along with the PEGC capabilities i.e., PEGC IDs, PIN Type supported, CN Connectivity parameters, QoS Support, 5G CN Identifier, Network slice etc.

### 6.4b.3 Impacts on Existing Nodes and Functionality

Editor's note: This clause captures impacts on existing 3GPP nodes and functional elements.

## 6.5 Solution #5: Solution for authorization and management of PIN and PIN Elements

### 6.5.1 Description

#### 6.5.1.1 Registration management of PEMC, PEGC and PINE

The registration management is used to register or deregister a PEMC/PEGC/PINE with the PIN Application Server, and maintain the user context in the network.

The Initial Registration procedure involves execution of PEMC/PEGC/PINE authentication and access authorization based on the configuration of the owner of the device.

Once registered and if applicable the PEMC/PEGC/PINE updates its registration with the PIN Application Server:

- periodically, in order to remain reachable; or

- to update its status, or

- to update its communication path; or

- to update its capabilities or parameters,

The profile of PINE/PEGC/PEMC is stored or updated in PIN AS after successful registration. The device profile may include following information:

- Device ID,

- Device name,

- MAC address or Bluetooth ID,

- GPSI of UE,

- Security related information,

- Device type e.g., PINE, PEMC, PEGC,

- Device communication capabilities,

- Device services capabilities.

A set of device context data of PINE or PEGC in a PIN may include following information:

- Associated PIN ID,

- Associated PEGC,

- Device state,

- Allocated IP addresses/IPv6 prefix,

- Authorized communication paths.

#### 6.5.1.2 Management of PIN and PINE Elements

The PEMC is registered into PIN AS and authorized to manage a PIN. The user of the PEMC can initiate the request to create a PIN via P4 reference point with PIN AS.

The PIN ID is allocated by PIN AS and an optional PIN Name can be allocated by the PEMC user. The profile and context data of the PIN is stored in PIN AS and synchronized with PEMC.

Following context data may be stored in the PIN profile:

- PIN state (active or inactive),

- List of serving PEMCs, include:

- PEMC ID,

- PEMC state,

- GPSI and PLMN ID.

- List of serving PEGCs, include:

- PEGC ID,

- PEGC state,

- GPSI and PLMN ID.

- List of PINEs

- PINE ID,

- PINE state,

- MAC address, BT ID, or GPSI and PLMN ID,

- The association with PEGC and other PINEs.

- The validity duration and the time validity of a PIN and PINE

The PEMC may invite/expel a PEGC or PINE in a PIN, and a PINE/PEGC may request to join/leave a PIN. All the request is routed to PIN AS for authorization. After successful authorization, PIN AS updated the PIN profile and modify the context data of the involved PEGC/PINE. The policy and parameters are provisioned to the PEGC via P3 reference point and to PINEs via P1 reference point to enforce the behaviour of the PINE and PEGC.

According to the policy of mobile operator, PIN AS may provision the PIN related information to the NEF, PCF, UDR or UDM for policy control or subscription management.

### 6.5.2 Procedures

#### 6.5.2.1 PIN Elements registration and PIN management

Figure 6.5.2.1-1 depicts a high-level procedure of PIN Elements registration, PIN management and invitation of PIN Elements to the PIN.

****

**Figure 6.5.2.1-1: PIN Elements registration and PIN management**

1-3. Registration of the PIN Elements (e.g., PINE, PEGC, PEMC) to the PIN, includes authentication and authorization of PIN Element, reporting of PIN Element ID and PIN Element profile to the PIN AS. It’s assumed that the PIN Elements can communicate with PIN AS via Internet.

4. After successful registration, the PEMC sends a request to the PIN AS to create a PIN. The PIN ID is assigned by the PIN AS to the PEMC.

5. The PEMC requests the PIN AS to add the PEGC into the PIN. If the invitation is accepted by the PEGC, the PIN AS updates the PIN profile and context data. The PIN AS sends configuration and parameters to the PEGC for PIN communication.

6 The PIN AS provisions PIN Service Specific Parameters to the UDR (via NEF) for policy control of the PEGC, include e.g., the PIN ID, default QoS requirement and valid time for PIN communication.

7. The PEMC requests the PIN AS to add the PINE into the PIN, includes the communication requirement of the PINE, e.g., associated PEGC, whether the PINE is authoried to access 5GS via PEGC, and the QoS requirement. If the invitation is accepted by the PINE, the PIN AS updates the PIN profile and context data. The PIN AS sends configuration and parameters to the PINE and PEGC for PIN communication.

8. The PIN AS provisions PIN Service specific Parameters to the UDR (via NEF) for the association of the PINE with the PEGC, include e.g. PINE ID, default QoS requirement and valid time for the PINE communication with 5GS.

#### 6.5.2.2 PINE accessing to 5GC via PEGC



**Figure 6.5.2.2-1: PINE accessing to 5GS via PEGC**

1. PDU Session of PEGC is established.

2. Application layer signaling 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.

NOTE: The signaling exchange between PINE and PEGC is based on non-3GPP access (e.g. WIFI, Bluetooth) and application layer deployment.

4. The PEGC authenticate and authorizes the access of the PINE, and allocates IP address for the PINE.

5. The PEGC initiates PDU Session modification as defined in clause 4.3.3.2 of TS 23.502 [3].

The PEGC sends the PINE information to the SMF via NAS signaling, include the PINE ID, IP address of the PINE, IP address and allocated port number in case of NAT applied.

6. The SMF updates the PCF with the PINE information in SM Policy Association Modification.

7. The PCF queries the UDR for PIN Specific Service Parameters with the PINE ID, 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.

8. The PDU Session Modification procedures as specified in clause 4.3.3.2 of TS 23.502 [3] continues from step 2. The QoS flow for the PINE communication with 5GS is established.

9. The PEGC sends a response to the PINE.

10. The application traffic of the PINE is relayed to the 5GS via the PEGC.

### 6.5.3 Impacts on Existing Nodes and Functionality

PIN AS: The PIN AS provisions PIN service specific parameters to the UDR (via NEF) for policy control of the PEGC.

UDR: In addition to the functions defined in TS 23.501 [2], the UDR performs the storage of PIN Service Parameters.

NEF: For PIN Application Functions to provide service specific parameters to the 3GPP network, the NEF supports additional PIN service parameters.

PCF: The PCF queries the UDR for PIN Service Parameters of a PINE and derives the PCC rules for the PINE communication with 5GS.

SMF: The SMF receives the PINE information via NAS message, and forwards it to PCF in SM Policy Association Modification request.

## 6.6 Solution #6: Management of PIN and PIN Elements

### 6.6.1 Description

This solution intends to enable the management of the PIN, such as creating/modifying a PIN and adding/removing the PIN Elements.

In this solution:

a) 5GC is responsible for management PIN and PIN Elements. In particular, P-NF is new 5GC network function dedicated to PIN, such as for management of PIN and of PIN Elements. The request to create a PIN is sent to the P-NF, and the P-NF can process the request and determine whether UE can act as a PEMC based on the information provided in the request.

b) P-NF is responsible for the identification of PIN and PIN Elements and for assigning the PIN identity. After P-NF allocates a globally unique PIN identifier in order to identify the uniquely the PIN).

Editor’s note: Format of PIN Identifier is FFS.

Note: For PIN Elements, it is allowed that a PINE can be added in more than one PIN. Thus, it is recommended to combine PIN ID and PINE ID to identify PIN Elements.

c) An authorized AF or UE can request to create a PIN. The request from AF contains the chosen PEMC information.

d) PEMC selects and determines a PEGC via PC5-based mechanism, e.g., ProSe discovery, or via means like Bluetooth. After PEMC selects a PEGC, they establish a PC5 connection or connection via transport layer.

e) Both PEMC and PEGC are authenticated by 5GC as UE using the 5G registration procedure.

f) Introduction of a new PIN functions in 5GC managing the PIN.

g) Definition of PIN layer which decouples the Transport part and the PIN functionalities from the functionalities of the UE or N3GPP devices in the scope of the PIN SID.

h) The PINE can only communicate to the PIN AF in DNN via user plane of the PEGC.

i) Only the PEMC and PEGC can communicate with the P-NF via the 5G NAS.

j) The PEMC and PEGC can directly communicate with the PIN AF via user plane PDU session.

k) The protocol between PINE, PEMC and PEGC over the user plane, i.e. via PDU session, is outside the scope of 3GPP.

l) The PEMC and PEGC belongs to the same PLMN. The roaming scenario is not supported

m) The solution assumes that the PEMC and the PEGC are located in the same PIN and they can communicate directly

Editor’s note: whether the PEMC can communicate when they are not in direct communication in PIN, e.g., the PEGC is in home and the PEMC is located in the PLMN network (e.g. in office) is FFS.

n) The PEMC manages the PIN network so it has visibility of all PINE currently members of the PIN, their identity and the

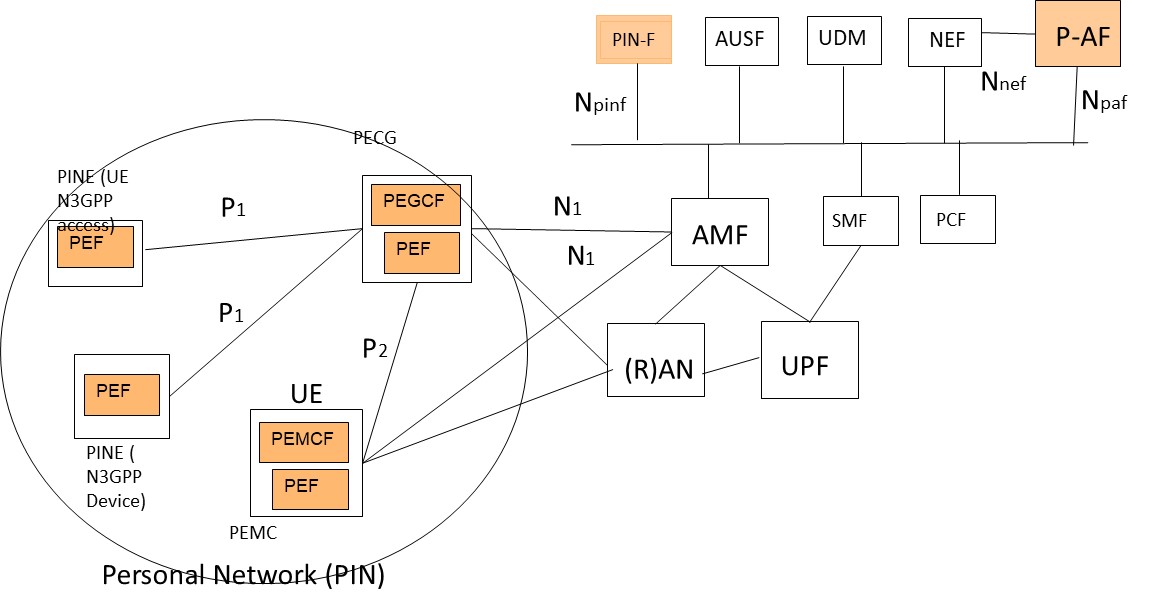
This solution addresses the following scenarios:

- How to create and identify a PIN in 5GC.

- How to choose UE(s) to be PEMC and/or PEGC.

- For PINE(s), how to join a PIN.

Figure 6.6.1-1 depicts the reference architecture for the solution. The PIN functions are defined in architecture assumption clause 4.



**Figure 6.6.1-1: Solution reference architecture**

The solution defines the following PIN functionalities:

- **PIN Element Function (PEF)** which represents the functionalities providing the communication within the PIN (via PIN direct connection or via PEGC), or outside the PIN via a PEGC. The PEF is able also to communicate with the PEMC for been configured, for discovery and for authentication and authorisation.

- **PIN Element Gateway Capability Function (PEGCF)** which represents the functionality providing the connectivity to and from the 5G network for other PIN Elements, or provide relay for the communication between PIN Elements

**- PIN Element Management Capability Function (PEMCF)** which represents the functionality providing the capability to manage the PIN

- **PIN Network Function(P-NF)** is a 5GC NF and represents the functionality providing the capability to manage the PIN in 5GC, e.g., processing the request of creating PIN, choosing a UE to be a PEMC and distribute a PIN ID to identify a PIN, etc.

The following definitions also apply:

- The PINE is a device supporting the PEF.

- The PEGC is an UE supporting the PEGCF

- The PEMC is an UE supporting the PEMCF

A UE can support both PEGCF and PEMCF, furthermore a UE can support the PEF function in order to exchange data information and/or provide PIN services to other PINE in the PIN.

The PINE per assumption can use the non-3GPP access (e.g. WIFI, Bluetooth) for direct communication to other PINE, PEGC and PEMC so the following type of device that contain the PEF are considered:

1) A Non-3GPP device, i.e. a device that does not support 3GPP Access or N3GPP Access to 5GC, but supports PEF. e.g. a device that uses Bluetooth or WiFi communication.

2) A UE that supports N3GPP Access to 5GC (i.e., N3IWF). The UE is restricted to only use the N3GPP interface for PIN direct communication

Editor’s note: Whether the device not supporting PIN Element Function (PEF) can participate to PIN network, e.g. as today when the UE share the 5G connection via WiFi, is FFS.

The following reference points are defined:

- P1 reference point between the PINE device(s).

- P2 reference point between the PEGC and PEMC device(s).

The P1 and P2 reference points are supported over Peer-to-Peer (P2P) transports, e.g. Bluetooth, WiFi, 5G Prose Direct Communication (i.e., UE-to-UE communication).

The following Service-based interfaces are defined

**Npinf:** Service-based provided by the P-NF.

**Npaf:** Service-based provided by AF dedicated to PIN network.

Figure 6.6.1-2 shows the typical implementation layers involved in a PIN network, the P2P transport and physical layer (e.g. Bluetooth, wifi, 54G ProSe..) the PIN layer which includes the PIN functionalities (i.e. the PEF, PEGC, PMEC) and the application layer which is out side the scope of 3GPP.

The device capable of participating in the PIN the PEF, PECGF, PEMCF and the Peer-to-peer transport layer.

The figure 6.6.1-3 shows the user plane protocol stack for PINE for the scenario (A) of transport of user application data to DNN via PEGC, e.g. web browsing to the internet DNN, for the scenario (B) for the transport of PIN application data exchange between the PINE and the PIN AF via PEGC. The figure 6.6.1-4 shows the control plane communication between the PINE and the PEGC. Figure 6.6.1-5 and Figure 6.6.1-6 show the user plane and control plane between PEMC and PEGC respectively.

Editor’s note:Whether the protocol of the PIN layer is defined by 3GPP or it uses IETF protocols or part of Prose signalling is FFS.



**Figure 6.6.1-2: Solution 6 Functional layer**



**Figure 6.6.1-3: PINE user plane protocol stacks for communication towards PIN AF in DNN via PEGC via 5GC user plane**



**Figure 6.6.1-4: PINE control plane protocol stacks**



**Figure 6.6.1-5: PEGC and PEMC user plane protocol stacks**



**Figure 6.6.1-5: PEGC and PEMC control plane protocol stacks.**

### 6.6.2 Procedures

Two flow charts about PIN creation and PINE authentication and registration are proposed in the following.

In PIN creation, the AF initiates a request to create a PIN, and the request contains the chosen PEMC information. After the PIN creation successful and the PEMC allocated, the PEGC needs to be assigned. A potential discovery method of PEGC is shown below. More details can be seen in 6.6.2.1.

#### 6.6.2.1 PIN creation

The PIN creation procedure is described in this clause.

PEMCF

PEGCF

RAN

AMF

P-NF

UDM

NEF

AF

UPF

0a) Registered to 5GC and establish a PDU session

0a) Registered to 5GC

0c. PIN specific interaction

1b. Npnf\_Setup Req (PEMC ID)

1a. Nnef\_PINSetup Req (PEMC ID)

2. Nudm\_Subscriber Data get (PEMC ID)

3a PIN Create

3b. Npnf\_Setup Resp (PEMC ID, PIN ID)

3c. Nnef\_PINSetup Resp (PEMC ID, PIN ID)

4a. Npnf\_PIN\_Create\_ Resp (PEMC ID, PIN ID)

4b. UL NAS Transport [P-NF container (PIN create resp (PEMC ID，PIN ID)]

5. Device connection setup

6a. UL NAS Transport [P-NF container (PEGC create req\_and\_auth (PEGC ID，PEMC ID, PIN ID)]

6b. Npnf\_Create\_ Req (PEGC ID, PIN ID)

7. Nudm\_Subscriber Data get (PEGC ID)

8 PIN Context update

9a. Npnf\_NotifyPEGC ID, PIN ID)

9b. Nnef\_PINNotifyPEGC ID, PIN ID)

10a. Npnf\_PIN\_Create\_ Resp (PEGC ID, PEMC ID, PIN ID)

10b. UL NAS Transport [PEGC authorize (PEGC ID，PEMC ID, PIN ID)]

10c. UL NAS Transport [P-NF container (PEGC create resp (PEGC ID，PIN ID)]

**Figure 6.6.2-1 Procedure for PIN Creation and Management**

0a-0b. The UE supporting the PEMC and PEGC functionality registered to 5GC before PIN creation. The PEMC may interact with the PIN AF over the user plane based PIN specific application mechanism and procedure which are transparent to 3GPP and out of the scope, for example the PIN AF may get a message informing that PEMC is connected and available.

1a-1b: AF can send a PIN setup request to P-NF via NEF to create the PIN network within the 5GC, and the request contains the chosen PEMC information.

2. When P-NF receives the request, it needs to send a request to get the chosen PEMC data in order to check whether the UE supporting PEMC functionality. As defined before, the PEMC functionality-supported UE is allowed to be PEMC.

3a-3c: After that P-NF receives the confirm from the UDM, it creates a PIN network generating the PIN ID associated to the PEMC ID requested from the AF. The response is sent to the requestor accordingly.

Editor’s Note: How the PIN ID is generated is FFS.

4a-4b: The P-NF send the indication of creation of PIN network to the PEMC which the PIN ID.

5: The PMEC can discover the presence of the PEGC via Prose Discovery mechanism and they establishes a Prose Direct communication

Editor’s Note: Whether the PEMC and PEGC are connected via WLAN or BT and how the discovery and connection is performed is FFS.

6a-6b: The PEMC sends a rested to authentication and authorisation of enabling the PEGC for the PIN via NAS to the P-NF indicating the identity of the PEGC and the PIN ID, and the PEGC ID can be a PEGC SUPI

Note: The PEMC can send a request to create PEGC before connection setup between PEMC and PEGC. PEMC may require a authentication of PEGC with the request.

7: The P-NF needs to send a request to get the UE data in order to check whether the UE supporting PEMC functionality.

8: After the P-NF receives the confirm from UDM, the P-NF update the PIN context adding the PEGC ID to the PIN network

9a-9b: The P-NF may notify to the PIN AF the addition of PEGC ID to the PIN ID if the PIN AF has been requested to be notified of PIN status changes in step 1a

10a-10b: The P-NF inform the chosen PEGC that it is authorized to be the gateway of the PIN network which PIN ID and of the PEMC ID

10c: The P-NF responds to the PMEC about the step 6a result.

#### 6.6.2.2 PINE authentication and registration

PINE authentication and registration procedure has the scope to perform the authentication and authorisation of PINE to be added to the PIN.

0) PIN selection

1）PIN Join(PINE ID, PIN ID)

6b.Npnf Notify (PINE ID, PIN ID)

5a) PIN Element authentication and Authorization

**PEF1**

**PEGCF**

**PEMCF**

**AMF**

**P-NF**

**NEF**

**UDM**

**AAA/AUSF**

2）PIN Join(PINE ID, PIN ID)

3a. PIN Identity Req (PINE ID, PEMCF ID)

3b. PIN Identity Req (PINE ID, PEMCF ID)

4a. PIN Identity Resp (PINE ID, PIN ID PEMCF ID)

4b.PIN Identity Resp (PINE ID, PIN ID, PEMCF ID)

6a.UL NAS Transport [P-NF container (PIN Update (PINE ID, PIN ID))]

7). PIN Successful auth Req (PINE ID temp, PIN ID, PIN sec key)

8 PIN Context update

9a.Npnf Notify (PINE ID, PIN ID)

9b.Nnef\_PINNotify (PINE ID, PIN ID)

**Figure 6.6.2.2-1 Procedure for PIN Element authentication**

0: The PINE performs the PIN network discovery procedure.

Editor’s Note: The PIN Network discovery procedure is FFS.

1: The PINE may send a PIN Join request to the PEGCF of the selected PIN providing its own Identity and the Requested PIN ID. If in step 0 the PINE is not able to identify the requested PIN ID, the device may send the join message to the available identified PEGCF.

2: When the PEGCF receives the PIN Join request from the PINE or when it performs the association for establishing the P2P transport layer can send the PIN Join request to the PEMCF without waiting the reception of the PIN Join message from PINE. This step may be specific for the P2P transport layer. The PINE ID may be derived from the previous association. e.g., from BT association, or the MAC address of the PINE.

Editor’s Note: The definition of PINE identity is FFS.

3a-3b: The PEMCF send a PIN identity request in order to trigger the PINE authentication & authorisation providing to the PINE the PIN ID and the PEMCF ID.

4a-4b: The PINE responds with its PINE ID and the information toward the PEMCF.

5: The PIN authentication is performed.

Editor’s Note: The detailed description of PIN authentication steps is FFS.

6a: When successfully authenticated the PEMC send a PIN update message toward the P-NF. The message is encapsulated in the PIN Container and transported over NAS.

6b: The AMF forwards the PIN message to P-NF in Npnf\_Notify.

7: The PEMCF send PIN successful authentication to PINE. The AF verifies that the PINE ID and whether is authorise dot be added to the PIN network.

8: The P-NF updates the PIN context adding the PINE ID to the PIN network identified by PIN ID.

9a-9b: The P-NF may notify to the PIN AF the addition of the PINE ID to the PIN ID if the PIN AF has been requested to be notified of PIN status changes.

Editor’s Note: The generation of PIN security key will be revised based on SA3 study.

### 6.6.3 Impacts on services, entities, and interfaces

**AMF:**

- Support P-NF container messages.

**P-NF:**

- Support the management of PIN, e.g., assign an authorised UE to be PEMC/PEGC, distribute a PIN ID to identify a PIN.

**NEF:**

- Interact with P-NF for exposure of PIN information toward AF.

## 6.7 Solution #7: PIN Management by 5GS.

### 6.7.1 Description

Once the PEMC/PEGC discovers other PINE with ProSe capabilities within the PIN, the next step is to Register the PIN with 5GS.

### 6.7.2 Procedures

****

**Fig 6.7.2-1: PIN Registration with 5GS**

The PEGC UE registers with the 5GS, with the following changes to the Registration procedure defined in clause 4.2.2.2.2 of 3GPP TS 23.502 [3]:

- In the Registration message the PEGC indicates PIN Gateway capability and also provides the list of PINE (which may access 5GS system via PEGC and hence needs authentication/authorization by the 5GS).

- For 3GPP PINE, authentication/authorization is done by 5GS with AUSF/UDM and for non-3GPP PINE using external/3rd party AAA server.

Editor's note: The details of PINE authentication/authorization is FFS

- After successful authentication/authorization, AMF gets the PIN subscription profile from the UDM which may contain information about the maximum number of PINE/PEGW allowed, PIN duration, allowed services.

- After successful registration (step 5a), based on the PIN subscription profile, AMF provides PIN group ID and may further provide duration allowed for the PIN and allowed list of PINE.

In case of failure during PIN registration (step 5b), AMF rejects the registration with appropriate cause code (e.g. Maximum PINE/PEGW reached, PIN not allowed.)

When a new PINE is added to the PIN or existing PINE is removed from the PIN and if those PINE may access 5GS via PEGC, where 5GS has its profile, PEGC triggers Registration procedure as indicated in Fig 6.7.2-1 to update the 5GS about the PINE.

NOTE 1: PINE that does not access 5GS and only uses direct communication between other PINE within PIN does not need to be authenticated/authorized by the 5GS and will not be included in the list of PINE by the PEGC in the Registration request during the Registration procedure.

When there is change in PEGC in a PIN, the new PEGC triggers Registration procedure as explained in Fig 6.7.2-1 and AMF updates the PEGC for the PIN accordingly. Old PEGC may or may not be part of the list of PINE provided by the new PEGC. If the old PEGC continues to access 5GS but no longer is the PIN gateway, then it indicates the same with Registration update procedure (with type mobility registration update).

NOTE 2: PINE may have individual 5GS subscription and when it registers with 5GS via PEGC of a PIN, the UDM updates the profile about the serving PIN group Id.

After the expiry of the PIN duration indicated to the PEGC by the AMF during the registration, AMF would initiate Network triggered de-registration procedure towards PEGC, as defined in 3GPP TS 23.502 [3], cl 4.2.2.3.3.

Editor's Note: It is FFS how the validity duration for individual PINE is handled.

NOTE 3: PINE management within PIN is managed by the PEMC without involvement of 5GS.

### 6.7.3 Impacts on services, entities and interfaces

The solution has the following impacts:

**UE:**

- UE shall indicate the list of other PINE that are served by the UE (acting as PEGC) within PIN to the 5GS.

**UDM:**

- UDM supports PIN subscription profile.

- Ability to update the individual subscription profile of an UE if its part of a PIN.

**AMF:**

- AMF supports PIN management, new failure cause code to indicate to the UE over NAS based on different failure conditions.

## 6.8 Solution #8: Management of PIN and PIN Elements

### 6.8.1 Description

This solution mainly addresses KI#3 “Management of PIN and PIN Elements” and KI#5 “Authorization for PIN”, i.e., authorization of PEMC management PIN and PEGC providing connectivity to and from 5G network. This solution also address part of KI#6 “Policy and parameters provisioning for PIN”, i.e., the RAT parameters and Discovery parameters provisioning.

The steps in the following call flows depicted as grey line in the figures, which are over application layer, are out of SA2 scope.

#### 6.8.1.1 Architecture reference model for application level

The following figure 6.8.1.1-1 depicts the reference architecture for PIN only on the application level.



NOTE 1: The PEMC can be a PINE when relayed by PEGC for visiting 5GS.

NOTE 2: The PEMC can also be a PEGC.

**Figure 6.8.1.1-1: Reference architecture on application level**

#### 6.8.1.2 Architecture reference model for 5GS level

The following figure 6.8.1.2-1 depicts the reference architecture for PIN only on 5GS level.



**Figure 6.8.2.2-1: Reference architecture on 5GS level**

#### 6.8.1.3 Reference points

The PIN System Architecture contains the following reference points on application level:

**Pin1:** Reference point between the PEMC and the PINE or PEGC.

**Pin2:** Reference point between the PINE and the PEGC.

**Pin3:** Reference point between the PEMC and the PINMF.

**Pin4:** Reference point between the PEGC and the PINMF.

### 6.8.2 Procedures

#### 6.8.2.1 Management of PIN

The procedure describes how a PINMF and 5GC authorize the PEMC to manage the PIIN, including creation/deletion and update the PIN, e.g., the duration of the PIN.



**Figure 6.8.2.1-1: Management of PIN**

1. The PEMC interacts with the PIN Management Function (PINMF). The PEMC can discover the PINMF based on DNS query, or preconfigured information.

2. The PINMF sends PIN Authorization Request (GPSI) to the NEF.

3. The NEF queries whether the PEMC has subscribed PIN service as a manager for a group or not.

4. The NEF responds to the PINMF based on the subscription, if the PEMC indicated by the GPSI has subscribed PIN service, then responds success.

#### 6.8.2.2 Management of PEGC and PINE

The procedure describes how a PEMC/PINMF adds/removes a PINE or PEGC into/from a PIN, and how 5GC authorizes the PEGC to joining into the PIN for query RAT and Discovery parameters to serving the PIN.



**Figure 6.8.2.2-1: Management of PEGC and PINE**

1. The PEGC or PINE may establish direct connection, e.g., the PEGC/PINE powered on with WiFi hotspot, and PEMC scans the bar code on the PINE/PEGC to have the parameters for connecting to the PEGC/PINE.

2. The PEMC may query device information from PEGC/PINE over application layer. The parameters for visiting the application in the PEGC/PINE may be documented via the bar code.

3. The PEMC interacts with PINMF over application layer, to indicate adding/deleting/updating the information for the PEGC/PIN.

4-5. The PINMF sends PIN configuration to the PEMC and to the PINE/PEGC via the PEMC over application layer. The configuration may include the PIN name/ID. For PINE, the configuration may include access information to discover/select and visit PEGCs, e.g., the allowed SSIDs, corresponding passwords, and PIN APP visiting parameters of PEGC, the SSID of the PINEs, etc. For PEGC, the configuration may include parameters such as SSID, password, parameters for visiting PINMF, etc.

6. In case of PEGC, the PEGC may close direct connection with PEMC. The PEGC connects to 5GS.

For PINE management, the procedure stops. For PEGC management, the following steps are performed.

7. The PEGC registers to the PINMF over application layer using the configured parameters obtained in step 5.

8. The PINMF sends Create/Update/Delete PIN Parameters Request (GPSI, PIN ID, RAT Info, Discovery Info) to the NEF. The RAT Info includes RAT configuration information, e.g., whether the SSID is hidden or not, activated RAT types (e.g., WiFi, BT), discovery methods (e.g., WiFi for open, BT for restrict), etc. The Discovery Info includes the allowed list or forbidden list of device information (e.g., MAC address, IP address) for authorization of the PINE discovering PEGC.

9. The NEF queries PIN subscription of the PEGC from UDM/UDR to check whether the PEGC is a group member in a group that also contains the PEMC. If the authorization fails, go to step 16.

10. The NEF sends Create/Update/Delete PIN Parameters Request (SUPI, PIN ID, RAT Info, Discovery Info) to the UDM/UDR.

11. The UDM/UDR stores the PIN related information and sends PIN Parameters Delivery (SUPI, PIN ID, RAT Info, Discovery Info) to the AMF.

12. The AMF sends the PIN ID, RAT Info, and Discovery Info to the PEGC.

13. If the UE supports PEGC, the UE sends result to the AMF.

14. If the result from the UE is received, or timed out for receiving the result from UE (i.e., the UE does not support PEGC), the AMF responds to the UDM/UDR.

15-16. The UDM/UDR responds to the NEF. The NEF responds to the PINMF.

17. The PINMF may update PIN configuration to the PEMC over application layer.

#### 6.8.2.3 Management of association between PEGC and PINE

The procedure describes how an association between PEGC and PINE is established and managed.



**Figure 6.8.2.3-1: Management of association between PEGC and PINE**

1. The PEGC has established PDU Session.

2. The PINE establishes direct connection with the PEGC using the parameters obtained in procedure described in clause 6.Y.2.2.

3. The PINE sends relay request over application layer to the PEGC. The parameters for visiting the PEGC over application layer can be obtained over application layer in procedure described in clause 6.Y.2.2.

4. The PEGC sends relay request over application layer to the PINMF. The parameters for visiting the PINMF over application layer can be obtained over application layer in procedure described in clause 6.Y.2.2.

5. The PINMF authorizes the request and initiates the relay path management procedures using solution 12 addresses to KI#4.

6-7. The PINMF sends relay response to the PEGC over application layer, and PEGC sends the relay response to the PINE over application layer.

8. The PINMF may update PIN configuration to the PEMC over application layer. The PINMF may perform further action, e.g., delete the PINE, re-configure the rule of the PINE communication, etc.

#### 6.8.2.4 Parameters provisioned to PEMC

The parameters provisioned to PEMC is over application layer. The parameters provisioned via application layer may include following:

- PIN name and PIN ID, as well as the PIN description.

- Characteristic of PIN, e.g., wearable, smart home, smart office, etc.

- List of PEGC

> Device Info, e.g., GPSI, IP address, name, description.

> Access RAT info, e.g., WiFi open/close, BT open/close, PC5 open/close, SSID hidden, etc.

> Discovery Info.

>> Connection parameters, e.g., SSID and Password for WiFi.

>> Discovery method, e.g., monitor, announcer, open, restrict, etc.

>> Restrict discovery info, e.g., list of allowed PINE info, list of forbidden PINE info.

> List of PINE associated with the PEGC.

>> Service type, e.g., printer, TV, etc.

>> Allowed peer info or forbidden peer info.

>> Access RAT info.

>> Discovery Info.

- List of PINE not associated with any PEGC

> Service type, e.g., printer, TV, etc.

> Access RAT info.

> Discovery Info.

#### 6.8.2.5 Parameters provisioned to PINE

The parameters provisioned to PINE is over application layer. The parameters provisioned via application layer may include following:

- PIN ID.

- List of PEGC

> Access RAT info.

> Discovery Info.

>> Connection parameters, e.g., SSID and Password for WiFi.

>> Discovery method, e.g., monitor, announcer, open, restrict, etc.

- List of PINE allowed to have direct communication

> Discovery Info.

#### 6.8.2.6 Parameters provisioned to PEGC

The parameters provisioned to PINE is over 5GC control plane. The parameters provisioned via 5GC control plane may include following:

- PIN ID.

- Access RAT info, e.g., WiFi open/close, BT open/close, PC5 open/close, SSID hidden, etc.

- Discovery Info.

> Connection parameters, e.g., SSID and Password for WiFi.

> Discovery method, e.g., monitor, announcer, open, restrict, etc.

> Restrict discovery info, e.g., list of allowed PINE info, list of forbidden PINE info.

### 6.8.3 Impacts on Existing Nodes and Functionality

**PINMF:**

- Support PIN ID assignment.

- Support PEMC authorization operation.

- Support PIN Parameters operations to provision RAT Info and Discovery Info to PEGC.

**NEF:**

- Support PEMC authorization operation.

- Support PIN Parameters operations and PEGC authorization.

**UDM:**

- Support PIN Parameters operations with NEF and delivery PIN parameters to UE via AMF

**UDR:**

- Support PIN subscription for PEMC and PEGC and PIN subscription query.

**UE (support PEGC):**

- Support PIN Parameters provisioning over NAS.

Editor's note: Additional impacts are FFS.

## 6.9 Solution #X: PIN management and PINE management

### 6.9.1 Description

This solution is to address the KI#3 “Management of PIN and PIN Elements”, how an authorized UE to create a PIN. And how to add a device (PINE) into a PIN, when a PIN is created and PEMC is available. In this solution, it assumed that UDM is used to create/update/remove PIN profile that includes PIN information and PINEs information, and allocate/manage the PIN ID. And may allocate/manage PINE ID for the PIN.

In this solution both PINE Info and PIN Info are defined as following:

**PINE Info:**

- **PINE ID**, unique ID within a PIN that could be allocated by PEMC locally, or network

- **PINE type**, indicating whether it is PEMC, or PEGC, normal PINE

- **PINE name**, human readable information, e.g., printer in bedroom, or lamp in living room.

- **Service**, what the PINE can provide, e.g., printer, or lamp, or camera, etc.

- **Valid time**, how long for the PINE to be as member in the PIN

- **Capability**, indicating the communication capability, e.g., WiFi, BT, etc.

**PIN Info:**

- **PIN ID**, unique ID within a PLMN and allocated by network,

- **PIN name**, is readable information for user

- **PIN Services**, the list of the services that the PINE(s) can provide, e.g., printer, lamp, camera, etc.

- **PIN valid time**, to define how long the PIN can work, e.g., 30 minutes

- **List of PINE Info**, including all the information of PINEs in this PIN

Editor's note: it is FFS how to authorize the UE to create PIN.

### 6.9.2 Procedures

#### 6.9.2.1 An authorized UE to create a PIN



**Figure 6.9.2-1: authorized UE creates a PIN**

Here the authorized UE is allowed by the PIN owner to initiate to create a PIN. When an authorized UE triggers a request to network for creating a PIN, it may bring the candidates **PIN Info, e.g., the PIN name, etc.**, optionally candidates **PINE Info**, which some of the **PIN/PINE Info** may be designed by user before creating the PIN, e.g., PINE name, capability, etc.

1. UE sends the request to AMF via gNB for creating a PIN, which including candidate PIN name, candidate PIN Service(s), candidate PIN valid time, optional if available, a list of candidates PINE information containing (candidates PINE ID, candidate PINE name, candidate PINE type, candidate PINE service, candidate PINE capability, candidate PINE valid time).

When PINE ID is allocated by network, the candidates PINE ID is not included.

NOTE: Create PIN request message can be carried by Registration Request.

Editor’s note: Whether Service Request or others possible is FFS.

2. AMF requests to UDM for creating the PIN, with information carried in step 1. AMF may check with UDM whether the UE is authorized to create PIN. If no, the AMF rejects the UE with proper cause.

3. AMF sends the Create PIN response to UE/PEMC if the request is rejected by AMF..

4. UDM allocates the PIN ID based on UE request, and may allocates PINE ID for each candidate PINE if PINE info included in the request, and create PIN profile in the UE’s subscription data, including e.g.,

**PIN Info:**

- PIN ID, e.g., xxxxx

**- PIN name**, e.g., Jian’s smart home

**- PIN Services**, e.g., printer service, lamp service, camera service.

**- PIN valid time**, e.g., 1 year

**- List of PINE Info**, including all the information of PINEs in this PIN

**PINE1 Info:**

**- PINE ID**, e.g., J001

**- PINE type**, e.g., PINE

**- PINE name**, e.g., printer in bedroom.

**- Service**, e.g., printer service.

**- Valid time**, e.g., 10:00-18:00 each day

**- Capability**, e.g., WiFi, BT.

**PINE 2 Info……**

**PINE 3 Info……**

5, UDM response to AMF with result of creating PIN, including the results, full PIN Info{PIN ID, PIN name, PIN Service, PIN valid time, optional list of PINE Info}

6, AMF sends the service accept to UE via gNB, including results, and full PIN Info.

#### 6.9.2.2 A device joins a PIN



**Figure 6.9.2-2: a device to join a PIN**

In this solution, it assumed that PEMC broadcasts PIN network information, e.g., PIN ID, PIN name, etc. so that the device discovers and selects the target PEMC, and connection between device and PEMC is established via non-3GPP RATs, e.g., WiFi, BT, etc.

1. A device sends the Join PIN Request to PEMC via the established connection between the device and PEMC, including PIN ID, Device ID, PINE type (optional), capability, Service, name, etc.

2. PEMC determines to accept the request. How to determine to accept the request is up to implementation. PEMC allocates the PINE ID for the device. And PEMC determines the PINE type, e.g., act as PEMC, or PEGC, or PINE.

3. PEMC sends the Join PIN response to the device, including result (accept, or reject), PIN Info and PINE Info as defined in 6.9.1.

**PIN info**: PIN ID, PIN name, PIN Service(s), PIN valid time, list of PINE info;

**PINE info**: PINE ID, PINE name, PINE type, capability, Service(s) and valid time.

4. PEMC sends the PIN update request to AMF via gNB, including UE ID, PIN Info container [PIN ID, new PINE info {PINE ID, PINE type, PINE name, capability, service, valid time}]

NOTE 1: The PIN update request can be carried by Registration Request.

Editor’s note; Whether Service Request or others possible is FFS.

5. AMF sends the Nudm\_UECM\_Registration Request to UDM for updating the UE’s PIN Info, including message received in step 4.

Before updating the PIN Info, UDM may determine whether to accept the updating, e.g., accept new PINE.

6. UDM updates the received PIN info to the UE’s subscription data.

When a PIN is created, the PIN related information is established as well in the requested UE’s subscription data.

7. UDM sends the response to AMF, including the results, and updated PIN Info.

8. AMF sends the PIN update response to PEMC with result (accept, or reject), and updated PIN Info.

9. For another option instead of step 3, PEMC sends the join PIN Response to device with result, and PIN/PINE info same as in step 3 after PEMC updating the PIN info to UDM.

NOTE 2: In step 1, 3 and 9, both application layer and new adapted layer are possible options for delivering the messages.

### 6.9.3 Impacts on Existing Nodes and Functionality

Network impacts:

- UDM allocates PIN ID for each create PIN request

- UDM allocates PINE ID for each requested PINE

- UDM manages the PIN info and PINE Info

- AMF requests management of PIN/PINE to UDM based on the PIN related request

## 6.10 Solution #10: Management of PIN and PIN Elements

### 6.10.1 Description

#### 6.10.1.1 Overall architecture

Service Request

PINE/PEGC

PEMC

PINE

Producer

Consumer

Broker

Authentication/Service Registration

Authentication/Service Discovery

**Figure 6.10.1.1-1: SBA Architecture for PIN discovery and selection**

This solution addresses KI#2 and describes the architecture of the PIN, PINE services discovery and selecting PEMC, PEGC and PINE functionality in the PIN network.

We propose Service Based Architecture (SBA) for PIN discovery, selection and communication in the Personal IoT Network (PIN). In this SBA, we use consumer, producer and broker model for the PINE to register and provide its services to other PINE and discover services of other PINE in the PIN as shown in Figure 6.X.1-1. The PINE in the PIN, communicates among each other using Request-Response and subscribe-notify mechanism.

We assume that the PIN Elements in a PIN network are reachable via a wireless link such as WiFi, Bluetooth, WiGi etc., and the procedure to form a reachable PIN network at wireless link is out of scope of this document. PEMC acts as a broker in the service and producer model with PINE/PEGC service repository function. Higher layer protocol such as http is used for internal PIN communication and 5G NAS signalling is used to communicate with 5G systems such as PIN registration. A device will discover a PEMC using Request-Response broadcast message and register its services with the PEMC of the appropriate PIN network. PINE with PEGC capability will register itself with the DNN and then discover PEMC to register its gateway and other services.

Security and authentication of the PINE with the PEMC is described in the solution for KI#5. PEMC will maintain a repository of the PIN elements services and its FQDN or IP address. A PINE in the PIN will discovery other PINE services and reachability from the PEMC for eg., A PINE such as printer or a UE with gateway functionality will register its FQDN and its services with the PEMC. The PINE would query the PEMC for the printer or gateway functionality and based on the management policies the appropriate FQDN and its services of the printer and gateway is sent to the PINE. Management and configuring policies are described in the solution for KI#3 and KI#6.

#### 6.10.1.2 Management of PIN and PIN Elements

PEMC/PEGC

PINE1

PINE2

PINEn

PINE3

Personal IoT Network (PIN)

5G System

**Figure 6.10.1.2-1: PIN Architecture and gateway to 5G System**

**Background on PIN Communication:** Higher layer protocol such as http is used for internal PIN communication and 5G NAS signalling is used to communicate with 5G systems such as PIN registration as described in solution to KI#4. We use IP broadcast message to discover PEMC. Unlike conventional http over TCP, we propose to send an Http discovery message over UDP + IP broadcast address, so that all the devices connected wirelessly get the http-based broadcast message. PIN elements can discover PEMC by broadcasting this http discovery broadcast message and the appropriate PEMC of different PIN(s) will respond to the queries. Similarly, PEMC will periodically and upon successful PIN registration will send http-based discovery message to all the wirelessly connected devices. Once PINE discovers PEMC and gets the registered services and IP address or FQDN, it can communicate with any PINE using http query-response messages as described in solution for KI#4.

**Operator Policies or 3rd party policies:** The operator policies are pushed to PIN from “PIN Control Function” (PINCTL) via NPINCTL of the 5GC to the PEMC of the PIN as described in solution for KI#1. PEMC will be NAS capable and register to the 5GC or it can register through PEGC. Upon registration and authentication with the 5G network, the PINCTL will communicate the policies to the PEMC. Similarly, the 3rd party configurations should be pushed to the PEMC to enforce them on the PIN network.

**PIN Management:** The operator or 3rd party policies will be pushed to the PEMC of the appropriate PIN and the PEMC will update the repositories and notify PIN elements appropriately. The following use cases will further elaborate on management of PIN.

**Case “Create PIN”:** PEMC will broadcast the new PIN announcement using the PIN discovery response message to the connected devices on the wireless network. The devices on the wireless network will intercept and based on its configuration and policies the devices will decide to join the PIN.

**Case “Modify PIN”:** PEMC will update its repository with the updated PIN modification and notify the PIN elements appropriately.

**Case “Delete PIN”:** PEMC will delete its PIN related repository and notify all the PINE about the deletion of the PIN. Once the PIN is deleted, any query-response and subscribe-notify from the PINE will not be honoured.

**Case “Activate PIN”:** PEMC will broadcast the activation of PIN so that the devices in the local wireless network can decide to join the PIN by authenticating and registering with the PEMC.

**Case “Deactivate PIN”:** PEMC will delete all its PIN related repository and it will broadcast about the de-activation of the PIN to the PIN elements. Once the PIN is de-activated, any query-response in the PIN will not be honoured.

**PIN Element Management:** The management of the PINE will be pushed to the PEMC either from the network operator or by the 3rd party.

**Case “Add or delete PINE”:** PEMC will add or delete a PINE’s FQDN or IP address and its services to the PEMC repository and notify all the registered PINE about the PINE addition or deletion. Once the PINE is deleted, any request and subscribe from the PINE will not be responded or registered respectively.

**Case “PEGC and PINE association”:** Any changes to the PEGC and PINE association will be updated in the PEMC repository and the appropriate PEGC and PINE will be notified about the changes. For eg. Suppose PINE1 was associated with PEGC1 and PEMC is the broker of a PIN network, and if there is policy from the 5GC or 3rd party to change the association of PEGC1 with PINE1 then PEMC will update the old PEMC repository of the association of PEGC1 with PINE1 to PEGC2 with PINE2 and will notify all PEGC1, PEGC2 and PINE1 about the new policy association. After the policy update, PEGC1 will terminate any ongoing association and will not honour any new association request from the PINE1 and PEGC2 will honour and accept all the association from PINE2.

**PIN Duration Validity:** PEMC of the PIN network can set a duration of the PIN network by starting a timer based on the allowed duration of the PIN, which will be a policy from the operator or 3rd party policies. At the end of the PIN allowable time, the PEMC will Deactivate the PIN as described in 6.X.1.2 section. Once the PIN is deactivated, the PEMC will update the PINCTL of the 5G-Core about the PIN deactivation. Optionally, PINCTL can also start a timer to make sure that the PIN is disabled as per the allowable duration.

### 6.10.2 Procedures

Editor's note: Detailed Procedure is FFS.

### 6.10.3 Impacts on services, entities and interfaces

The solution largely re-uses existing functionality

The solution has the following impacts:

Impact to the UE (PEMC):

- Ability to support http broadcast messages, http request-response and http based subscribe-notify features

- Ability to maintain a list of all the PINE and its supported services

Impact to the UE (PINE/PEGC):

- Ability to support http broadcast messages, http request-response and http based subscribe-notify features

Impact to the 5G System:

- Add new Network Function (PINCTL) to the NAS

- Add new fields to the Registration request such as “PIN capable”

- Add new fields to the Registration Accept message such as “PIN allowable”, “PIN Name”

- Add the following fields or parameters to the AMF paging

- Updated “PINE list”, which contains a list of PINE elements and its associated policies and parameters. For eg. A typical “PINE list” will be as follows:

- PINE1, PEMC = FALSE, PEGC=FALSE, 5G\_Aceess=TRUE, PINE\_TO\_PINE=TRUE, DURATION = UNLIMITED

- PINE2, PEMC = TRUE, PEGC=FALSE, 5G\_Aceess=TRUE, PINE\_TO\_PINE=TRUE, DURATION = UNLIMITED

## 6.11 Solution #11: Differentiated QoS between a PINE and 5GS when a PEGC is used for the relay

### 6.11.1 Description

#### 6.11.1.1 Introduction

QoS experienced by PINEs connected behind a PEGC depends on the end-to-end path between a PINE and the application server, i.e. depends on the QoS differentiation in both the 3GPP network and the non-3GPP network attached to the PEGC.

For example, a certain Packet Error Ratio (PER) can only be successfully ensured if it is enforced in both the 3GPP network and the non-3GPP network attached to the PEGC.

To address this shortcoming, this solution proposes to indicate Non-3GPP QoS assistance information to the PEGC to enable the PEGC to perform QoS differentiation for the PINEs in the non-3GPP network behind the PEGC.

Note that this is conceptually similar as providing Additional QoS Information to a UE for trusted/untrusted access to 5GC as defined in TS 23.502 [3], which enables the UE to reserve resources in the non-3GPP network. The difference is that the Non-3GPP QoS assistance information is used to reserve resource in the non-3GPP network attached to the PEGC. In line with the definition of Additional QoS information, the details of how to enforce QoS in the non-3GPP network based on the Non-3GPP QoS assistance information are beyond the scope of 3GPP.

#### 6.11.1.2 Solution principles

The solution is based on the following principles:

- This solution focuses on the AF requested QoS control of PINE communication to 5GS via PEGC, which has no dependence on the PIN management capability.

- During PDU session establishment and PDU session modification, if the SMF provides the PEGC with QoS flow descriptions, the SMF may, based on subscription, additionally signal non-3GPP QoS assistance information for each QoS flow to the PEGC. The non-3GPP QoS assistance information consists of the following QoS information (if available at the SMF): QoS characteristics, GFBR/MFBR (if applicable), ARP, Periodicity.

- Based on the non-3GPP QoS assistance information together with QoS rule information, the PEGC may reserve resources in the non-3GPP network.

NOTE: The details of how to enforce QoS based on the Non-3GPP QoS assistance information in the non-3GPP network are not subject of this solution and are considered to be beyond the scope of 3GPP.

### 6.11.2 Procedures



**Figure 6.11.2-1: Providing Non-3GPP QoS assistance information to the PEGC to enable the PEGC to ensure QoS in the non-3GPP network attached to the PEGC**

1. PDU Session is established

2. Application layer signaling is exchanged between an application on a PINE connected to the PEGC and an application function (AF)

3. Based on the application layer signaling, the AF requests QoS for application flows.

NOTE 1: If the AF is not considered trusted, then the AF interacts with the NEF instead. If the AF provides explicit QoS parameters, then AF (or NEF in case the AF is not trusted) interacts with PCF as defined in TS 23.502 [3] clause 4.15.6.6.

4. PCF sends PCC rules to the SMF.

NOTE 2: Steps 1-4 are following existing Rel-17 specifications.

5. SMF performs PDU Session modification as defined in TS 23.502 [3] clause 4.3.2 and may include, based on subscription, in the N1 SM container per QoS-flow Non-3GPP QoS assistance information. The Non-3GPP QoS assistance information contains (if available at the SMF): QoS characteristics, GFBR/MFBR (if applicable), ARP, Periodicity.

Editor’s note: Which information triggers the delivery of Non-3GPP QoS assistant information is FFS.

6. Based on the non-3GPP QoS assistance information and QoS rule information, the PEGC may reserve resources in the non-3GPP network.

### 6.11.3 Impacts on Existing Nodes and Functionality

**SMF:**

- To provide per-QoS flow Non-3GPP QoS assistance information

**PEGC:**

- To receive additional Non-3GPP QoS assistance information in NAS- Optionally enforce QoS in the non-3GPP network. The details of how to enforce QoS in the non-3GPP network are not subject of this solution and are considered to be beyond the scope of 3GPP.

## 6.12 Solution #12: Communication of PIN

### 6.12.1 Description

This solution mainly addresses KI#4 “Communication of PIN”. This solution also addresses some part of the KI#6 “Policy and parameters provisioning for PIN”, i.e., UE to UE relay parameter provisioning and QoS parameter provisioning.

The steps in the following call flows depicted as grey line in the figures are out of SA2 scope.

This solution is related to the solution 8 "management of PIN and PIN Elements" addresses to KI#3, where the solution 8 described the architecture view of the solution.

### 6.12.2 Procedures

#### 6.12.2.1 Management of relay path



**Figure 6.12.2.1-1: Management of relay path**

1. The PEGC has established PDU Session that may involve framed routing as described in TS 23.501 [2] clause 5.6.14.

2. The PINE establishes direct connection with the PEGC using the parameters obtained in management procedure addresses KI#3. The direct connection could be WiFi, BT, PC5, etc.

3. The PINE sends relay request over application layer to the PEGC. The parameters for visiting the PEGC over application layer can be obtained over application layer in solution 8 addresses to KI#3.

4. The PEGC sends relay request over application layer to the PINMF. The parameters for visiting the PINMF over application layer can be obtained over application layer in solution 8 addresses to KI#3. The PEGC requests the PINMF with the Assistance Info relate to the PINE, e.g., MAC address, IP address that used between the PINE and the PEGC.

5. The PINMF authorizes the request and sends Create/Update/Delete Association Request (GPSI, [UE address, DNN/S-NSSAI], PIN ID, U2N Routing Info, [Framed Route Info], Assistance Info) to the NEF if authorization succeeds. The U2N Routing Info includes packet filters that the PEGC is able to relay and may include service requirements for the PINE associated with the packet filters. If it is the first time for creating the association for the PEGC, the Framed Route Info may be included and used by the SMF to configure framed routing as described in TS 23.501 [2] clause 5.6.14 for the PDU Session of the PEGC.

6. The NEF may interact with PCF for setting DNAI and may change the Framed Route Info to the PDU Session of the PEGC.

7. The procedure described in TS 23.502 [3] clause 4.3.5 may be performed to change the serving SMF that supports PIN according to the DNAI. The SMF uses the Framed Route Info to configure framed routing as described in TS 23.501 [2] clause 5.6.14 with the UPF for the PDU Session of the PEGC.

8. If the PEGC has subscribed to be in a group that includes the member of the PEGC and the PEMC, the SMF initiates SMF-NEF connection setup with NEF similar as described in TS 23.502 [3] clause 4.25.2 and 5.2.6.15, the difference is that the subscription data includes "NEF ID for PIN" instead of "NEF ID for NIDD", and the name of "NIDD information" is changed to "PIN information" that contains same thing, i.e., GPSI and AF ID.

9. The NEF sends Create/Update/Delete Association Request (SUPI, PIN ID, U2N Routing Info, Assistance Info) to the SMF.

10. The SMF may trigger authentication and authorization procedure between PINE and UDM, or between PINE and external DN-AAA, via the PEGC, i.e., the SMF sends EAP Identity Request to the PINE. EAP framework is used for the authentication and authorization.

Editor's note: The authentication and authorization procedure need coordination with SA3.

11. The SMF interacts with PCF for the flow descriptions in the U2N Routing Info related to the PINE. The PCF uses the policy of the PEGC to authorize the QoS requirements for the PINE.

12. The SMF performs PDU Session Modification with the PEGC, may add, update, or remove QoS flows serve the PINE, and delivers the PIN ID and U2N Routing Info to the PEGC via N1 message during the PDU Session Modification.

The QoS rules provided to the PEGC includes packet filters corresponds to PINEs, e.g., IP range, or port range, or both, the PEGC performs U2N relay and maps traffic with the QoS flow based on the QoS rules. The PCF may consider the type of direct connection (e.g., WiFi, BT, PC5) to deduce the QoS rules, e.g., uses a fixed value for the delay of direct connection.

During the PDU Session Modification procedure, the SMF allocates the IP address and PINE ID for the PINE and sends the IP address, PINE ID, and the Assistance Info to the PEGC via N1 message. The PEGC associates the PINE ID and IP address with the PINE that related to the Assistance Info, the PEGC transfers the inner address of the PINE to the IP address received. The PEGC responds to the SMF. The SMF can identify the PINE via the PINE ID and the UPF can identify the PINE via the IP address.

The SMF may frequently change the PINE ID for the sake of privacy, so that the PEGC can perform the PDU Session Modification on behalf of the PINE with the PINE ID, which is frequently changed.

13-14. The SMF responds to the NEF. The NEF responds to the PINMF.

15-16. The PINMF sends relay response to the PEGC over application layer, and PEGC sends the relay response to the PINE over application layer.

#### 6.12.2.2 Management of communication via 5GC



**Figure 6.12.2.2-1: Management of communication via 5GC**

1. The PEGC established a PDU Session with SMF supporting PIN.

2. The PEMC configures a whitelist or blacklist for communications via 5GC, e.g., for visiting internet, for communicating with a PINE from internet or from other PINEs, etc.

3. The PINMF authorizes the request and sends Create/Update/Delete Association Request (GPSI, [UE address, DNN/S-NSSAI], PIN ID, PIN Routing Info) to the NEF if authorization succeeds. The PIN Routing Info includes the information whether some PINEs are allowed/disallowed to access internet or a specific internet service or other PINEs. The NEF authorize the request.

4. Steps 6-8 in clause 6.Y.2.1 may be performed to setup the SMF-NEF connection.

5. The NEF sends Create/Update/Delete Association Request (SUPI, PIN ID, Routing Info) to the SMF.

6. The SMF interacts with UPF serving the PDU Session of the PEGC for installing, updating, removing a corresponding FWA from the UPF.

7-8. The SMF responds to the NEF. The NEF responds to the PINMF.

#### 6.12.2.3 Management of communication via PEGC



**Figure 6.12.2.3-1: Management of communication via PEGC**

1. The PEGC established a PDU Session with SMF supporting PIN, and SMF-NEF connection for managing PIN has been setup.

2. The PEMC configures a whitelist or blacklist for PINEs to communicate via the PEGC.

3. The PINMF authorizes the request and sends Create/Update/Delete Association Request (GPSI, [UE address, DNN/S-NSSAI], PIN ID, U2U Routing Info) to the NEF if authorization succeeds. The U2U Routing Info includes the information whether some PINEs are allowed/disallowed to communicate with other PINEs via the PEGC.

4. The NEF sends Create/Update/Delete Association Request (SUPI, PIN ID, U2U Relay Info) to the SMF.

5-6. The SMF sends N1 message (PIN ID, U2U Routing Info) via the AMF to the PEGC.

7-8. The UE responds with a result.

9-10. The SMF responds to the NEF, the NEF responds to the PINMF.

#### 6.12.2.4 Mobile termination procedure for PINE



**Figure 6.12.2.4-1: Mobile termination procedure for PINE**

1. The PEGC established a PDU Session with SMF supporting PIN.

2. The PINMF sends Create/Update/Delete Association Request (GPSI, [UE address, DNN/S-NSSAI], PIN ID, PINE Status Info) to the NEF. The PINE Status Info includes the type of the PINE, which indicates whether the PINE is notifiable, e.g., when the PINE can be reached by other way (e.g., the PINE has dual registration with different address with the PINMF), or the PINE is a listener and PEGC is announcer over the, e.g., WiFi, BT, etc.

Steps 6-8 in clause 6.Y.2.1 may be performed to setup the SMF-NEF connection.

3. The NEF sends Create/Update/Delete Association Request (SUPI, PIN ID, PINE Status Info) to the SMF.

4-5. The SMF responds to the NEF. The NEF responds to the PINMF.

6. The PIN APP on the PEGC may detect that the communication with the PINE is not available, the PEGC sends information to PINMF over application layer. The PINMF authorizes the request and sends Update Association Request (GPSI, [UE address, DNN/S-NSSAI], PIN ID, PINE Status Info) to the NEF if authorization succeeds. The PINE Status Info includes the information of the PINEs that are unreachable. The NEF sends Update Association Request (SUPI, PIN ID, PINE Status Info) to the SMF. The SMF responds to the NEF. The NEF responds to the PINMF.

The PEGC may detect that the direct connection with the PINE is lost, the PEGC initiates PDU Session Modification indicating the PINE is unreachable.

The PEGC may transit into CM-IDLE state or the PDU Session for relay may be inactive, the PEGC initiates PDU Session Modification.

7. According to the information received in step 6 and the PINE Status Info, the SMF interacts with the UPF serving the PDU Session of the PEGC for instructing that DL data notification for the PINE is needed.

8. When DL data to the PINE is arrived and DL data notification is instructed, the UPF sends DL data notification related to the PINE to the SMF.

9. According to the type of the PINE in the Routing Info, the SMF sends Message Delivery to the NEF to indicate the data arrival for a PINE.

10. The NEF sends Message Delivery to the PINMF.

11. The PINMF instructs the PINE via another address or instructs the PEGC over application layer.

12. The PINE or PEGC establish the direct connection according to the instruction.

13. The PEGC requests the PINMF to establish the relay path for the PINE over application layer.

### 6.12.3 Impacts on Existing Nodes and Functionality

**PINMF:**

- Support PIN ID assignment.

- Support PIN Association operations to provision U2U Routing Info and U2N Routing Info to PEGC.

- Support PIN Association operations to provision PIN Routing Info and PINE Status Info to UPF for the PDU Session of PEGC for relay.

**NEF:**

- Support PIN Association operations with PINMF and SMF.

- Support indicating DNAI related to PIN to PCF.

**SMF:**

- Support SMF-NEF connection setup based on PIN subscription.

- Support PIN Association operations with NEF.

- Support instructing UPF for rules related to PIN Elements.

- Support provisioning relay information to PEGC over NAS.

- Support delivering message related to DL data notification to NEF.

- Support triggering authentication and authorization procedure between PINE and UDM/external DN-AAA.

- Support PINE ID and IP address provisioning for PINE to PEGC over NAS.

**PCF:**

- Support authorizing the QoS requirements for PINE associated with the PEGC.

**UE (support PEGC):**

- Support relay information provisioning for PIN over NAS.

- Support proxy authentication and authorization procedure between PINE and UDM/external DN-AAA.

- Support PINE ID and IP address provisioning for PINE over NAS, and perform NAT for the PINE with the IP address.

Editor's note: Additional impacts are FFS.

## 6.13 Solution #13: Communication of PIN

### 6.13.1 Description

The solution describes the following PIN communication aspects:

1) Communication between PIN Elements within a PIN via PEGC, via 5GS and direct.

2) PIN Element relay path setup with 5GS via PEGC

3) 5GS QoS differentiation for PINE via PEGC

#### 6.13.1.1 Communication between PINE and 5GS via PEGC

The architecture for providing relay path between PINE and 5GS via PEGC

PEGC

AN

UPF

UPF

UPF

PINE1

PINE2

PINE3

.

.

.

.

PDU Session 1

PDU Session 1

PDU Session n

AMF

N3

SMF

N1

N4

N11

**Figure 6.13.1.1-1: Relay Path Architecture between PINE and 5GS via PEGC**

Assumption: that the PIN elements are connected to a wireless LAN/ PAN network and each element are reachable via the wireless link. The procedure to connect to the wireless network and assign IP address is out of the scope of this document.

The salient feature of this solution is as follows:

**- Setup.** PINE in the PIN will request PEGC for 5G session establishment using request-response queries. The PEGC will establish a PDU session with the 5G network based on the existing procedure defined in TS 23.501 clause-X.

- PINE will configure PEGC as its default gateway, so that all the traffic is sent to the 5G network via PEGC relay.

- PEGC acts as a Network Address Translator (NAT) between 5G network and the PIN by representing a unique IP address to all the PINE and PEMC in the PIN network.

- PEGC establishes a unique PDU session with 5G network for every PINE requesting for 5GS relay access through PEGC.

- PEGC maps local FQDN or IP address of the PINE to the PDU session ID and uses this mapping to forward the data from/to PINE and 5G PDU unique session.

**- QoS differentiation.** We propose following two ways to achieve differentiated services

- PINE requesting for a desired QoS will request the PEGC to setup a PDU session using control signals (Http messages) with the intended QoS, and PEGC will setup appropriate PDU session. All the traffic from the PIN will be forwarded to the PDU session with the desired QoS.

- PINE will use DSCP markings on the IP packet in the PIN to indicate the desired QoS and PEGC will setup an appropriate 5QI PDU session with the DNN, and further PEGC will reset the QoS marking on the IP packet and forward it to the established PDU session.

- PEGC will also provide the necessary QoS as indicated by the PINE on the IP packets in the PIN network.

**- Release.** PINE in the PIN will request PEGC for 5G session release using request-response quires. The PEGC will release the respective PDU associated with the PINE – PEGC uses PDU ID and PINE FQDN or IP address of the PINE in the local PIN.

#### 6.13.1.2 Communication between PIN elements within PIN

The architecture for providing communications between PINE in the PIN.

PINE

PINE

Request

Response

Subscribe

Notify

**Figure 6.13.1.2-1: Relay Path Architecture between PINE and 5GS via PEGC**

Assumption: that the PIN elements are connected to a wireless LAN/ PAN network and each element are reachable via the wireless link. The procedure to connect to the wireless network and assign IP address is out of the scope of this document.

The salient feature of this solution is as follows:

**- Direct Communication.** PINE, PEGC and PEMC will use Request-response and Subscribe-Notify methods to communicate with each other. Since PINE are reachable via direct or in LAN connection, PINE will communicate with each other directly using intended PINE’s FQDN or IP address.

**- Via PEGC.** PINE should set PEGC as its default gateway so that all the communication is via PEGC. Packets from PINE intended to other PIN elements in the PIN related to local services or local communication are routed by the PEGC locally, since PEGC has PINE repositories which includes FQDN or IP address of the PINE in the PIN.

**- Via 5GS.**

Editor’s note: Via 5GS is FFS

### 6.13.2 Procedures

Editor's note: Detailed Procedure is FFS.

### 6.13.3 Impacts on services, entities and interfaces

The solution largely re-uses existing functionality

The solution has the following impacts:

Impact to the UE (PEMC):

- Ability to support http broadcast messages, http request-response and http based subscribe-notify features

- Ability to maintain a list of all the PINE and its supported services

- Ability to respond to PINE and its service discovery queries from the PINE

Impact to the PINE:

- Ability to support http broadcast messages, http request-response and http based subscribe-notify features

- Ability to request QoS using http request to the PEGC

Impact to the UE (PEGC):

- Ability to support http broadcast messages, http request-response and http based subscribe-notify features

- Ability to register its gateway functionality to PEMC

- Ability to accept http QoS request from the PINE and setup multiple PDU session with the 5G System

- Ability to map PDU session ID to the IP address of the PINE and forward packets to/from the corresponding PDU session

## 6.X Solution #X: <Solution Title>

### 6.X.1 Description

Editor's note: This clause will describe the solution principles and architecture assumptions for corresponding key issue(s). (Sub) clause(s) may be added to capture details.

### 6.X.2 Procedures

Editor's note: This clause describes high-level procedures and information flows for the solution.

### 6.X.3 Impacts on Existing Nodes and Functionality

Editor's note: This clause captures impacts on existing 3GPP nodes and functional elements.

# 7 Evaluation

Editor's note: This clause will provide evaluation of different solutions.

# 8 Conclusions

Editor's note: This clause will list conclusions that have been agreed during the course of the study item activities.

Annex A:  
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Change history | | | | | | | |
| Date | Meeting | TDoc | CR | Rev | Cat | Subject/Comment | New version |
| 2022-02 | SA2#149e | S2-2201792 |  |  |  | TR23.700-88 skeleton | 0.0.0 |
| 2022-02 | SA2#149e | S2-2201793 |  |  |  | Scope of PIN study | 0.1.0 |
| 2022-02 | SA2#149e | S2-2201794 |  |  |  | Definitions of terms and abbreviations | 0.1.0 |
| 2022-02 | SA2#149e | S2-2201795 |  |  |  | Architectural assumptions and principles | 0.1.0 |
| 2022-02 | SA2#149e | S2-2201796 |  |  |  | Key Issue: 5GC architecture enhancements to support PIN | 0.1.0 |
| 2022-02 | SA2#149e | S2-2201797 |  |  |  | Key Issue: 5GC supports authorization in PIN | 0.1.0 |
| 2022-02 | SA2#149e | S2-2201798 |  |  |  | Key Issue of support for management of the PIN and its elements | 0.1.0 |
| 2022-02 | SA2#149e | S2-2201799 |  |  |  | New KI: PIN discovery and selection | 0.1.0 |
| 2022-02 | SA2#149e | S2-2201800 |  |  |  | New KI: PIN connectivity | 0.1.0 |
| 2022-02 | SA2#149e | S2-2201801 |  |  |  | Key Issue: Authorization and policy/parameters provisioning for PIN | 0.1.0 |
| 2022-04 | SA2#150e | S2-2203515 |  |  |  | New KI and Solution: Identification assignment for PIN Elements | 0.2.0 |
| 2022-04 | SA2#150e | S2-2203516 |  |  |  | KI#2: New Solution: PIN and PIN element discovery and selection | 0.2.0 |
| 2022-04 | SA2#150e | S2-2203517 |  |  |  | KI#2: New solution for PIN and PIN element discovery and selection | 0.2.0 |
| 2022-04 | SA2#150e | S2-2203518 |  |  |  | (KI#2) Solution for PIN and PIN Elements discovery and selection | 0.2.0 |
| 2022-04 | SA2#150e | S2-2203519 |  |  |  | Solution for KI#2: PIN and PIN Element discovery. | 0.2.0 |
| 2022-04 | SA2#150e | S2-2203520 |  |  |  | Solution of authorization and management of PIN and PIN Elements. | 0.2.0 |
| 2022-04 | SA2#150e | S2-2203521 |  |  |  | Solution for KI #3 Management of PIN and PIN Elements | 0.2.0 |
| 2022-04 | SA2#150e | S2-2203522 |  |  |  | Solution for KI#3; PIN Management by 5GS | 0.2.0 |
| 2022-04 | SA2#150e | S2-2203523 |  |  |  | New Solution: Management PIN and PIN Elements | 0.2.0 |
| 2022-04 | SA2#150e | S2-2203524 |  |  |  | Solution for KI#3: one authorized UE creates a PIN. | 0.2.0 |
| 2022-04 | SA2#150e | S2-2203525 |  |  |  | KI#3: New solution for Management of PIN and PIN Elements | 0.2.0 |
| 2022-04 | SA2#150e | S2-2203526 |  |  |  | Solutions for QoS control between PINE and 5GS when a PEGC is used for the relay | 0.2.0 |
| 2022-04 | SA2#150e | S2-2203527 |  |  |  | New Solution: Communication of PIN | 0.2.0 |
| 2022-04 | SA2#150e | S2-2203528 |  |  |  | KI#4: New solution for communication of PIN | 0.2.0 |