|  |  |
| --- | --- |
| 3GPP TR 23.700-78 V18.1.0 (2023-03) | |
| Technical Report | |
| 3rd Generation Partnership Project;  Technical Specification Group Services and System Aspects;  Study on Application layer support for Personal IoT Network;  (Release 18) | |
|  | |
|  | 3GPP-logo_web |
|  | |
| The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP. The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented. This Specification is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification. Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices. | |

|  |
| --- |
|  |
| ***3GPP***  Postal address  3GPP support office address  650 Route des Lucioles - Sophia Antipolis  Valbonne - FRANCE  Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16  Internet  http://www.3gpp.org |
| ***Copyright Notification***  No part may be reproduced except as authorized by written permission. The copyright and the foregoing restriction extend to reproduction in all media.  © 2023, 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 7

Introduction 8

1 Scope 9

2 References 9

3 Definitions of terms, symbols and abbreviations 9

3.1 Terms 9

3.2 Symbols 10

3.3 Abbreviations 10

4 Key issues 10

4.1 Key issue #1: PIN Management 10

4.2 Key issue #2: PINAPP accesses 5G network by application mechanism 11

4.3 Key issue #3: Service switch in PIN 11

4.4 Key issue #4: PIN Application Server Discovery 11

4.5 Key issue #5: Service continuity 12

4.6 Key issue #6: PEMC/PEGC replacement in PIN 12

5 Architecture requirements 13

5.1 General 13

5.2 Requirements 13

5.2.1 General requirements 13

5.2.1.1 General 13

5.2.1.2 Requirements 13

5.2.2 PIN Management 13

5.2.2.1 General 13

5.2.2.2 Requirements 13

5.2.3 PIN enable 5GS communication 14

5.2.3.1 General 14

5.2.3.2 Requirements 14

5.2.4 Service Switch 14

5.2.4.1 General 14

5.2.4.2 Requirements 14

5.2.5 Application server discovery 14

5.2.5.1 General 14

5.2.5.2 Requirements 14

5.2.6 Service continuity 14

5.2.6.1 General 14

5.2.6.2 Requirements 15

6 Architecture 15

6.1 General 15

7 Solutions 16

7.1 Mapping of solutions to key issues 16

7.2 Solution #1: PINAPP architecture 16

7.2.1 Architecture assumption 16

7.2.1.1 User accessing services provided by PIN Element from outside the PIN 17

7.2.2 Functional elements 18

7.2.2.1 PIN element with Management Capabilities (PEMC) 18

7.2.2.2 PIN Server 18

7.2.2.3 PIN element with Gateway Capabilities (PEGC) 19

7.2.2.4 PIN client 19

7.2.2.5 Application client 19

7.2.3 Reference Points 19

7.2.4 Functional Entity Cardinality 20

7.2.4.1 PEMC 20

7.2.4.2 PEGC 20

7.2.4.3 PIN server 20

7.2.4.4 PIN client 21

7.2.4.5 Application client 21

7.2.5 Identities 21

7.2.5.1 PIN ID 21

7.2.5.2 UE identifier 21

7.2.5.3 PIN client ID 21

7.2.5.4 Application Client ID 21

7.2.5.5 PIN server ID 21

7.3 Solution #2: PIN management 21

7.3.1 Architecture enhancements 21

7.3.2 Solution description 21

7.3.2.1 General 21

7.3.2.2 Procedures of Creation of PIN 22

7.3.2.3 Procedures of Modification of PIN 24

7.3.2.3.1 PIN modification triggered by PEMC 24

7.3.2.3.2 PIN modification triggered by event of PEGC 26

7.3.2.3.3 PEMC replacement triggered by PIN server 26

7.3.2.3.4 PEMC replacement triggered internally within the PIN 27

7.3.2.3.5 PEGC replacement triggered by PEMC 28

7.3.2.3.6 PIN modification triggered by PEGC 29

7.3.2.3.7 PIN modification triggered after local PEMC failure 31

7.3.2.3.8 PIN management with multiple PEGCs 31

7.3.2.3.9 PIN management with multiple PEMCs 32

7.3.2.4 Procedures of PIN Profile retrieval 33

7.3.3 Solution evaluation 34

7.4 Solution #3: Insertion and remove of PIN elements in a PIN 34

7.4.1 Architecture enhancements 34

7.4.2 Solution description 34

7.4.2.1 General 34

7.4.2.2 Procedures 35

7.4.2.2.1 PIN client requests to join into a PIN 35

7.4.2.2.2 The PEMC removes the PIN elements from a PIN 36

7.4.2.2.3 The PIN elements decides to leave the PIN 37

7.5 Solution #4: PIN delete 38

7.5.1 Architecture enhancements 38

7.5.2 Solution description 38

7.5.2.1 General 38

7.5.2.2 Procedures of Delete of PIN 38

7.5.2.2.1 PIN delete triggered by PEMC 38

7.5.2.2.2 PIN delete triggered by PIN server 39

7.5.2.2.3 PIN delete locally by PEMC 40

7.6 Solution #5: PIN discovery 41

7.6.1 Architecture enhancements 41

7.6.2 Solution description 41

7.6.2.1 General 41

7.6.2.2 Procedures of PIN discovery 42

7.6.2.2.1 Procedures of PIN discovery based on PEMC 42

7.6.2.2.2 Procedures of PIN discovery with assistance of PIN server via PEGC 43

7.7 Solution #6: PIN Profile 44

7.7.1 Architecture enhancements 44

7.7.2 Solution description 44

7.7.2.1 General 44

7.7.2.2 PIN Profile in a PIN 45

7.7.2.3 Dynamic profile information of a PIN 45

7.7.2.4 PIN client profile 47

7.7.3 Solution evaluation 47

7.8 Solution #7: PIN server discovery 48

7.8.1 Architecture enhancements 48

7.8.2 Solution description 48

7.8.2.1 General 48

7.8.2.2 Procedures of PIN server discovery 48

7.8.2.2.1 Procedures of PIN server discovery based on receiving PIN server endpoint information 48

7.8.2.2.2 Procedures of PIN server discovery via PEGC 48

7.8.2.2.3 Procedures of PIN server discovery from PEMC 49

7.9 Solution #8: Service switch in a PIN 50

7.9.1 Architecture enhancements 50

7.9.2 Solution description 50

7.9.2.1 General 50

7.9.2.2 Procedure 50

7.9.2.2.1 Functional entities 50

7.9.2.2.2 Procedures of PIN Service Switch 50

7.9.3 Solution evaluation 52

7.10 Solution #9: PINAPP role change 53

7.10.1 Architecture enhancements 53

7.10.2 Solution description 53

7.10.2.1 General 53

7.10.2.2 Procedure 53

7.10.3 Solution evaluation 54

7.11 Solution #10: Service switch internal PIN 54

7.11.1 Architecture assumptions 54

7.11.2 Solution description 54

7.11.2.1 General 54

7.11.2.2 Procedure of service switch internal PIN 55

7.11.3 Solution evaluation 56

7.12 Solution #11: Application Server Discovery in a PIN 56

7.12.1 Architecture enhancements 56

7.12.2 Solution description 56

7.12.2.1 General 56

7.12.2.2 Procedure 56

7.12.2.2.1 Functional entities 57

7.12.2.2.2 Procedures of PIN Application Server Discovery 57

7.12.3 Solution evaluation 58

7.13 Solution #12: PEMC registration to PIN server 58

7.13.1 Architecture enhancements 58

7.13.2 Solution description 58

7.13.2.1 General 58

7.13.2.2 Procedures of PEMC registration 59

7.13.2.3 Procedures of PINE/PEGC registration 59

7.14 Solution #13: SEAL enabled PINAPP architecture and PIN management 60

7.14.1 Architecture assumption 60

7.14.2 PIN creation 61

7.14.3 PIN update 61

7.14.4 PIN deletion 61

7.14.5 PIN discovery and PIN element discovery 61

7.15 Solution #14: PIN communication via 5GS 61

7.15.1 Architecture enhancements 61

7.15.2 Solution description 61

7.15.2.1 General 61

7.15.2.2 Procedures of PIN communication via 5GS 62

7.15.2.3 Procedures of credential provisioning to PINE via 5GS 63

7.16 Solution #15: Service continuity 65

7.16.1 Architecture enhancements 65

7.16.2 Solution description 65

7.16.2.1 General 65

7.16.2.2 Procedures to support service continuity 66

7.16.2.2.1 PEGC relocation 66

7.16.2.2.2 Change application layer communication to communication via 5GS, with the support of PIN server 67

8 Deployment scenarios 76

8.1 General 76

8.x Deployment scenario #x: <Title> 76

9 Overall evaluation 76

9.1 Architecture enhancements 76

9.2 Key issue evaluations 76

9.2.1 General 76

9.2.2 Evaluation of key issue #1: PIN Management 78

9.2.3 Evaluation of key issue #2: PINAPP accesses 5G network by application mechanism 81

9.2.4 Evaluation of key issue #3: Service switch in PIN 81

9.2.5 Evaluation of key issue #4: PIN Application Server Discovery 83

9.2.6 Evaluation of key issue #5: Service continuity 83

9.2.7 Evaluation of key issue #6: PEMC/PEGC replacement in PIN 84

9.2.8 Evaluation of PINAPP architecture 85

10 Conclusions 85

10.1 Conclusion of PIN management of KI#1 85

10.2 Conclusion of KI#2 87

10.3 Conclusion of Service Switch of KI#3 88

Annex A (informative): Change history 90

# 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.

# Introduction

Personal IoT Networks (PIN) is based on the greatly increasing number of consumers IoT devices. These devices can either be wearable devices or can be IoT devices in the home. Users create Personal IoT Networks out of all these Personal IoT devices mainly in their homes or around their body. This technical report identifies the key issues and corresponding application architecture and related solutions with recommendations for the normative work based on 3GPP TS 22.261 [2] and 3GPP TR 22.859 [3]. 3GPP TS 22.261 [2] also refer to requirements in 3GPP TS 22.101 [5] clause 26a that apply to Personal IoT Networks.

# 1 Scope

The present document is a technical report capturing the study on application layer support for Personal IoT networks (PIN). The aspects of the study include analyzing application layer architecture requirements of PIN, identifying key issues and supporting PIN application layer functional model. The study also includes information and support from 3GPP network to PIN, service or applications discovery within a PIN or by the UE outside of a PIN via 3GPP network.

The study takes into consideration the work done for PIN in 3GPP TS 23.700-88 [4] and other related work in 3GPP.

# 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 22.261: "Service requirements for the 5G system".

[3] 3GPP TR 22.859: "Study on Personal Internet of Things (PIoT) networks".

[4] 3GPP TR 23.700-88: "Study on architecture enhancements for Personal IoT Network (PIN)".

[5] 3GPP TS 22.101: "Service Principles".

# 3 Definitions of terms, symbols and abbreviations

## 3.1 Terms

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

**Access Control Information:** A set of information that assists the authorized PINE in a PIN to access 5GS network via PEGC, for example, the username or password.

**PIN enabler:** Refers to the overall functionality provided by the entities such as PIN Client, PIN Gateway Client, PIN Management Client, and PIN server in support of applications as per the architecture defined in solution 7.2.

**PIN management:** Refers to the set of operations related to creation, modification, maintenance and removal of PIN.

**PIN Profile:** A set of data and information about the PIN and PIN elements resides in the PIN. **Service Switch:** A mechanism to switch the service traffic flow between Application server and PINE to application server and other PINE.

NOTE: 3GPP TS 22.101 [5] clause 26a lists information that can be included in a PINE profile.

For the purposes of the present document, the following terms given in 3GPP TS 22.261 [2] apply:

**Personal IoT Network**

**PIN direct connection**

**PIN Element**

**PIN Element with Gateway Capability**

**PIN Element with Management Capability**

## 3.2 Symbols

For the purposes of the present document, the following symbols apply:

<symbol> <Explanation>

## 3.3 Abbreviations

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

PIN Personal IoT Network

PINAPP Personal IoT Network Application

PEMC PIN Element with Management Capability

PEGC PIN Element Gateway Capability

PINE PIN Element

# 4 Key issues

## 4.1 Key issue #1: PIN Management

As indicated in clause 6.38 of TS 22.261[2], the following requirements will be studied in this TR phase and reflect in this key issues:

- The 5G system shall support mechanisms to identify a PIN, a PIN Element.

- The 5G system shall be able to support PINs with PIN Elements subscribed to more than one network operator (e.g., a PIN Element that is a MUSIM UE and subscribes to different operators respectively, one PIN Element subscribed to network operator A and another PIN Element subscribed to network operator B).

In order to avail PIN management, for example, PIN creating/modifying/deleting UE or PINAPP should be able to trigger PIN management request to MNO. What is critical is whether and how the UE or PINAPP triggers PIN managment request.

After creating a PIN, in order to avail PIN service to other PIN elements (e.g.: IoT device), the PIN elements should be able to newly added into a PIN. So for the management of PIN, add or remove the PIN elements into a PIN is nessasary. Also, one of the most important features of PIN is PEGC that enables PIN elements to communicate with 5G network and some of the PIN elements interact directly to other PIN elements within PIN. How to manage the specific permissions, for example, communicate with UE outside of PIN or connect to 5G network are important.

It is required to study the following:

- Who can manage (create/modify/delete) a PIN?

- Whether and how to trigger a PIN network management request, for example, PIN creation/modification/deletion. What parameters are required in PIN network management request?

- How to add/remove PIN elements into a PIN after PIN establishment? What parameters or information are needed during adding/removing PIN elements into a PIN? How to configure newly added PIN element?

- Determine the certain PIN services in PIN.

- What information about the PIN and PIN elements needs to be maintained at the PIN server, PEMC and PEGC for the management of PIN and its elements and whether and how they are notified about the changes to this information.

- What set of events occurring in the PIN (e.g., PIN element added, PIN element removed etc.,) need to trigger the updates to the information maintained at the PIN server, PEMC and PEGC.

- What information can be created or modified or deleted by the authorized user.

NOTE: PIN management services defined by SA2 will be reused and under consideration in PINAPP.

## 4.2 Key issue #2: PINAPP accesses 5G network by application mechanism

As indicated in clause 6.38 of TS 22.261[2], the following requirements will be studied in this TR phase and reflect in this key issues:

- The 5G system shall enable the network operator to provide any 5G services to any UE via a PEGC.

- The 5G system shall support applications on an Application Server connected to a PIN.

As a feature, PINAPP within a PIN can communicate with other devices, services and applications within the same PIN. Furthermore, PINAPP can connect with the 5G Network via a PEGC. Also, as a feature, some of the PINAPP in PIN has the permissions that they can communicate with other UE or application outside of PIN with the help of 5GC.

From the aspects of PINAPP accesses 5G network by application mechanism, it is required to study the following:

- How to realize that PINAPP access 5G network by application mechanism?

NOTE: How to derive the route control information for PINAPP to access 5GS is in the scope of SA2, and not discussed in SA6.

## 4.3 Key issue #3: Service switch in PIN

As indicated in clause 6.38 of TS 22.261[2], the following requirements will be studied in this TR phase and reflect in this key issues:

- The 5G system shall support mechanisms to aggregate, switch or split the service between non-3GPP RAT and PIN direct connections using licensed spectrum.

- The 5G system shall support applications on an Application Server connected to a CPN or PIN.

When UE is located outside of PIN, the UE has the direct connection to application server via 5GS. When UE moves into the coverage of PIN, some of the PIN application in PIN has the capability, for example, to terminate the application traffic from application server. These PIN applications have better experience than the UE, in screen or sound.

It is required to study the following:

- How to support application mechanism for service switching in a PIN between different PIN applications for achieving better service experience?

NOTE: The coordination with SA2 about the support for switching application traffic between RATs is needed.

## 4.4 Key issue #4: PIN Application Server Discovery

As indicated in 3GPP TS 22.261 [2], clause 6.38.2.1, the following requirement will be studied in this TR:

- The 5G system shall support applications on an Application Server connected to a PIN.

Supporting Application Servers connected to a PIN can involve service or applications discovery by PIN Elements or by a UE outside of a PIN via 3GPP network.

Application clients can be running on PIN elements in a PIN and may want to discover and connect to an Application Server connected to the PIN. At the same time UEs running Application Clients outside of a PIN may try to discover and connect to an Application Server connected to the PIN.

It is required to study the following:

- How to enable discovery of Application Server, connected to a PIN, by Application Clients running in the same PIN?

- How to enable discovery of Application Server, connected to a PIN, by Application Clients running in a different PIN?

- How to enable discovery of Application Server, connected to a PIN, by Application Clients running in a UE outside of the PIN over 3gpp network?

- How to manage Application Server discovery by MNOs or third-party application service providers?

- Evaluate the applicability of Edge Enabler Layer and CAPIF for PIN application service discovery.

## 4.5 Key issue #5: Service continuity

As indicated in clause 6.38 of TS 22.261[2], the following requirements that describes the service continuity will be studied in this TR phase and reflect in this key issues:

- The 5G system shall be able to minimize service disruption when a PIN Element changes the communication path from one PIN Element (e.g. PIN Element with Gateway Capability) to another PIN Element or operator provided mobile access. The communication path between PIN Elements may include licensed and unlicensed spectrum as well as 3GPP and non-3GPP access.

The PIN application is the application deployed on PIN elements (for example, the UE) in PIN. One of the PIN application features is, the PIN application in UE can have a direct communication with other PIN application into a PIN, without have any routing from 5GS.

But, there are the situations that may have a service disruption or relocation:

- When UE moves out of a PIN or the terminal PIN application is in the status of moving, the original direct communication between two PIN applications may be influenced and changed (for example, the direct communication between two PIN applications may be routed via PEGC);

- Usually if a PIN application on a UE is consuming service from an application server and due to UE mobility, the PIN application on the UE should continue to receive services from the application server.

It is required to study the following:

- How to the support the service continuity when the UE hosting PIN application is in the status of moving?

- How to the support the service continuity when UE moves out of a PIN and keep the communication towards the PIN application?

NOTE: Some of the service continuity work has relationship to SA2 work and depends on the SA2's feedback later.

## 4.6 Key issue #6: PEMC/PEGC replacement in PIN

For the management of PIN and to enable PIN elements communicate with 5GC, each active PIN will have atleast one PEMC and PEGC PIN elements sucessfully configured and registered. The PEMC or PEGC PIN elements may cease to perform their role because of any of the following reasons :

1. Power drain of PIN elements acting as PEMC or PEGC

2. Their validity duration allowed to perform the role of PEMC or PEGC is expiring

3. PEMC or PEGC PIN elements moving out of coverage of cellular network

Hence there is a need for other existing PIN elements to take the role of PEMC or PEGC inorder to succesfully manage the PIN and to avoid service disruption.

It is required to study the following:

- Whether and how the need for PEMC or PEGC role change is determined?

- How another active PIN element take over the role or is assigned the role of PEMC or PEGC?

- Whether and how the existing active PIN elements is notified about the role change?

- Whether and how the required dynamic or context information of PIN is made available to the new element taking the role of PEMC or PEGC

# 5 Architecture requirements

## 5.1 General

## 5.2 Requirements

### 5.2.1 General requirements

#### 5.2.1.1 General

This clause specifies general requirements for the architecture.

#### 5.2.1.2 Requirements

[AR-5.2.1.2-a] The application layer architecture shall support deployment of personal IoT network.

[AR-5.2.1.2-b] The application layer architecture shall support different deployment models in conjunction with an operator's 3GPP network.

[AR-5.2.1.2-c] The application layer architecture shall be compatible with the 3GPP network system.

### 5.2.2 PIN Management

#### 5.2.2.1 General

This clause specifies PIN management requirements for the architecture.

#### 5.2.2.2 Requirements

[AR-5.2.2.2-a] The application layer architecture shall provide mechanisms to create PIN for UE or PIN elements.

[AR-5.2.2.2-b] The application layer architecture shall provide mechanisms to delete PIN, either triggered by PINEs or by PIN server.

[AR-5.2.2.2-c] The application layer architecture shall support the mechanisms of PIN modification procdure, for example, PEMC/PEGC relocation.

[AR-5.2.2.2-d] The application layer architecture shall support the deployment and mechanism of multiple PEMCs/PEGCs.

[AR-5.2.2.2-e] The application layer architecture shall support mechanisms to obtain PIN server endpoint address.

[AR-5.2.2.2-f] The application layer architecture shall support the mechanisms to perform PIN discovery, and enable the PINEs to join/leave the PIN.

[AR-5.2.2.2-g] The application layer architecture shall support the mechanisms of PINE registration to PIN server.

[AR-5.2.2.2-h] The application layer architecture shall support mechanisms to maintain, configure, update the PIN profile/PIN client profile.

### 5.2.3 PIN enable 5GS communication

#### 5.2.3.1 General

This clause specifies PIN communication requirements for the architecture.

#### 5.2.3.2 Requirements

[AR-5.2.3.2-a] The application layer architecture shall provide mechanisms to configure routing information in PEGC to enable the PINE to access the network provided by PEGC.

[AR-5.2.3.2-b] The application layer architecture shall provide mechanisms to support the PIN and the PINEs in PIN to consume the 5GS communication.

[AR-5.2.3.2-c] The application layer architecture shall provide mechanisms to support the PEMC/PEGC to request the 5GS resource for PIN.

### 5.2.4 Service Switch

#### 5.2.4.1 General

This clause specifies service switch requirements for the architecture.

#### 5.2.4.2 Requirements

[AR-5.2.4.2-a] The application layer architecture shall provide mechanisms to support the service switching in a PIN between different PINE for achieving better service experience.

### 5.2.5 Application server discovery

#### 5.2.5.1 General

This clause specifies application server discovery requirements for the architecture.

#### 5.2.5.2 Requirements

[AR-5.2.5.2-a] The application layer architecture shall provide mechanisms to support the application server discovery for PIN.

### 5.2.6 Service continuity

#### 5.2.6.1 General

This clause specifies service continuity requirements for the architecture.

#### 5.2.6.2 Requirements

[AR-5.2.6.2-a] The application layer architecture shall provide mechanisms to support the PEGC relocation procedure to enable service continuity.

[AR-5.2.6.2-b] The application layer architecture shall provide mechanisms to change the communication from via PEGC to via 5GS, and enable the service continuity.

# 6 Architecture

## 6.1 General

This clause provides a general description of the architecture of PINAPP.

# 7 Solutions

## 7.1 Mapping of solutions to key issues

Table 7.2-1 Mapping of solutions to key issues

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | KI #1 | KI #2 | KI #3 | KI #4 | KI #5 | KI #6 |
| Sol #1 | **X** |  |  |  |  |  |
| Sol #2 | **X** |  |  |  |  | X |
| Sol #3 | **X** |  |  |  |  |  |
| Sol #4 | **X** |  |  |  |  |  |
| Sol #5 | **X** |  |  |  |  |  |
| Sol #6 | **X** |  |  |  |  |  |
| Sol #7 | **X** |  |  |  |  |  |
| Sol #8 |  |  | **X** |  |  |  |
| Sol #9 |  |  |  |  |  | **X** |
| Sol #10 |  |  | **X** |  |  |  |
| Sol #11 |  |  |  | **X** |  |  |
| Sol #12 | **X** |  |  |  |  |  |
| Sol #13 | **X** |  |  |  |  |  |
| Sol #14 |  | **X** |  |  |  |  |
| Sol #15 |  | **X** |  |  | X |  |
| Sol #16 | **X** |  |  |  |  |  |
| Sol #17 |  |  |  |  | X |  |

## 7.2 Solution #1: PINAPP architecture

### 7.2.1 Architecture assumption

The Figure 7.2.1-1 shows the application architecture for enabling PINAPP.



Figure 7.2.1-1: PINAPP architecture

The UE or PIN elements have PIN client. The UE or PIN Element with gateway capability (PEGC) performs the role of an entity supporting gateway capability for PIN. The PEGC provides gateway functionality for the PIN elements. The UE or PIN Element with management capability (PEMC) performs the role of an entity supporting management capability for PIN. The PEMC provides management functionality for the PIN elements.

The interactions between PEMC and PIN client are supported over PIN-3. The interactions between PEMC and PEGC are supported over PIN-4. The interactions between PEGC and PIN client are supported over PIN-2. The interactions between PIN clients from different UEs or PIN elements are supported over PIN-5.

NOTE 1: It is possible that an application client on PIN elements can communicate with application server directly via 5GS or indirectly via PEGC.

NOTE 2: It is possible that an application client can communicate with other application client in the same PIN directly or via PEGC.

NOTE 3: It is possible that an application client can communicate with other application client in another PIN via PEGC.

#### 7.2.1.1 User accessing services provided by PIN Element from outside the PIN

The Figure 7.2.1.1-1 shows the application architecture updates to enable authorized user to access services provided by PIN element behind the PEGC. For simplicity, not all functional elements of Figure 7.2.1-1 are shown in below Figure 7.2.1.1-1.



Figure 7.2.1.1-1: PINAPP architecture

The interactions between PEGC and PIN client of the authorized user are supported over interface PIN-11. The interactions between PEMC and PIN client of the authorized user are supported over interface PIN-12. The authorized user uses PIN-12 to configure the policies in a PIN.

NOTE: The authorized user is allowed to manage a PIN due to authorized user has PIN-12 interface to communicate with PEMC.7.2.1.2 PIN Localization

Personal IoT Networks enable the communication needs of IoT devices within the constraints of a localized, private network. IoT devices using 3GPP or non-3GPP access may be members of a PIN. The PIN may consist of wearable IoT devices or IoT devices used in home automation. A PIN client that is authorized to access the PIN may access the PIN locally within the coverage area of the PIN or remotely over the 5G network. PIN localization refers to the main coverage area of the PIN and may be mobile if the PIN consists of wearable IoT devices and is being used by a user of the PIN who is mobile.

### 7.2.2 Functional elements

The functional entities of the application architecture for enabling PINAPP are described in this clause.

#### 7.2.2.1 PIN element with Management Capabilities (PEMC)

PEMC: A PIN Element with Management Capability is a PIN Element that provides a means for an authorised administrator to configure and manage a PIN.

It provides following functionalities:

- For a network operator or authorized user to configure the policies of the PIN;

- Provide life span information of the PIN to the authorized user or the PIN elements;

- Maintain the UEs or PIN elements who joined the PIN. It includes maintaining available services, capability to act as a relay to other UEs or PIN elements; and

- Maintain the PIN profile for each PIN and PINE in PIN;

- To configure and manage a PIN; including:

- authorizing the UEs or PIN elements requesting to join the PIN;

- authorizing the PEGC and configure the parameters in PEGC to support PINE communication (via 5GS or direct communication);

- configuring UEs or PIN elements to enable service discovery of other UEs or PIN Elements;

- add new UEs or PIN elements to the PIN;

- configure UEs and PIN elements to enable direct communications; and

- configure UEs and PIN elements to communicate with each other when gateway device is unavailable.

- support the PIN server endpoint address delivery to UEs or PIN elements;

- support the credentials delivery to UEs or PIN elements;

NOTE: When gateway device is unavailable, the configurations are required to enable direct communication.

#### 7.2.2.2 PIN Server

PIN server: Deployed by operator in network, and provisioning of configuration information to UE (PINAPP). Authorization of the Creation request of PIN, and arranges the PEGC information about access control to PIN.

- Maintain the PIN profile for each PIN and PINE in PIN;

- Authorized the PIN create/PIN modification/PIN delete

- Determine the access control information of PEGC/PINE in PIN

- Authorized the PINE to be added/removed into/from the PIN

- Support PIN discovery and application server discovery

#### 7.2.2.3 PIN element with Gateway Capabilities (PEGC)

PEGC: A PIN Element with Gateway Capability is a PIN Element that provide any 5G services to any UE or PINAPP.

- Maintain the PIN profile for each PIN and PINE in PIN;

- Maintain the access control information for each PIN and each PINE in PIN, and authorized whether the PINE can access the network provided by PIN;

- Support to trigger the PDU session modification towards 5GS to request the resource for PIN;

- Enable the 5GS communication or direct communication;

- Support to PIN server address delivery;

- Support to deliver the credentials to PINE;

- Support PIN discovery function

#### 7.2.2.4 PIN client

PIN client: The PIN enabler layer deployed in PIN elements to enable the management procedure to PEMC and routing control procedure to PEGC.

It provides the following functionalities for the application clients in the UE or PIN element:

- Registering the available service and capabilities;

- Perform service discovery of other UEs or PIN elements;

- Communicate with PIN clients of other UEs or PIN elements;

- Act as a relay for other UEs or PIN elements;

- Selects relay for direct communication; and

- Indicate whether the UE or PIN element, in which the PIN client resides, is discoverable or not.

- Maintain the PIN profile;

- Support to do application server discovery;

- Perform to join/leave a PIN;

- Support to discover the available PIN.

- Support to receive the information to access the network provided by PEGC;

#### 7.2.2.5 Application client

Application client: AC is the application resident in the PIN elements performing the client function.

### 7.2.3 Reference Points

PIN - 1: The interactions related to enabling PINAPP, between the Application client and the PIN client.

PIN - 2: This reference point exists between PIN client and PEGC which connects PIN client of UE to PEGC. The PIN client uses this interface to communicate with other PIN clients within PIN or to access 3GPP network..

PIN - 3: This reference point exists between the PIN client and PEMC and following functionalities are supported over this reference point:

- Authorizing PIN clients to access PIN;

- Service discovery of other UEs or PIN elements;

- Discovery and selection of relay UEs or PIN elements;

- Notifying the PIN information modification details (e.g. PEMC change, PEGC change, PIN capabilities change).

PIN - 4: This reference point exists between between the PEGC and PEMC and following functionalities are supported over this reference point:

- Authorizing PEGC for PIN access;

- Notification of PIN elements joining or leaving the PIN by PEMC to PEGC;

- Delivery of PIN dynamic profile information by PEMC to PEGC whenever it changes;

PIN - 5: This reference point exists between the one PIN client and another PIN client and it supports direct connection over 3GPP or non-3GPP RAT. It also connects to PIN client of a UE or PIN element to the PIN client of another UE or PIN element acting as a relay.

PIN - 6: This reference point exists between the PEMC and PIN server and supports the following functionalities:

- Authorization of PEMC;

- Notifying PIN server whenever a PIN element joins or leaves the PIN, whenever a PIN client updates its capabilities;

- Notifying PIN server of PEGC replacement;

- Delivery of PIN dynamic profile information;

PIN - 7: The interactions related to enabling PINAPP, between the one PEGC and PIN server.

PIN - 8: The interactions related to enabling PINAPP, between the one PIN server and 3GPP core network.

PIN - 9: The interactions related to enabling PINAPP, between the application server and PIN server.

PIN – 10: The interactions related to enabling PINAPP, between the PIN client in PIN element and PIN server.

PIN – 11: The interactions related to enabling PINAPP, between the PEGC and PIN client from outside the PIN to access the services provided by PIN elements within the PIN.

PIN – 12: The interactions related to enabling PINAPP, between the PEMC and PIN client for configuring and managing the PIN from outside the PIN.

### 7.2.4 Functional Entity Cardinality

#### 7.2.4.1 PEMC

The following cardinality rules apply for PEMC:

a) one or more PEMCs per PIN.

#### 7.2.4.2 PEGC

The following cardinality rules apply for PEGC:

a) one or more PEGCs per PIN.

#### 7.2.4.3 PIN server

The following cardinality rules apply for PIN server:

a) one PIN server per PIN.

b) Multiple PINs per PIN server.

NOTE: There might be multiple PIN servers deployed in a PLMN.

#### 7.2.4.4 PIN client

The following cardinality rules apply for PIN client:

a) one or more PIN clients per PIN.

b) one PIN client per PIN element.

#### 7.2.4.5 Application client

The following cardinality rules apply for application client:

a) one or more application clients per PIN client.

### 7.2.5 Identities

#### 7.2.5.1 PIN ID

The PIN ID is a unique value in PLMN that identifies the PIN.

#### 7.2.5.2 UE identifier

The UE ID uniquely identifies a particular UE within a PLMN domain. Following identities are examples that can be used:

a) GPSI, as defined in 3GPP TS 23.501 [02].

NOTE: To protect privacy of the user, MSISDN can be used as GPSI only after obtaining user's consent.

#### 7.2.5.3 PIN client ID

The PIN client ID is a globally unique value that identifies the PIN client.

#### 7.2.5.4 Application Client ID

The ACID identifies the client side of a particular application, for e.g. SA6Video viewer, SA6MsgClient etc. For example, all SA6MsgClient clients will share the same ACID.

In case that the UE is running mobile OS, the ACID is a pair of OSId and OSAppId.

#### 7.2.5.5 PIN server ID

The PIN server ID is a unique value in PLMN domain that identifies the PIN server.

## 7.3 Solution #2: PIN management

### 7.3.1 Architecture enhancements

The architecture of PIN is referred to the solution 1 in clause 7.

### 7.3.2 Solution description

#### 7.3.2.1 General

This solution addresses aspects of Key Issue #1.

After the UE or PINAPP acquires the role of PEMC, the PINAPP can trigger a creation of PIN towards PIN server.

When the PINAPP as a PEMC to trigger the creation of PIN, there may the two situations below:

- There is only one element in PIN, and the PEMC manages itself;

- There are already serveral PIN elements or PEMC. The other PIN elements or PEGC have communication links with PEMC via non-3GPP access and the PEMC can trigger creation of PIN with these PIN elements in group.

After the creation of PIN is accepted by network, the PIN server response with the PIN ID, the PEGC information about access control configured in PEGC.

At the network side, a PIN server should be deployed. The PIN server (represent the operator) is responsible for the authorization of the Creation request of PIN, and arranges the PEGC information about access control to PIN.

How the PIN server receives or derives PEGC information about access control is in the scope of SA2.

For an established PIN, the PIN can be modified in the following situation:

- Changes of PEMC. For example, the current PEMC may no longer be provide management of PIN and the role of PEMC will be changed to another PIN elements.

- Changes of PEGC. For example, if the current PEGC has broken down or is switched off, or the PEGC moves out of the direct communication proximity of the PINE client(s). The current PEGC is no longer suitable and enforcing another PIN element as PEGC is needed.

- Update of PIN service. If the service that a PINE (in a PIN) or PIN can provide is updated, the PEMC should trigger the modification of PIN towards PIN server to update the PIN service.

- Update of PIN service remotely by authorised administrator after local PEMC failure. An authorised administrator is the owner of the PIN and needs to reconfigure the PIN after a communication failure with the local PEMC. The authorised administrator can access the PIN and the PIN server only through the 5G network.

Editor's note: The access control information should be coordinated with SA2 and wait for further update.

#### 7.3.2.2 Procedures of Creation of PIN

This procedure presents a high-level overview of Solution #X.

Figure 7.3.2.2.2.-1 illustrates PIN creation procedure based on request/response model.

Pre-conditions:

1. The UE (PINAPP) has been pre-configured or has discovered the address (e.g. IP address, FQDN, URI) of the PIN server;

2. The UE Identifier or PIN client Identifier is available;

3. The PINAPP has been authorized to communicate with the PIN server;

4. The PINE-1 has already received the role of PEMC from PIN server;



Figure 7.3.2.2.2-1: Creation of PIN

1. The PEMC sends a PIN creation request to the PIN server in-order to create a PIN. The PIN creation request includes the security credentials of the UE or PINAPP received during PINAPP authorization procedure and may include the UE identifier such as GPSI, PIN client ID, UE location and PINAPP profile(s) information. The PEMC can also indicate the PIN service that the PIN can provide to PIN server.

The PEMC can request to create a PIN including the details of other PIN elements that has already communicated with it .The details of the PIN elements could be for example, UE identifier such as GPSI, PIN client ID, UE location and PINAPP profile(s) information.

If there are no other PIN elements in the request, the PEMC requests to create a PIN including itself.

NOTE 1: In order to save the procedure of several PEMCs to be involved into the certain PIN as individual PEMC, the PEMC can have the additional PEMC GPSIs in the PIN create request, to indicate additional PEMCs that are allowed to manage the PIN. This procedure doesn’t have conflict with that other PEMC requests to join the certain PIN and becomes PEMC separately.

NOTE 2: For a certain PIN, only one PEMC at a time can be assigned with primary role and other PEMCs if any are assigned with secondary role..

2. Upon receiving the request, the PIN server performs an authorization check to verify whether the PINE-1 (PEMC) has authorization to perform the operation.

Editor's Note: Whether and how the 5GC involved in the PIN creation is FFS.

3. The PIN server sends a successful response to PINE-1PEMC, which includes a newly assigned PIN ID to indicate the PIN. It also includes the list of PIN elements and their identifier which are authorized and made as member of the newly created PIN if the PIN creation request contains the list of PIN elements to be included in the PIN. If the PIN creation request fails, the PIN server should give the failure response indicating the cause of PIN creation request failure.

If there are no other PIN elements in the PIN creation request and the PIN creation is successful, the PEMC indicates the PINAPP (PEMC) to be the PEGC. The PINAPP who has already had the role of PEMC can also has the role of PEGC.

If the PEGC is indicated, the PIN server sends PIN client ID (that represents the PEGC), assigned IP address or port number in successful response to PEMC. And, the PIN Server also sends the PEGC information about access control in the response, including:

- Access control information includes: user name, account, SSID, BSSID. All the information is used by PIN elements in PIN to access 5G or access other application outside of PIN;

The PIN server or PEMC can decide the access control information in certain PEGC.

- If the access control information decided by PIN server, the PIN server sends the access control information to PEMC. And the PEMC delivers the access control information to PEGC.

- If the access control information decided by PEMC, the PEMC delivers the access control information to PEGC.

4a-4c. [Optional] If the response of creation of PIN contains the list of PIN elements, the PINE-1 (PEMC) generates the PIN created notification request to individual PIN elements based on the list received in step 3. This notification request includes the PIN ID of the newly created PIN and also contains an indication that the PIN element is made the member of the newly created PIN.

5a-5c. [Optional] The individual PIN elements sends the PIN created notification response to acknowledge the receipt of the notification. The PIN elements receiving the PIN creation notification request with joined indication shall not join the PIN by issuing the PIN join request since they are already made as the member of the PIN.

After the procedure above, the PINAPP (PEMC) creates a PIN with PINAPP(PEGC) and other accepted PIN elements in PIN.

The following procedure defines how to provide PEGC information (for example, the access control information) to PINE over direct connection which enables the PINE to connect to PEGC.



Figure 7.3.2.2.2-2: Deliver access related information to PINE for connecting to PEGC

1. The PEMC sends request ([Connection Info], [Authorization Info]) to the PINE. The Connection Info contains the access control information. The Auth Info may be included for authenticating/authorizing PINE connecting to PEGC.

2. The PINE responds to the PEMC.

After receiving the access control information, the PINE can access into the network that PEGC provide and after the authorization/authentication with PEMC, the PINE can finally use the gateway service to communication.

NOTE: The access control information is per-PINE/per-PIN information. Each PINE uses this information to access the network provided by PEGC for a PIN. And the PEGC uses this access control information to authorize that whether the PINE can consume the network provided by PEGC in a PIN.

#### 7.3.2.3 Procedures of Modification of PIN

##### 7.3.2.3.1 PIN modification triggered by PEMC

If the management of PIN should be changed to other PIN elements in UE, the original PEMC of a PIN should trigger the PIN modification procedure to PIN server.

Figure 7.3.2.3.1-1 illustrates PIN modification procedure based on request/response model.

Pre-conditions:

1. The PEMC in a PIN has been pre-configured or has discovered the address (e.g. IP address, FQDN, URI) of the PIN server;

2. The PIN has already been created and a PIN ID is distributed by PIN server;

3. The PEMC has been authorized to communicate with the PIN server;

4. A PIN client has already received the role of PEMC from PIN server;



Figure 7.3.2.3.2-1: Modification of PIN triggered by PEMC

1. The PEMC sends a PIN modification request to the PIN server to request to change the role of PIN management. The PIN modification request includes the security credentials of the PIN client received during PIN client authorization procedure and may include the UE identifier such as GPSI, PIN client ID, UE location and PIN client profile(s) information and PIN ID. The PIN ID indicates the management of this PIN will be changed.

The PEMC can also include the potential PEMC in this PIN that represented by GPSI, PIN client ID. But this propose by PEMC is only for recommendation towards PIN server. If there are more than one potential PEMCs are included in PIN modification request, the original PEMC can label the priority of these potential PEMCs.

Also, if the PIN service in PIN has updated, for example, the service in PINE (in this PIN) is newly added or the service in PINE (in this PIN) is deactivated or disabled, the PEMC should trigger PIN modification request includes the updated PIN services.

2. Upon receiving the request, the PIN server performs an authorization check to verify whether the PEMC has authorization to perform the operation. The PIN server also updates and stores the PIN service of this PIN as PIN profile.

3. The PIN server sends a successful response to original PEMC, which includes a stop of administrator permissions of PIN and the PIN client ID of the new PEMC. If the PIN modification request fails, the PIN server should give the failure response to indicates that indicates the cause of PIN modification request failure.

The PIN server can decide the new PEMC from the PIN elements in the PIN, and can also consider the potential PEMC that indicated by old PEMC.

After the new PEMC is selected, the new PEMC can either be configured with the PIN Profile information by PIN server, or the PIN Profile information can be configured by the old PEMC. The PIN Profile information includes the PIN elements in PIN (for example, IP address or ID), access control information of each PIN elements.

4. After receiving the successful of PIN modification response, the old PEMC stops the administrator permissions of a PIN which is represented by PIN ID. And the PIN server delivers the PIN Profile information to the new PEMC according to new PEMC IP address or ID indicated in successful PIN modification request.

##### 7.3.2.3.2 PIN modification triggered by event of PEGC

If the current PEGC is broken down or switched off, or the PEGC moves out of the direct communication proximity of the PINE clients(s). It is not properly to keep this PEGC, and enforces another PIN element as PEGC is needed.

Figure 7.3.2.3.2-1 illustrates PIN modification procedure triggered by event of PEGC.

Pre-conditions:

1. The PEGC in a PIN has been pre-configured or has discovered the address (e.g. IP address, FQDN, URI) of the PIN server;

2. The PIN has already been created and a PIN ID is distributed by PIN server;

3. The PEGC has been authorized to communicate with the PIN server;



Figure 7.3.2.3.2-1: Modification of PIN triggered by PEGC

0. The PIN server or PEMC can subscribe the mobility of PEGC that when the PEGC moves out of the area of interests (for example, leave home or office). Or the PIN server and PEMC can subscribe the status of PEGC that when the PEGC switches off and the PIN server can be notified by the PEGC. After receiving the event notification, the PIN server can trigger the modification of PEGC.

1. The PIN server or PEMC is notified by PEGC of event notification.

2. The PIN server or PEMC decides to modify the PIN with changing PEGC.

3. The PIN server or PEMC sends a successful response to original PEGC, which includes a stop of access control information in PEGC. If the PIN modification request fails, the PIN server should give the failure response to indicates that indicates the cause of PIN modification request failure.

The PIN server or PEMC can decide the new PEGC from the PIN elements in the PIN.

4. After receiving the successful of PIN modification response, the old PEGC stops the routing control of a PIN which is represented by PIN ID. And the PIN server delivers the access control information to the new PEGC.

##### 7.3.2.3.3 PEMC replacement triggered by PIN server

The following solution corresponds to the key issue #6 on PEMC/PEGC replacement in PIN as specified in clause 4.6.

In some scenarios, like hardware failure, crash or power drain, the current PEMC may not be in a position to indicate to the PIN server or request the PIN server to assign the role of PEMC to another PIN element. In these cases, the PIN server on detecting the unavailability of the PIN element acting as PEMC, need to assign the role to another PINE and transfer the PIN dynamic profile information to the new PEMC.

Figure 7.3.2.3.3-1 illustrates PEMC replacement procedure triggered by PIN server on detecting current PEMC is unavailable.

Pre-conditions:

1. PEMC-2 PIN element has already indicated that it can act as PEMC during the registration process.

2. Dynamic profile information about the PIN is available at the PIN server



Figure 7.3.2.3.3-1: PEMC replacement triggered by PIN server

1. PEMC-1, PEMC-2, PEGC, PINE-1 and PINE-2 are part of same PIN. PEMC-1 is currently the PEMC of the PIN.

2. The PIN server identifies that PEMC-1 is down or crash or its duration to act as PEMC is ending. How PIN server identifies that the current PINE acting as PEMC is crashed or down is not in the scope of this specification.

3. The PIN server looks into the PIN profile and PIN dynamic profile information to identify the new PINE which can take up the role of PEMC (here PEMC-2 PIN element) and requests PEMC-2 to take the role of PEMC.

4. If the PEMC-2 PINE decides to take up the role of PEMC it sends the success response to the PIN server.

5. The PIN server delivers the PIN dynamic profile information to the PEMC-2.

6a,6b,6c. Once the PEMC replacement process is success, the PEMC-2 signals all the PINEs in the PIN including the PEGC about the change in the PIN element acting as PEMC and its reachability information.

##### 7.3.2.3.4 PEMC replacement triggered internally within the PIN

The following solution corresponds to the key issue #6 on PEMC/PEGC replacement in PIN as specified in clause 4.6.

A PIN element could have been authorized to act as PEMC for a certain duration after which it is either removed from the PIN or de-authorized to act as PEMC. Another PIN element in the PIN takes over the role of PEMC.

When the duration of its role as PEMC is expiring or for some other reasons (which could be implementation specific) the current PEMC requests another PINE to take the role of PEMC. Once the role assignment succeeds, the PIN server and other PIN elements including PEGC are notified of this role change.

Figure 7.3.2.3.X-1 illustrates PEMC replacement procedure triggered internally within the PIN by current PEMC.

Pre-conditions:

1. PEMC-2 PIN element has already indicated that it can act as PEMC during the registration process.

2. Dynamic profile information about the PIN is available at the current PEMC and PIN server



Figure 7.3.2.3.4-1: PEMC replacement triggered internally within the PIN

1. PEMC-1, PEMC-2, PEGC, PINE-1 and PINE-2 are part of same PIN. PEMC-1 is currently the PEMC of the PIN.

2. PEMC-1 decides to relinquish its PEMC role and handover to another PIN element. It may decide if it detects that its UE power is draining or its role as PEMC is nearing expiry.

3. The PEMC-1 looks into the PIN dynamic profile information to identify the new PINE which can take up the role of PEMC (here PEMC-2 PIN element) and requests PEMC-2 to take the role of PEMC.

4. If the PEMC-2 PINE decides to take up the role of PEMC it sends the success response to the PEMC-1.

5. The PEMC-1 updates the PIN dynamic profile information with this role change details and delivers the PIN dynamic profile information to the PEMC-2.

6. The PEMC-1 signals all the PINEs in the PIN including the PEGC and PIN server about the change in the PIN element acting as PEMC and its reachability information. On receiving this notification PIN server and PEGC updates the PIN dynamic profile information with the details of PEMC-2.

##### 7.3.2.3.5 PEGC replacement triggered by PEMC

The following solution corresponds to the key issue #6 on PEMC/PEGC replacement in PIN as specified in clause 4.6.

In some scenarios, like hardware failure, crash or power drain, the current PEGC may not be in a position to indicate to the PIN server or request the PIN server to assign the role of PEGC to another PIN element. In these cases, the PEMC on detecting the unavailability of the PIN element acting as PEGC, need to assign the role to another PINE and transfer the PIN information to the new PEGC.

Figure 7.3.2.3.5-1 illustrates PEGC replacement procedure triggered by PEMC on detecting current PEGC is unavailable or PEGC role change is required.

Pre-conditions:

1. PEGC-2 PIN element has already indicated that it can act as PEGC during the registration process.

2. Dynamic information about the PIN is available at the PEMC



Figure 7.3.2.3.5-1: PEGC replacement triggered by PEMC

1. PEMC, PEGC-1, PEGC-2, PINE-1 and PINE-2 are part of same PIN. PEGC-1 is currently the PEGC of the PIN.

2. The PEMC identifies that PEMC-1 is down or crash or its duration to act as PEGC is ending. How PEMC identifies that the current PINE acting as PEGC is crashed or down is not in the scope of this specification.

3. The PEMC looks into the PIN profile and PIN dynamic information to identify the new PINE which can take up the role of PEGC (here PEGC-2 PIN element) and requests PEGC-2 to take the role of PEGC.

4. If the PEGC-2 PINE decides to take up the role of PEGC it sends the success response to the PEMC.

5. The PEMC notifies the PIN server that PEGC-2 is the new PEGC of the PIN and it is releasing PEGC-1 from its role as PEGC

6. The PEMC and PIN server updates the PIN dynamic information with the relevant details of PEGC-2.

7. The PEMC delivers the PIN dynamic information to the PEGC-2.

8a,8b. The PEMC notifies all the PINEs in the PIN about the change in the PIN element acting as PEGC and its reachability information.

NOTE: The PINEs are considered to be implicitly subscribed for notifying about the changes in the PIN.

##### 7.3.2.3.6 PIN modification triggered by PEGC

The current PEGC decides to relinquish the role of PEGC and requests the PIN server to assign the role to other PINE. The PIN server chooses a PINE and assigns the PEGC role to it.

Figure 7.3.2.3.6-1 illustrates PIN modification procedure triggered by PIN server based on request from the current PEGC.

Pre-conditions:

1. The PEGC in a PIN has been pre-configured or has discovered the address (e.g. IP address, FQDN, URI) of the PIN server;

2. The PIN has already been created and a PIN ID is distributed by PIN server;

3. The PEGC has been authorized to communicate with the PIN server;



Figure 7.3.2.3.6-1: Modification of PIN triggered by PEGC

1. The PEGC (old) sends a PIN modification request to the PIN server to request to change the role of PEGC. The PIN modification request includes the security credentials of the PIN client received during PIN client authorization procedure and may include the UE identifier such as GPSI, PIN client ID, UE location and PIN ID.

2. Upon receiving the request, the PIN server performs an authorization check to verify whether the PEGC has authorization to perform the operation.

3. The PIN server sends a successful response to original PEGC, which includes a stop of access control information in PEGC. If the PIN modification request fails, the PIN server should give the failure response to indicates that indicates the cause of PIN modification request failure. After receiving the successful of PIN modification response, the old PEGC stops the routing control of a PIN, which is represented by PIN ID.

4. The PIN server can identify the new PEGC by looking into the capabilities of the PIN elements from PIN dynamic profile information. PIN server requests the PEGC (new) to take the role of PEGC.

5. PEGC (new) if it can take the role of PEGC, sends the success response to the PIN server.

6. PIN server delivers the PIN dynamic profile information to the PEGC (new).

7. PIN server notifies the PEMC and other PIN elements about the change in the PEGC role and its reachability information.

8. PIN server and PEMC updates the PIN dynamic profile information with the details of PEGC (new).

##### 7.3.2.3.7 PIN modification triggered after local PEMC failure

An authorised administrator is the owner of a PIN and accesses PIN configuration using an application on a UE, which is one of the PEMC for the PIN. The authorised administrator leaves the local area of the PIN (e.g. in a home) and is able to access the PIN remotely through the 5G network. The authorised administrator is able to manage the PIN through the 5G network.

Pre-conditions:

1. The PIN server has authorised the creation of the PIN.

2. The authorised administrator is the owner of the PIN and has created the PIN.

3. The authorised administrator configures PEMC2 to provide PIN management for the PIN. PEMC2 becomes the active PEMC and UE/PEMC1 is an inactive PEMC.

4. PEMC2, PEGC, PINE-1, PINE-2, and the UE/PEMC1 are members of the PIN. PINE-1 has PEMC capability.



Figure 7.3.2.3.7-1: PIN Modification after local PEMC failure

1. UE/PEMC1 receives a notification from PEGC that there is a communication failure with PEMC2.

2. An authorised administrator on UE/PEMC1 sends a PIN modification request to the PIN server through the 5G network. The modification request includes the security credentials of the authorised administrator, the UE ID, the PIN ID, PIN member ID, and a request that PINE-1 be assigned the new PEMC.

3. The PIN server processes the modification request and checks if the authorised administrator is allowed to modify the PIN.

4. If the authorised administrator is allowed to perform PIN modification, the PIN server sends a request to PINE-1 to assign PINE-1 as the new PEMC and provides PIN profile and dynamic profile information to PINE-1.

5. PINE-1 returns an accept response to the PIN server.

6. The PIN server notifies the other members of the PIN that PINE-1 will be the new PEMC for the PIN.

7. The PIN server sends a response to the PIN modification request with updated information for the PIN profile and the dynamic profile information.

8. PIN communications resume with PINE-1 serving as the new PEMC.

##### 7.3.2.3.8 PIN management with multiple PEGCs

This solution targets KI#1 on PIN management and KI#6 on PEMC/PEGC replacement in PIN, and applies for PIN eployement with a large number of PIN members. In these cases, multiple PIN Elements may be assigned with Gateway Capability to distribute relaying PIN communications among the different PEGCs. The multiple PEGCs in a PIN also provide redundancy for PIN communication should one of the PEGC fails.

Precondition:

1. A homeowner creates a PIN and assigns multiple PEGCs for relaying PIN communications.



Figure 7.3.2.3.8-1: Multiple PEGC configuration for a PIN

1. A PIN Element with Management Capability, PEMC, requests and is authorized by the PIN server to create a PIN.

2. PEMC creates the PIN and configures PEGC-A and PEGC-B as PIN Element with Gateway Capability. The PIN owner plans to add a large number of devices to the PIN and wants to distribute PIN communications between PEGC-A and PEGC-B to avoid overloading one PEGC. In addition, PEGC-A and PEGC-B can offer redundancy in case either PEGC-A or PEGC-B fails. PEMC sends a PIN profile update to the PIN server of the configuration of PEGC-A and PEGC-B as PEGCs.

3. PINE-1 sends a PIN join request to the PEMC. PIN Client Profile information (required KPIs, location and schedule) is included in the request which PEMC uses to determine the optimal default and backup PEGCs for PINE-1. PEMC assigns PEGC-A as the default PEGC for PINE-1 and PEGC-B as the backup PEGC for PINE-1. PINE-1 will use PEGC-A as the primary PEGC to relay PIN communications and will use PEGC-B to relay PIN communications only if PEGC-A is not available.

4. The PEMC notifies PEGC-A and PEGC-B of their PEGC roles: PEGC-A will serve as the default PEGC and PEGC-B will serve as the backup PEGC for PINE-1.

5. PEMC returns a response to the join request and includes the PEGC configuration that PEGC-A will serve as the default PEGC and PEGC-B will serve as the backup PEGC.

6. Steps 3 to 5 are repeated for PINE-2. PEMC configures that PEGC-B will serve as the default PEGC and PEGC-A will serve as the backup PEGC for PINE-2.

7. PEMC sends a PIN profile update to the PIN server informing the PIN server of the PEGC configurations for PINE-1 and PINE-2.

##### 7.3.2.3.9 PIN management with multiple PEMCs

This solution targets KI#1 on PIN management and applicable for PIN with a large number of PIN elements and including multiple PIN elements with management capabilities. In these cases, multiple PIN Elements may be assigned with PEMC role for ease and effective management by the PIN owner or PIN admin.

Precondition:

1. A homeowner creates a PIN and configured multiple PEMCs.

2. PEMC-S is assigned with the role of secondary PEMC and PEMC-P is assigned with the role of primary PEMC.

2. PEMC-S has direct connection or PIN direct connection with the PEMC-P.



Figure 7.3.2.3.9-1: PIN management with multiple PEMCs

1. The PEMC-S may already have an application layer connection established with PEMC-P.

2. PEMC-S rreceives a request from PIN owner/PIN admin to perform any of the PIN management operations. These operations could be PIN element removal, PIN element addition, PIN deletion, PIN configuration update etc.

3. PEMC-S prepares the corresponding request including the required details for the requested operation and sends it to PEMC-P. These requests shall carry the PIN client ID of the PEMC-S mandatorily.

4. PEMC-P on receiving the request checks whether the PEMC-S is authorized as secondary PEMC in-order to perform the operation.

5. If the authorization succeeds, PEMC-P proceeds with the requested operation.

6. PEMC-P sends the response to PEMC-S containing the status/result of the requested operation.

NOTE: Only the operations that are required to be performed by the PIN owner/PIN admin can be performed through secondary PEMC and all other operations like PIN discovery, PIN service discovery, authorizing PIN elements to join PIN etc., cannot be handled by the secondary PEMC.

#### 7.3.2.4 Procedures of PIN Profile retrieval

The procedure describes how a PEMC queries the PIN server to obtain the information of a PIN that pre-configured or dynamically created by the PEMC.

Pre-conditions:

1. The PEMC in a PIN has been pre-configured or has discovered the address (e.g. IP address, FQDN, URI) of the PIN server;

2. The PIN has already been created and a PIN ID is distributed by PIN server;

3. The PEMC has been authorized to communicate with the PIN server;

4. A PIN client has already received the role of PEMC from PIN server;



Figure 7.3.2.4-1: Query PIN information

1. The PEMC sends PIN Profile Query requests (PEMC ID, PIN ID) to the PIN server. If the PEMC is behind a PEGC, the message is encapsulated in the user plane packet.

2. [Optional] The PIN server determines whether the PEMC is one of the managers of the PIN. The PIN server can have the verification procedure with 5GS.

3. The PIN server responds to the PEMC with the PIN Profile, which includes for example, the PIN name, PIN description, List of Device Info (PINE), PIN duration, PEGC information or others. The device information is the information of PINE that in the PIN.

### 7.3.3 Solution evaluation

This solution addresses KI#1 about " Whether and how to triggers a PIN network management request, for example, PIN creating/modifying/deleting? What parameters are required in PIN network management request? ".

This solution firstly solves the problem that only the PEMC can trigger a PIN network management request. Before the creation of PIN, the PINAPP or UE should be a PEMC first. And, when the PEMC triggers the PIN creating towards PIN server, some of the parameters are needed in the request.

## 7.4 Solution #3: Insertion and remove of PIN elements in a PIN

### 7.4.1 Architecture enhancements

The architecture of PIN is referred to the solution 1 in clause 7.

### 7.4.2 Solution description

#### 7.4.2.1 General

This solution addresses aspects of Key Issue #1.

After the PIN is created by the PEMC, the other PIN elements can be added into the PIN. For the PIN elements that have already added into the PIN, they can be removed from a certain PIN by the PEMC.

When a PIN element is added into a PIN, the PEMC should configure with the PIN elements with the necessary permission, for example, to be able to access to 5GS via the PEGC.

Before the PIN element to be added into a PIN, the PEMC should discover the PIN element first, or the PIN element receives the lists of PIN Profile first (for example, the list of PIN ID, PIN description information).

When a PIN element is added into a PIN, the PINE can indicate the service it can provide. The service includes both the service that PIN client in PINE can provide and the service that application client on PINE can provide.

#### 7.4.2.2 Procedures

##### 7.4.2.2.1 PIN client requests to join into a PIN

Pre-conditions:

1. The UE (PIN client) has been pre-configured or has discovered the address (e.g. IP address, FQDN, URI) of the PEMC;

2. The UE Identifier or PIN client Identifier is available;

3. The PIN client has been authorized to communicate with the PEMC;

4. The PIN client has already received the list of PIN ID, corresponding PEMC IP address;

For a certain PIN element, it can receive the PIN profile from PEMC. The configuration includes PIN ID, PIN description (Human-readable description of the PIN, for example, the company name, location or the type of service) and the PEMC IP address.

After receiving the PIN profile from PEMC, the PIN client can decide to join the PIN.



Figure 7.4.2.2.1-1: PIN element requests to join a PIN towards PEMC

1. The PIN element already has an application layer connection with a PEMC which manages the PIN.

NOTE: If the PIN client communicates with PEMC via WiFi or Bluetooth provided by PEMC, the PEMC can identify the PIN elements by the account number and password that PEMC distributed and the PIN client ID, UE GPSI if available.

And the PEMC has already send the PIN profile to PIN elements. The configuration includes PIN ID, PIN description (Human-readable description of the PIN, for example, the company name, location or the type of service) and the PEMC IP address.

2. The PIN client sends the request to PEMC to join the PIN. The request includes the security credentials of the PIN client received during PINAPP authorization procedure and may include the UE identifier such as GPSI, PIN client ID, UE location, PIN ID and PIN client profile(s) information as shown in Table 7.7.2.2.1-1. The request also includes service that PINE can provide. In the request, both the service that PIN client in PINE can provide and the service that application client on PINE can provide.

Editor's note: The authorization procedure between PIN client and PEMC should be captured in SA3 scope.

3. Upon receiving the request, the PEMC performs an authorization check to verify whether the PIN client has authorization to join the PIN.

4. The PEMC sends a successful response to PIN client. Also, the access control information for the PIN client is also included, for example, user name, account, SSID, BSSID. All the information is used by PIN elements (PINAPP) in PIN to access 5G or access other application outside of PIN. The PEMC also provides lifetime of the PIN, identity, address of PEGC and may also provide unique PIN client ID to identify the PIN element within a PIN.

Editor's note: The access control information should be coordinated with SA2 for further study.

5. The PEMC notifies the PIN server containing the details of the new PIN client that joined the PIN

6. The PEMC notifies the PEGC and other PIN elements containing the details of the new PIN client that joined the PIN. And the PEGC decides to enables the PINE to access 5GS.

7. The PEMC updates PIN profile with the details of the new PIN client that joined the PIN and the service that the PINE can provide.

8. The PEGC updates the PIN profile with the details of the new PIN client that joined the PIN and the service that the PINE can provide.

9. The PIN server updates the PIN profile with the details of the new PIN client that joined the PIN and the service that the PINE can provide.

##### 7.4.2.2.2 The PEMC removes the PIN elements from a PIN

Pre-conditions:

1. The PIN client has already been added into a PIN;

2. The UE Identifier or PIN client Identifier is available;

3. The PIN client has been authorized to communicate with the PEMC;

The PEMC can decide to remove a PIN client from a PIN, for example, the PIN client may not belong to the group.



Figure 7.4.2.2.2-1: Remove a PIN element from a PIN by PEMC

1. The PIN element already has an application layer connection with a PEMC which manages the PIN.

2. The PEMC decides to remove a PIN client from a PIN which indicated by PIN client ID or UE GPSI.

3. The PEMC sends the notification to PIN client to notify that the PIN client is included in the PIN any more.

4. The PEMC notifies the PEGC containing the details of the PIN client that has been removed from the PIN.

5. The PEMC notifies the PIN server containing the details of the PIN client that has been removed from the PIN.

6. The PEMC updates the PIN profile to remove the details of the PIN client that has been removed from the PIN.

7. The PEGC updates the PIN profile to remove the details of the PIN client that has been removed from the PIN. The PEGC disable this PIN client to access 5GS.

8. The PIN server updates the PIN profile to remove the details of the PIN client that has been removed from the PIN.

##### 7.4.2.2.3 The PIN elements decides to leave the PIN

Pre-conditions:

1. The PIN client has already been added into a PIN;

2. The UE Identifier or PIN client Identifier is available;

3. The PIN client has been authorized to communicate with the PEMC;

The PIN client can decide to leave a PIN, for example, the PIN client has long route to the PIN and is not received service from PIN.



Figure 7.4.2.2.3-1: PIN client decides to leave a PIN

1. The PIN element already has an application layer connection with a PEMC which manages the PIN.

2. The PIN client decides to leave a PIN, and sends the request to PEMC to leave the PIN. The request includes the security credentials of the UE or PIN client received during PINAPP authorization procedure and may include the UE identifier such as GPSI, PIN client ID, UE location and PIN ID.

Editor's note: The authorization procedure between PIN client and PEMC should be captured in SA3 scope.

3. The PEMC authorizes the request, and decides to remove a PIN client from a PIN which indicated by PIN client ID or UE GPSI.

4. The PEMC sends the response to PIN client to notify that the PIN client may not be included in the PIN anymore.5. The PEMC notifies the PEGC containing the details of the PIN client that requested to leave the PIN.

5. The PEMC notifies the PIN server containing the details of the PIN client that requested to leave the PIN.

6. The PEMC updates the PIN profile and remove the details of the PIN client that requested to leave the PIN.

7. The PEGC updates the PIN profile to remove the details of the PIN client that requested to leave the PIN. The PEGC disable this PIN client to access 5GS.

8. The PIN server updates the PIN profile to remove the details of the PIN client that requested to leave the PIN.

## 7.5 Solution #4: PIN delete

### 7.5.1 Architecture enhancements

The architecture of PIN is referred to the solution 1 in clause 7.

### 7.5.2 Solution description

#### 7.5.2.1 General

This solution addresses aspects of Key Issue #1.

For an established PIN, the PIN can be deleted by the following situation:

- Decided by PEMC. The PEMC of a PIN decides to delete the PIN and sends request to PIN server. The PIN server accepts the requests and deletes the PIN. The PIN elements in this PIN can’t access to 5GS via PEGC anymore.

- Decided by PIN server. For each PIN, it has the life cycle that the PIN can exists. If the PIN has been in existence for longer than the life cycle, the PIN server can decide to delete the PIN and release the resource.

After the delete of PIN, the PIN elements in PIN can’t access to other PIN elements or application server via PEGC by 5GS.

Due to the PEMC can store the lifecycle of a PIN locally, and when the lifecycle of PIN comes to the end, the PEMC can directly delete the PIN locally and without authorized by PIN server. After the PIN is deleted by PEMC, the PEMC can update the status of PIN to PIN server.

#### 7.5.2.2 Procedures of Delete of PIN

##### 7.5.2.2.1 PIN delete triggered by PEMC

The PEMC can trigger the PIN delete to PIN server that the PIN doesn’t need any more.

Figure 7.5.2.2.1-1 illustrates PIN delete procedure based on request/response model.

Pre-conditions:

1. The PEMC in a PIN has been pre-configured or has discovered the address (e.g. IP address, FQDN, URI) of the PIN server;

2. The PIN has already been created and a PIN ID is distributed by PIN server;

3. The PEMC has been authorized to communicate with the PIN server;

4. A PIN client has already received the role of PEMC from PIN server;



Figure 7.5.2.2.1-1: Delete of PIN triggered by PEMC

1. The PEMC sends a PIN delete request to the PIN server to request to delete the PIN. The PIN delete request includes the security credentials of the PIN client received during PIN client authorization procedure and PIN ID. The PIN ID indicates this PIN will be deleted.

Editor's note: The security credentials design and the authorization procedure is in the scope of SA3.

2. Upon receiving the request, the PIN server validates the PIN delete request and verifies the security credentials.

3. Upon successful authorization, the PIN server sends a successful delete response.

After the PIN is deleted which is indicated by PIN ID, the access control information in PEGC is also disabled and the PIN elements in this PIN can’t access to 5GS via PEGC anymore when the PIN is deleted. The PEGC may not be the gateway and for PIN element to access to 5GS for this PIN.

4. Before the PIN deleted, the PEMC notifies the PEGC of PIN delete that identified by PIN ID, and PEGC disables the 5GS connection permission and access control information for the PIN elements in this PIN.

5. Before the PIN deleted, the PEMC notifies the PIN elements in this PIN of PIN delete that identified by PIN ID. The PIN elements in this PIN can delete the information about this PIN, for example, the PIN profile.

##### 7.5.2.2.2 PIN delete triggered by PIN server

The PIN server can trigger the PIN delete procedure, for example, when the life cycle of PIN is end or the PIN server decides to stop the PIN service in this PIN.

Figure 7.5.2.2.2-1 illustrates PIN delete procedure based on request/response model.

Pre-conditions:

1. The PEMC in a PIN has been pre-configured or has discovered the address (e.g. IP address, FQDN, URI) of the PIN server;

2. The PIN has already been created and a PIN ID is distributed by PIN server;

3. The PEMC has been authorized to communicate with the PIN server;

4. A PIN client has already received the role of PEMC from PIN server;

5. It is assumed that PIN server manages the PIN life cycle;



Figure 7.5.2.2.2-1: Delete of PIN triggered by PIN server

1. An event occurs at the PIN server that satisfies trigger conditions for notifying a subscribed PEMC of a PIN. If the life cycle of a PIN is end or the PIN server decides to not provide any PIN service in this PIN, the PIN server should trigger a PIN delete procedure to the PEMC which manages the PIN.

2. The PIN server sends PIN delete notification to the PEMC. The PIN server includes the PIN ID, security credentials in the notification.

After the PIN is deleted which is indicated by PIN ID, the access control information in PEGC is also disabled and the PIN elements in this PIN can’t access to 5GS via PEGC anymore when the PIN is deleted. The PEGC may not be the gateway and for PIN element to access to 5GS for this PIN.

Editor's note: The access control information in PEGC should be coordinated with SA2.

3. Before the PIN deleted, the PEMC notifies the PEGC of PIN delete that identified by PIN ID, and PEGC disables the 5GS connection permission and access control information for the PIN elements in this PIN.

4. Before the PIN deleted, the PEMC notifies the PIN elements in this PIN of PIN delete that identified by PIN ID. The PIN elements in this PIN can delete the information about this PIN, for example, the PIN profile.

##### 7.5.2.2.3 PIN delete locally by PEMC

The PEMC can directly trigger the PIN delete procedure, for example, when the life cycle of PIN is end, without authorization from PIN server. After the PIN is deleted successfully, the PEMC updates the PIN status to PIN server.

Figure 7.5.2.2.3-1 illustrates PIN delete procedure based on request/response model.

Pre-conditions:

1. The PEMC in a PIN has been pre-configured or has discovered the address (e.g. IP address, FQDN, URI) of the PIN server;

2. The PIN has already been created and a PIN ID is distributed by PIN server;

3. The PEMC has been authorized to communicate with the PIN server;

4. A PIN client has already received the role of PEMC from PIN server;

5. It is assumed that PEMC manages or stores the PIN life cycle;



Figure 7.5.2.2.3-1: Delete of PIN locally by PEMC

0. The PEMC stores the lifecycle of PIN locally, and the lifecycle of PIN which indicated by PIN ID comes to the end.

1. The PEMC deletes the PIN which indicated by PIN ID locally, and the information in PIN profile related to this PIN is deleted too.

2. The PEMC indicates the PEGC to deactivate the access control information of this PIN. After the deactivation, the PINE in this PIN can’t access the 5GS any more.

3. The PEGC sends response to PEMC that the access control information has been deactivated successfully.

4. The PEMC sends requests to PINE in this PIN to delete the PIN profile related to this PIN that represented by PIN ID.

5. The PEMC sends a PIN status update notification to the PIN server to indicate the PIN has been deleted. In this notification, the PIN ID is included.

6. The PIN server responses to the notification.

7. The PIN server updates the PIN profile to remove the details of the PIN which represented by PIN ID.

## 7.6 Solution #5: PIN discovery

### 7.6.1 Architecture enhancements

The architecture of PIN is referred to the solution 1 in clause 7.

### 7.6.2 Solution description

#### 7.6.2.1 General

This solution addresses aspects of Key Issue #1.

For a certain PIN element, the PIN should be discovered and the PIN element can decide whether to join in the PIN. There are three situations that the PIN elements can discover the PIN as following:

- If the PIN elements can have an application layer communication with the PEMC which manages a PIN, the PIN elements can receive the PIN ID,PIN description and the PIN service that a PIN can provide, and decides whether to join the PIN;

- The PEGC can be set as open access and the PIN element can communicate with PIN server to receive the PIN ID,PIN description and the PIN service that a PIN can provide from PIN server via the PEGC.

#### 7.6.2.2 Procedures of PIN discovery

##### 7.6.2.2.1 Procedures of PIN discovery based on PEMC

Pre-conditions:

1. The UE Identifier or PIN client Identifier is available;

2. The PIN client has been authorized to communicate with the PEMC;

3. The UE or PIN client has already received the role of PEMC from PIN server;

If the PIN element has already had a communication connection with the PEMC, which managements of a PIN, the PIN element can receive the PIN ID, PIN description information and IP address of PEMC and decides whether to join the PIN.



Figure 7.6.2.2.2-1: Procedures of PIN discovery based on PEMC

1. The PIN element has already had an application layer connection with a PEMC which manages a PIN.

If the PIN client communicates with PEMC via WiFi provided by PEMC, the PEMC can identify the PIN elements by the account number and password that PEMC distributed and the PIN client ID, UE GPSI if available.

If the PIN client communicates with PEMC via Bluetooth provided by PEMC, the PEMC can identify the PIN elements by the PIN client ID, UE GPSI if available.

NOTE: The RAT (e.g. wifi) between the PIN client and the PEGC/PEMC is out of scope of SA6

2. The PIN client sends the PIN discovery request to PEMC. The PIN discovery request includes the security credentials of the UE or PIN client and may include the UE identifier such as GPSI if available, PIN client ID, UE location, the service that PINE wants to consume and PIN client profile(s) information

3. The PEMC performs an authorization check to verify whether PINE is allowed to perform the operation.

Editor's note: The authorization and authentication procedure should be defined in SA3 and wait for SA3 to reply.

4. The PEMC sends the PIN discovery response to PIN element including the configuration information of the PIN(s), which are offering the services requested by the PINE in the PIN discovery request. The configuration information includes PIN ID, PIN description (Human-readable description of the PIN, for example, the company name, location or the type of service) , services that each PIN can provide and the PEMC IP address.

The PIN client receives the configuration information and decides whether to join in the PIN.

##### 7.6.2.2.2 Procedures of PIN discovery with assistance of PIN server via PEGC

Due to for some of the PIN elements can have the application interaction towards the PEGC, for example, via WiFi or Bluetooth pairing, and the PIN element can have the communication with PIN server to receive the lists of PIN ID and corresponding PIN description information. And the PIN elements can decide whether to join in the PIN.

Figure 7.6.2.2.2-1 illustrates PIN server discovery via PEGC based on request/response model.

Pre-conditions:

1. The PIN elements or PIN client has application layer connection with PEGC;

2. The UE Identifier or PIN client Identifier is available;

3. The PEGC has been authorized to communicate with the PIN server;



Figure 7.6.2.2.2-1: PIN discovery via PEGC

1. (optional) The PIN element or PIN clients has already had the application layer connection towards PEGC. For example, the PIN elements can communicate with PEGC via WiFi or Bluetooth.

The PIN client can communicate with the PIN server via PEGC.

If the PIN client communicates with PEGC via WiFi provided by PEGC, the PEGC can identify the PIN elements by the account number and password that PEGC distributed and the PIN client ID, UE GPSI if available.

If the PIN client communicates with PEGC via Bluetooth provided by PEGC, the PEGC can identify the PIN elements by the PIN client ID, UE GPSI if available.

NOTE 1: The RAT (e.g. wifi) between the PIN client and the PEGC/PEMC is out of scope of SA6

NOTE 2: The PEGC can serve the PIN client which triggers the PIN discovery via relay PEGC.

2. The PIN client sends the PIN discovery request to PIN server. The PIN discovery request includes the security credentials of the UE or PIN client and may include the UE identifier such as GPSI, PIN client ID, UE location, the service that PINE wants to consume and PIN client profile(s) information.

The PIN client can have the filter information in the PIN discovery request for example, the interesting area, the interesting type of PIN and etc.

3. Upon receiving the request, the PIN server performs an authorization check to verify whether the PIN client has authorization to perform the operation.

4. The PIN server sends a successful response to PIN client, which includes the configuration information to PIN elements. The configuration includes PIN ID, PIN description (Human-readable description of the PIN, for example, the company name, location or the type of service) , services that each PIN can provide and the corresponding PEMC IP address.

## 7.7 Solution #6: PIN Profile

### 7.7.1 Architecture enhancements

The architecture of PIN is referred to the solution 1 in clause 7.

### 7.7.2 Solution description

#### 7.7.2.1 General

This solution addresses aspects of Key Issue #1.

For an established PIN, the PIN should have the profile or configuration information in PIN server, PEMC and PEGC.

Also the PIN server, PEMC and PEGC shall maintain the dynamic profile information related to the PIN which needs to be updated based on the events (e.g. PIN element joining or leaving, PIN element capability is changed) occuring in the PIN.

#### 7.7.2.2 PIN Profile in a PIN

Table 7.7.2.2.1-1: PIN Profile in PIN server, PEMC, PEGC and PINE

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Parameter Name | Parameter Description | PIN Server | PEMC | PEGC | PINE |
| PIN ID | The identifier of the PIN | Y | Y | Y | Y |
| PIN Description | Human-readable description of the PIN, for example, the company name, location or the type of service. | Y | Y | Y | Y |
| Duration | Specifies the time period of how long the PIN can be active | Y | Y | Y | Y |
| Maximum number of PIN elements | Maximum number of PIN elements allowed to join the PIN | Y | Y | N | N |
| PIN service | List of service that a PIN can provide, including the PINE service or the service that can provided by application client on PINE:  > PIN service Provider Identifier  > PIN service type  > PIN service Feature | Y | Y | N | Y |
| PEMC list | The list of identifiers of the PIN elements which can be allowed to take the role as PEMC (e.g.: PIN client ID, UE GPSI etc.,) and also it contains whether the role is primary or secondary | Y | Y | Y | Y |
| PEGC ID list | The list of identifiers of the PIN elements which can be allowed to take the role as PEGC (e.g.: PIN client ID, UE GPSI etc.,) | Y | Y | Y | Y |
| PIN Server ID | The identifier of the PIN server that serves the PIN | N | Y | Y | Y |
| PIN server Endpoint | Endpoint information (e.g. URI, FQDN, IP address) used to communicate with the PIN server. | N | Y | Y | Y |
| PIN Elements List | List of PIN elements which can be allowed to join the PIN  > PIN element ID | Y | Y | Y | N |

#### 7.7.2.3 Dynamic profile information of a PIN

Table 7.7.2.3-1 describes the list of parameters that are classified as dynamic profile information and which are maintained at the PIN server, PEMC and PEGC. Dynamic profile information maintained at these entities are updated based on the following events occurring in the PIN:

- PINE joins or leaves the PIN;

- Role of PEMC or PEGC changes;

- When the services offered by the PIN changes;

- When a PINE updates the services it offers;

- When a PINE joins or leaves the PIN;

Table 7.7.2.3-1: Dynamic profile information of a PIN

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Parameter Name | Parameter Description | PIN Server | PEMC | PEGC |
| PIN ID | The identifier of the PIN | Y | Y | Y |
| PIN Description | Human-readable description of the PIN, for example, the company name, location or the type of service. | Y | Y | Y |
| Services offered | List of services offered by the PIN | Y | Y | N |
| Duration | Time period specifying how long the PIN can be active |  |  |  |
| PEMC list | The list of identifiers of the PIN elements which are currently serving as PEMC (e.g.: PIN client ID, UE GPSI etc.,) and whether the PEMC is authorized as primary PEMC or secondary PEMC | Y | Y | Y |
| > PEMC Endpoint | Endpoint information of each PEMC (e.g. URI, FQDN, IP address) used to communicate with the PEMC. |  |  |  |
| > Duration | Time period of being PEMC |  |  |  |
| PEGC list | The list of identifiers of the PIN elements which are currently serving as PEGC (e.g.: PIN client ID, UE GPSI etc.,) | Y | Y | Y |
| > PEGC Endpoint | Endpoint information of each PEGC (e.g. URI, FQDN, IP address) used to communicate with the PEGC. |  |  |  |
| > Duration | Time period of being PEGC |  |  |  |
| > PEGC Supported KPIs | KPIs supported by this PEGC (e.g., maximum number of assigned PIN elements) | Y | Y | Y |
| > PEGC Schedule | Scheduled times when this PEGC is available to service PIN elements (e.g., time window). | Y | Y | Y |
| > PIN Elements details | List of PIN elements being served by PEGC and their connectivity information |  |  |  |
| PIN Server ID | The identifier of the PIN server that serves the PIN | N | Y | Y |
| PIN server Endpoint | Endpoint information (e.g. URI, FQDN, IP address) used to communicate with the PIN server. | N | Y | Y |
| PIN Elements List | List of PIN elements currently registered/joined the PIN | Y | Y | N |
| > PIN Element ID | Identifty of the PIN element |  |  |  |
| > Services offered | Services offered by the the PIN element |  |  |  |
| > Reachability information | Reachability information of the PIN element |  |  |  |
| > Application List | List of application clients for this PIN element including:  > Minimum KPIs required by each application client to operate effectively within the PIN (e.g., PIN bandwidth, PIN request rate, PIN response time)  > Operational schedules of each application client (e.g., time windows) | Y | Y | Y |
| > Default PEGC | Identifier of the default PEGC authorized to service this PIN element. The PIN element will use this PEGC as the primary PEGC to relay PIN communications. Location and/or schedule information for the default PEGC may also be included such that the default PEGC may be selected by the PIN element based on its current location and proximity to the default PEGC and/or the availability schedule of the default PEGC. | Y | Y | Y |
| > Backup PEGCs List | Identifiers of backup PEGCs authorized to service this PIN element. The list is in prioritized order (the first PEGC listed will serve as the first backup PEGC). If the default PEGC is not available, the PIN element will use this prioritized list of PEGCs to relay PIN communications.Location and/or schedule information for each of the backup PEGCs may also be included such that a backup PEGC may be selected by the PIN element based on its current location and proximity to a backup PEGC and/or the availability schedule of the PEGC. | Y | Y | Y |

#### 7.7.2.4 PIN client profile

Table 7.7.2.4-1 describes the list of PIN element maintained by a PIN client. These parameters are exchanged between the PIN client and PEMC (e.g., when the PIN client is joining or registering to the PIN). Depending on the parameter, the PIN client or the PEMC may configure the value of the parameter during the PIN client and PEMC exchange.

Table 7.7.2.4-1: PIN Client Profile

|  |  |  |
| --- | --- | --- |
| Parameter Name | Status | Parameter Description |
| PIN ID | M | The identifier of the PIN where the PIN client is joined |
| UE identifier | O | PIN Element or UE identifier |
| PIN client ID | M | The unique identity of the PIN client within PIN |
| Name of the device | O | Human-readable name of the device (i.e. door sensor, watch, smart TV, etc) along with manufacturer details |
| Access control information | O | Used for PINE to access the network provided by PEGC. Used for PEGC to control the PINE to access 5GS. Each PIN may be associated with different access control information.  > user name, account, SSID, BSSID |
| Application List | O | List of application identities |
| > Application Identity | O | Identity of the application |
| > Application schedule | O | Operational schedules of each application (e.g., time windows) which the |
| > Application KPIs | O | Minimum KPIs required by each application to operate effectively within the PIN (e.g., PIN bandwidth, PIN request rate, PIN response time) |
| capabilities | M | capabilities of the PIN client like supports relay capability for other PIN elements |
| Visibility | M | Determines whether this PIN element is discoverable by other PIN elements within PIN, discoverable by other UEs outside the PIN etc., |
| access type | M | Access type supported for the communication |
| Layer-2 details | O | Layer-2 address of the PIN element |
| Required services | O | Identifies the list of services the PINE wants to consume |
| Supported services | O | Identifies the list of services the PINE is providing and allowed to be accessed |
| Default PEGC | MO | Identifier of the default PEGC assigned by the PEMC to the PIN element. The PIN element will use this PEGC as the primary PEGC to relay PIN communications. Location and/or schedule information for the default PEGC may also be included such that the default PEGC may be selected by the PIN element based on its current location and proximity to the default PEGC and/or the availability schedule of the default PEGC. |
| Backup PEGCs list | O | Identifiers of backup PEGCs assigned by the PEMC to the PIN element. The list is in prioritized order (the first PEGC listed will serve as the first backup PEGC). If the default PEGC is not available, the PEGC will use this prioritized list of PEGCs to relay PIN communications. Location and/or schedule information for each of the backup PEGCs may also be included such that a backup PEGC may be selected by the PIN element based on its current location and proximity to a backup PEGC and/or the availability schedule of the PEGC. |

### 7.7.3 Solution evaluation

This solution captures the details of the information that needs to be maintained at the each entities that are part of the PIN. PIN profile and PIN dynamic profile information are maintained at the PIN server, PEMC and PEGC. PIN profile information is maintained till the life time of the PIN i.e., until it is deleted. PIN dynamic profile information is maintained till the PIN is in active state and it is updated based on the events occuing in the PIN. PIN elements sends the PIN client profile while joining or registering to the PIN.

## 7.8 Solution #7: PIN server discovery

### 7.8.1 Architecture enhancements

The architecture of PIN is referred to the solution 1 in clause 7.

### 7.8.2 Solution description

#### 7.8.2.1 General

This solution addresses aspects of Key Issue #1.

Before the PEMC triggers the PIN establishment, or the PEMC triggers PIN modification or PIN delete, a certain PIN server should be discovered. The PIN server is responsible to perform the request of PIN create, PIN modification and PIN delete from PEMC of a PIN.

Due to the PIN server in a PLMN can be multiple, so it is important to PIN elements to discover the appropriate PIN server to connect.

#### 7.8.2.2 Procedures of PIN server discovery

##### 7.8.2.2.1 Procedures of PIN server discovery based on receiving PIN server endpoint information

The aim of PIN server discovery procedure is to receive one or more endpoint information (e.g. URI(s), FQDN(s), IP address(es)) of PIN server. And the PEMC, PEGC, PIN elements are all able to receive the PIN server endpoint information.

The PIN server can be discovered by the following method:

- pre-configured in the PIN elements or PIN clients;

- configured by the user;

- provisioned by MNO through 5GC procedure; or

- derived from HPLMN identifier for non-roaming scenario or from VPLMN identifier for roaming scenario.

It may be possible to provide the PIN server endpoint information to the PIN client or PIN elements from the 5GC. If the PIN server endpoint information is provided by 5GC and available at the PEMC, the PEMC shall use the information for the PIN management procedure (e.g.: PIN creation/modification/delete).

Otherwise, the PEMC shall use pre-configured PIN server endpoint information for PIN management procedure if pre-configured PIN server endpoint information is available in PEMC.

##### 7.8.2.2.2 Procedures of PIN server discovery via PEGC

Due to for some of the PIN elements can have the application interaction towards the PEGC, for example, via WiFi or Bluetooth pairing, so the PEGC can provide the PIN server end point information to PIN elements.

For some of the PEGC, it has the open access capability to accept the application layer connection from the PIN elements.

Figure 7.8.2.2.2.-1 illustrates PIN server discovery via PEGC based on request/response model.

Pre-conditions:

1. The PIN elements or PIN client has application layer connection with PEGC;

2. The UE Identifier or PIN client Identifier is available;



Figure 7.8.2.2.2-1: PIN server discovery via PEGC

1. The PIN element or PIN clients has already had the application layer connection towards PEGC. For example, the PIN elements can communicate with PEGC via WiFi or Bluetooth. The PINE can also have the open access to PEGC that with no user name or password. For this situation, the PINE can’t consume the communication service that provided by PEGC, but can have communication with the PEMC behind the PEGC.

2. The PINE sends PIN server discovery request to PEGC. The requests include the GPSI, MAC address, if has, UE location.

3. The PEGC can directly deliver the PIN server end point information to PIN elements or PIN client. The end point information of PIN server includes URI(s), FQDN(s), IP address(es)) of PIN server.

4. If the PINE has open access to PEGC, that the PEGC should route the request to PEMC that behind the PEGC.

5-6. The PEMC delivers the PIN server end point information to PIN elements or PIN client via PEGC. The end point information of PIN server includes URI(s), FQDN(s), IP address(es)) of PIN server.

##### 7.8.2.2.3 Procedures of PIN server discovery from PEMC

Due to for some of the PIN elements can have the application interaction towards the PEMC, for example, via WiFi or Bluetooth pairing, so the PEMC can provide the PIN server end point information to PIN elements.

Figure 7.8.2.2.3-1 illustrates PIN server discovery from PEMC based on request/response model.

Pre-conditions:

1. The PIN elements or PIN client has application layer connection with PEMC;

2. The UE Identifier or PIN client Identifier is available;



Figure 7.8.2.2.3-1: PIN server discovery via PEGC

1. The PIN element or PIN clients has already had the application layer connection towards PEMC. For example, the PIN elements can communicate with PEMC via WiFi or Bluetooth.

2. The PINE sends PIN server discovery request to PEMC. The requests include the GPSI, MAC address, UE location.

3. The PEMC delivers the PIN server end point information to PIN elements or PIN client. The end point information of PIN server includes URI(s), FQDN(s), IP address(es)) of PIN server. 7.9 Solution #8: Service switch in a PIN

## 7.9 Solution #8: Service switch in a PIN

### 7.9.1 Architecture enhancements

The architecture of PIN is referred to the solution 1 in clause 7.

### 7.9.2 Solution description

#### 7.9.2.1 General

This solution addresses Key Issue #3. The principles of this solution are:

- The PIN Application Client in UE can discover or get notified about available PINs where an application service can be switched to.

- Once the PIN Application Client selects the PIN, it can request that the PIN Server trigger service switch procedure and obtain the necessary information for performing the service switch from the PIN Server.

- The PIN server can identify the PIN Applications in PINE, where the service can be split and terminated.

- The PIN Server instructs PIN Management Client to execute service switch procedure.

- The PIN Management client configures PIN Gateway client and PINEs for service switch.

- The PIN Gateway client uses the configuration information from the PIN Management Client to configure the PEGC which implements service switch function.

#### 7.9.2.2 Procedure

This procedure presents a high-level overview of Solution #1.

##### 7.9.2.2.1 Functional entities

PIN Application Client: A PINAPP function in UE, PINE, which initiates discovery, service switch, configuration.

PIN Management Client: A PINAPP in PEMC, configures PEGC and PINE for service switch.

PIN Gateway Client: A PINAPP in PEGC, obtains configuration from PEMC and executes service switch.

PIN Server: Supports PIN Application Client by providing PIN information and executes service switch procedure when requested by PIN Application Client.

##### 7.9.2.2.2 Procedures of PIN Service Switch

Figure 7.9.2.2.2.-1 illustrates a discovery and service switch procedure based on request/response model.



Figure 7.9.2.2.2-1: PIN Service Switch

Pre-conditions:

- The PIN Client in UE has been pre-configured or has discovered the address (e.g. IP address, FQDN, URI) of the PIN server;

- The PIN Client in UE has been authorized to communicate with the PIN server;

- The PIN Management Client supports functionality to execute the service switch procedure;

- The PIN Gateway Client supports functionality to execute the service switch procedure;

- The PIN Server has capability to communicate with Application server to identify application session and provide information about any changes to the end points of the session;

- There is an ongoing application session from AS to UE.

1. A PIN Client in a UE, triggered by an Application Client, sends a discovery request to a PIN Server. The purpose of the discovery request is to discover a PIN that can support a certain application in a certain location. The discovery request includes Location information, Application requirements such as Display characteristics, Audio characteristics, etc. The PIN Client can also subscribe to be notified when a PIN is available in a location and can support the application requirements.

2. The PIN Server based on Location and application service requirement can send a notification to the PIN Client with the following information: discovered PIN ID, details of PINAPP capabilities and corresponding PE IDs, such as Device ID, IP address and Port number. PIN Client forwards the information to Application Client in UE.

3. The Application Client in UE initiates service switch with the PIN Client, which sends a "Service switch request" to the PIN Server with information about the service to be switched. The information about the service to be switched includes Application session ID, Destination PIN ID, and an IP 4 Tuple that describes the session. The IP 4 tuple may include the IP Address of the UE, the IP Address of the Server that provides the service, and the UE port numbers that are associated with the service, and the port numbers on the server that are associated with the service. The PIN Server accepts the request and informs the Application Client.

4. PIN Server sends the "Switch Application Session" request to the PIN Management Client. The request includes information such as

- The Application Session Id,

- The, Destination PINE: PE IDs (1..N), can include IP address, Port number, URL etc.

- If the Application session needs to be split among multiple PINEs (i.e. split into sub-flows), it is indicated by setting the flag SPLIT == FALSE or TRUE. SPLIT can be set to TRUE only if the request includes multiple PINEs.

- The IP 4 Tuple

- Security related information elements required to successfully transfer the session context.

NOTE: Security related information elements are in the scope of SA WG3

5. The PIN Management Client starts configuring PEGC by sending "Configure Service Switch" to PIN Gateway Client, which includes:

- The Session ID

- Destination PINE information, which is a list of PEID, IP address, Port number or URL, where the sub-flows will be terminated.

- The flag SPLIT is set to TRUE or FALSE, if the session needs to be split to multiple PINEs and more than one PINE information is included in the TerminatingPineList. It can also include information about PINE to sub-flow mapping.

6. The PIN Management Client also configures PINE to prepare for terminating application session. The configuration information is sent to the PIN Client and Application Client in PINE.

7. The PIN Management Client responds to PIN server to indicate that configuration of PEGC and PINE has happened successfully, with information such as

- The Terminating PEGC ID and

- The Terminating PEGC reachability information, such as IP address, port number, URL etc.

- The Terminating Destination PINE reachability information, such as IP address, port number, URL etc.

8. PIN Server informs Application Server to switch the application session to a new destination IP address. PIN Server provides information such as:

- Application Session ID: identifies the application session to be switched to new end point

- Term IP Address: IP address of the PEGC where the application session will be terminated.

9. PIN Gateway Client interacts with the AS, to get authorized by the AS for the service switch, by sending the information from Step 4. This authorization operation is in the scope of SA WG3. Once authorized, the TCP session up continues between the PEGC and the AS.

10. The PEGC may trigger a PDU Session Modification procedure in order to obtain QoS Rules for the new flow. PEGC can setup paths with one or more PINEs to split the main session flow into sub-flows. PEGC can also interact with PIN Server to maintain synchronization among the sub-flows.

11. Once the path from PINE Application Client to AS is available, Application Client can use application level mechanism to pull video stream, play and again pull.

### 7.9.3 Solution evaluation

This solution addresses KI#3 about "How to support application mechanism for service switching in a PIN between different PIN applications for achieving better service experience".

The application-level mechanism described here allows the Application server, PEGC and PINEs to become aware of the new endpoints to execute service switch. Based on these information, PINE, PEGC, 5GS and Application Server executes session setup, modify procedures.

## 7.10 Solution #9: PINAPP role change

### 7.10.1 Architecture enhancements

The architecture of PIN is referred to the solution 1 in clause 7.

### 7.10.2 Solution description

#### 7.10.2.1 General

This solution addresses Key Issue #6.

A UE that is serving the role of a PEGC for a PIN leaves the coverage area of the PIN. The PEMC detects that the UE has left the coverage area of the PIN and makes a request to the PIN server to select a new PEGC.

#### 7.10.2.2 Procedure

Pre-conditions:

1. The PIN server has authorized the PEMC to create PINs.

2. The PEMC creates a local PIN with members: PEMC, UE serving as PEGC, PINE1, and PINE2.

3. The PEMC maintains a PIN profile with information of capabilities for each PIN member.

4. PINE2 is a PIN member that also has gateway capability.



Figure 7.10.2.2-1: PINAPP Role Change

1. The UE leaves the local coverage area of the PIN.

2. The PEMC detects that the UE is no longer providing the PEGC service. For example, the PEMC may not be getting responses from the UE or either PINE1 or PINE2 has informed the PEMC that PIN routing via the UE is not available.

NOTE: A corresponding event subscription/ notification is to be specified in the normative phase to enable this detection.

3. The PEMC sends a PIN role change request to the PIN server to select a new PEGC. The request includes the PIN ID, the PEMC ID, the UE ID or the PEGC ID for the UE, the ID of a PIN member that can serve as the new PEGC (e.g. PINE2), and a timestamp.

4. The PIN server considers which member of the PIN can serve as the new PEGC, including the PIN member the PEMC provided, and selects a PIN member to serve as the new PEGC. The PIN server sends a response to the PEMC with the status of the request, the ID of the new PEGC, and PIN traffic routing rules for the role change. The PIN server may also inform the PEMC to notify other PIN members of the PEGC role change.

5. The PIN server delivers management information to PINE2 to inform PINE2 to serve as the new PEGC. The management information includes PIN traffic routing rules that PINE2 would need to make routing decisions.

6. The PEMC notifies other members of the PIN that PINE2 will serve as the new PEGC. The PEMC includes the contact information of PINE2 and traffic routing rules that may be applicable to each member.

### 7.10.3 Solution evaluation

This solution addresses KI #6 on PEMC/PEGC replacement in PIN. The PEGC of the PIN leaves the coverage area of the PIN and PEMC detects that PIN gateway functionality is not available. The PEMC makes a request to the PIN server to assign a new PEGC for the PIN. The PIN server assigns PINE 2 as the new PEGC and provides PINE 2 with management information to route traffic for the PIN. PEMC notifies the other members of the PIN that PINE 2 is the new PEGC.

The solution provides a procedure for role change of PEGC to ensure PIN routing is available for the PIN if the PEGC is not available.

## 7.11 Solution #10: Service switch internal PIN

### 7.11.1 Architecture assumptions

The architecture assumptions of Solution #1 are also assumed in this solution.

### 7.11.2 Solution description

#### 7.11.2.1 General



Figure 7.11.2.1-1: PIN Service Switch internal PIN

In Figure 7.11.2.1-1, it describes the service switch scenario.

The PINE A has the application communication with application server. And when the PINE A decides to select other alternative PINE B to apply the traffic flow, the PINE A firstly should discover a PIN and join in. And then, in the PIN, there should exist the PINE that can be hosted with the same service type as PINE A, for example, the video flow, music flow or game flow.

The PINE A can send the request to PEMC to determine the PINE B to host the application traffic. After the determination, the PEMC sends the endpoint information to PINE A and the PINE A can offload the traffic either directly to PINE B or via PEGC.

#### 7.11.2.2 Procedure of service switch internal PIN

Pre-conditions:

1. The UE Identifier or PIN client Identifier of PINE A or PINE B is available;

2. The PIN client in PINE A or PINE B has been authorized to communicate with the PEMC;

3. The PIN client in PINE B can provide the same PIN service as PINE A’s traffic flow.



Figure 7.11.2.2-1: Service switch procedure internal PIN

0. The PINE A has application layer communication with application server. And the PINE A decides to do the service switch to other PINEs. And the PINE A has already been in a PIN.

1. The PINE A trigger the PIN service discovery procedure towards PEMC. This request carries the list of services the PINE wants to consume.

2. Upon receiving the request, the PEMC performs an authorization check to verify whether the PINE A has authorization to perform the operation.

Editor's note: The authorization check needs SA3 for feedback.

3. The PEMC provides the list of PINE endpoint(s), application client endpoint(s) information that are offereing the requested services to PINE A. The PIN service can be represented by service type that PINE provides or the application client on PINE. If the request fails, the PEMC should give the failure response to indicates the cause of request failure.

4. The PINE A determines the PINE B for service switch as follow:

Option A: The PINE A maintains the service towards AS and the service corresponds to a service type, for example, music or streaming media. The PINE A determines the potential PINE B for service switch according to whether this PINE has the capability to carry the service.

Option B: The PINE A maintains the service towards AS by application client which represented by Application Client ID. The PINE A determines the potential PINE B for service switch according to whether this PINE has deployed the same application client as PINE A.

5. (Use PINE B as example) The PINE A has two options to switch the service traffic to PINE B:

Option A: Step 5a, the PINE A switches the traffic flow directly to PINE B via direct communication or via PEGC, just like the projection.

Option B: Step 5b, the PINE A relocates the application context from application client in PINE A to application client in PINE B. After the context relocation, the application client in PINE A triggers the application relocation to PINE B. If the PIN client in PINE A or PIN client in PINE B can directly communicate with AS, the application client behaviour in step 5b is replaced by PINE A/B.

### 7.11.3 Solution evaluation

This solution addresses KI#3 about " How to support application mechanism for service switching in a PIN between different PIN applications for achieving better service experience ".

This solution relies on the PEMC to select the potential PINE for service switch according to the service type.

## 7.12 Solution #11: Application Server Discovery in a PIN

### 7.12.1 Architecture enhancements

The architecture of PIN is referred to the solution 1 in clause 7. Additionally, this solution introduces a PIN-11 reference point.

PIN – 11: The interactions related to enabling PINAPP, between an AS and PIN Management Client.

As shown in solution 1 in clause 7, the solution assumes a PIN-9 interface between the AS and PIN Server and a PIN-6 interface between the PIN Management Client and the PIN Server. The PIN-11 interface may be an extension so these interfaces (i.e. may re-use certain operations).

### 7.12.2 Solution description

#### 7.12.2.1 General

This solution addresses aspects of Key Issue #4.

One or more PINAPP(s) (e.g. in a PEMC or in a PIN server) can maintain a registry to manage information about AS(s) that are available to the PIN. The AS(s) register their availability with the PINAPP.

The PINAPP(s) can update the PIN Server with information about the registry. The information about the registry can include the PIN ID, the PIN Location and an address (e.g. URL) of the PINAPP registry.

The PINAPPs provide information from the registry to other PINAPPs about available AS(s).

Application clients in a PINE can be provisioned with contact information for the PINAPP registry. Alternatively, Application clients can obtain contact information for the PINAPP registry by querying a PIN Server.

Application clients can query the PINAPP registry for information about an AS. If the query cannot be resolved, it can be forwarded to another PINAPP.

#### 7.12.2.2 Procedure

This procedure presents a high-level overview of Solution #11.

##### 7.12.2.2.1 Functional entities

PINAPP: A PIN function, which can maintain information about AS(s) available to a PIN. The AS information can include Location and address (e.g. URL).

PIN Server: The PIN Server can maintain information about PINAPPs including PINAPPs, which maintain AS registry functionality.

PIN Application Client: Application clients running in PINE.

##### 7.12.2.2.2 Procedures of PIN Application Server Discovery

Figure 7.12.2.2.2.-1 illustrates an initial provisioning and AS discovery procedure based on request/response model.

Pre-conditions:

- The PINAPP with an AS registry has been pre-configured or has discovered the address (e.g. IP address, FQDN, URI) of the PIN Server.

- The PINAPP with an AS registry has been authorized to communicate with the PIN server.

- The PINAPP with an AS registry supports functionality to maintain a registry of AS(s). The PINAPP with an AS registry can be deployed in PEMC. When the AS Registry is in the PEMC, and AS interacts with the PIN Management Client via the PIN-11 reference point.

- The PIN Server also supports functionality to maintain a registry of AS(s).

- The PIN Server supports functionality to maintain information about PINAPPs which support an AS Registry (i.e. the PIN Server knows which PINAPPs support AS Registry Functionality).



Figure 7.12.2.2.2-1: PIN AS Discovery

1. A PIN has been successfully created. An AS registers with the PINAPP by sending information such as: AS name, InstanceID, and address (e.g. URL). The AS can be deployed anytime and can update its registration information in the PINAPP by sending a new Registration message. The PINAPP stores the AS information in its registry.

2. The PINAPP updates the PIN Server by sending the PIN Server information from its registry.

3. If the PIN Server’s registry has information from AS(s) that are not in the PINAPP’s registry, then the PIN Server can also update the PINAPP with information about AS(s) that are stored in the registry of the PIN Server. Furthermore, the PIN Server can configure the PINAPP with Usage Policies for the AS(s) that are in the PINAPP’s registry. The Usage Policy can indicate what types of Application Clients may discover the AS, the identity of Application Client(s) that may discover the AS, and times of day when the AS is available.

4. An Application Client, which wants to discover an AS, requests information from the PIN Server about how to reach the registry functions.

5. The PIN Server sends the Application Client information about the registry function PINAPP (e.g. a URL).

6. The Application client sends a Query for the PINAPP in order to obtain contact information for an AS. The query includes the name of the AS that the application client wants to contact.

7. If the query can be resolved, PINAPP responds with an address of the AS (e.g. URL).

8. If the query cannot be resolved, PINAPP forwards the query to PIN Server.

9. PIN server responds to Application Client with the details of the AS (e.g. URL).

After the procedure above, Application Client in a PINE can start interacting with the AS.

### 7.12.3 Solution evaluation

This solution addresses KI#4 about " How to enable discovery of Application Server, connected to a PIN, by Application Clients running in the same PIN?".

A PINAPP, which maintains AS information, helps Application Clients discover AS(s). The PINAPP can be discovered by PIN Application clients. In certain situations, if an AS is not found in the PINAPP, information can be fetched from other PINAPP(s) (e.g. a PIN Server).

This solution allows flexibility in deploying AS(s) because new AS instances can store their information in registries so that they can be discovered.

## 7.13 Solution #12: PEMC registration to PIN server

### 7.13.1 Architecture enhancements

The architecture of PIN is referred to the solution 1 in clause 7.

### 7.13.2 Solution description

#### 7.13.2.1 General

This solution addresses aspects of Key Issue #1.

Before the PEMC triggering the creation of PIN to network, the PEMC (for example, the UE) should receive the role of PEMC first from network. Only the PEMC can trigger creation of PIN.

PEMC (PIN Element Management Control) is a PIN Element with Management Capability. A PIN Element with Management Capability is a PIN Element that provides a means for an authorised administrator to configure and manage a PIN. Only after the PINE becoming the PEMC, the PINE can trigger the PIN create request to network.

At the network side, a PIN server should be deployed. The PIN server is responsible for the authorization of the request of the role of PEMC from PINE. The PIN server has this verification procedure with 5GC, which the procedure is defined in SA2 specification.

And the PINE/PEGC should also have the registration procedure to PIN server. For the PINE and PEGC registration, in order to reduce the signal interaction, it can be accomplished by the PEMC. The registration of PINE/PEGC includes the Device Metadata includes MAC address, vendor name, device description, PINE/PEGC Address.

#### 7.13.2.2 Procedures of PEMC registration

Pre-conditions:

1. The PEMC has been pre-configured or has discovered the address (e.g. IP address, FQDN, URI) of the PIN server;

2. The UE Identifier or PIN client Identifier is available;

3. The PEMC has been authorized to communicate with the PIN server;

Figure 7.13.2.2.2.-1 illustrates service provisioning procedure based on request/response model.



Figure 7.13.2.2.2-1: PEMC requests to register on PIN server

1. The PEMC sends Registration Request (GPSI) to the PIN server. The service provisioning request includes the security credentials of the PEMC received during authorization procedure and may include the GPSI. The registration request carries the PIN ID of the PIN for which it is intending to register as PEMC and the PIN element may indicate whether it is to be assigned with primary or secondary PEMC role.

2. The PIN server interacts with the 5GS to check whether the UE identified by the GPSI has subscribed to be a PEMC. If subscribed, it checks the PIN profile whether the requesting PIN element can be assigned with primary or secondary role and authorize the PIN element accordingly. In case if the PIN has already been created, the requesting PIN element is assigned with the secondary PEMC role irrespective of the role requested by the PIN element.

Editor's note: whether and how to 5GS check the UE identified by the GPSI has subscribed to be a PEMC is in SA2 scope.

3. The PIN server responds to the PEMC with allocated PEMC ID in successful response. If the registration procedure fails, the PIN server should give the failure response to indicates that indicates the cause of registration request failure.

#### 7.13.2.3 Procedures of PINE/PEGC registration

Pre-conditions:

1. The PEMC has been pre-configured or has discovered the address (e.g. IP address, FQDN, URI) of the PIN server;

2. The UE Identifier or PIN client Identifier is available;

3. The PEMC has been authorized to communicate with the PIN server;

4. The PINE/PEGC has already received the IP address of PEMC.



Figure 7.13.2.3-1: PINE/PEGC register on PIN server

1. The PINE/PEGC sends Registration Request (Device Metadata) to the PEMC. The Device Metadata includes the information that related to PINE/PEGC, including MAC address, vendor name, device description, PINE/PEGC Address.

2. The PEMC sends Registration Request (PEMC ID, Device Metadata) to the PIN server.

3. The PIN server responds to the PEMC with the allocated PINE/PEGC ID in successful response.

4. The PEMC sends Registration Response (PINE ID) to the PINE/PEGC.

## 7.14 Solution #13: SEAL enabled PINAPP architecture and PIN management

### 7.14.1 Architecture assumption

The Figure 7.14.1-1 shows the SEAL based application architecture for enabling PINAPP.



Figure 7.14.1-1: SEAL based PINAPP architecture

The following difference is applied compared with Sol#1.

- The UE also has a SEAL group management client, and the PIN client interact with the SEAL group management client via the GM-C to achieve PIN management;

- The PIN server interacts with the SEAL group management server via the GM-S reference point to accomplish PIN management;

- The SEAL group management client in the PEGC and PEMC interacts with the SEAL group management server via GM-UU;

- The SEAL group management client in the PIN element interacts with the SEAL group management client in the PEMC via the GM-X/GM-Y which is over the non-3GPP RAT.

- The PIN is the VAL group, and the PIN elements is the group member.

Editor's Note: The relationship between GM-X/GM-Y and PC5 is FFS.

### 7.14.2 PIN creation

The SEAL group management client at the PEMC, or the PIN server triggers the PIN creation (e.g., add PIN elements to the PIN or remove PIN elements from the PIN) as described in clause 10.3.3 of 3GPP TS 23.434. The SEAL group management client at the PEMC

### 7.14.3 PIN update

The SEAL group management client at the PEMC, or the PIN server triggers the PIN update as described in clause 10.3.5.2 of 3GPP TS 23.434.

The PIN elements initiates to join the PIN as described in the clause 10.3.8 of 3GPP TS 23.434.

The PIN elements initiates to leave the PIN as described in the clause 10.3.9 of 3GPP TS 23.434.

### 7.14.4 PIN deletion

The SEAL group management client at the PEMC, or the PIN server triggers the PIN deletion as described in clause 10.3.13 of 3GPP TS 23.434.

### 7.14.5 PIN discovery and PIN element discovery

The SEAL group management client at the PIN element discovers the PIN from the server as described in clause 10.3.8 (i.e., the group announcement in step 5) and clause 10.3.11 of 3GPP TS 23.434.

The SEAL group management client at the PIN element discovers the PIN element from the server as described in clause 10.3.4 of 3GPP TS 23.434.

## 7.15 Solution #14: PIN communication via 5GS

### 7.15.1 Architecture enhancements

The architecture of PIN is referred to the solution 1 in clause 7.

### 7.15.2 Solution description

#### 7.15.2.1 General

This solution addresses aspects of Key Issue #2.

For a certain PINE, it has the subscription whether the PINE has the permission to use 5GS to communicate.

As a feature indicated in SA1 and KI#2, the PIN client within a PIN can communicate with other devices, services and applications within the same PIN. Furthermore, PIN client can connect the 5G Network via a PEGC. Also, as a feature, some of the PIN client in PIN has the permissions that they can communicate with other UE or application outside of PIN with the help of 5GC.

In this solution, the PINE establishes direct connection with PEGC first. The PINE connects to PEGC via the password or username which is used for PINE to initial connect.

And then, the PINE sends the relay request to PEMC or PIN server, to relay the traffic to other PINE via PEGC by 5GS. If the request is related to internet services, the DN-specific ID may be included.

The PEMC requests to activate the relay request to PIN server and the PIN server can request the 5GS to establish the PDU session which is the procedure defined in SA2. The PIN server sends the parameters in relay request to 5GS to request to establish the PDU session.

And according to the SA1 requirement of PIN, the TS 22.101 specifies that 5GS supports secure provisioning of credentials to a non-3GPP device via a gateway UE, whose User Identifier has been linked with the 3GPP subscription of the gateway UE, to enable the non-3GPP device to access the network and its services according to the linked 3GPP subscription when connected via non-3GPP access. So, the PIN server also supports to deliver the security credentials to PINE via application layer procedure with the support of 5GS network.

Another way to configure PIN of 5GS communication is, the PEMC commands a PEGC to configure the allowed/disallowed traffic flow and corresponding requested QoS if allowed. And the PEGC triggers the PDU session establishment or modification towards 5GS, which is the conclusion reflected in TR 23.700-88[4]. The information of PEMC commands PEGC is the same as the PIN server trigger QoS establishment procedure.

#### 7.15.2.2 Procedures of PIN communication via 5GS

This procedure presents a high-level overview of Solution 1.

Figure 7.15.2.2-1 illustrates PIN communication via 5GS procedure based on request/response model.

Pre-conditions:

1. The PINE is able to connected into PEGC via password and username;

2. The UE Identifier or PIN client Identifier is available for PINE;

3. The PIN client has been authorized to communicate with the PIN server and PEMC;

4. The PINE has the subscription that it can communicate via 5GS;

5. The PINE has already received the IP address of other PINE.

NOTE: How to PINE receive the other PINE IP address are related to the procedure in section 7.3.2.3.



Figure 7.15.2.2-1: PIN communication via 5GS

0. The PINE establishes direct connection with PEGC. The PINE connects to the PEGC by means of the password and username, as indicated in section 7.3.2.2 of solution 2.

1. The PINE sends PINE 5GS connection request (PIN ID, PINE ID, Packet filters, [DN-specific ID]) to the PEGC. If the request is related to internet services, the DN-specific ID may be included. The packet filters include the target PINEs IP address or FQDN that wants to communicate. The PINE should discover the other PINE’s IP address first.

2. If step 2 is performed, the PEGC sends the PINE 5GS connection request to the PEMC directly, or sends PEMC Notification (PEGC ID, PINE 5GS connection request) to PIN server and PIN server sends PEMC Event Notification (PEGC ID, PINE 5GS connection request) to the PEMC.

3. The PEMC sends PINE 5GS connection request (PIN ID, PEMC ID, PEGC ID, PINE ID, Packet filters) to the PIN server. The request will be sent to other PINE via 5GS.

4. The PIN server will check with the 5GS that whether this PINE has the subscription to communicate with other PINE via 5GS. And if the PINE has the subscription, the PIN server will interact with 5GS to create/update the QoS flow of PEGC for the PINE.

Editor's note: How to the PIN server interacts with 5GS to establish PDU session for PINE is in SA2 scope.

5. (Optional) If the IP address of the PEMC/PEGC is changed, the PEMC/PEGC sends Event Notification (PEMC/PEGC ID, old IP address, new IP address) to the PIN server.

6. The PIN server sends response to PEMC for successfully establish the PDU session.

7. The PEMC sends response to PINE.

#### 7.15.2.3 Procedures of credential provisioning to PINE via 5GS

Pre-conditions:

1. The PINE is able to connected into PEGC via password and username;

2. The UE Identifier or PIN client Identifier is available for PINE;

3. The PIN client has been authorized to communicate with the PIN server and PEMC;

4. The PINE has the subscription that it can communicate via 5GS;



Figure 7.15.2.3-1: Credential Provisioning by 5GS

0. The PINE establishes direct connection with PEGC. The PINE connects to the PEGC by means of the password and username, as indicated in section 7.3.2.2 of solution 2.

1. The PINE sends Credential Provisioning Request (PIN ID, PINE ID, Duration) to the PEGC. The Duration indicates the lifetime of the path for the remote provisioning.

2. The PEGC sends the Credential Provisioning Request to the PEMC directly, or sends PEMC Notification (PEGC ID, Credential Provisioning Request) to PIN server and PIN server sends PEMC Event Notification (PEGC ID, Credential Provisioning Request) to the PEMC.

3. The PEMC sends Credential Provisioning Request (PIN ID, PEMC ID, PEGC ID, PINE ID, Duration) to the PIN server.

4. The PIN server interacts with 5GS and receives the credential from 5GS.

Editor's note: How to the PIN server interacts with 5GS to receive credentials is in SA2 scope. And the definition and architecture of credentials for PINE is in SA3 scope.

5. The PIN server responds to the PEMC with the credentials, and the PEMC responses to PINE with credentials.

7.15.2.4 Procedures of PIN communication via 5GS triggered by PEGC

This procedure presents a high-level overview of Solution 1.

Figure 7.15.2.4-1 illustrates PIN communication via 5GS procedure based on request/response model.

Pre-conditions:

1. The PINE is able to connected into PEGC via password and username;

2. The UE Identifier or PIN client Identifier is available for PINE;

3. The PIN client has been authorized to communicate with PEMC;

4. The PINE has the subscription that it can communicate via 5GS;

5. The PINE has already received the IP address of other PINE.

6. The communication between PEMC and PEGC is available.

NOTE: How to PINE receive the other PINE IP address are related to the procedure in section 7.3.2.3.



Figure 7.15.2.4-1: PIN communication configuration

1. [Optional] The PINE may send traffic to PEGC, triggered by the traffic, the PEGC sends PIN Communication Request (PIN ID, MAC address/IP address, Traffic descriptors) to the PEMC.

2. The PEMC sends Create/Update/Remove Communication Request (PIN ID, Packet filters, requested QoS) to the PEGC. The PEGC configures the local rule accordingly.

3. [Optional] According to the Packet filters, the PEGC may initiate PDU Session Modification with the Packet filters and requested QoS towards 5G system in order to make 5GC configure the N4 rules for UPF(s).

If the PEGC has already got the information to trigger the PDU session, the interaction between PEMC and PEGC will be saved. If the PEGC doesn’t have the related information (PIN ID, Packet filters, requested QoS), the procedure needs the PEMC to send related information to PEGC.

NOTE: How to the PEGC interacts with 5GS to initiate PDU Session Modification is in SA2 scope.

## 7.16 Solution #15: Service continuity

### 7.16.1 Architecture enhancements

The architecture of PIN is referred to the solution 1 in clause 7.

### 7.16.2 Solution description

#### 7.16.2.1 General

This solution addresses aspects of Key Issue #5 and some of Key Issue #2.

As indicated in clause 6.38 of TS 22.261[2], the following requirements that describes the service continuity will be studied in this TR phase and reflect in this key issues 2:

- The 5G system shall be able to minimize service disruption when a PIN Element changes the communication path from one PIN Element (e.g. PIN Element with Gateway Capability) to another PIN Element or operator provided mobile access. The communication path between PIN Elements may include licensed and unlicensed spectrum as well as 3GPP and non-3GPP access.

In PIN architecture, there are four potential communication type for PINE/PEMC or other elements:

- the PINE has direct communication with other PINE via Bluetooth or Wi-Fi

- the PINE has communication with other PINE via PEGC (scenario 1)

- the PINE has communication with other PINE via PEGC and by means of the 5GS (scenario 2)

- the PINE has communication with other PINE via PEGC and by means of the PIN server (scenario 3)



Figure 7.16.2.1-1: Communication type for PINE

For scenario 1, the PEMC communicates with the PINE via PEGC. And the PEMC and PEGC has the same private IP range and the PEGC can easily route the information to PINE under the same PEGC.

For scenario 2, the PEMC communicates with the PINE via two PEGCs. The PINE and PEMC are not under the same PEGC, and the PEMC should communicate with the PINE with the help of 5GS as indicated in the KI#2. The two PEGCs act as the 5G-LAN communication.

For scenario 3, as the default communication, the PEMC communicates with the PINE via PIN server. The PIN server supports both the user plane and control plane interactions.

But in order to coordinated with the SA1 requirements, it describes the changing of access of PINE. So, only two situation of continuity should be studied in TR:

Firstly, the PEGC relocation. The PINE changes the gateway to communicate with other PINEs in PIN.

Secondly, change the communication from via PEGC to via 5GS. The PINE when move out of PEGC coverage, the PINE can change the communicate via 5GS.

#### 7.16.2.2 Procedures to support service continuity

##### 7.16.2.2.1 PEGC relocation

This procedure solves the situation, that PINE A has application layer communication with PINE B via PEGC 1. And for some reasons, the PEGC 1 should relocate to PEGC 2. And the PINE1 should continue to communicate with PINE 2 via PEGC 2.

Figure 7.16.2.2.1-1 illustrates the service continuity to change the application layer communication to communication via different PEGC based on request/response model.

Pre-conditions:

1. The PEMC in a PIN has been pre-configured or has discovered the address (e.g. IP address, FQDN, URI) of the PIN server;

2. The PIN has already been created and a PIN ID is distributed by PIN server;

3. The PEMC has been authorized to communicate with the PIN server;

4. The PINE A and PINE B are both in the same PIN, and can communicate with PEGC 1;

5. The PEGC 2 is another PEGC that in this PIN;



Figure 7.16.2.2.1-1: PEGC relocation in PIN

1. The PINE A has application layer communication with PINE B via PEGC 1 in the PIN.

2. The PEGC 1 detects that PEGC 1 needs relocation, for example, the PEGC 1 will power down or will breakdown.

3a. The PEGC 1 discovers the PEGC 2 internal PIN. The PEGC 2 should be the PINE in the same PIN and should have the capability of gateway.

3b. If the PEGC 1 doesn’t discover another potential gateway in PIN, the PEGC 1 can send the request to PEMC to request to discover a new PEGC in PIN.

4a. If in step 3a, the PEGC 1 determines the PEGC 2 itself, the PEGC 1 indicates the address information about PEGC 2 to PEMC. This PEGC address information including gateway ID or IP address will be taken into consideration when PEMC determines the new gateway.

5. The PEMC determines the new gateway. For example, the PEGC 2 to replace the PEGC 1.

6. The PEMC configures the new access control information to PEGC 2, for example, the user name, account, SSID, BSSID. This information is used to control the PINE to access the network.

7. The PEMC also responses to PEGC 1 that the new PEGC 2 has been determined. And before the PEGC 1 offline, the PEGC 1 triggers the PIN profile relocation to new PEGC 2, because the profile and the route information that configured in PEGC 1 can still be used by the PEGC 2.

8. The PEMC also sends the updated access control information and authorization information to PINE A. The Auth Info may be included for authenticating/authorizing PINE connecting to PEGC 2.

9. The PINE A can connect into the PEGC 2 and communicate with PINE B.

##### 7.16.2.2.2 Change application layer communication to communication via 5GS, with the support of PIN server

This procedure solves the situation, that PINE A has application layer communication with PINE B via PEGC. But when the communication via PEGC is not viable, for example, the PINB moves out of the coverage of PEGC 1, only newly establish the 5GS communication to connect PINE B is the potential way.

Figure 7.16.2.2.2-1 illustrates the service continuity to change application layer communication to communication via PEGC + 5GS based on request/response model.

Pre-conditions:

1. The PEMC in a PIN has been pre-configured or has discovered the address (e.g. IP address, FQDN, URI) of the PIN server;

2. The PIN has already been created and a PIN ID is distributed by PIN server;

3. The PEMC has been authorized to communicate with the PIN server;

4. The PINE A has the subscription that can communicate with PINE B via 5GS;



Figure 7.16.2.2.2-1: Change application layer communication to communication via PEGC + 5GS

1. The PINE A has application layer communication with PINE B via PEGC 1.

2. The PEGC 1 decides to use the 5GS communication to substitute the direct routing via PEGC 1. For example, if the PINE B move out of the coverage of PEGC 1 and can not communicate with PINE 1 via PEGC 1 directly anymore.

3. The PEGC 1 requests to establish the QoS towards PINE 2, reusing the procedure defined in solution 14. The PEGC 1 sends PINE 5GS connection request (PIN ID, PINE ID, Packet filters, [DN-specific ID]) to the PEMC. The PEMC sends PINE 5GS connection request (PIN ID, PEMC ID, PEGC ID, PINE ID, Packet filters) to the PIN server.

4. The PIN server will check with the 5GS that whether this PINE has the subscription to communicate with other PINE via 5GS. And if the PINE has the subscription, the PIN server will interact with 5GS to create/update the QoS flow of PEGC for the PINE.

5. According to the QoS flow establishment, the PIN server updates the route information and QoS information towards PINE 1 in PEGC 1 or the PIN server requests the PEMC to update.

6. The PINE A communicates with PINE 2 via 5GS.

7.17 Solution #16: PINE registration via the PEGC

7.17.1 Architecture assumptions

The architecture of PIN is referred to the solution 1 in clause 7.

7.17.2 Solution description

7.17.2.1 General

This solution addresses aspects of Key Issue #1.

A PINE may need to perform the PIN registration towards the PIN server to get essential authorizations for the following PIN operations like PIN join.

The PINE is provisioned the PIN server address during the communication with PEMC.

7.17.2.2 Procedures of PINE registration via the PEGC

Pre-conditions:

1. The PINE has been pre-configured or has discovered the address (e.g. IP address, FQDN, URI) of the PIN server;

2. The PINE already establishes the connection with PEGC;

Figure 7.17.2.2-1 illustrates the PIN registration via the PEGC procedure based on request/response model.



Figure 7.17.2.2-1: PINE registration to PIN server via PEGC

1. The PINE sends PIN registration request to the PIN server. The PIN registration request is routed to the PEGC. The PINE device identity, device credentials and other necessary formation which is also needed for PIN service authorization are included.

2. The PEGC identifies the received message is the PIN registration request which is allowed to be forwarded regardless the PINE is authorized or not.

3. The PEGC forwards the PIN registration request towards the PIN server.

4. The PIN server performs service authorization and verifies the PINE device with the information in the registration request. If authorized, the PIN server allocates the PIN client ID, authorization and security credentials for the PINE.

5. The PINE server returns the PIN registration response to the PEGC.

6. The PEGC forwards the PIN registration response to the PINE.

7.17.2.3 Procedures of PINE registration during the PIN join via the PEGC

Pre-conditions:

1. The PINE has been pre-configured or has discovered the address (e.g. IP address, FQDN, URI) of the PIN server;

2. The PINE already establishes the connection with PEGC;

3. The PINE may get the PIN information from the PEMC, PEGC via PIN announcement after connecting to PEMC or PEGC.

Figure 7.17.2.3.-1 illustrates the PINE registration during the PIN join via the PEGC procedure based on request/response model.



Figure 7.17.2.3-1: PINE registration to PIN server via PEGC

1. The PINE sends PIN join/discovery request to the PEGC. The PINE device identity is included.

- For the PIN join request, the PIN ID is included.

- For the PIN discovery request, the discovery criteria are included.

2. The PEGC identifies the received message is the PIN join/discovery request, and the PINE is not registered and authorized due to no PIN client ID and credentials in the message.

3. The PEGC returns the PIN join/discovery reject message to the PINE. The registration and authorization indication are also included to instruct the PINE to perform registration.

4. The PINE if not registered, initiates the PIN registration towards the PIN server via the PEGC as described in clause 7.17.2.2.

5. After the registration, the PINE will use the PIN client ID and credentials to initiate the PIN join/discovery again.

7.18 Solution #17: Service Continuity in a PIN

7.18.1 Architecture enhancements

None.

7.18.2 Solution description

7.18.2.1 General

This solution addresses aspects of Key Issue #5. The solution focuses on how a PIN application on a UE can continue to receive services from an application server after it moved out of reach of PIN element like PEGC or another PINE due to mobility. PIN service continuity in this context is maintaining reachability due to UE mobility. This solution is based on the following principles.

- The PINE can subscribe for service continuity for one or more ongoing services involving application clients. Third party service provider and application developers, based on response to the subscription request, can make sure that the feature is available and supported for the application. The service continuity feature can be chosen for a specific application and ignored for others. E.g. service continuity can be enabled for gaming and not for TV application inside the house.

- The subscription can be authorized by PIN server and provide a service continuity policy to the PINE. PIN server is assumed to be the main trusted entity to authorize the subscription request coming from PINE.

- The PIN server informs the PEMC about allowed UE and applications which can be supported with service continuity feature.

- The PEMC configures PEGC about the PINE, which has subscribed for service continuity of a specific service. The PEGC can report back to PEMC when the UE is not reachable. The PEMC can decide at that time if it wants to trigger service continuity procedure.

- The PINE can also report about lost service to PEMC and about the available PEGCs in the PINE’s proximity. The PINE reports those PEGCs, which it can reach.

- The PEMC configures a PEGC for service continuity and informs the PIN Server about the new PEGC.

- The PIN Server can expose standard APIs, to expose service continuity information to the AS. The application layer can have mechanisms to deal with service disruptions independent of any communication path changes (e.g. TCP operations), but the exposed APIs can assist the application layer to implement its own mechanism.

NOTE: This solution is a feature that is provided by the PINAPP layer. An application can also support service continuity via procedures that are outside of 3GPP’s scope and, in such a scenario, would not support this service continuity procedure. Further, an application can decide to not support this service continuity procedure if the application e.g. has particular requirements for authentication.

7.18.2.2 Procedure

This section provides details of Solution #17.

7.18.2.2.1 Functional entities

PIN Client: A PINAPP function in UE, PINE, which subscribes for service continuity and informs when service is lost.

PIN Management Client (PEMC Client): A PINAPP in PEMC, configures the PEGC and PINE for service continuity. Informs PIN server about updates related to service continuity.

PIN Gateway Client (PEGC Client): A PINAPP in PEGC, obtains configuration from PEMC and executes service continuity procedure.

PIN Server: Supports PIN Client, PIN Management Client by providing service continuity related information when requested by PIN Management Client. It can expose service continuity information to external entities through APIs.

7.18.2.2.2 Procedures of PIN Service Continuity while the PINE is connected to a PEGC

Figure 7.18.2.2.2-1 illustrates a service continuity procedure for scenario 1, based on request/response model.



Figure 7.18.2.2.2-1: PIN Service Continuity when the PINE is connected via PEGC

Pre-conditions:

- More than one PEGC is serving the PIN.

- PEMC connectivity is not lost by a PINE.

- The PIN Client in UE has been either pre-configured or has discovered the address (e.g. IP address, FQDN, URI) of the PEMC Client, PIN server.

- The PEMC Client supports functionality to execute the service continuity procedure.

- The PEGC Client supports functionality to execute the service continuity procedure.

- The PIN Server has capability to expose service continuity information to external entities such as identification of a service and any changes to the end points of the service.

1. A PIN Client in a UE subscribes for service continuity with the PEMC and PIN server. The purpose of the subscription request is to inform the PEMC and PIN Server that the PINE would like to continue an ongoing service if it loses connectivity with PEGC. The subscription request includes application level IDs such as, PEID, one or more Service identifiers which need service continuity, Application session ID, Destination PIN ID, and an IPv4 Tuple that describes the session. The IPv4 tuple can include the IP Address of the UE, the IP Address of the Server that provides the service, the UE port numbers that are associated with the service, and the port numbers on the server that are associated with the service.

The PIN Server authorizes the subscription request, and provides PEMC Client with policy information about service continuity for the PINE.

The PEMC configures PEGC for service continuity procedure by providing PEID, Service ID.

The PEMC client informs the PINE if service continuity for the requested services is allowed or not.

2. The PINE moves and loses contact with the PEGC. The loss of connectivity with the PINE can trigger service continuity procedure in the PEGC based on PEID and Service ID.

3. The PEGC Client informs the PEMC Client about the service discontinuity of the PINE by sending an “Activate service continuity” message, which includes PEID, Service ID. As an alternative PINE can also inform PEMC to activate the service continuity procedure.

4. The PEMC client decides if it is required to initiate service continuity procedure, and of so informs the PIN Server to update about the service continuity procedure, initiated by PEGC or PINE. The PEMC client sends an “Update Service Continuity information” to the PIN server with information such as the PEID, Service ID, Service continuity status like Started, Executing, Completed. This allows the PIN server to immediately update service continuity information and share with AS, rather than waiting for PINE to discover a new PEGC and update service continuity status.

5. The PIN server updates information about the service continuity such as identification of the service, involved PINEs and service continuity status to an external AS.

6. It is assumed that the PINE has the information about other available PEGCs in the PIN (possibly provided by PEMC during start-up procedure). The PINE is able to find and connect to another PEGC in the PIN. It is also assumed that PEMC Client becomes aware of the PINE connecting to the new PEGC.

7. The PEMC client determines, based on PEID, Service continuity policy, that the new PEGC can be configured to handle service continuity for the PINE. The PEMC Client sends a “Configure new PEGC” message to configure the PEGC with:

a) Session ID;

b) destination PINE information, which is a list of PEID, IP address, Port number or URL; and

c) Application Server information, which will resume service with the PEGC. Information includes Application Server ID, Application Server port-number, so that the new PEGC can configure to receive information from the Application Server.

PEMC also collects the PEGC IP address and PEGC port-number, in the response message.

8. The PIN Management Client sends an “Update Service continuity information” to the PIN server, to indicate that configuration of PEGC and PINE has happened successfully, and the service can be resumed, with information such as:

a) Service ID: Service to be resumed;

b) Application Server ID: Identifies the Application Server, which was providing service;

c) Terminating PEGC ID;

d) Terminating PEGC reachability information, such as IP address, port number, URL etc.; and

e)Terminating Destination PINE reachability information, such as IP address, port number, URL etc.

9. PIN Gateway Client informs PIN Server that it is ready to resume the service with identification information from step 7. PIN Server updates this information and makes available for external entities.

10. The IP address of PINE and PEGC can change or at application-level IP preserving technique can be applied. PIN Server updates all information for service continuity, which can be used to resume the service to a new destination IP address. PIN Server updates an external AS with the new service continuity information such as:

a) Application Session ID: identifies the application session to be switched to new endpoint; and

b) Terminating IP Address:

- IP address of PINE, port-number where the service will be terminated; and

- IP address of the PEGC, which will forward the service to PINE.

7.18.2.2.3 Procedures of PIN Service Continuity while the PINEs are connected directly

Figure 7.18.2.2.3-1 illustrates a service continuity procedure for scenario 2, based on request/response model.

This procedure involves finding a new PEGC for a PINE’s indirect communication by the PEMC. Selection of the new PEGC is dependent upon having connectivity between the PEMC and the PINEs (e.g. PINE1 and PINE2) involved. When the direct connection between PINEs is lost, the PEMC cannot determine correctly a PEGC which has connections to both PINEs. The PEMC requests that the PINEs to PEGCs which it can connect to. Then PEMC can select a PEGC, which has connectivity to both PINEs. These steps differentiate the service continuity procedure from PEGC reselection procedure.



Figure 7.18.2.2.3-1: PIN Service Continuity when PINEs are connected directly

Pre-conditions:

- One or more PEGC is serving the PIN.

- PEMC connectivity is not lost by a PINE.

- The PIN Client in UE has been pre-configured or has discovered the address (e.g. IP address, FQDN, URI) of the PEMC Client.

- PIN client is capable of triggering PEGC discovery procedure by PINE and provide report about the discovered PEGCs.

- The PEMC Client supports functionality to execute the service continuity procedure.

- The PEGC Client supports functionality to execute the service continuity procedure.

- The PIN Server has capability to communicate with Application Server to identify a direct service and provide policy and authorization information.

1. A PIN Client in a UE, subscribes for service continuity with PEMC or PIN server. The purpose of the subscription request is to inform that PINE would like to continue an ongoing service with another PINE, connected directly. The subscription request includes PEID, one or more Service identifiers which need service continuity, Destination PIN ID, and an IPv4 Tuple that describes the session. The IPv4 tuple can include the IP Address of the first UE, the IP Address of the second UE and the UE port numbers that are associated with the service.

a) The PIN Server authorizes the subscription request and provides PEMC Client with policy information about service continuity for the PINEs.

b) PEMC client informs the PINE if service continuity for the requested services is allowed or not and policy information related to service continuity.

2. The PINE moves and loses contact with other PINE. The loss of connectivity results in service discontinuity between the PINEs. PIN Client informs PEMC Client about the service discontinuity by sending an “Inform SC lost” message, which includes PEIDs, Service ID.

3. Triggering PEGC discovery by PINE, allows PEMC to be sure that the PINE can connect to the selected PEGC. If PEMC selects a PEGC using its own knowledge, there is a possibility that the PINE cannot connect to it. All the involved PINEs start PEGC discovery and reports back to PEMC, a list of discovered PEGCs with the OK message.

4. PEMC client goes through one or more lists sent by one or more PINEs and selects one or more optimal PEGCs for service continuity. The PEMC Client sends a “Configure new PEGC” message to PEGC Client to configure PEGC with the following information, so that PEGC can setup forwarding path between the two PINEs.

a) Service ID: The service that needs to be handled by PEGC.

b) Destination PINE information, which is a list of PEID, IP address, Port number or URL.

5. PEMC client configures PINE with the new PEGC information such as IP address, port-number, URL, and triggers connection setup.

6. Once the connection between PINE and PEGC is successful, the service resumes.

7.18.3 Solution evaluation

The solution addresses the problem when PIN application on a UE is consuming service from an application server and due to UE mobility, how the PIN application on the UE can continue to receive services from the application server. Due to mobility the UE can go out of reach of the PEGC which was delivering service.

The solution describes how the service continuity procedure is initiated. Serving PEGC detects that the UE is out of reach and informs PEMC client. PEMC client updates PIN server about the Service Continuity procedure status.

To continue the service, UE can connect to a new PEGC, and inform PEMC client. To complete service continuity, PEMC configures the new PEGC to support service continuity and updates PIN server about the status of the procedure and new end point information. Once configuration is complete, service resumes towards the UE through the new PEGC.

The detailed role of PEGC involvement for service continuity procedures requires further evaluation considering different PINE status and application scenarios.

# 8 Deployment scenarios

## 8.1 General

This clause provides a general description of the deployment scenarios.

## 8.x Deployment scenario #x: <Title>

Provide an illustrative description of the deployment scenario.

# 9 Overall evaluation

This clause provides a summary of architecture enhancements and solution evaluations.

## 9.1 Architecture enhancements

## 9.2 Key issue evaluations

### 9.2.1 General

All the key issues, solutions and architecture enhancements specified in this technical report are listed in Table 9.2.1-1.

Table 9.2.1-1 provides a mapping of the key issues to the related solutions.

Table 9.2.1-1 Key issue and solutions

| Key issues (evaluation clause reference) | Solution | Architectural enhancement  (clause reference) | Enhancements required | Dependency on other working groups |
| --- | --- | --- | --- | --- |
| *KI#1: PIN Management* | *Solution #x: <title>* | *6.x* | *Architecture / None* | *<WG>* |
| *Solution #y: <title>* | *6.y* | *Architecture / None* | *<WG>* |
| *KI#2: PINAPP accesses 5G network by application mechanism* | *Solution #x: <title>* | *6.x* | *Architecture / None* | *<WG>* |
| *KI#3: Service switch in PIN* |  |  |  |  |
| *KI#4: PIN Application Server Discovery* | *Solution #11: Application Server Discovery in a PIN* |  |  |  |
| *KI#5: Service continuity* |  |  |  |  |
| *KI#6: PEMC/PEGC replacement in PIN* |  |  |  |  |

For KI#1 and KI#6, they describe the management (control plane interaction) of PIN.

**Phase 1: Prepare phase, before PIN create.**

Before the PIN create, two procedures should be done.

Firstly, as solution 12 describes, the PEMC, PEGC, PINE should register into the PIN server first. This procedure has two purpose. The fist is some of the PINE can receive the role of PEMC from PIN server. The second purpose is the device metadata of PINE, for example, the MAC address, GPSI, PIN client ID and etc can be obtained by PIN server.

Secondly, as solution 7 describes, the PIN server discovery. Some of the PIN management procedures needs the PIN server to help. So, the PINE should receive the PIN server endpoint address first and then trigger the phase 2 procedure.

**Phase 2: PIN management procedure.**

In phase 2, it is the real PIN management procedure. And during the PIN management procedure, it can be divided as the following parts:

1. PIN lifecycle: PIN create/delete.

2. PIN management procedure internal PIN (PIN modification): Including the PEMC/PEGC changes and PIN Profile recover.

3. Member management: Including add PINE into a PIN or delete a PINE from PIN.

4. PIN configuration: PIN Profile.

For the PIN lifecycle, it includes the PIN create/modification/delete. The PIN create (solution 2) can only be triggered by PEMC, and approved by PIN server. For the PIN delete (solution 10), the PEMC can trigger the delete either internally or with the help of PIN server’s authorization that a PIN is not needed. Also, the PIN server can trigger the PIN release for example, the life cycle of PIN comes to the end.

For the PIN management procedure internal PIN (PIN modification), it includes the role changes of PEMC/PEGC. For the PEMC changes, it includes the PEMC changes itself (Solution 2), PIN server triggers PEMC changing (Solution 2), PEMC failure triggers the relocation (Solution 9). For PEGC relocation, it includes (Solution 2) the PEGC relocation itself, PEMC triggers the PEGC relocation, PIN server triggers the PEGC relocation. During the PEMC/PEGC relocation procedure, the PIN profile also need to recover. (Solution 2) A PIN profile recover procedure that recover the profile from PIN server is defined.

For the member management, it includes the add PINE into a PIN or delete a PINE from PIN. For adding the PINE into a PIN, only the PINE takes the initiative to join the PIN is defined. (Solution 5) The PINE discovers the PIN from PEMC/PIN server first, and the PINE joins the PIN (Solution 3). For removing a PINE from PIN, one possible way is (Solution 3) the PINE leaves a PIN and this PINE is removed. Another possible way is (Solution 3) the PEMC/PIN server removes the PINE in a PIN.

For the PIN configuration, it is related to the definition of PIN profile. (Solution 6) PIN profile and dynamic PIN Profile are defined to describe the related information about PINE, PEMC and PEGC. For example, the ID, endpoint address and etc. This information is important for a PIN, and can be seen as the control plane management information for the PIN.

**Phase 3: Enhancement function of PIN**

After the PIN management procedure, some of the enhancement functions are defined in the PIN, including:

1. PINE communication via 5GS: the most important and fundamental features that PIN provide

2. Service Switch: offload the application traffic to internal PIN or changes the traffic termination

3. Application Server Discovery in a PIN: enhance the PIN to support application server procedure

4. PIN Continuity: A variety of PIN device interaction and changes the communication path, for example, via Gateway or via 5GS.

For PINE communication via 5GS, (solution 14) PIN server triggers the QoS establishment or the PEGC triggers the PDU session establishment/modification (to coordinate with SA2).

For Service Switch, two possible solutions are defined: (Solution 8) PIN server assisted service switch and (Solution 10) Service switch internal PIN.

For Application Server Discovery in a PIN, (Solution 11) one or more PINAPP(s) (e.g. in a PEMC or in a PIN server) can maintain a registry to manage information about AS(s) that are available to the PIN. The AS(s) register their availability with the PINAPP. And the AS can be discovered at PIN server.

Editor's note: PIN Continuity parts need to update later.

**Phase 4: Architectures of PIN**

(Solution 1) PIN enabler architecture needs a new design of PIN enabler layer that both supports AC and the 3GPP communication layer.

(Solution 13) Another SEAL enhancement architecture is the UE also has a SEAL group management client, and the PIN client interact with the SEAL group management client via the GM-C to achieve PIN management.

### 9.2.2 Evaluation of key issue #1: PIN Management

For PIN create that addressed in KI#1, solution 2 gives the solution of the PIN create procedure with the following principle:

- The PIN creation can only be triggered by the PEMC. The PINE receives the role of PEMC during the registration procedure towards PIN server as indicated in solution 12. And the PEMC receives the PIN server endpoint address before triggering the creation.

- The PEMC sends the PIN create request to PIN server with the GPSI, PIN client ID, UE location, security credential and PIN profile. The PIN profile includes some of the information that PEMC can request defined in solution 6, for example, the description of PIN, duration of PIN and etc.

- The PIN server sends a successful response to PEMC, which includes a newly assigned PIN ID to indicate the PIN. Also, the PIN lifetime or duration can be indicated to PEMC. If the PIN creation request fails, the PIN server should give the failure response to indicates that indicates the cause of PIN creation request failure.

- After the PIN create successfully, the PIN server or PEMC can allocate the access control information to PEGC if the gateway is selected for the PIN and delivers the access control information to PINEs. The access control information includes: user name, account, SSID, BSSID and etc. All the information is used by PINE in PIN to access the PEGC or benefited by 5GS communication.

For PIN delete that addressed in KI#1, solution 4 gives the solution of the PIN delete procedure with the following principle:

- The PIN delete can be triggered either by PEMC or PIN server. All these two situations are valuable.

- The PEMC decides to delete the PIN due to the PIN is not needed or the lifecycle of PIN comes to the end. The PEMC can delete the PIN locally or request PIN server to delete the PIN

- The PIN server can trigger the PIN delete procedure, for example, when the life cycle of PIN is end or the PIN server decides to stop the PIN service in this PIN and release the PIN resource.

- For PEMC triggers PIN delete and sends request to PIN server: the PEMC sends a PIN delete request to the PIN server to request to delete the PIN. The PIN delete request includes the security credentials of the PIN client received during PIN client authorization procedure and PIN ID. The PIN ID indicates this PIN will be deleted.

- If the PEMC detects that the lifecycle of PIN comes to the end, the PEMC can decide to delete the PIN locally. And the PEMC shall indicate the deletion of PIN to PIN server which includes the PIN ID.

- For PIN server deletes the PIN: An event occurs at the PIN server that satisfies trigger conditions for notifying a subscribed PEMC of a PIN. If the life cycle of a PIN is end or the PIN server decides to not provide any PIN resource in this PIN, the PIN server should trigger a PIN delete procedure to the PEMC.

If a PIN is deleted, the PIN resource will be released and the PIN service will be stopped. Some of the procedure related to the deleted PIN defined in solution 4 addresses the principle below:

- After PIN delete, the PEMC sends the notification to PEGC and PINE that in this PIN to delete the PIN profile related to the deleted PIN, which indicated by PIN ID. This is a notification procedure.

- The access control information in PEGC that related to this PIN and PINE in this PIN should be deactivated.

- After PIN delete, if PIN is deleted by PEMC locally, the PEMC sends a PIN status update notification to the PIN server to indicate the PIN has been deleted. In this notification, the PIN ID is included. The PIN server updates the PIN profile to remove the details of this PIN which represented by PIN ID.

- After PIN delete, if the PIN is deleted by the PIN server, the PIN server sends the PIN status update notification to the PEMC to indicate the PIN has been deleted. In this notification, the PIN ID is included. The PEMC updates the PIN profile to remove the details of this PIN which represented by PIN ID and triggers other notification towards the PINE/PEGC in this PIN.

Solution 7 addresses Key Issue 1 and describes the aspects of PIN server discovery. All of the PINE, including PEMC, PINE and PEGC should discover the PIN server first, and then have the interaction towards PIN server. The PIN server discovery procedure should be done before the PIN management.

- Solution #7 addresses the procedure of PIN server discovery. The PIN server can be discovered by the following method as indicated in Solution #7:

- pre-configured in the PIN elements or PIN clients;

- configured by the user;

- provisioned by MNO through 5GC procedure; or

- derived from HPLMN identifier for non-roaming scenario or from VPLMN identifier for roaming scenario.

For the provisioned by MNO through 5GC procedure, this has several drawbacks. Firstly, this has the impact to 5GC NAS procedure. Secondly, in order to deliver the PIN server endpoint address to the PIN enabler layer, the UE OS should have an enhancement. At last, if the PIN procedure are all happen in the application layer scope, that the 5GS is not aware of PIN, and this needs the 5GC impact that AF provides the PIN server endpoint address to 5GC. But whether SA2 support this is FFS. So, the PIN server endpoint address that provisioned by MNO through 5GC procedure is not appropriate to be included in the method of PIN server discovery.

Solution 7 also addresses the method that due to PINE receives the PIN server endpoint address from the PEGC and PEMC.

For example, if PINE has application layer connection with PEGC, for example, via WiFi or Bluetooth pairing, so there are two ways for PINE discovering PIN server:

- If the PINE connects to PEGC with user name and password, the PINE sends PIN server discovery request to PEGC. The requests include the GPSI, PIN client ID if has, UE location. PEGC can response with PIN server end point address directly.

- If the PINE has the open access to PEGC that with no user name or password. For this situation, the PINE can’t consume the communication service that provided by PEGC, but can have communication with the PEMC behind the PEGC. The PINE sends PIN server discovery request to PEGC and the PEGC routes the requests to PEMC. The request includes the GPSI, PIN client ID if has, UE location. PEMC can response with PIN server end point address to PINE via PEGC.

Due to for some of the PIN elements can have the application interaction towards the PEMC, for example, via WiFi or Bluetooth pairing, so the PEMC can provide the PIN server end point information to PIN elements. The PINE sends PIN server discovery request to PEMC. The requests include the GPSI, PIN client ID if has, UE location. The PEMC delivers the PIN server end point information to PIN elements or PIN client. The end point information of PIN server includes URI(s), FQDN(s), IP address(es)) of PIN server.

For PIN discovery of PINE that addressed in KI#1, solution 5 gives the solution of the PINE discovers the PIN with the following principle:

- The PINE can discover the available PIN from two methods:

- The PINE can send PIN discovery request to PEMC of a PIN.

- The PINE can send PIN discovery request to PIN server.

- If the PINE has already had an application layer connection with a PEMC which manages a PIN, the PINE sends the PIN discovery request to PEMC. The PIN discovery request includes the security credentials of the UE or PIN client and may include the UE identifier such as GPSI if available, PIN client ID, UE location, the service that PINE wants to consume and PIN client profile(s) information.

- If the PINE has already had the application layer connection towards PEGC, and the PINE has already received the PIN server endpoint address, the PINE sends the PIN discovery request to PIN server. The PIN discovery request includes the security credentials of the UE or PIN client and may include the UE identifier such as GPSI, PIN client ID, UE location, the service that PINE wants to consume and PIN client profile(s) information.

- In the PIN discovery request to both PEMC or PIN server, the PINE can have the filter information in the PIN discovery request for example, the interesting area, the interesting type of PIN and etc. The filter information can be used for providing certain PIN information.

Solution 12 and solution #16 addresses Key Issue 1 and describes the aspects of PINE/PEMC/PEGC registration procedure that ahead of PIN creation.

- Solution #12 addresses the procedure that happens before PIN create.

- For the PEMC, the PEMC sends Registration Request (GPSI) to the PIN server. After successful registration in PIN server, the PIN server allocates the PIN client ID to this PEMC and the PEMC receives the role of PEMC.

- For the PINE and PEGC, the PINE/PEGC registers itself into PEMC with the device metadata (MAC address, vendor name, device description, PINE/PEGC Address). And the PEMC substitutes the PINE/PEGC to register on PIN server. After successful registration in PIN server, the PIN server allocates the PIN client ID to PINE/PEGC.

- Solution #16 addresses the procedure that happens before PINE joining any PIN.

- The PINE initiates the PIN registration towards the PIN server via the PEGC with the device information. And the PEGC is designed to identify the PIN registration message and forwards such message regardless of the PINE is authorized or not. The PINE gets the PIN clients ID, necessary authorization and security credentials from the PIN server via this PIN registration.

- If the PINE initiates the PIN join/discovery request without the registration and authorization, the PEGC rejects such PIN messages, and trigger the PINE to initiate the PIN registration towards the PIN server.

Solution 6 addresses the aspects of Key Issue 1 related to what information needs to be maintained at the PIN server, PEMC, PEGC and PIN elements. Information maintained at these entities are classified into 2 types – PIN profile and dynamic profile information. Solution 6 captures the information that needs to be maintained at each of the PIN entities in detail.

Solution 3 addresses Key Issue 1 and describes the aspects of PINE join into a PIN and remove the PINE from a certain PIN. Solution #3 addresses the procedure that happens after PINE accomplish PIN discovery, and the PINE has the application layer connection with PEMC

For PINE joins into a PIN:

- The PINE sends the request to PEMC to join the PIN. The request includes the security credentials of the PIN client, UE identifier such as GPSI, UE location, PIN ID and PIN client profile(s). After PEMC authorizes the request and accept the PINE to join the PIN, the PEMC notifies to PEGC/PIN server in PIN. The PEMC/PEGC/PIN server updates the PIN profile. The access control information in PEGC for this PINE is delivered by PEMC during the notification.

- During PIN create procedure, the PEMC can request to create a PIN including the potential PIN elements to be added into a PIN.

- The PINE sends PIN join/discovery request to the PEGC. The PEGC identifies the received message is the PIN join/discovery request, and the if the PINE is not registered and authorized due to no PIN client ID and credentials in the message, the PINE registration procedure will be also included.

For removing PINE from a PIN, two potential ways:

- The PEMC removes a PINE from PIN, and notify the result to PEGC/PIN server. The PEMC/PEGC/PIN server updates the PIN profile. The access control information in PEGC for this PINE is disabled after receiving the notification from PEMC.

- If the PINE decides to leave the PIN, the PINE sends the request to PEMC to leave the PIN. The request includes the security credentials of the PIN client, UE identifier such as GPSI, UE location, PIN ID and PIN client profile(s). After PEMC authorizes the request and accept the PINE to leave the PIN, the PEMC notifies to PEGC/PIN server in PIN. The PEMC/PEGC/PIN server updates the PIN profile. The access control information in PEGC for this PINE is disabled after receiving the notification from PEMC.

Optionally, the PIN server can also be involved in the procedure of PINE added/removed into/from PIN. The PIN server can decide the PINE added/removed into/from PIN or the PIN server can be notified by the result of PINE added/removed into/from PIN.

Solution 14 addresses Key Issue 1 and describes the aspects of credentials provisioning procedure.

- Solution #14 addresses the procedure below:

- The PINE sends Credential Provisioning Request (PIN ID, PINE ID, Duration) to the PEGC.

- The PEGC sends the Credential Provisioning Request to the PEMC directly, or sends PEMC Notification (PEGC ID, Credential Provisioning Request) to PIN server and PIN server sends PEMC Event Notification (PEGC ID, Credential Provisioning Request) to the PEMC.

- The PEMC/PEGC sends Credentials Provisioning Response to PINE.

NOTE: Which entity that the PEMC/PEGC obtains the Credentials, for example, the PIN server, 5GS or other NFs, is in the scope of SA3.

### 9.2.3 Evaluation of key issue #2: PINAPP accesses 5G network by application mechanism

Solution 14 addresses Key Issue 2 and describes how to enable the PIN with 5GS communication. For the PIN that support 5GS communication, the PIN can trigger to establish the PDU session or QoS for PINE.

- Solution #14 addresses two procedures that enable the PIN with 5GS communication:

- Establish QoS for PINE with PIN server support.

- PEGC triggers PDU session establishment/modification for PINE when no PIN server deployed.

For the PIN server requests 5GS to establish QoS for PINE, this reuses the procedure defined in SA2 that AF triggers the QoS establishment procedure. No impact to SA2 procedure. After receiving the destination IP address of other UEs or application clients, the PINE sends PINE 5GS connection request (PIN ID, PINE ID, Packet filters, [DN-specific ID]) to the PEMC, via PEGC. And the PEMC sends PINE 5GS connection request (PIN ID, PEMC ID, PEGC ID, PINE ID, Packet filters) to the PIN server. The PIN server should receive the Packet filters, DN-specific ID from PEMC that these parameters are used for AF to trigger the QoS. If the IP address of the PEMC/PEGC is changed, the PEMC/PEGC sends Event Notification (PEMC/PEGC ID, old IP address, new IP address) to the PIN server.

Another alternative procedure is PEGC triggering PDU session establishment/modification for PINE without PIN server. This procedure is applied to adapt to SA2 PIN. The PINE may send traffic to PEGC, triggered by the traffic, the PEGC sends PIN Communication Request (PIN ID, MAC address/IP address, Traffic descriptors) to the PEMC. The PEMC sends Create/Update/Remove Communication Request (PIN ID, Packet filters, requested QoS) to the PEGC. The PEGC configures the local rule accordingly. According to the Packet filters, the PEGC may initiate PDU Session Modification with the Packet filters and requested QoS towards 5G system in order to make 5GC configure the N4 rules for UPF(s).

### 9.2.4 Evaluation of key issue #3: Service switch in PIN

This clause provides an overall evaluation for Key Issue #3, "Service switch in PIN".

Solution #8 and #10 address aspects of Key Issue #3.

Key Issue #3 studies how to support an application mechanism for service switching in a PIN between different PIN applications.

a) To execute a service switch, a PIN, which can handle the service must be discovered.

Solution #8:

- Describes application-level discovery of available PIN, where a PIN Client in a UE sends a discovery request to a PIN Server.

- Discovery request includes Location information, Application requirements such as Display characteristics, Audio characteristics.

- PIN Server based on Location and application service requirement can provide the PIN Client with information about, one or more available PIN IDs, details of PINAPP capabilities and corresponding PE IDs, such as Device ID, IP address and Port number for each PIN.

Solution #10:

- PINE is part of the PIN and initiates service discovery with PEMC.

- PEMC provides the details of the PIN Service (e.g. service type) and the PINE end point and application end point information.

b) Among available PINs, the Application client can select a PIN and initiate service switch procedure.

Solution #8:

- PIN Application Client selects a PIN and requests that the PIN Server trigger a service switch procedure.

- PIN Application Client sends information such as Application session ID, Destination PIN ID, and an IP 4 Tuple that describes the session.

- PIN Server accepts the request and sends acknowledgement to PIN Client.

Solution #10:

- PIN Application client and the corresponding PINE is part of the PIN, selects the suitable PINE where the service can be switched.

- Selection is based on the following principles: firstly, whether this potential PINE has deployed the same application client as PINE and, secondly, whether this potential PINE can maintain the same service type as PINE

c) The service switch procedure is handled differently in the two solutions.

Solution #8:

- PIN server can select the PIN Applications in PINE and instruct the PIN Management Client to execute service switch procedure.

- Information sent to PEMC Client includes Application Session ID, Destination PINE information, which includes PE ID, IP Address, Port number, URL.

- PEMC configures PEGC and PINE and sends end point information to PIN server. A flag is used to indicate PEGC, if the session needs to be split among more than one PINEs.

NOTE: The target PINE and PEMC are assumed to have already performed an authentication and authorization procedure.

- Thus, the solution relies on the PEMC to configure the target PINE and direct interaction between the original PINE and target PINE can be avoided.

- PIN server stores updated service switch related end point information and can make available to external AS through APIs, if it wants to use for its own service switch method.

Solution #10:

- Service switch being handled via direct interaction between the PINEs.

- Switch traffic flow directly from one PINE to another via direct communication method or via the PEGC. The destination IP address is always the original PINE and the original PINE forwards the traffic to the new PINE.

- Application context is relocated along with application context to another PINE and the service resumes. After the context relocation, the application client in PINE triggers the application relocation to potential PINE. Note that this procedure changes the destination IP address

- In order to maintain the integrity of the application process, the application traffic from application server should be terminated at the PINE first. The PINE transfers the application traffic to the potential PINE directly or via the PEGC.

### 9.2.5 Evaluation of key issue #4: PIN Application Server Discovery

This clause provides an overall evaluation for Key Issue #4, "PIN Application Server Discovery".

Solution #11 is the only solution that addresses Key Issue #4.

- Solution #11 maintains a registry of PIN AS in the PINAPP, which is used to discover PIN AS by Application clients.

- The registry function can be part of the PEMC Client and PIN Server.

- This registry function information can be provisioned or configured in the UE or PIN Client.

- Registry function information can be an address, endpoint, or service API information.

- PIN Clients use the registry function information to query about PIN AS.

- Application clients in the PIN can register with the Registry function, through PIN client using the registry information.

- The PINAPP registry functions in a PIN can communicate and update information about PIN AS that are stored in the registry. Furthermore, the PIN Server can configure the PINAPP with Usage Policies

- PINAPP registry function in PIN server can communicate with the registry function in other PIN servers, which belong to different PIN.

### 9.2.6 Evaluation of key issue #5: Service continuity

Solution #17 and #15 address aspects of Key Issue #5.

To execute a service continuity, first it needs to be detected that the mobile PINE is out of reach of the serving PEGC or another PINE in case of direct communication. After detection, the service continuity procedure can be triggered.

- Solution #17 describes application-level detection by the serving PEGC, which was delivering service, that the PINE is out of reach. The PEGC informs PEMC about the condition that the service to the PINE may be disrupted. In the case of direct communication, the PINE informs PEMC about the loss of direct communication.

- Solution #15, addresses the situation where PINEs are interacting via PEGC and a PINE moves out of reach of the PEGC. The PEGC detects the PINEs are out of reach and initiates service continuity procedure. The PEGC discovers another PEGC or requests that PEMC discover another PEGC for the service.

The service continuity procedure is executed similarly in the two solutions

- Solution #17 describes that the PEMC selects the new PEGC and configures the new PEGC to support service continuity by providing information about the PINE and Service details. The PEMC also updates PIN server about the status of the service continuity procedure including the PINE and PEGC information.

- Solution #15 describes that the PEMC discovers a PEGC and configures it for service continuity. The configuration step includes providing access control information and exchanging profile information among PEGC. The PEMC also configures PINE if required.

- Solution #15 also covers the scenario where the PINE moves out of range of the PIN and the service will need to be provided via the 5GS. In this scenario, the PEGC notifies the PEMC and the PEMC notifies the PIN Server about the need for service continuity. The PIN Server is then able to configure QoS for the flows that are associated with the service. The PIN Server will then provide the updated route information to the PEGC.

The solutions propose role assignments for PINE, PEGC, PEMC and PIN server for service continuity procedures considering certain impact to the application layer itself. These roles may require further modification or enhancement considering PINE status and application scenarios.

### 9.2.7 Evaluation of key issue #6: PEMC/PEGC replacement in PIN

This clause provides an overall evaluation for Key Issue #6, "PEMC/PEGC replacement in PIN".

Various procedures documented as part of Solution #2 in the clause 7.3.2.3 addresses the aspects of Key Issue #6.

Key Issue #6 studies the following open issues:

a) Whether and how the need for PEMC or PEGC role change is determined?

b) How another active PIN element take over the role or is assigned the role of PEMC or PEGC?

c) Whether and how the existing active PIN elements is notified about the role change?

d) Whether and how the required dynamic or context information of PIN is made available to the new element taking the role of PEMC or PEGC

- Procedures documented as part of the clause 7.3.2.3 considers the PIN modification as means to assign the role of PEMC and PEGC to another PINE. The need of the role change could be because of the current PIN element assigned with the role of PEGC or PEMC is no more available or the duration associated with the role is expired.

- Role change is achieved based on the following principles:

a) The current PEMC or PEGC triggering the role change to another PINE by requesting PIN server – Clause 7.3.2.3.1 describes the procedure for PEMC role change which is triggered by the current PEMC requesting the PIN server to assign the PEMC role to another PINE. As part of the request PEMC may include the list of potential candidate(s). Clause 7.3.2.3.6 describes the procedure for PEGC role change which is triggered by the current PEGC to assign the PEGC role to another PINE. Solution 9 describes the procedure for PEGC role change which is triggered by the PEMC on detecting the unavailability of PEGC. On detecting the unavailability of PEGC, PEMC requests the PIN server to assign the PEGC role to another PIN element which has the gateway capability.

b) Role change triggered by the PIN server – Clause 7.3.2.3.2 describes the PEGC role change procedure by the PIN server on detecting the unavailability of the PIN element which is currently the PEGC. Clause 7.3.2.3.3 describes the PEMC role change procedure by the PIN server on detecting the unavailability of the PIN element which is currently the PEMC.

c) Role change triggered internally within the PIN without involving PIN server - Clause 7.3.2.3.4 describes the procedure of how the current PEMC requesting another PIN element to take the role of PEMC. Once the role assignment succeeds, the PIN server, PEGC and other PIN elements are notified of the role change. Clause 7.3.2.3.5 describes the procedure of how the PEMC requesting another PIN element to take the role of PEGC. In this case the decision of role change is determined and executed by the PEMC and PIN server and other PIN elements are notified of the role change. Clause 7.3.2.3.8 describes the procedure where multiple PEGCs serve two groups of PINEs in a PIN and upon the failure of one of the PEGCs, a backup PEGC assumes the role of the new PEGC.

d) PEMC Role change triggered by authorized administrator residing outside the PIN – Clause 7.3.2.3.7 describes the procedure of how the authorized administrator on a UE requests the PIN server through the 5G network to modify the role of PEMC to another PIN element. The authorized administrator on a UE receives the notification from PEGC about the failure/unavailability of current PEMC.

e) Role change notification to the PIN entities – In all the procedures related to the role change in the PIN, the corresponding PIN entities (PIN server, PEMC, PEGC and PIN elements) are notified about the role change and the PIN dynamic profile information maintained at these entities are updated accordingly.

### 9.2.8 Evaluation of PINAPP architecture

The solutions 1 addresses the key issue related to PINAPP architecture, to support the PIN management and the PIN communication. Also, in the PINAPP architecture supports the service switch, application server discovery and service continuity.

# 10 Conclusions

This clause provides conclusions of the study.

## 10.1 Conclusion of PIN management of KI#1

The following principle is considered normative for PIN create:

- The PIN creation can only be triggered by the PEMC. The PINE receives the role of PEMC first during the registration procedure towards PIN server.

- The PEMC sends the PIN create request to PIN server with the GPSI, PIN client ID, UE location, security credential and PIN profile. In order to save the procedure of several PEMCs to be involved into the certain PIN as individual PEMC, the PEMC can have the additional PEMC GPSIs/PIN client ID in the PIN create request, to indicate additional PEMCs that are allowed to manage the PIN. In order to save the procedure of several PINEs to be involved into the certain PIN, the PEMC can have the lists of PINEs GPSIs/PIN client ID in the PIN create request, to indicate additional PINEs that are allowed to join the PIN.

- The PIN server sends a successful response to PEMC, which includes a newly assigned PIN ID to indicate the PIN. Also, the PIN lifetime or duration can be indicated to PEMC. If the PIN creation request fails, the PIN server should give the failure response to indicates that indicates the cause of PIN creation request failure.

- After the PIN create successfully, the PIN server or PEMC can allocate the access control information to PEGC if the gateway is selected for the PIN and delivers the access control information to PINEs. The access control information includes: user name, account, SSID, BSSID and etc. All the information is used by PINE in PIN to access the PEGC or benefited by 5GS communication.

Editor's note: Whether Access control information is determined by 5GC or PIN server itself depends on SA2 feedback and needs further update.

The following principles are considered normative for PIN delete:

- The PIN delete procedure can be triggered either by PEMC or PIN server.

- The PEMC sends a PIN delete request to the PIN server to request to delete the PIN.

- The PEMC can decide to delete the PIN locally. After PIN deleted locally, the PEMC indicates the deletion of PIN to PIN server which includes the PIN ID.

- The PIN server deletes the PIN when events occur and satisfies trigger conditions for PIN delete. For example, the event includes the life cycle of a PIN is end or the PIN server decides to not provide any PIN resource in this PIN.

The PIN delete request includes the security credentials of the PIN client received during PIN client authorization procedure and PIN ID. The PIN ID indicates this PIN will be deleted.

The PEMC can delete the PIN locally based on some pre-configuration information on PEMC, for example, the according to the life time configured on PEMC.

If a PIN is deleted, the PIN resource will be released and the PIN service will be stopped. Some of the procedure related to the deleted PIN should be normative:

- After PIN delete, the PEMC sends the notification to PEGC and PINE to delete the PIN profile related to the deleted PIN.

- The access control information in PEGC that related to this PIN and PINE in this PIN should be deactivated.

- If PIN is deleted by PEMC locally, the PEMC sends a PIN status update notification to the PIN server to indicate the PIN has been deleted. In this notification, the PIN ID is included. The PIN server updates the PIN profile to remove the details of this PIN which represented by PIN ID.

- If the PIN is deleted by the PIN server, the PIN server sends the PIN status update notification to the PEMC to indicate the PIN has been deleted. In this notification, the PIN ID is included. The PEMC updates the PIN profile to remove the details of this PIN which represented by PIN ID and triggers other notification towards the PINE/PEGC in this PIN.

NOTE: The interaction between PINE and PEMC may be directly interaction or interaction via PEGC.

The following principle is considered normative for PIN server discovery:

The general static configuration of PIN server in PIN can be consumed as the following methods:

- pre-configured in the PIN elements or PIN clients;

- configured by the user;

- derived from HPLMN identifier for non-roaming scenario or from VPLMN identifier for roaming scenario.

The dynamic discovery of PIN server in PIN can be consumed as the following methods. If the PINE has the application layer connection to PEGC or PEMC:

- If the PINE connects to PEGC with user name and password, the PINE sends PIN server discovery request to PEGC. The PEGC can response with PIN server end point address directly.

- If the PINE has the open access to PEGC, the PINE sends PIN server discovery request to PEGC and the PEGC routes the requests to PEMC. The PEMC can response with PIN server end point address to PINE via PEGC. Authorization information and procedure is needed between PEMC and PINE.

- If the PINE has the application interaction towards the PEMC, the PINE sends PIN server discovery request to PEMC. The PEMC delivers the PIN server end point information to PIN elements or PIN client.

In the PIN server discovery request, the following parameters are included: GPSI, PIN client ID if has, UE location. And in the PIN server discovery response, the endpoint address information of PIN server is included, for example, the IP address, FQDN, or URI.

NOTE: The PEGC is responsible for response the PIN server address to PINE directly or route the PIN server request to PEMC. If the PEGC is associated with multiple PIN and PEMC, the PEGC route the PIN server request to multiple PEMC separately.

The following principle is considered normative for PIN discovery:

- The PINE can discover the available PIN from two methods:

- The PINE can send PIN discovery request to PEMC of a PIN.

- The PINE can send PIN discovery request to PIN server.

- If the PINE has already had an application layer connection with a PEMC which manages a PIN, the PINE sends the PIN discovery request to PEMC.

- If the PINE has already had the application layer connection towards PEGC, and the PINE has already received the PIN server endpoint address, the PINE sends the PIN discovery request to PIN server.

The PIN discovery request includes the security credentials of the UE or PIN client and may include the UE identifier such as GPSI if available, UE location, the service that PINE wants to consume and PIN client profile(s) information.

In the PIN discovery request to both PEMC or PIN server, the PINE can have the filter information in the PIN discovery request for example, the interesting area, the interesting type of PIN and etc. The filter information can be used for providing certain PIN information.

The following principle is considered normative for PINE/PEMC/PEGC registration:

- For the PEMC, the PEMC sends Registration Request (GPSI) to the PIN server. After successful registration in PIN server, the PIN server allocates the PIN client ID to this PEMC and the PEMC receives the role of PEMC.

- For the PINE and PEGC, the PEMC substitutes the PINE/PEGC to register on PIN server with the device metadata from PINE/PEGC (MAC address, vendor name, device description, PINE/PEGC Address). After successful registration in PIN server, the PIN server allocates the PIN client ID to PINE/PEGC.

- The PINE can also directly register to the PIN server via the PEGC, if the PEMC/PIN server has already provided the PIN server address to the PINE. And if the PINE is accessing the PEGC without any registration and authorization, the PEGC may reject the message from the PINE and request the PINE to perform the registration.

For managing the PIN, it is required to maintain the information related to the PIN and PIN elements. Information captured as part of Solution 6 can serve as basis for the normative work and further information if any required can be decided during the normative work.

The following principle is considered normative for adding/removing PINE into/from a PIN:

For PINE joins into a PIN:

- The PINE sends the request to PEMC to join the PIN. The request includes the security credentials of the PIN client, UE identifier such as GPSI, UE location, PIN ID and some of PIN client profile(s). After PEMC authorizes the request and accept the PINE to join the PIN, the PEMC notifies to PEGC/PIN server in PIN. The PEMC/PEGC/PIN server updates the PIN profile. The access control information in PEGC for this PINE is delivered by PEMC during the notification.

- During PIN create procedure, the PEMC can request to create a PIN including the potential PIN elements to be added into a PIN.

- The PINE sends PIN join/discovery request to the PEGC. The PEGC identifies the received message is the PIN join/discovery request, and the if the PINE is not registered and authorized due to no PIN client ID and credentials in the message, the PINE registration procedure will be also included.

For removing PINE from a PIN, two potential ways:

- The PEMC removes a PINE from PIN, and notify the result to PEGC/PIN server. The PEMC/PEGC/PIN server updates the PIN profile. The access control information in PEGC for this PINE is disabled after receiving the notification from PEMC.

- If the PINE decides to leave the PIN, the PINE sends the request to PEMC to leave the PIN. The request includes the security credentials of the PIN client, UE identifier such as GPSI, UE location, PIN ID and PIN client profile(s). After PEMC authorizes the request and accept the PINE to leave the PIN, the PEMC notifies to PEGC/PIN server in PIN. The PEMC/PEGC/PIN server updates the PIN profile. The access control information in PEGC for this PINE is disabled after receiving the notification from PEMC.

Optionally, the PIN server can also be involved in the procedure of PINE added/removed into/from PIN. The PIN server can decide the PINE added/removed into/from PIN or the PIN server can be notified by the result of PINE added/removed into/from PIN.

The following principle is considered normative for credential provisioning:

- The PINE sends Credential Provisioning Request (PIN ID, PINE ID, Duration) to the PEGC.

- The PEGC sends the Credential Provisioning Request to the PEMC directly, or sends PEMC Notification (PEGC ID, Credential Provisioning Request) to PIN server and PIN server sends PEMC Event Notification (PEGC ID, Credential Provisioning Request) to the PEMC.

- The PEMC/PEGC sends Credentials Provisioning Response (Credentials) to PINE.

## 10.2 Conclusion of KI#2

The following principle is considered normative for KI#2:

- There are two methods to enable the PIN with 5GS communication:

- Establish QoS for PINE with AF support.

- PEGC triggers PDU session establishment/modification for PINE when no PIN server deployed.

For the AF related procedure, the AF trigger the QoS create/modification procedure with parameters of Packet filters, DN specific ID, to request the 5GS to arrange resource for PIN.

For PEGC related procedure, the PEGC sends PIN Communication Request to the PEMC. The PEMC sends Create/Update/Remove Communication Request (PIN ID, Packet filters, requested QoS) to the PEGC. The PEGC configures the local rule accordingly, or according to the Packet filters, the PEGC may initiate PDU Session Modification with the Packet filters and requested QoS towards 5G system in order to make 5GC configure the N4 rules for UPF(s).

The PIN Communication Request includes the following parameters: PIN ID, MAC address/IP address, Traffic descriptors. The Create/Update/Remove Communication Request includes PIN ID, Packet filters, requested QoS.

During the QoS or PDU session establishment procedure, if the IP address of the PEMC/PEGC is changed, the PEMC/PEGC sends Event Notification (PEMC/PEGC ID, old IP address, new IP address) to the PIN server.

## 10.3 Conclusion of Service Switch of KI#3

There are two solutions that solution 8 and solution 10 for service switch should be normative with the following principle:

The Solution 10 is service switch accomplished internal PIN. The following principle is considered normative for Solution 10:

- The PINE joins into a PIN and discovers the candidate PINE internal PIN to do the service switch. The candidates PINE should deploy the same application client or can maintains the service towards AS and the service corresponds to the same service type.

- After the traffic terminated at the PINE, the PINE offloads the traffic to candidate PINE directly or via PEGC if direct communication is not viable.

The Solution 8 is service switch with support from PIN server. The following principle is considered normative for Solution 8:

- The PINE discovers a PIN and decide a potential candidate PINE to be the target of service switch with the help of PIN server.

- And the PIN server requests the PEMC to configure PEGC, PINE, as well as informs AS to trigger another new application layer traffic to candidate PINE/AS.

- And after the new application layer is established, that some of the application client context relocation may needed between two clients.

10.4 Conclusion of KI#4

Solution 11 reflects the KI#4. The following principle is considered normative for KI#4:

- The application server registers into AS registry function (can be deployed in PEMC, PIN server) with the endpoint information. The AS registry function can store the information about AS for PINE to discover the appropriate AS.

- The PINE triggers the application server discovery request to the AS registry function in PEMC, which can be forwarded to the registry function in PIN server, and receives the endpoint address of AS

- Application clients in the PIN can register with the Registry function, through PIN client using the registry information, obtained by the PIN client from PIN server.

10.5 Conclusion of KI#5: Service continuity

In order to support the service continuity scenarios of Key Issue #5, the principles of Solution #15 and Solution #17 will be followed where the PEMC detects that a service continuity procedure is needed, selects a new PEGC to handle the service, configures the PEGC to handle the service, and can notify the PIN Server about the service continuity procedure. The PEMC detects that a service continuity procedure is needed based on a notification from a PEGC or, in the case of a service that is using direct PINE-to-PINE communication, a notification from a PINE.

The principles of Solution #15 will be followed to cover the scenario where the PINE moves out of range of the PIN and the service will need to be provided via the 5GS. The PEGC notifies the PEMC and the PEMC notifies the PIN Server about the need for service continuity. The PIN Server is then able to configure QoS for the flows that are associated with the service. The PIN Server will then provide the updated route information to the PEGC.

The service continuity role assignments for PINE, PEGC, PEMC and PIN server can be further modified or enhanced in the normative work considering different PINE status and applications scenarios.

10.6 Conclusion of KI#6

The Key Issue #6, "PEMC/PEGC replacement in PIN" studied the open issues related to the PIN modification which is about the re-assignment of PEMC and PEGC role to another PIN element. Various procedures documented as part of Solution #2 in the clause 7.3.2.3 addresses the aspects of Key Issue #6.

Following methods are considered for the normative work related to PEMC role change:

1. Current PEMC requesting the PIN server to assign the PEMC role to another PIN element (clause 7.3.2.3.1).

2. PIN server assigning the PEMC role to another PIN element on detecting the unavailability of current PEMC (clause 7.3.2.3.3).

3. Current PEMC requesting another PIN element to take the role of PEMC (clause 7.3.2.3.4).

4. Authorized user from outside PIN requesting PIN server to assign to PEMC role another PIN element (clause 7.3.2.3.7)

All the above methods require the consent from the new PIN element to be assigned with the role of PEMC. All other PIN elements including PEGC are to be notified about the change in the PEMC role and the PIN dynamic profile information is updated accordingly.

Following methods are considered for the normative work related to PEGC role change:

1. PIN server assigning the PEGC role to another PIN element on detecting the unavailability of current PEGC (clause 7.3.2.3.2).

2. PEMC assigning the PEGC role to another PIN element on detecting the unavailability of current PEGC (clause 7.3.2.3.5).

3. Current PEGC requesting the PIN server to assign the role to another PIN element (clause 7.3.2.3.6, clause 7.3.2.3.8)

All the above methods require the consent from the new PIN element to be assigned with the role of PEGC. All other PIN elements including PEMC are to be notified about the change in the PEGC role and the PIN dynamic profile information is updated accordingly.

10.7 Conclusion of PINAPP architecture

It is supposed to use Solution 1 as baseline for normative PINAPP architecture.

Annex A (informative):  
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2022-02 | SA6#47-e |  |  |  |  | TS skeleton (version 0.0.0) approved in S6-220374  Implementation of the following pCRs approved by SA6:  S6-220375, S6-220376, S6-220475, S6-220476 | 0.1.0 |
| 2022-04 | SA6#48-e |  |  |  |  | Implementation of the following pCRs approved by SA6:  S6-220805, S6-220851, S6-220973, S6-220974 | 0.2.0 |
| 2022-05 | SA6#49-e |  |  |  |  | Implementation of the following pCRs approved by SA6:  S6-221475, S6-221476, S6-221477, S6-221478, S6-221336, S6-221479, S6-221480, S6-221163, S6-221361, S6-221481. | 0.3.0 |
| 2022-07 | SA6#49-bis-e |  |  |  |  | Implementation of the following pCRs approved by SA6:  S6-221549, S6-221571, S6-221615, S6-221788, S6-221804, S6-221806, S6-221807, S6-221808, S6-221826, S6-221828, S6-221831, S6-221834, S6-221867, S6-221895, S6-221900, S6-221993, S6-221994. | 0.4.0 |
| 2022-08 | SA6#50-e |  |  |  |  | Implementation of the following pCRs approved by SA6:  S6-222172, S6-222389, S6-222402, S6-222409, S6-222410, S6-222411, S6-222418, S6-222536, S6-222566, S6-222567, S6-222568, S6-222569, S6-222570. | 0.5.0 |
| 2022-10 | SA6#51-e |  |  |  |  | Implementation of the following pCRs approved by SA6:  S6-222651, S6-222746, S6-222747, S6-222858, S6-222904, S6-222905, S6-222906, S6-222907, S6-222910, S6-222911, S6-222912, S6-222914, S6-222916, S6-222959, S6-222972, S6-222973, S6-223047, S6-223048, S6-223049 | 0.6.0 |
| 2022-11 | SA6#51-e |  |  |  |  | Reimplementation of S6-222912 and editorial corrections | 0.6.1 |
| 2022-11 | SA6#52 |  |  |  |  | Implementation of the following pCRs approved by SA6: S6-222651, S6-223170, S6-223172, S6-223186, S6-223191, S6-223265, S6-223362, S6-223370, S6-223384, S6-223385, S6-223524, S6-223525, S6-223526, S6-223527, S6-223528, S6-223529, S6-223530, S6-223533, S6-223535, S6-223550, S6-223577, S6-223578, S6-223593, S6-223594. | 0.7.0 |
| 2022-11 | SA6#52 |  |  |  |  | Correction of the implementation of pCR S6-223577 | 0.7.1 |
| 2022-12 | SA#98-e | SP-221219 |  |  |  | Submitted for Approval at SA#98-e | 1.0.0 |
| 2022-12 | SA#98-e | SP-221219 |  |  |  | MCC Editorial update for publication after TSG SA approval (SA#98‑e) | 18.0.0 |
| 2023-03 | SA#99 | SP-230280 | 0001 |  | B | Conclusion update for additional PEMCs and PINEs in PIN creation | 18.1.0 |
| 2023-03 | SA#99 | SP-230280 | 0002 |  | B | Requirement update for PIN | 18.1.0 |