ETSI TS 123 542 V18.4.0 (2024-07)

TECHNICAL SPECIFICATION

5G; Application layer support for Personal IoT Network (3GPP TS 23.542 version 18.4.0 Release 18)

Reference

RTS/TSGS-0623542vi40

Keywords

5G

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from the
ETSI Search & Browse Standards application.

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format on ETSI deliver.

Users should be aware that the present document may be revised or have its status changed, this information is available in the Milestones listing.

If you find errors in the present document, please send your comments to the relevant service listed under Committee Support Staff.

If you find a security vulnerability in the present document, please report it through our Coordinated Vulnerability Disclosure (CVD) program.

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Legal Notice

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 3GPP and ETSI identities can be found under https://webapp.etsi.org/key/queryform.asp.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Foreword

This Technical Specification 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.

Introduction

Personal IoT Networks (PIN) is based on the greatly increasing number of consumers IoT devices. Users create Personal IoT Networks out of all these Personal IoT devices mainly in their homes or wearables. This technical specification provides application enabler layer architecture and related procedures for enabling PIN applications over 3GPP networks.

The application enabler layer capabilities take into consideration the stage 1 requirements specified in clause 6.38 of 3GPP TS 22.261 [2] and stage 2 architecture for 3GPP networks supporting PIN as specified in clause 5.44 of 3GPP TS 23.501 [4].

1 Scope

The present document specifies the application enabler layer architecture, procedures and information flows necessary for enabling PIN applications over 3GPP networks. The specification includes the capabilities (e.g. PIN management, discovery of elements, capabilities and services related to PIN) at the application enablement layer that fulfil the deployment and operational requirements of PIN applications over 3GPP networks. The PIN enabler capabilities applies to 5GS.

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 TS 22.101: "Service Principles".

[4] 3GPP TS 23.501: "System architecture for the 5G System (5GS)"

[5] 3GPP TS 23.502: "Procedures for the 5G System (5GS)"

[6] 3GPP TS 37.355: "LTE Positioning Protocol (LPP)"

[7] 3GPP TS 23.222: "Functional architecture and information flows to support Common API Framework for 3GPP Northbound APIs; Stage 2"

[8] 3GPP TS 33.122: "Security aspects of Common API Framework (CAPIF) for 3GPP northbound APIs"

3 Definitions of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in 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 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 specified in clause 6

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 belonging to a PIN.

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

Service Switch: A mechanism to switch the service traffic flow between Application server and PINE to application server and other PINE.

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 format (EW)

<symbol>	<Explanation>

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 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 TR 21.905 [1].

PIN	Personal IoT Network
PINAPP	Personal IoT Network Application
PEMC	PIN Element with Management Capability
PEGC	PIN Element with Gateway Capability
PINE	PIN Element

4 Overview

4.1 General

5 Architectural requirements

5.1 General

This clause specifies architectural requirements for enabling Personal IoT Networks in different functional aspects.

5.2 Architectural 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 enablement layer architecture shall support deployment of personal IoT network.

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

[AR-5.2.1.2-c] The application enablement 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 enablement layer architecture shall provide mechanisms to create PIN for UE or PIN elements.

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

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

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

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

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

[AR-5.2.2.2-h] The application enablement 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 enablement 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 enablement 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 enablement 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 enablement 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 enablement 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 enablement layer architecture shall provide mechanisms to support the PEGC relocation procedure to enable service continuity.

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

5.2.7 Security

5.2.7.1 General

This clause specifies PIN security requirements.

5.2.7.2 Requirements

[AR-5.2.7.2-a] Communication between the functional entities of the application enablement layer architecture shall be protected.

[AR-5.2.7.2-b] Access control mechanisms for authenticating functional entities of the application enablement layer architecture shall be provided.

[AR-5.2.7.2-c] Access control mechanisms for authorizing interactions between functional entities of the application enablement layer architecture shall be provided.

[AR-5.2.7.2-d] Mutual authentication and authorization between functional entities of the application enablement layer architecture shall be provided.

[AR-5.2.7.2-e] Mechanisms for replay protection of messages exchanged between functional entities of the application enablement layer architecture shall be provided.

[AR-5.2.7.2-f] Mechanisms for integrity protection of messages exchanged between functional entities of the application enablement layer architecture shall be provided.

[AR-5.2.7.2-g] Mechanisms for privacy protection of the user shall be provided.

[AR-5.2.7.2-h] Mechanisms for confidentiality protection of the user's sensitive information (e.g., identity, location) shall be provided.

5.2.8 Subscription service

5.2.8.1 General

This clause specifies the requirements for PIN subscription service.

5.2.8.2 Requirements

[AR-5.2.8.2-a] The application enablement layer architecture shall provide subscription and notification mechanisms enabling to receive PIN modification information changes.

[AR-5.2.8.2-b] The application enablement layer architecture shall provide subscription and notification mechanisms enabling to receive PIN management information changes.

[AR-5.2.8.2-c] The application enablement layer architecture shall provide subscription and notification mechanisms enabling to receive PIN profile information changes.

[AR-5.2.8.2-d] The application architecture shall provide subscription and notification mechanisms enabling to receive PIN connectivity information changes.

[AR-5.2.8.2-e] The application enablement architecture shall provide subscription and notification mechanisms enabling to receive PIN service continuity information changes.

[AR-5.2.7.2-f] The application enablement layer architecture shall provide subscription and notification mechanisms enabling a PINE/PEGC/PIN server to receive changes in PIN status information of PIN from an PEMC.

5.2.9 PIN application KPIs

5.2.9.1 General

This clause specifies the requirements for PIN application KPIs.

5.2.9.2 Requirements

[AR-5.2.9.2-a] The application enablement layer architecture shall provide mechanisms for the PEGC to publish its KPIs that the PEGC supported or gateway requirements.

[AR-5.2.9.2-b] The application enablement layer architecture shall provide mechanisms for the application client to publish its KPIs to operate effectively within the PIN or application level requirements.

6 Application enablement layer architecture

6.1 General

This clause provides the overall architecture description:

- Clause 6.2 describes the functional architecture;
- Clause 6.3 describes the functional entities;
- Clause 6.4 describes the reference points;
- Clause 6.5 describes the cardinality of functional entities and reference points.

6.2 Architecture

This clause describes the architecture for enabling personal IoT networks in a reference point representation, where existing interactions between any two functions (e.g., PINE, PEGC, PEMC, PIN-Server, etc.) is shown by an appropriate reference point (e.g. PIN-1, PIN-2, etc.).

This clause provides the reference point representation:

- Clause 6.2.1 describes the reference point representation of the general architecture.
- Clause 6.2.2 describes the reference point representation for users accessing PIN services from outside the PIN.

6.2.1 General Architecture

Figure 6.2.1-1 illustrates the reference point representation of the architecture for PINAPP.

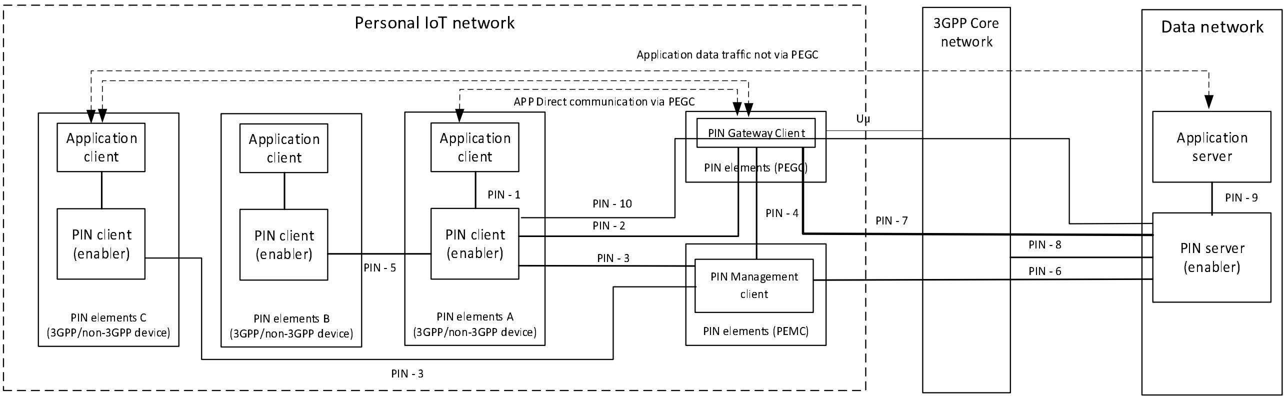

Figure 6.2.1-1: PINAPP architecture

The PIN elements contains PIN client and/or application clients. The PIN Element with gateway capability (PEGC) performs the role of an entity supporting gateway capability for PIN. The PIN Element with management capability (PEMC) performs the role of an entity supporting management capability for PIN. A PIN includes at least one PEGC and at least one PEMC. The roles of UEs acting as PEGC and PEMC in 5GS are specified in clause 5.44 of 3GPP TS 23.501 [4].

The PIN enabler architecture consists of PIN client deployed in PIN element and PIN server deployed in Data network. The following interaction are supported in the PIN enabler architecture:

- The PIN client interacts with Application Client on the PINE over PIN-1 to provide and consume services in the PIN.
- The PIN server interacts with Application Server(s) over PIN-9. These interactions are supported using the CAPIF architecture as specified in 3GPP TS 23.222 [7].
- The PIN server interacts with 3GPP networks over PIN-8 to consume 3GPP network services.
- The PIN management client(s) interact with PIN server over PIN-6 for services related to management of PIN.
- The PIN client(s) interact with PIN server over PIN-10. These interactions traverse via the PEGC.

- The PIN gateway client(s) interact with PIN server over PIN-7.

- PIN client(s) interact with PIN gateway client over PIN-2.

- PIN management client interacts with PIN gateway client(s) over PIN-4.

- PIN management client interacts with PIN client(s) over PIN-3.

- A PIN client interacts with other PIN client(s) 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.

NOTE 4: There is no restrict that only one PEMC/PEGC deployed in PIN. It is possible that in a PIN, multiple PEMCs/PEGCs are deployed.

NOTE 5: PIN-5 is out-of-scope of the current release of the specification.

6.2.2 Architecture of user accessing services provided by PIN Element from outside the PIN

The Figure 6.2.2-1 shows the application architecture to enable authorized user to access services provided by PIN element behind the PEGC. For simplicity, not all functional elements of Figure 6.2.2-1 are shown in below Figure 6.2.2-1.

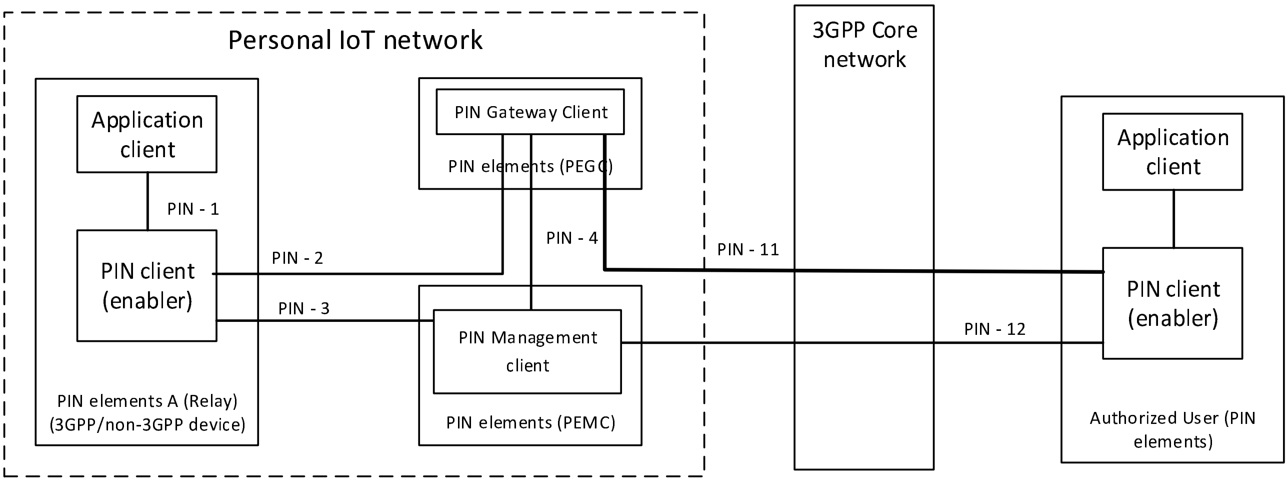

Figure 6.2.2-1: PINAPP architecture of User accessing services provided by PIN Element from outside the PIN

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.

NOTE1: The authorized user is allowed to manage a PIN due to authorized user has PIN-12 interface to communicate with PEMC.

6.3 Functional entities

6.3.1 General

This clause describes the functional entities of the architecture for enabling personal IoT networks.

6.3.2 PIN client

The PIN enabler layer entity residing in the PIN elements that provides the client side functionalities required for application clients in order to consume the services offered by the PIN or to offer services for other PIN elements to consume.

It provides the following functionalities:

- Registration of the available service and capabilities;
- Service discovery of other PIN elements and application server;
- Communication with PIN clients of other PIN elements;
- Selection of relay for direct communication;
- Maintaining the PIN profile;
- Perform to join/leave a PIN;
- Support to discover the available PIN; and
- Support to receive the information to access the 5G core network via PEGC.
- Support service switch internal PIN.
- Support PIN service continuity of PEGC relocation or changing to 5GS communication.

6.3.3 PIN Management Client

A PIN Element with Management Capability is a PIN Element that provides a means for an authorized 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 list of PIN elements who joined the PIN. Maintaining available PIN services;
- Maintain the PIN profile for each PIN and PINE in PIN;
- To configure and manage a PIN, including:
    - authorizing the 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 PIN elements to enable discovery of services offered by other PIN Elements;
    - add PIN elements to the PIN;
    - configure PIN elements to enable direct communications;
    - configure PIN elements to communicate with each other when gateway device is unavailable.
    - support the PIN server endpoint address delivery to PIN elements;

- support the credentials delivery to PIN elements;

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

- Support service switch internal PIN.
- Support PIN service continuity of PEGC relocation or changing to 5GS communication.

6.3.4 PIN Gateway Client

A PIN Element with Gateway Capability is a PIN Element that has the ability to provide connectivity to a PINE for data and signaling exchange with PEMC, other PIN Elements or the DN. It may act as both the Layer-3 type relay which transparently forwards the traffic for PINE, and the application layer relay which terminates the PIN-2 reference points, processes the PIN management messages from/to the PINE, and performs authorization check.

It provides the following functionalities when acting as application layer relay:

- Maintain the PIN profile for each PIN and PINE in PIN;
- Maintain the access control information for each PIN and each PINE in PIN;
- Support to trigger the PDU session modification towards 5GS to request the resource for PIN;
- Enable the 5GS communication or direct communication;
- Support delivery of PIN server address;
- Support to deliver the credentials to PINE;
- Support PIN discovery function;
- Support service switch within the PIN.
- Support PIN service continuity of PEGC relocation or changing to 5GS communication.

It provides the following functionalities when acting as Layer-3 type relay:

- Receives the packet from the PINE and forwards the traffic to network transparently
- Receives the packet from the PINE and forwards the traffic transparently or another PINE transparently
- Receives the packet from the Network and forwards the packet towards to the PINE transparently

6.3.5 PIN server

A PIN server is deployed at network that provides server side functionalities required for managing the PIN.

It provides the following functionalities:

- Provisioning of configuration information to the PIN elements;
- Maintain the PIN profile for each PIN and PINE in PIN;
- PIN Management (Creation, modification and deletion) of PIN;
- Determine the access control information of PEGC/PINE in PIN;
- Authorization of the PINE to be added/removed into/from the PIN
- Support PIN discovery and application server discovery
- Support service switch internal PIN.
- Support PIN service continuity of PEGC relocation or changing to 5GS communication.

6.3.6 Application Client

An application client is the application resident in the PIN elements.

6.4 Reference Points

6.4.1 General

This clause defines the reference points between functional entities of PINAPP.

6.4.2 PIN-1

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

6.4.3 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.

6.4.4 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;
- Discovery of services offered by other PIN elements;
- Discovery and selection of PIN elements;
- Notifying the PIN information modification details (e.g. PEMC change, PEGC change, PIN capabilities change).

6.4.5 PIN-4

This reference point exists 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;

6.4.6 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 PIN element to the PIN client of another PIN element.

NOTE: PIN-5 is out-of-scope of this release.

6.4.7 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;

6.4.8 PIN-7

This reference point exists between the PEGC and PIN server for the interactions related to enabling PINAPP

6.4.9 PIN-8

This reference point exists between the PIN server and 3GPP core network for the interactions related to enabling PINAPP. It supports:

- UE's (PINE) location information retrieval as specified in clause 4.15.3 of 3GPP TS 23.502 [5].

6.4.10 PIN-9

This reference point exists between the application server and PIN server for the interactions related to enabling PINAPP. This reference point is an instance of CAPIF-2/2e reference point as specified in 3GPP TS 23.222 [7].

6.4.11 PIN-10

This reference point exists between the PIN client in PIN element and PIN server for the interactions related to enabling PINAPP.

6.4.12 PIN-11

This reference point exists between the PEGC and PIN client from outside the PIN to access the services provided by PIN elements within the PIN.

PIN-11 utilizes Uu reference point as described in 3GPP TS 23.501[4].

6.4.13 PIN-12

This reference point exists between the PEMC and PIN client for configuring and managing the PIN from outside the PIN.

PIN-12 utilizes Uu reference point as described in 3GPP TS 23.501[5].

6.5 Cardinality rules

6.5.1 Application Client (AC)

The following cardinality rules apply for application client:

a) one or more application clients per PIN client.

6.5.2 PEMC

The following cardinality rules apply for PEMC:

a) one or more PEMCs per PIN.

b) Only one PEMC in certain PIN is assigned as primary role and other PEMCs if any are assigned with secondary role.

c) One PEMC can act as PEMC for multiple PINs.

d) One PEMC per UE.

6.5.3 PEGC

The following cardinality rules apply for PEGC:

a) one or more PEGCs per PIN.

a) For a certain PINE in PIN, one PEGC acts as default PEGC and other PEGCs act as backup.

c) One PEGC can act as PEGC for multiple PINs.

d) One PEGC per UE.

6.5.4 PIN server

The following cardinality rules apply for PIN server:

a) one PIN server per PIN.

b) Multiple PINs per PIN server.

6.5.5 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.

c) one PIN client per UE.

7 Identities and commonly used values

7.1 General

The following clauses list identities and commonly used values that are used in this technical specification.

7.2 Identities

7.2.1 General

The following clauses specify a collection of identities that are associated with entities defined and being used in this specification.

7.2.2 PIN ID

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

The PIN ID consists of two parts as follow:

- A string assigned by the PIN server which is unique for each PIN; and

- An identifier of PIN server (i.e. PIN server ID or domain name).

7.2.3 PIN server ID

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

7.2.4 PIN client ID

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

The PIN client ID is used for general identities for PINE, PEMC and PEGC.

For PEMC and PEGC, the PIN client ID may also be PEMC ID and PEGC ID.

For the PINE, the PIN client ID may also be PINE ID.

7.2.5 Application Client ID (ACID)

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.

7.2.6 UE ID

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 [4].

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

7.2.7 UE Location

The UE location identifies where the UE is connected to the network or the position of the UE. It provides consistent definition of the UE's location across the UE and network entities. Following values are examples of UE locations that can be used:

a) Cell Identity, Tracking Area Identity, GPS Coordinates, Geographical/Geodetic Information, Current Location Retrieved, Age of Location Information, Current RAT Type or civic addresses as defined in 3GPP TS 23.502 [5] clause 4.15.3 and TS 37.355[6].

8 Procedures and information flows

8.1 General

The PINE communicates with the PEMC via direct way (i.e., via WiFi, BlueTooth), or indirect way relayed by a PEGC. PINE determines to use direct way or indirect way based on the capabilites of access types supported by the PINE, PEMC and PEGC.

The Application layer must be able to influence the RAT selection for establishing connectivity to the PIN.

NOTE 1: How the Application layer is able to influence the RAT selection is up to implementation.

In order to support the PIN enabler layer communication, the IP address or port number of PIN enabler layer (PIN client) should be negotiated among PINE, PEGC and PEMC, for example, during PIN create procedure or device direct connection.

NOTE 2: If the direct connection is not available, the PINE/PEMC/PEGC sends the broadcast message to network with dedicate port number, and only the target port number of PIN client can response the message, which the procedure is out of scope.

8.2 Common Information Elements

8.2.1 General

This clause provides descriptions for Information Elements which are commonly used in several procedures.

8.2.2 PIN Profile

8.2.2.0 PIN Profile in a PIN

PIN profile information include static and semi-static data and default configuration that are needed for configuration of Personal IoT Networks, such as the PEMC, PEGC and PIN server end point addresses. Information in a PIN profile is infrequently changed.

Dynamic PIN profile information includes data that are updated more frequently due to operations of a PIN, e.g. caused by PINE join or PINE leave operations. Example information include PINE lists and the services that PINEs provide.

8.2.2.1 PIN Profile in a PIN

PIN profile includes information about the static data needed for configuration for the Personal IoT networks.

Table 8.2.2.1-1: PIN Profile

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
Duration	Specifies the time period of how long the PIN can be active	Y	Y	Y
Maximum number of PIN elements	Maximum number of PINEs allowed to join the PIN	Y	Y	N
Allowed PIN service	List of service that can be offered within a PIN: > PIN service Provider Identifier > PIN service type > PIN service Feature	Y	Y	N
Allowed PEMC list	The list of PINE static information for PINE(s) that can be allowed to take the role of PEMC: > PINE ID > GPSI > Role (e.g., primary, secondary or both) > Port number (see NOTE)	Y	Y	Y
Allowed PEGC list	The list of PINE static information for PINE(s) that can be allowed to take the role as PEGC: > PINE identifier > GPSI > Role (e.g., primary, backup or both) > Port number (see NOTE)	Y	Y	Y
PIN Server ID	The identifier of the PIN server that serves the PIN	N	Y	Y
PIN server Endpoint	The endpoint information (e.g., URI, FQDN) or a static IP address used to communicate with the PIN server.	N	Y	Y
Allowed PIN elements list	List of PINEs which can be allowed to join the PIN > PINE ID	Y	Y	Y

NOTE: NAT aspects are not specified in the current release.

8.2.2.2 Dynamic profile information of a PIN

Dynamic profile information of a PIN contains the PIN dynamic data needed for management of the Personal IoT networks.

Table 8.2.2.2-1 describes the list of parameters that are classified as dynamic profile information and which are maintained at the PIN server, PEMC and PEGC. PIN dynamic profile information maintained at these entities are updated based on the events occurring in the PIN. Below are some of the events (not exhaustive):

- 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 8.2.2.2-1: Dynamic profile information of a PIN

Parameter Name	Parameter Description	PIN Server	PEMC	PEGC
PIN ID	The identifier of the PIN	Y	Y	Y
Current PIN services	List of services that are currently offered within a PIN	Y	Y	N
PIN state	Indicates the current state of the PIN (activated or de-activated). When the PIN is in deactivated state services offered by the PIN are inaccessible and no PIN elements can join the PIN. Also PEGC closes all the communication channel it has created for the flow of application traffic from PIN elements via 5GS to the application server	Y	Y	Y
Current PEMC list	The list of PINE dynamic information for PINE(s) that currently have the role of PEMC: > PINE identifier > Role (e.g., primary or secondary) > PEMC current IP address > Duration or time period allowed as PEMC > Heartbeat timer value (see NOTE 2)	Y	Y	Y
Current PEGC list	The list of PINE dynamic information for PINE(s) that currently have the role of PEGC: > PINE identifier > Role (e.g., primary or backup) > PEGC current IP address > Duration or time period allowed as PEGC > Maximum number of served PINE(s) > List of currently served PINE(s) information > Heartbeat timer value (see NOTE 3)	Y	Y	Y
PIN Elements List	List of PIN elements currently registered/joined the PIN and their details			
	> PINE ID	Y	Y	Y
	> Endpoint information of each PINE (e.g. URI, FQDN, IP address, port number) used to communicate with the PINE (NOTE 1).	Y	Y	Y
	> Services offered by the PIN element	Y	Y	N
	> Reachability information of the PIN element NOTE: Reachability information of the PIN element may include the IP address which is internally routable via PEGC (like LAN or Layer 2 gateway) or routable via 5GS.	Y	Y	Y
	> List of application clients for this PIN element:	Y	Y	Y
	>> Minimum KPIs required by each application client to operate effectively within the PIN (e.g., PIN bandwidth, PIN request rate, PIN response time)	Y	Y	Y
	>> Operational schedules of each application client (e.g., time windows)	Y	Y	Y
	> 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
	> 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
	> Heartbeat timer value defining the periodicity of heartbeat requests this PIN element sends to the PEMC to indicate this PIN element is still available within the PIN.	Y	Y	Y

NOTE 1: The port number is the port used by a PINE to expose a service within the PIN.
NOTE 2: The heartbeat timer value defining the periodicity of heartbeat requests that the PEMC sends to the PIN server to indicate the PEMC is still available and serving as a PEMC.
NOTE 3: The heartbeat timer value defining the periodicity of heartbeat requests that the PEGC sends to the PEMC to indicate the PEGC is still available and serving as a PEGC.

8.2.2.3 PIN client profile

Table 8.2.2.3-1 describes the list of information elements that needs to be shared by the PIN element when requesting to join the PIN.

Table 8.2.2.3-1: PIN client profile

Parameter Name	Status	Parameter Description
PIN ID	M	The identifier of the PIN to which the PIN element wants to join
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
PINE role	O	Role of PINE: PEMC, PEGC, other
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 whether it can be assigned with the role of PEMC or PEGC etc.
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.
Port number	M	Port number of PIN client on PINE to support PIN enabler layer communication. NOTE: The port number is the port used by a PINE to expose a service within the PIN.

8.3 PIN server discovery

8.3.1 General

Some of the PIN management procedures involves the PIN server and hence the PINE requires the PIN server endpoint address before triggering the PIN management procedures, for example, the PIN creation procedure. Also there could be multiple PIN servers deployed within a PLMN and it is important to PIN elements to discover the appropriate PIN server to connect.

8.3.2 Procedure

8.3.2.1 Static PIN server discovery

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;
- derived from HPLMN identifier for non-roaming scenario or from VPLMN identifier for roaming scenario.
- DNS query for PIN server.

8.3.2.2 Procedures of PIN server discovery via PEGC

Some of the PIN elements can have the application interaction towards the PEGC, for example, via WiFi or Bluetooth, and in these case 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.

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 supports the open access and can reroute the request from PINE to PEMC behind the PEGC;

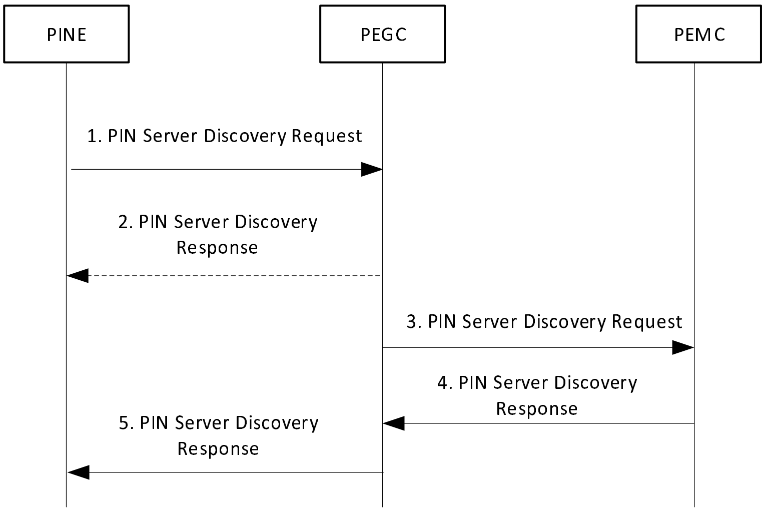
PINE
PEGC
PEMC
1. PIN Server Discovery Request
2. PIN Server Discovery Response
3. PIN Server Discovery Request
4. PIN Server Discovery Response
5. PIN Server Discovery Response

Figure 8.3.2.2-1: Procedures of PIN server discovery via PEGC

1. The PINE sends PIN server discovery request to PEGC. The requests include the GPSI, MAC address, if has, UE location.
2. (Optional) The PEGC can directly deliver the PIN server discovery response to PINE, including PIN server end point information to PIN elements. The end point information of PIN server includes URI(s), FQDN(s), IP address(es)) of PIN server.
3. If the PINE has open access to PEGC, that the PEGC should route the PIN server discovery request to PEMC that behind the PEGC.

4-5. The PEMC delivers the PIN server discovery response to PEGC and the PEGC routes the response to PINE, including PIN server end point information to PIN elements. The end point information of PIN server includes URI(s), FQDN(s), IP address(es)) of PIN server.

8.3.3 Information flows

8.3.3.1 General

The following information flows are specified for PIN creation:

- PIN server discovery request and response;

8.3.3.2 PIN server discovery request

Table 8.3.3.2-1 describes information elements in the PIN server discovery request from the PINE to the PEGC/PEMC.

Table 8.3.3.2-1: PIN server discovery request

Information element	Status	Description
UE Identifier	M	The identifier of the hosting UE (i.e. GPSI or identity token) or PINE.
MAC address	O	MAC address of the device.
UE location	O	The location information of the UE. The UE location is described in clause 7.2.7.

8.3.3.3 PIN server discovery response

Table 8.3.3.3-1 describes information elements in the PIN server discovery response from the PEGC/PEMC to the PINE.

Table 8.3.3.3-1: PIN server discovery response

Information element	Status	Description
Successful response	O (see NOTE)	Indicates that the PIN server discovery request was successful.
> PIN server endpoint information	M	Includes URI(s), FQDN(s), IP address(es)) of PIN server.
Failure response	O (see NOTE)	Indicates that the PIN server discovery request failed.
> Cause	M	Provides the cause for PIN server discovery request failure.
NOTE: At least one of the IE shall be present.		

8.4 Registration

8.4.1 General

The PINE (including PEMC and PEGC) should have a registration procedure in PIN server, before consuming the certain PIN service.

The registration procedure includes the direct registration and indirect registration.

- Direct registration:
    - For the PEMC, the PEMC sends PINE Registration Request (MAC address, vendor name, device description, PEMC Address) 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.
    - 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.

- Indirect registration:
  - 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.

At the network side, a PIN server should be deployed. During the PINE registration procedure, 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.

8.4.2 Registration Procedure

8.4.2.1 General

The PINE may register to the PIN server via either the PEMC or the PEGC depends on the communication range, supported RATs.

8.4.2.2 Procedure

8.4.2.2.1 PINE registration directly to PIN server

Figure 8.4.2.2.1-1 illustrates PIN registration procedure based on request/response model.

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 UE Identifier is available;
3. The PINE has been authorized to communicate with the PIN server;

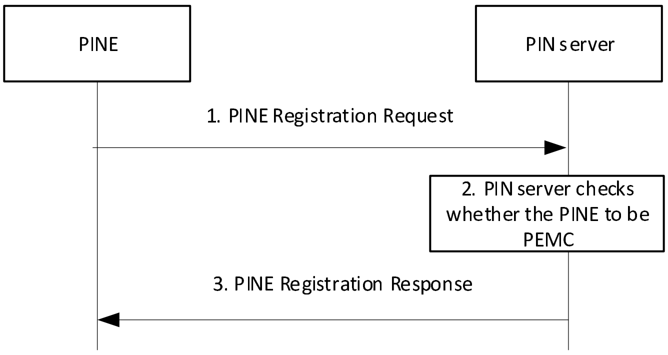
PINE
PIN server
1. PINE Registration Request
2. PIN server checks whether the PINE to be PEMC
3. PINE Registration Response

Figure 8.4.2.2.1-1: PINE registration directly to PIN server

1. The PINE (including PINE/PEMC/PEGC) sends a PINE Registration Request to the PIN server. The request includes the security credentials of the PINE received during authorization procedure and also the request may include the GPSI, MAC address, vendor name, device description, PINE Address.

   If the PEMC trigger the request, this 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 checks whether the UE identified by the GPSI has subscribed to be a PEMC. Also, the PIN server can check the whether the UE identified by the GPSI has subscribed to be a PEMC itself. If subscribed, it checks the subscription of PINE 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.

3. The PIN server responds to the PINE with PINE Registration Response with allocated PIN client ID in successful response.

If the registration procedure fails, the PIN server should give the failure response that indicates the cause of registration request failure.

8.4.2.2.2 PINE registration indirectly to PIN server

The following procedure defines the PEMC can substitute the PINE/PEGC to register into PIN server.

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.

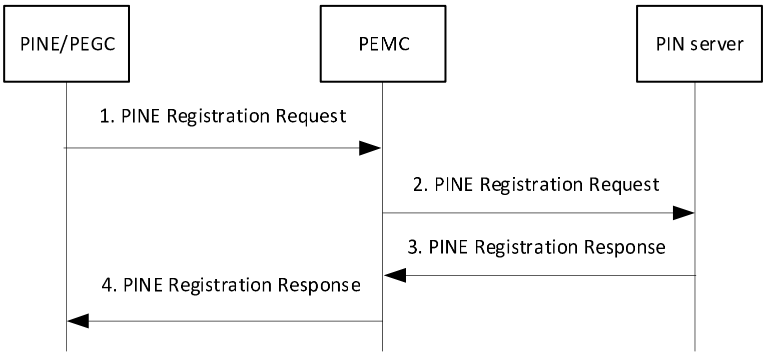
PINE/PEGC
PEMC
PIN server
1. PINE Registration Request
2. PINE Registration Request
3. PINE Registration Response
4. PINE Registration Response

Figure 8.4.2.2.2-1: PINE registration indirectly to PIN server

1. The PINE/PEGC sends PINE Registration Request to the PEMC. The request includes the security credentials of the PINE received during authorization procedure and also the request may include the GPSI, MAC address, vendor name, device description, PINE Address.
2. If the PEMC receives the PINE Registration Request from PINE, the PEMC may represent the PINE to register into PIN server by sending the PINE registration request to PIN server.

   If the PEMC represents the PINEs to perform registration procedure, it should send a PINE Registration Request to PIN server including an Indication of representation registration and Lists of PINEs/PEGCs.
3. The PIN server responds to the PEMC with PINE Registration Response with allocated PIN client ID in successful response.

   When the PINE Registration Request that containing Indication of representation registration, the PIN server shall verify whether PINE(s) and PEGC(s) included in the List of PINEs/PEGCs are allowed to fullfill the requested role or not. The PIN server responses to PEMC with a successful response and may include a list of accepted registration information and a list of rejected registration information (if any). If all the PINEs in the Lists of PINEs/PEGCs are rejected, the PIN server sends a failure response including the failure cause.
4. The PEMC sends the response received in step 3 to the PINE/PEGC.

   When the PEMC receiving the PINE Registration response from PIN server, the PEMC should extract the accepted registration information and rejected registration information (if any) for all the PINEs, and send the result to each PINE in the Lists of PINEs/PEGCs.

8.4.2.2.3 PINE registration via PEGC before join

The PINE registration towards the PIN server via the PEGC based on request/response model is depicted in figure 8.4.2.2.3-1.

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;

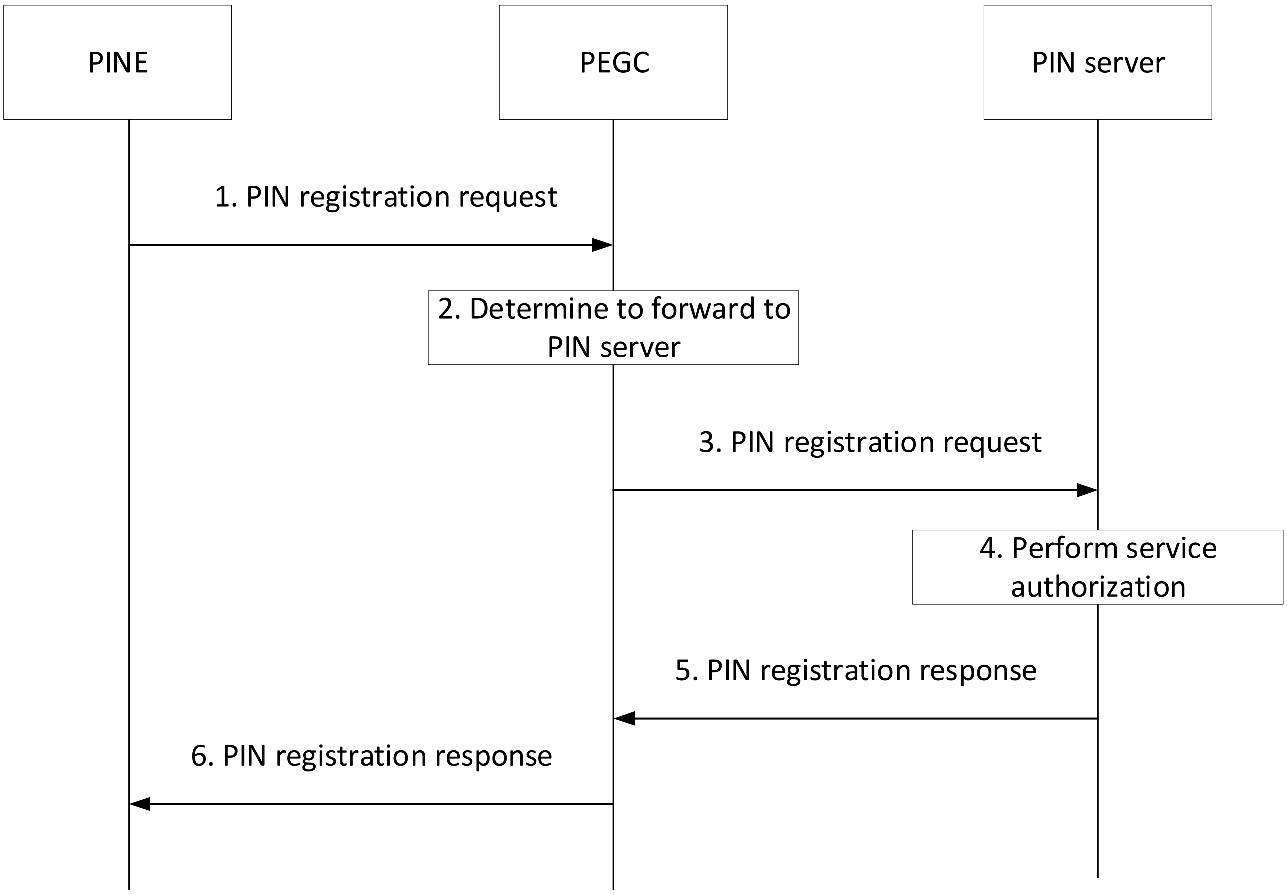
PINE
PEGC
PIN server
1. PIN registration request
2. Determine to forward to PIN server
3. PIN registration request
4. Perform service authorization
5. PIN registration response
6. PIN registration response

Figure 8.4.2.2.3-1: PINE registration to PIN server via PEGC before join

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.

8.4.2.2.4 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 8.4.2.2.4-1 illustrates the PINE registration during the PIN join via the PEGC procedure based on request/response model.

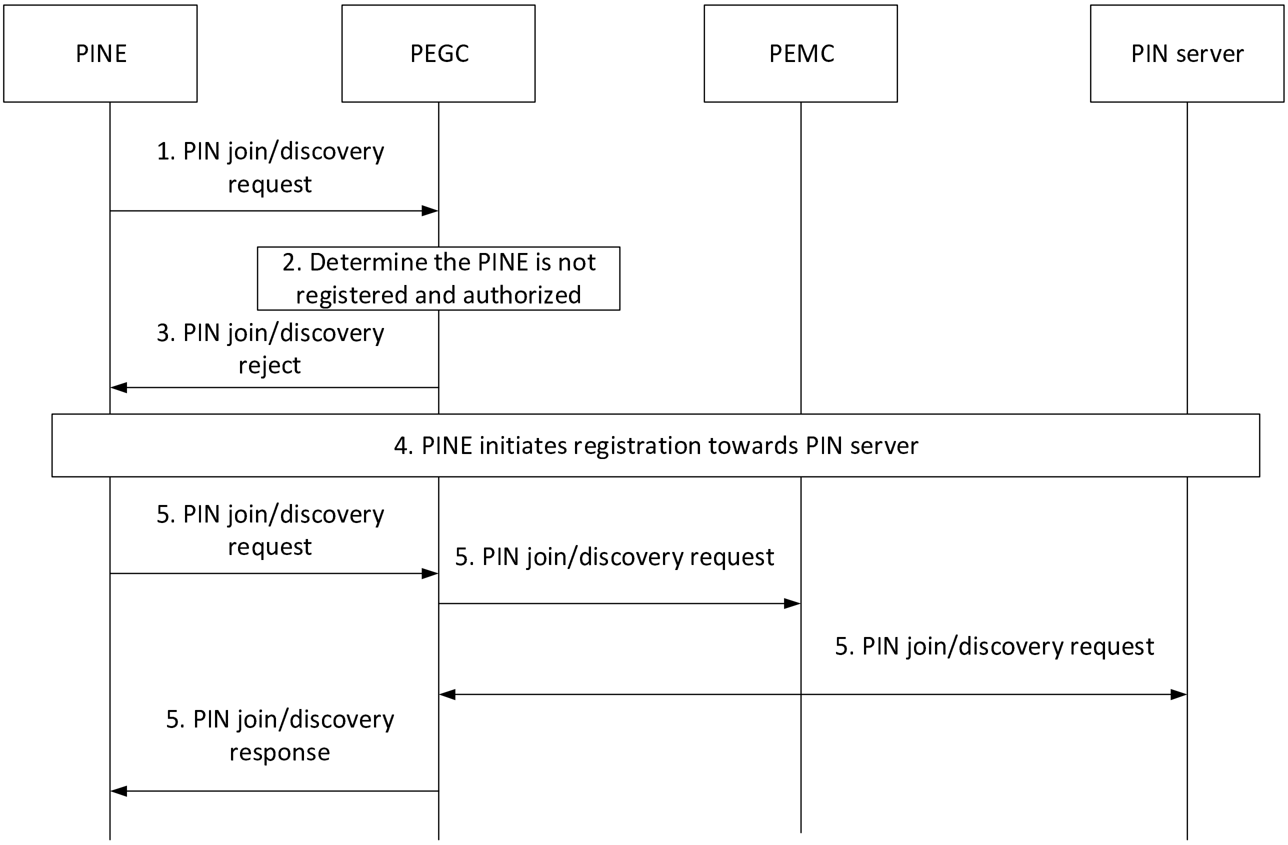
PINE
PEGC
PEMC
PIN server
1. PIN join/discovery request
2. Determine the PINE is not registered and authorized
3. PIN join/discovery reject
4. PINE initiates registration towards PIN server
5. PIN join/discovery request
5. PIN join/discovery request
5. PIN join/discovery request
5. PIN join/discovery response

Figure 8.4.2.2.4-1: PINE registration to PIN server during PIN join 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 8.4.2.2.1.

5-6. After the registration, the PINE will use the PIN client ID and credentials to initiate the PIN join/discovery again.

8.4.2.2.5 PINE de-registration directly to PIN server

Figure 8.4.2.2.5-1 illustrates PIN de-registration procedure based on request/response model.

Pre-conditions:

1. The PINE has been pre-configured or has discovered the address (e.g. IP address, FQDN, URI) of the PIN server and is already registered with the PIN server;
2. The UE Identifier is available;
3. The PINE has been authorized to communicate with the PIN server;

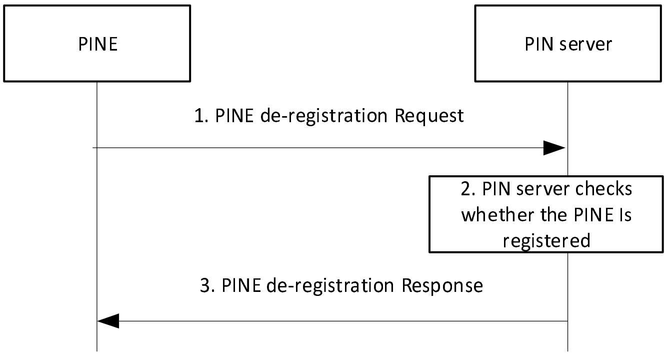
PINE
PIN server
1. PINE de-registration Request
2. PIN server checks whether the PINE Is registered
3. PINE de-registration Response

Figure 8.4.2.2.5-1: PINE de-registration directly to PIN server

1. The PINE (including PINE/PEMC/PEGC) sends a PINE de-registration Request to the PIN server. The request includes the security credentials of the PINE received during authorization procedure and also the request may include the GPSI, MAC address, vendor name, device description, PIN element ID/PIN client ID, PINE Address.
2. The PIN server checks whether the UE identified by the GPSI has active registration with the PIN server.
3. The PIN server responds to the PINE with PINE de-registration response which contains the status of the PINE de-registration request. If the PINE is successfully de-registered, the PIN server deletes all the configuration information it has related to the PIN element that is being de-registered. If the de-registration procedure fails, the PIN server should give the failure response to indicates that indicates the cause of de-registration request failure.

8.4.2.2.6 PINE de-registration indirectly to PIN server

Figure 8.4.2.2.6-1 illustrates PINE De-registration request to PIN Server indirectly via PEMC based on request/response model.

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.

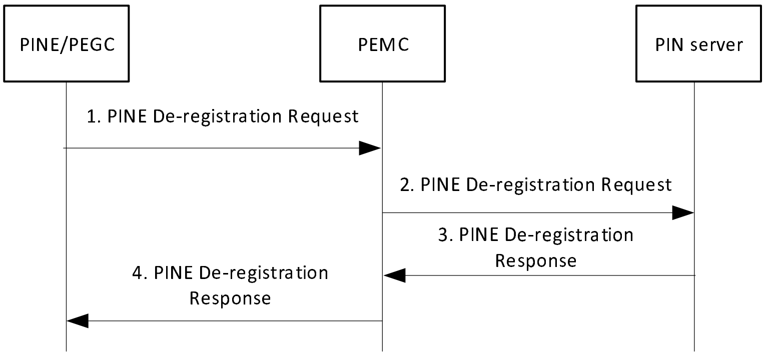
PINE/PEGC
PEMC
PIN server
1. PINE De-registration Request
2. PINE De-registration Request
3. PINE De-registration Response
4. PINE De-registration Response

Figure 8.4.2.2.6-1: PINE de-registration indirectly to PIN server

1. The PINE (including PINE/PEMC/PEGC) sends a PINE de-registration Request to the PEMC. The request includes the security credentials of the PINE received during authorization procedure and also the request may include the GPSI, MAC address, vendor name, device description, PIN element ID/PIN client ID, PIN ID, PINE Address.
2. The PEMC sends the PINE de-registration request to PIN server.
3. The PIN server checks whether the UE identified by the GPSI has active registration with the PIN server. The PIN server responds to the PINE with PINE de-registration response which contains the status of the PINE de-registration request. If the PINE is successfully de-registered, the PIN server deletes all the configuration information it has related to the PIN element that is being de-registered. If the de-registration procedure fails, the PIN server should give the failure response that indicates the cause of de-registration request failure.
4. The PEMC sends the response received in step 3 to the PINE/PEGC.

8.4.2.2.7 PINE update registration to PIN server

Figure 8.4.2.2.7-1 illustrates PIN update registration procedure based on request/response model.

Pre-conditions:

1. The PINE has been pre-configured or has discovered the address (e.g. IP address, FQDN, URI) of the PIN server and is already registered with the PIN server;
2. The UE Identifier is available;
3. The PINE has been authorized to communicate with the PIN server;

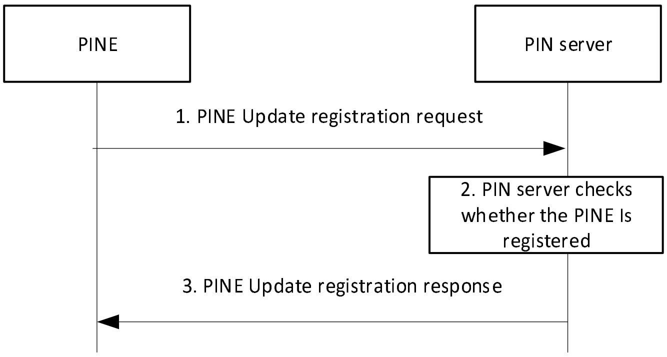
PINE
PIN server
1. PINE Update registration request
2. PIN server checks whether the PINE Is registered
3. PINE Update registration response

Figure 8.4.2.2.7-1: PINE update registration to PIN server

1. The PINE (including PINE/PEMC/PEGC) sends a PINE update registration request to the PIN server directly or via PEGC. The request includes the security credentials of the PINE received during authorization procedure and also the request may include the GPSI, MAC address, vendor name, device description, PIN element ID/PIN client ID, PINE Address.

   If the registration request is sent from PINE to PEGC, the PEGC delivers the PINE update registration request to the PIN server.
2. The PIN server checks whether the UE identified by the GPSI has active registration with the PIN server.
3. The PIN server responds to the PINE with PINE update registration response directly or via PEGC which contains the status of the PINE update registration request. If the update registration procedure fails, the PIN server should give the failure response to indicates that indicates the cause of update registration request failure.

8.4.2.3 Information flow/elements

8.4.2.3.1 General

The following information flows are specified for PIN registration:

- PINE Registration request and response;

8.4.2.3.2 PINE Registration request

Table 8.4.2.3.2-1 describes information elements in the PINE Registration request from the PINE (including PEMC, PEGC, PINEs) to the PIN server.

Table 8.4.2.3.2-1: PINE Registration request (PINE/PEGC to PIN server, or PEMC represents PINE/PEGC to PIN server)

Information element	Status	Description
UE Identifier	M	The identifier of the hosting UE (i.e. GPSI or identity token) of PINE/ PEMC/PEGC
Security credentials	M	Security credentials resulting from a successful authorization for the PIN service.
Indication of representation registration	O	If PEMC represents PINE/PEGC to perform registration to PIN server, this indication is included.
Lists of PINEs/PEGCs		
> MAC address	O	MAC address of the requested PINEs.
> Vendor name	O	The vendor name of the PINE
> Device description	O	Description of the device.
> PINE Address	M	The IP address of PINE, if available.
> Port number	M	Port number of PIN client on PINE/PEMC/PEGC to support PIN enabler layer communication. The port number is the port used by a PINE to expose a service within the PIN.
> PINE Capabilities	O	Identify whether the PINE is capable of becoming a PEMC, a PEGC or both.
> > Maximum number of PINEs (see NOTE)	O	Indicates the maximum number of PINE that can be managed by the PEMC or PEGC
Services that PINE provide	O	Indicate the service that PINE can provide.
NOTE: Only present if PINE Capabilities is present.		

8.4.2.3.3 PINE Registration response

Table 8.4.2.3.3-1 describes information elements in the PINE Registration response from the PIN server to the PINE (including PEMC, PEGC, PINEs).

Table 8.4.2.3.3-1: PINE Registration response

Information element	Status	Description
Successful response	O (see NOTE)	Indicates that the PINE Registration request was successful.
> PIN client ID	M	Identifier of the newly assigned PIN client ID to PINEs.
> Role of PEMC	O	The UE identified by the GPSI has subscribed to be a PEMC.
> Role of PEGC	O	The UE identified by the GPSI has subscribed to be a PEGC.
Failure response	O (see NOTE)	Indicates that the PIN registration request failed.
> Cause	M	Provides the cause for PIN registration request failure.
NOTE: At least one of the IE shall be present.		

8.4.2.3.4 PINE de-registration request

Table 8.4.2.3.4-1 describes information elements in the PINE de-registration request from the PINE (including PEMC, PEGC, PINEs) to the PIN server.

Table 8.4.2.3.4-1: PINE de-registration request

Information element	Status	Description
UE Identifier	M	The identifier of the hosting UE (i.e. GPSI or identity token) of PINE/PEMC/PEGC
Security credentials	M	Security credentials resulting from a successful authorization for the PIN service.
MAC address	O	MAC address of the requested PINEs.
Vendor name	O	The vendor name of the PINE
Device description	O	Give the description of the device.
PINE Address	O	The IP address of PINE, if available.

8.4.2.3.5 PINE de-registration response

Table 8.4.2.3.5-1 describes information elements in the PINE de-registration response from the PIN server to the PINE (including PEMC, PEGC, PINEs).

Table 8.4.2.3.5-1: PINE de-registration response

Information element	Status	Description
De-registration status	M	Indicates whether the PINE de-registration request was successful or not. Includes the cause of the failure if the de-registration fails.

8.4.2.3.6 PINE update registration request

Table 8.4.2.3.6-1 describes information elements in the PINE update registration request from the PINE (including PEMC, PEGC, PINEs) to the PIN server.

Table 8.4.2.3.6-1: PINE update registration request

Information element	Status	Description
UE Identifier	M	The identifier of the hosting UE (i.e. GPSI or identity token) of PINE/PEMC/PEGC
Security credentials	M	Security credentials resulting from a successful authorization for the PIN service.
MAC address	O	MAC address of the requested PINEs.
Vendor name	O	The vendor name of the PINE
Device description	O	Give the description of the device.
PINE Address	O	The IP address of PINE, if available.
Port number	M	Port number of PIN client on PINE/PEMC/PEGC to support PIN enabler layer communication. The port number is the port used by a PINE to expose a service within the PIN.
PINE Capabilities	O	Identify whether the PINE is capable of becoming a PEMC, a PEGC or both.
> Maximum number of PINEs (see NOTE)	O	Indicates the maximum number of PINE that can be managed by the PEMC or PEGC
Services that PINE provide	O	Indicate the service that PINE can provide.
NOTE: Only present if PINE Capabilities is present.		

8.4.2.3.7 PINE update registration response

Table 8.4.2.3.7-1 describes information elements in the PINE de-registration response from the PIN server to the PINE (including PEMC, PEGC, PINEs).

Table 8.4.2.3.7-1: PINE update registration response

Information element	Status	Description
Update registration status	M	Indicates whether the PINE update registration request was successful or not. Includes the cause of the failure if the update registration fails.

8.5 PIN Management

8.5.1 General

8.5.2 PIN Create

8.5.2.1 General

After the UE or PINE acquires the role of PEMC and receives the address of PIN server, the UE or PINE can trigger a creation of PIN towards PIN server.

Below are the possible scenarios when the PEMC request for the creation of PIN:

- No PIN elements or PEGC have established connection with PEMC;
- One or more PIN elements including PEGCs, PEMCs have established connection with PEMC via non-3GPP access. In this case 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 responds to PEMC containing the details of the PIN including the PIN ID, the PEGC information, access control information configured in PEGC etc.

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

8.5.2.2 Procedure

8.5.2.2.1 PIN creation procedure

Figure 8.5.2.2.1-1 illustrates PIN creation procedure based on request/response model.

Pre-conditions:

1. The UE or PINE 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 UE or PINE has already been registered in PIN server;
4. The UE or PINE has been authorized to communicate with the PIN server;
5. PINE 1 is assigned the role of PEMC by PIN server and PINE-2 is the PEGC of the PIN;

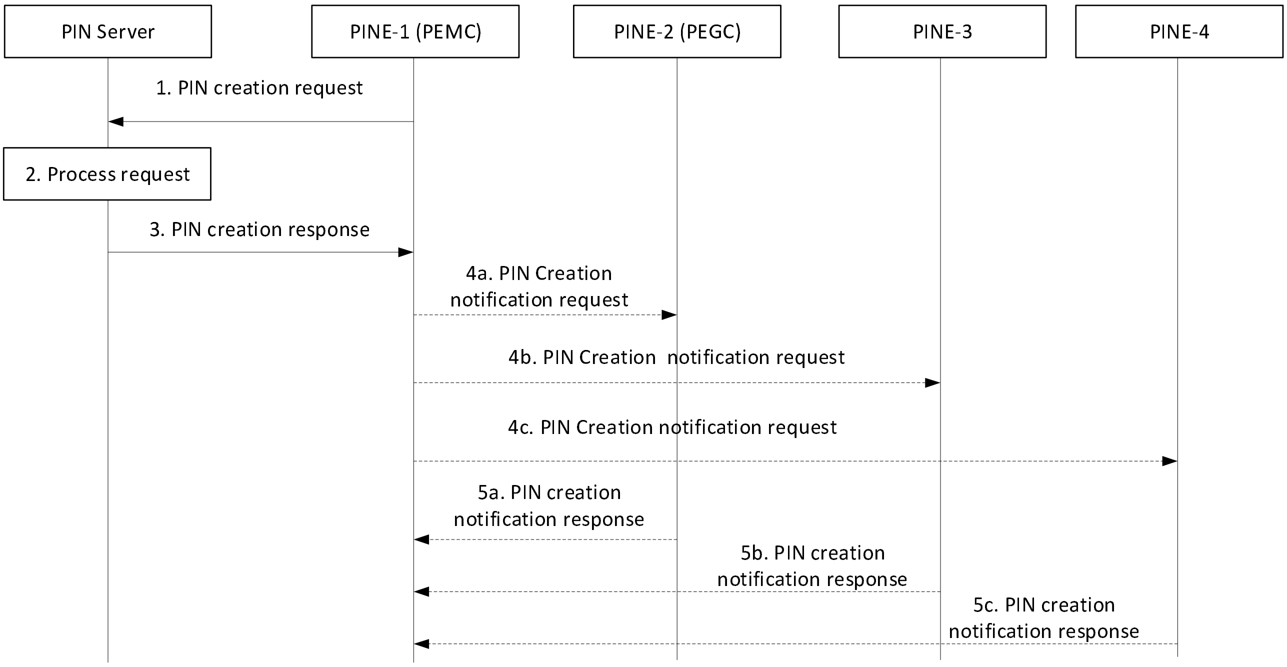
PIN Server
PINE-1 (PEMC)
PINE-2 (PEGC)
PINE-3
PINE-4
1. PIN creation request
2. Process request
3. PIN creation response
4a. PIN Creation notification request
4b. PIN Creation notification request
4c. PIN Creation notification request
5a. PIN creation notification response
5b. PIN creation notification response
5c. PIN creation notification response

Figure 8.5.2.2.1-1: PIN creation procedure

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 PINE-1 received during authorization procedure and may include the UE identifier such as GPSI, PIN client ID, UE location and PIN client profile(s) information.

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

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

   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. This procedure doesn't have conflict with that other PEMC requests to join the certain PIN and becomes PEMC separately.

   The PEMC creates the PIN profile and delivers the PIN profile to PIN server.

NOTE 1: 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.

The PIN creation request also includes service that PINE can provide.

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

3. The PIN server sends a successful PIN creation response to PEMC, 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.

   The member of newly created PIN may include PEMC and (optional) the list of PIN elements which are authorized to be added into the PIN by PIN server.

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

   The PIN server may determine the list of candidates PEGCs for this PIN according to the gateway capability provided by PINE during PINE registration procedure. Only the PINE that has the capability of gateway can be selected as the PEGCs for this PIN.

   If no PEGCs are available for this PIN, the PIN server initiates PIN create response with PIN creation failure to PEMC.

NOTE 2: The PEMC may validate if the PEGCs provided by the PIN server are available at the PINE by performing the PEGC discovery procedure as described in clause 8.9.2.1.5.

   If the one or more PEGCs are indicated in the PIN creation response, the PIN server indicates the PIN client ID/GPSI of one PINE to be the PEGC. Also, the assigned IP address or port number is delivered in the PIN creation 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 via PIN creation response. And the PEMC delivers the access control information to PEGC via PIN creation notification request.

   - If the access control information decided by PEMC, the PEMC delivers the access control information to PEGC via PIN creation notification request.

   It is possible for PIN server to indicate several devices as PEGCs in a PIN. And it is possible for PIN server to indicate the PEGC and PEMC is the same device in a PIN.

   The PIN server may update the PIN profile and delivers the updated PIN profile to PEMC.

4a-4c. [Optional] If the PIN creation response contains the list of PIN elements, the PEMC generates the PIN creation notification request to individual PINEs 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.

   During this step, the PEMC may distribute the Access control information to PINE, to be used by PIN elements in PIN to access 5G or access other application outside of PIN.

   The updated the PIN profile may be synchronized to PEGC or PINEs.

5a-5c. [Optional] The individual PIN elements sends the PIN creation 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 PINE-1 (PEMC) creates a PIN with PEGC (PINE-2) and other accepted PIN elements in PIN.

8.5.2.3 Information flows

8.5.2.3.1 General

The following information flows are specified for PIN creation:

- PIN creation request and response;
- PIN creation notification request and response;

8.5.2.3.2 PIN creation request

Table 8.5.2.3.2-1 describes information elements in the PIN creation request from the PINE/PEGC to the PIN server.

Table 8.5.2.3.2-1: PIN creation request

Information element	Status	Description
UE Identifier	M	The identifier of the hosting UE (i.e. GPSI or identity token) or the PIN client ID of PEMC
Security credentials	M	Security credentials resulting from a successful authorization for the PIN service.
PIN client profile(s)	O	Profiles of PIN clients. The PIN client profiles are further described in Table 8.2.2.3.
UE location	O	The location information of the UE. The UE location is described in clause 7.2.7.
Lists of PINEs	O	The PINEs that has already communicated with PEMC directly, and intend to add these PINE into PIN.
Additional PEMCs	O	Indicate additional PEMCs that are allowed to manage the PIN.
Services that PINE provide	O	Indicate the service that PINE can provide.

8.5.2.3.3 PIN creation response

Table 8.5.2.3.3-1 describes information elements in the PIN creation response from the PIN server to the PEMC.

Table 8.5.2.3.3-1: PIN creation response

Information element	Status	Description
Successful response	O	Indicates that the PIN creation request was successful.
> PIN ID	M	Identifier of the newly created PIN.
> Expiration time	M	Indicates the expiration time of the PIN.
> Heartbeat Timer	M	Assigned PEMC/PEGC/PINE heartbeat timer. The PIN server assigns the heartbeat to PEMC/PEGC/PINE individually.
> Lists of PINEs	O	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.
> PEGC information	O	Includes the PEGC information for example,
>> Identifier of PEGCs	M	Indicates the PINE identifier authorized to be the PEGCs of this PIN.
>> PEGC address	O	Assigned IP address or port number of PEGC
>> Access control information	O	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
Failure response	O	Indicates that the PIN creation request failed.
> Cause	M	Provides the cause for PIN creation request failure.

8.5.2.3.4 PIN creation notification request

Table 8.5.2.3.4-1 describes information elements in the PIN creation notification request from the PEMC to the PEGC and PIN elements.

Table 8.5.2.3.4-1: PIN creation notification request

Information element	Status	Description
PIN ID	M	Identifier of the newly created PIN.
Indication	M	Indicates whether the PIN element is made the member of the newly created PIN.
> PEGC information	O	Includes the PEGC information for example,
>> Identifier of PEGCs	O	Indicates the PINE identifier that to be the PEGCs of this PIN.
>> PEGC address	O	Assigned IP address or port number of PEGC
>> Access control information	O	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
> Heartbeat Timer	M	Heartbeat timer value assigned to PEGC/PINE

8.5.2.3.5 PIN creation notification response

Table 8.5.2.3.5-1 describes information elements in the PIN creation notification response from the PEGC, PIN elements to the PEMC.

Table 8.5.2.3.5-1: PIN creation notification response

Information element	Status	Description
Successful response	O (see NOTE)	Indicates that the PIN creation notification request was successful.
Failure response	O (see NOTE)	Indicates that the PIN creation notification request failed.
> Cause	M	Indicates the cause of PIN creation notification request failure.
NOTE: At least one of the IE shall be present.		

8.5.3 PIN delete

8.5.3.1 General

The PIN which is in use can be deleted based on the decision by PEMC or PIN server as described below:

- Decided by PEMC. The PEMC of a PIN decides to delete the PIN and sends request to PIN server. The PIN server accepts the request and deletes the PIN.
- Decided by PIN server. If the PIN is configured to exist for a particular duration and if it continues to exist post the duration the PIN server can decide to delete the PIN and release the resources associated with the PIN.

Once the PIN is deleted, the PIN elements in PIN shall not be able to utilize the services by the PIN or 5GS anymore and cannot access the application server. The network resources allocated for this PIN will be released.

Since the configuration related to the duration of the PIN is available with PEMC and when the duration of the PIN expires, the PEMC can directly delete the PIN locally and without having to be authorized by the PIN server. After the PIN is deleted by PEMC, the PEMC can update the status of PIN to the PIN server.

8.5.3.2 Procedure

8.5.3.2.1 PIN delete procedure involving PIN server

Figure 8.5.3.2.1-1 illustrates PIN delete procedure triggered by PEMC based on request/response model.

Pre-conditions:

1. PIN is successfully created and in use;
2. PEMC of the PIN decides to delete the PIN which could be based on the request from the authorized user or for any other reason which are implementation specific.

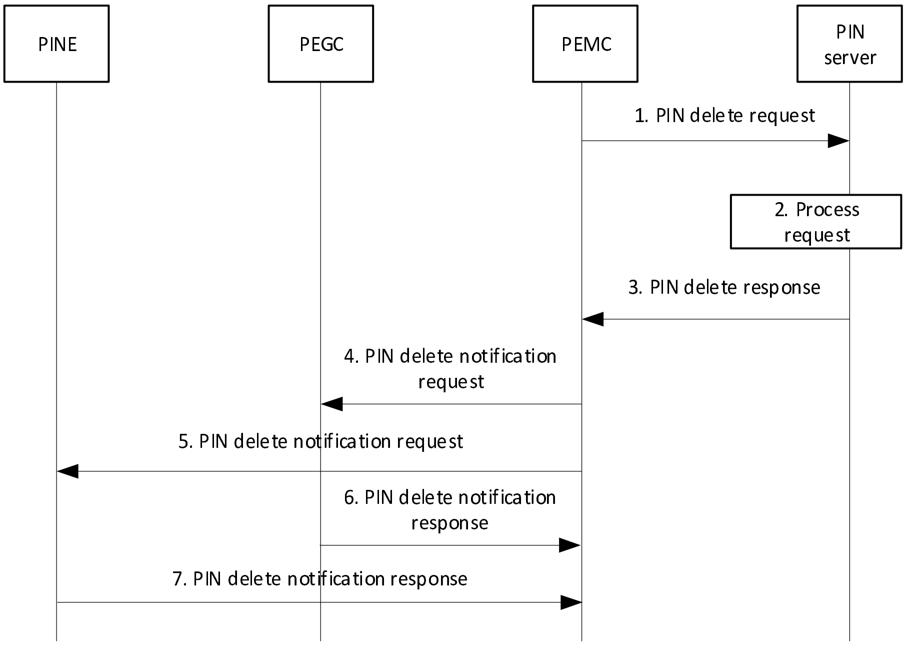
PINE
PEGC
PEMC
PIN server
1. PIN delete request
2. Process request
3. PIN delete response
4. PIN delete notification request
5. PIN delete notification request
6. PIN delete notification response
7. PIN delete notification response

Figure 8.5.3.2.1-1: PIN delete procedure involving PIN server

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 identifies the PIN to be deleted.

NOTE: The security credentials delivery and the authorization procedure happen at application layer.

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 PIN delete response to PEMC.

   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 cannot access to 5GS via PEGC anymore.
4. When the PIN is deleted, the PEMC sends the PIN delete notification request to the PEGC containing the PIN ID of the deleted PIN.
5. PEMC sends the PIN delete notification request to the PIN elements containing the PIN ID of the deleted PIN.
6. The PEGC sends the PIN delete notification response to acknowledge the receipt of the notification and disables the 5GS connection permission and access control information for the PIN elements in this PIN.
7. The PIN elements in this PIN sends the PIN delete notification response to acknowledge the receipt of the notification. The PIN elements in this PIN can delete the information about this PIN, for example, the PIN profile.

8.5.3.2.2 PEMC decided PIN deletion

The PEMC can directly trigger the PIN delete procedure, for example, when the duration associated with the PIN expires, without having to be authorized from PIN server. After the PIN is deleted successfully, the PEMC updates the PIN status to PIN server.

Figure 8.5.3.2.2-1 illustrates PIN delete locally procedure triggered by PEMC based on request/response model.

Pre-conditions:

1. PIN is successfully created and in use;
2. PEMC of the PIN decides to delete the PIN.

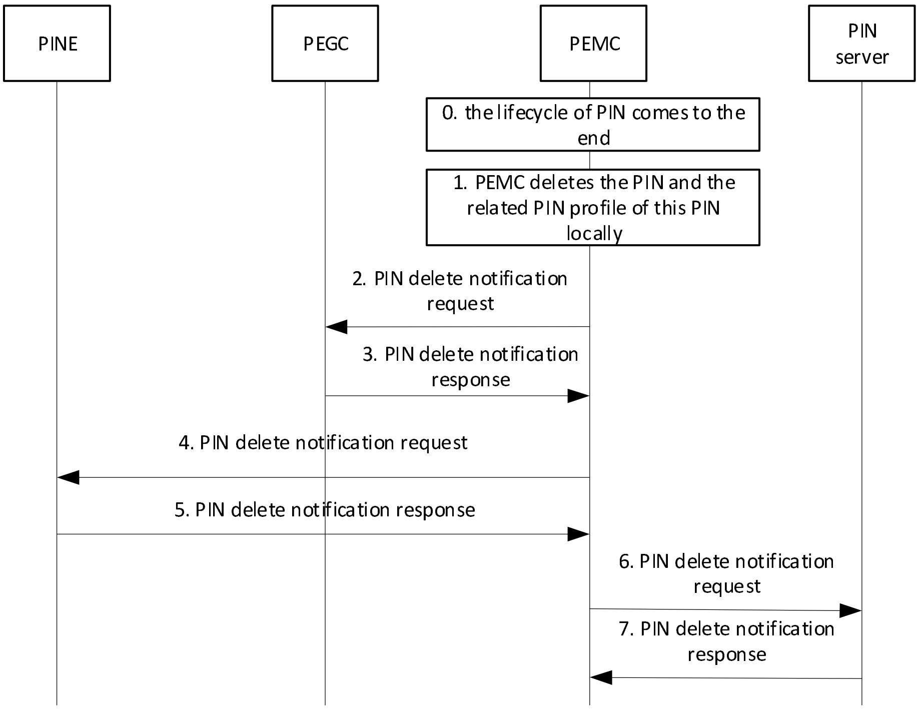
PINE
PEGC
PEMC
PIN server
0. the lifecycle of PIN comes to the end
1. PEMC deletes the PIN and the related PIN profile of this PIN locally
2. PIN delete notification request
3. PIN delete notification response
4. PIN delete notification request
5. PIN delete notification response
6. PIN delete notification request
7. PIN delete notification response

Figure 8.5.3.2.2-1: PIN delete locally by PEMC

0. The duration associated with the PIN expires and PEMC decides to delete the PIN.

1. The PEMC deletes the PIN which indicated by PIN ID locally. The PEGC information and the information related to this PIN such as PIN profile, PIN dynamic profile are also deleted.

2-5. The same procedures as step 4-7 defined in Figure 8.5.2.2.1-1.

6. The PEMC sends the PIN delete notification request to the PIN server that the PIN is deleted locally and this notification request contains the PIN ID of the deleted PIN.

7. The PIN server sends the PIN delete notification response to acknowledge the receipt of the notification.

8.5.3.2.3 PIN delete procedure triggered by PIN server

Figure 8.5.3.2.3-1 illustrates PIN delete procedure triggered by PIN server based on request/response model.

Pre-conditions:

1. PIN is successfully created and in use;

2. The PIN server decides to delete a PIN.

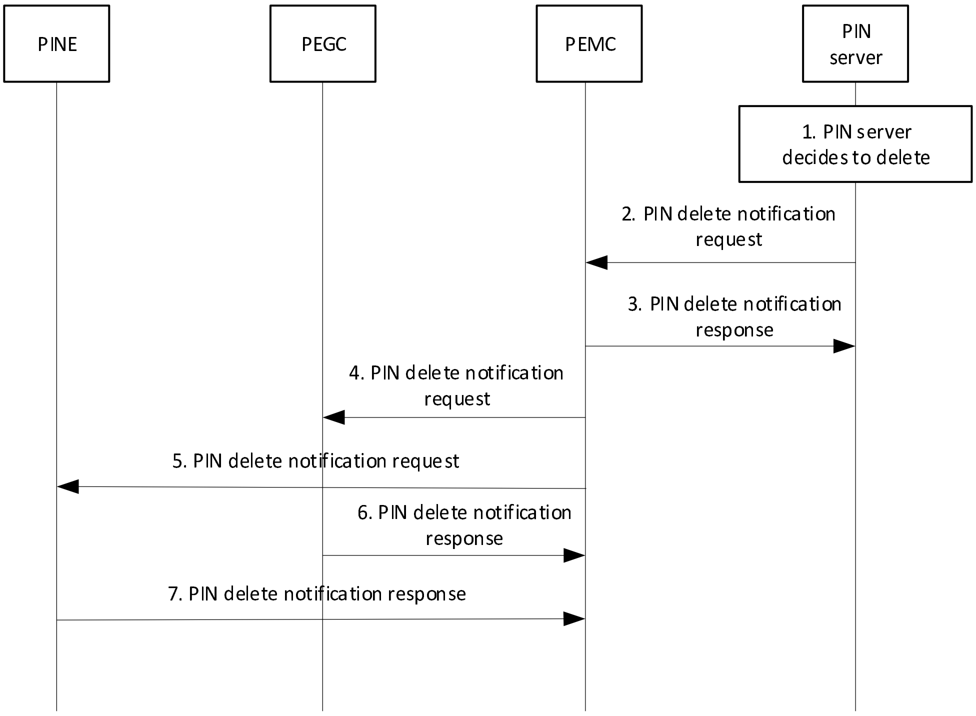
PINE
PEGC
PEMC
PIN server
1. PIN server decides to delete
2. PIN delete notification request
3. PIN delete notification response
4. PIN delete notification request
5. PIN delete notification request
6. PIN delete notification response
7. PIN delete notification response

Figure 8.5.3.2.3-1: PIN delete procedure triggered by PEMC

1. An event occurs at the PIN server that satisfies the trigger conditions for deleting the PIN. This event could the PIN continues to exist post the expiry of duration associated with it or the PIN server decides to not provide any PIN service in this PIN.

2. If the PIN server decides to delete the PIN, the PIN server sends a PIN delete notification request to PEMC.

3. The PEMC sends the PIN delete notification response to the PIN server to acknowledge the receipt of the notification.

4-7. The same as step 4 – 7 in Figure 8.5.3.2.2-1

8.5.3.3 Information flows

8.5.3.3.1 General

The following information flows are specified for PIN creation:

- PIN delete request and response;
- PIN delete notification request and response;

8.5.3.3.2 PIN delete request

Table 8.5.3.3.2-1 describes information elements in the PIN delete request from the PEMC to the PIN server.

Table 8.5.3.3.2-1: PIN delete request

Information element	Status	Description
PIN ID	M	Identifier of the deleted PIN.
Security credentials	M	Security credentials resulting from a successful authorization for the PIN service.

8.5.3.3.3 PIN delete response

Table 8.5.3.3.3-1: PIN delete response

Information element	Status	Description
Successful response	O	Indicates that the PIN delete request was successful.
Failure response	O	Indicates that the PIN delete request failed.
> Cause	M	Provides the cause for PIN delete request failure.

8.5.3.3.4 PIN delete notification request

Table 8.5.3.3.4-1: PIN delete notification request

Information element	Status	Description
PIN ID	M	Identifier of the deleted PIN.

8.5.3.3.5 PIN delete notification response

Table 8.5.3.3.5-1: PIN delete notification response

Information element	Status	Description
Successful response	O	Indicates that the PIN delete notification request was successful.
Failure response	O	Indicates that the PIN delete notification request failed.
> Cause	O	Indicates the cause of PIN delete notification request failure.

8.5.4 Multiple PEMCs/PEGCs

8.5.4.1 General

This clause describes the procedures for the configuration and use of multiple PEMCs and PEGCs in a PIN.

For a PIN having a large number of PIN elements, covering a large area, and/or requiring extra reliability, multiple PIN Elements may be assigned the role of PEMC and/or PEGC.

8.5.4.2 Procedure

8.5.4.2.1 PIN configuration with default and backup PEGCs

Figure 8.5.4.2.1-1 illustrates a procedure for configuring a new PIN Element, when requesting to join, with a default PEGC and one or more backup PEGCs.

Pre-conditions:

1. The PEMC is pre-configured or has discovered the address (e.g. IP address, FQDN, URI) of the PIN server.
2. The PEMC is authorized to access the PIN server.
3. The PEMC has registered to the PIN server.
4. The PEMC has requested and has been authorized by the PIN server to create a PIN.
5. The required KPIs of the PIN have been configured.
6. PINE-1, PINE-2, PEGC-A and PEGC-B have registered to the PEMC and PIN server.
7. PINE-1, PINE-2, PEGC-A and PEGC-B have subscribed with the PEMC for the PIN status as specified in clause 8.5.X.2.1.

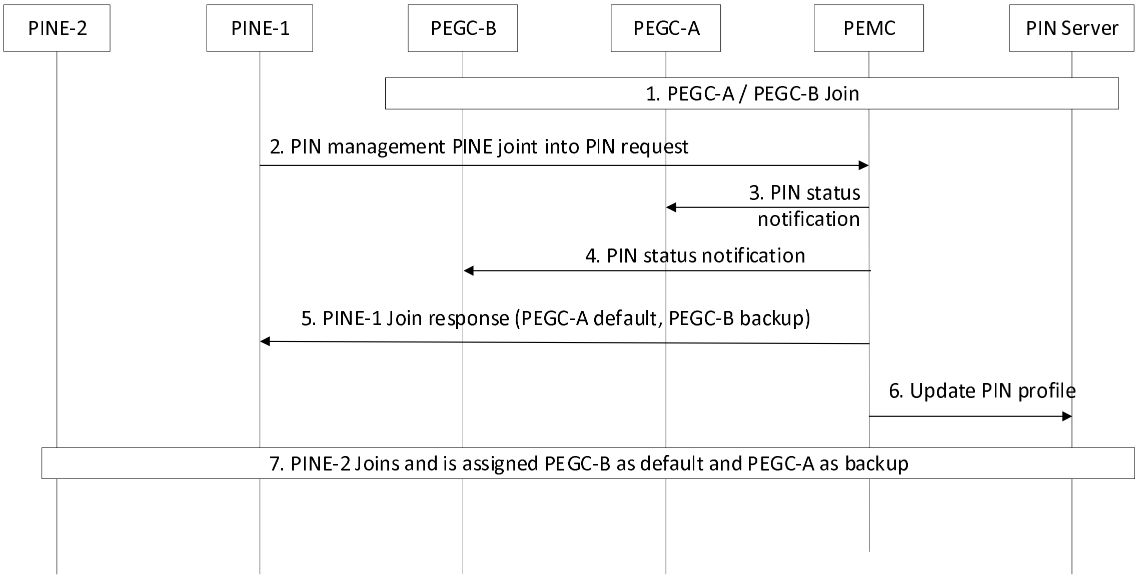
PINE-2
PINE-1
PEGC-B
PEGC-A
PEMC
PIN Server
1. PEGC-A / PEGC-B Join
2. PIN management PINE joint into PIN request
3. PIN status notification
4. PIN status notification
5. PINE-1 Join response (PEGC-A default, PEGC-B backup)
6. Update PIN profile
7. PINE-2 Joins and is assigned PEGC-B as default and PEGC-A as backup

Figure 8.5.4.2.2-1: Multiple PEGC configuration for a PIN

1. PEGCs (e.g., PEGC-A and PEGC-B) shall join the PIN by sending PIN management PINE join into PIN requests to the PEMC. The PIN Client Profile information (supported PIN roles, supported PEGC KPIs, Supported PEGC schedule, UE location) shall be included in the requests. The PEMC shall use this information to determine whether multiple PEGCs are needed to meet the required KPIs of the PIN and which PIN elements (e.g., PEGC-A and PEGC-B) are able to serve as PEGCs. The PEMC shall configure multiple PEGCs (e.g., PEGC-A and PEGC-B) with a role of PEGC if needed. The PEMC shall then send a PIN profile update to the PIN server informing the PIN server that of the multiple PEGCs.
2. When PINEs (e.g., PINE-1) send a PIN management PINE join into PIN request to the PEMC, PIN Client Profile information (application client KPIs, application client schedule, UE location) shall be included in the request. The PEMC shall use this information and the PEGC information the PEMC received in step 1 to determine the optimal default and backup PEGCs for the PINE. For example, PEMC assigns PEGC-A as the default PEGC for PINE-1, and PEGC-B as the backup PEGC for PINE-1.

3. The PEMC shall send a default PEGC (e.g., PEGC-A) PIN status notification to update its local PIN Profile information to reflect that a PINE (e.g., PINE-1) is authorized to relay PIN communications via the PEGC.

4. The PEMC shall send any backup PEGCs (e.g., PEGC-B) PIN status notification to update their local PIN Profile information to reflect that a PINE (e.g., PINE-1) is authorized to relay PIN communications via the PEGC.

5. The PEMC shall return a PIN management PINE join into PIN response to PINE-1. The response shall include updated PIN client profile information informing the PINE that it shall use a specified PEGC (e.g., PEGC-A) as its default PEGC, and a specified PEGC (e.g., PEGC-B) as its backup PEGC.

6. The PEMC shall send a PIN profile update to the PIN server informing the PIN server of a PEGC (e.g., PEGC-A) serving as the default PEGC for a PINE (e.g., PINE-1) and any PEGCs (e.g., PEGC-B) serving as backup PEGCs for a PINE.

7. Steps 2 to 6 may be repeated for any additional PINEs joining the PIN. For example, based on PIN client profile information provided by PINE-2, the PEMC configures PEGC-B to serve as the default PEGC for PINE-2 and PEGC-A to serve as the backup PEGC for PINE-2.

8.5.4.2.2 PIN management with multiple PEMCs

Figure 8.5.4.2.2-1 illustrates a procedure for managing the PIN with multiple PEMCs. PIN elements when registering with the PIN indicates that they have the capability to act as PEMC and are assigned with primary or secondary PEMC role as described in the subclause 8.4.2.2.1.

Pre-conditions:

1. A PIN owner or admin 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.

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

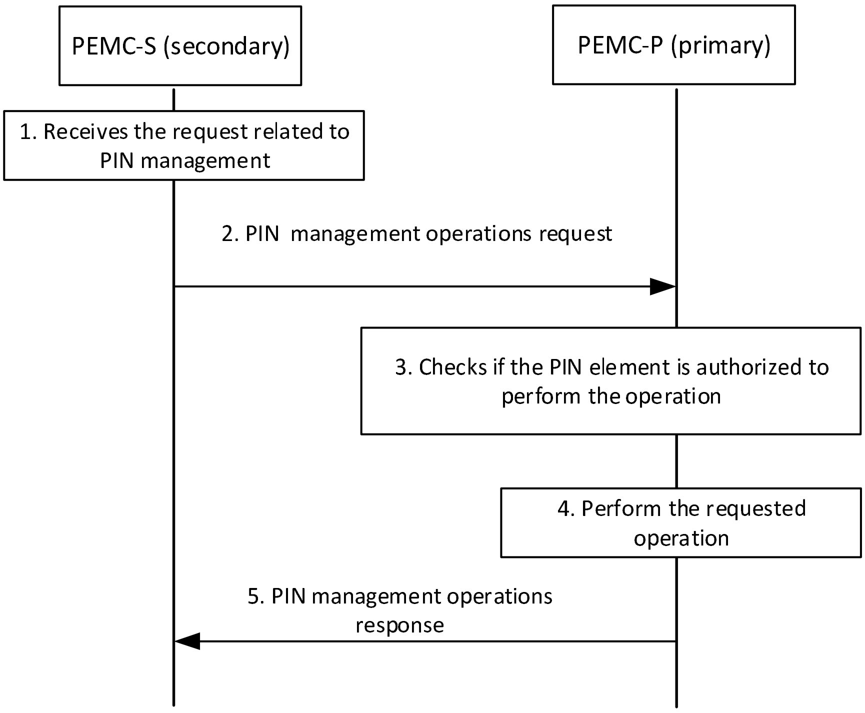
PEMC-S (secondary)
PEMC-P (primary)
1. Receives the request related to PIN management
2. PIN management operations request
3. Checks if the PIN element is authorized to perform the operation
4. Perform the requested operation
5. PIN management operations response

Figure 8.5.4.2.2-1: PIN management with multiple PEMCs

1. PEMC-S receives a request from PIN owner or PIN admin to perform any of the PIN management operations. Some of the PIN management operations (PIN profile update, PIN element removal) shall be performed by secondary PEMC (PEMC-S) itself and some operations (PIN deletion, PIN activation and PIN deactivation) can be sent to primary PEMC (PEMC-P) which shall be validated and executed by the PEMC-P.
2. 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.
3. PEMC-P on receiving the request checks whether the PEMC-S is authorized as secondary PEMC in-order to perform the operation.
4. If the authorization succeeds, PEMC-P proceeds with the requested operation.
5. PEMC-P sends the response to PEMC-S containing the status or result of the requested operation.

NOTE: Only the operations that are required to be performed by the PIN owner or 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.

8.5.4.2.3 Notifying the PIN elements of PEGC details

Figure 8.5.4.2.3-1 illustrates a procedure for notifying the PIN elements about the change in default or backup PEGC when multiple PIN elements have the PEGC capability.

Pre-conditions:

1. The PIN is configured and PEGC-1 is the designed PEGC.
2. PIN elements have subscribed for PIN status as specified in clause 8.5.9.2.1.

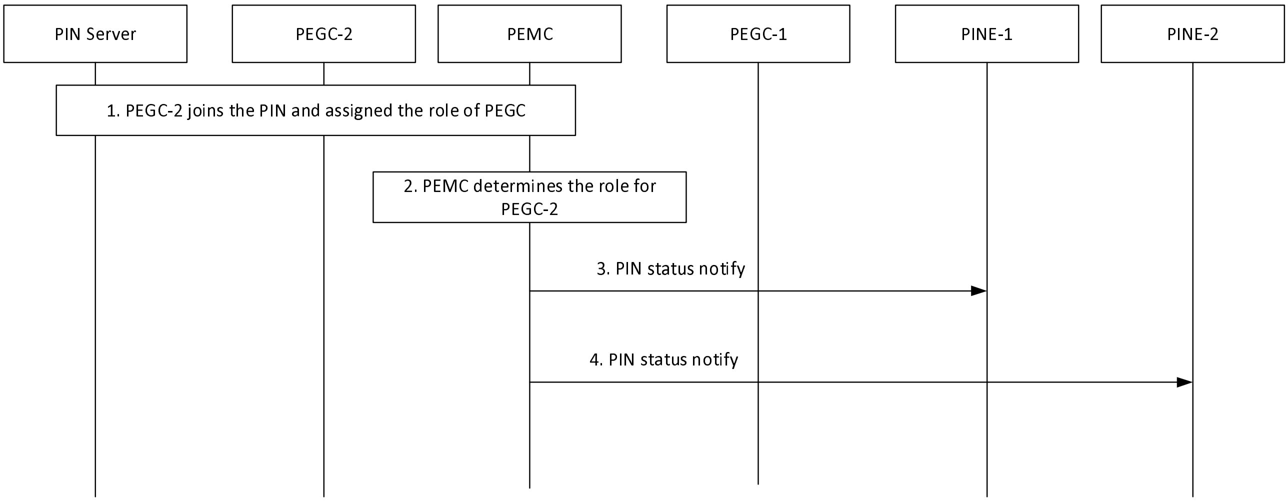
PIN Server
PEGC-2
PEMC
PEGC-1
PINE-1
PINE-2
1. PEGC-2 joins the PIN and assigned the role of PEGC
2. PEMC determines the role for PEGC-2
3. PIN status notify
4. PIN status notify

Figure 8.5.4.2.3-1: Notifying the PIN elements of PEGC details

1. PEGC-2 is authorized to join the PIN as specified in the sub-clause 8.4 and is assigned with the role of PEGC.
2. Upon joining the PIN, the PEMC determines the list of PIN elements for which PEGC-2 can act as default PEGC or backup PEGC. (e.g. PEGC-2 is designated to be the backup PEGC for PINE-1 and default for PINE-2).
3. The PEMC sends the PIN status notify to PINE-1 indicating that PEGC-2 is the backup PEGC for PINE-1 as specified in as specified in clause 8.5.9.2.2.
4. The PEMC sends the PIN status notify to PINE-2 indicating that PEGC-2 is the default PEGC for PINE-2 as specified in as specified in clause 8.5.9.2.2.

8.5.4.3 Void

8.5.4.3.1 Void

8.5.5 PIN Profile Recovery

8.5.5.1 General

The PIN profile recovery procedure describes how the PEMC retrieves a PIN profile from a PIN server.

8.5.5.2 Procedure

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;

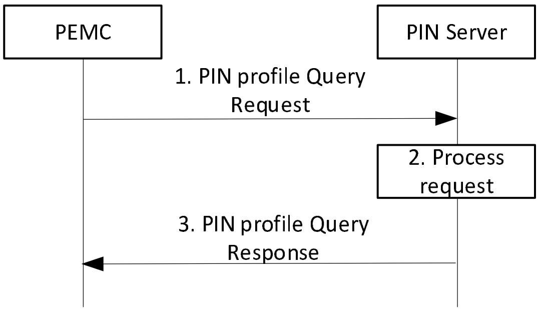

Figure 8.5.5.2-1: Query PIN profile procedure

1. The PEMC sends PIN Profile Query requests (PEMC ID, PIN ID) to the PIN server.
2. The PIN server determines whether the PEMC is one of the managers of the PIN. The PIN Server validates if the PEMC is authorized to perform the operation; if the PEMC is authorized, the PIN Server verifies if the PEMC is authorized to manage the PIN. The PIN server processes the request.
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.

8.5.5.3 Information flows

8.5.5.3.1 General

The following information flows are specified for PIN profile retrieval:

- PIN Profile Query request and response;

8.5.5.3.2 PIN Profile Query request

Table 8.5.5.3.2-1 describes information elements in the PIN Profile Query request from the PEMC to the PIN server.

Table 8.5.5.3.2-1: PIN Profile Query request

Information element	Status	Description
PIN ID	M	Identifier of the deleted PIN.
Security credentials	M	Security credentials resulting from a successful authorization for the PIN service.
Identifier of PEMC	M	Indicates the PINE identifier authorized to be the PEMC of this PIN.

8.5.5.3.3 PIN Profile Query Response

Table 8.5.5.3.3-1 describes information elements in the PIN Profile Query response from the PIN server to PEMC.

Table 8.5.5.3.3-1: PIN Profile Query Response

Information element	Status	Description
Successful response	O	Indicates that the PIN Profile Query request was successful.
> PIN profile	M	The PIN profile information retrieved from PIN server. The details of PIN profile information is described in clause 8.2.2.1.
Failure response	O	Indicates that the PIN Profile Query request failed.
> Cause	O	Indicates the cause of PIN Profile Query request failure.

8.5.6 Credential Provision

NOTE: In the current release, PIN client authentication (e.g.: PINE, PEMC or PEGC) relies on pre-provisioned information and no dynamic credential provision procedure is defined, and authorization within the PIN is defined in clause 8.10.

8.5.7 PIN discovery

8.5.7.1 General

Before the PINE trigger the PINE join into the PIN, the PINE should discover the available PIN.

For a certain PIN element, the PIN should be discovered and the PIN element can decide whether to join in the PIN. There are two 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.

8.5.7.2 Procedure

8.5.7.2.1 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;

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

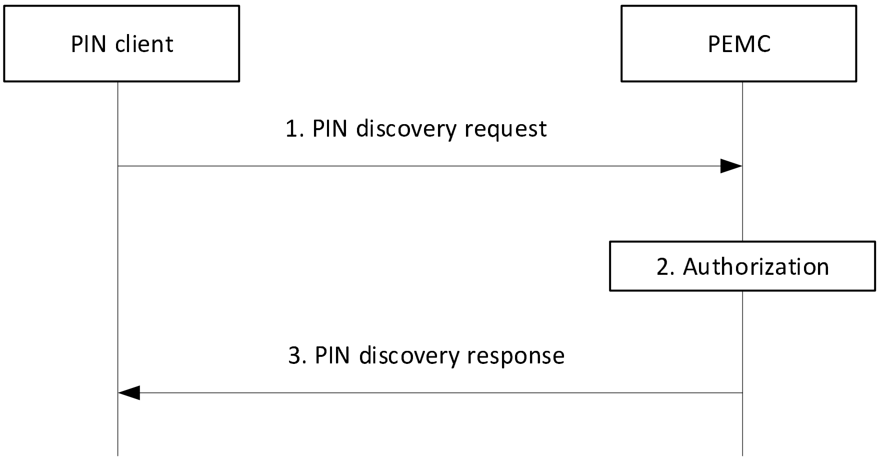

Figure 8.5.7.2.1-1: Procedures of PIN discovery based on PEMC

1. 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, Security credentials, the service that PINE wants to consume.

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

3. 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.

   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.

8.5.7.2.2 Procedures of PIN discovery with assistance of PIN server via PEGC

Some of the PIN elements can have the application layer connection with the PEGC, for example, via WiFi or Bluetooth, 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 8.5.7.2.2-1 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;

4. The PIN element has already had an application layer connection with a PEGC, and the PEGC can route the PIN discovery request to PIN server.

5. The PINE has already received the PIN server IP address.

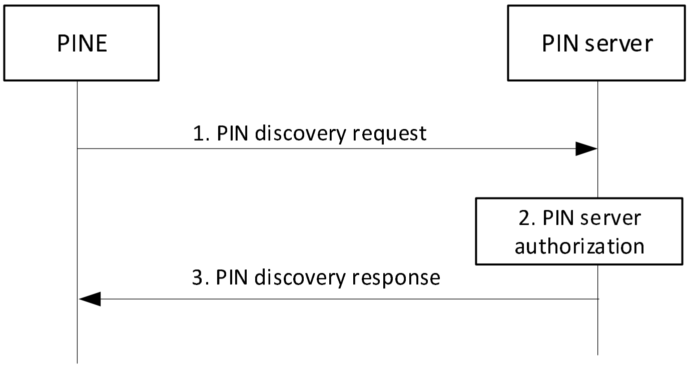

Figure 8.5.7.2.2-1: PIN discovery based on PIN server

1. The PIN client sends the PIN discovery request to PIN server via PEGC. The PEGC routes 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, Security credentials, the service that PINE wants to consume.

   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.

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

   The PIN server can decide the candidate PINs according to the filter information from PIN discovery request and the PIN Profile. The PIN server may determine the PIN which the PIN profile accords with the filter information in PIN discovery request. The candidate PINs can be multiple.

3. The PIN server sends a successful PIN discovery response to PIN client via PEGC, 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.

8.5.7.3 Information flows

8.5.7.3.1 General

The following information flows are specified for PIN discovery:

- PIN discovery request and response;

8.5.7.3.2 PIN discovery request

Table 8.5.7.3.2-1 describes information elements in the PIN discovery request from the PINE to the PEMC/PIN server.

Table 8.5.7.3.2-1: PIN discovery request

Information element	Status	Description
UE identifier	M	The identifier of the hosting UE (i.e. GPSI or identity token) of PINE
Security credentials	M	Security credentials resulting from a successful authorization for the PIN service.
UE location	O	The location information of the UE. The UE location is described in clause 7.2.7.
Filter information	O	Set of characteristics to determine required PIN
> Requested PIN service	O	Indicate the service that PINE wants to consume in the PIN
> Service area	O	Indicate the service area of a PIN.

8.5.7.3.3 PIN discovery response

Table 8.5.7.3.3-1 describes information elements in the PIN discovery response from the PEMC/PIN server to PINE.

Table 8.5.7.3.3-1: PIN discovery response

Information element	Status	Description
Successful response	O (see NOTE)	Indicates that the PIN discovery request was successful.
> PIN IDs	M	Identifier of the candidate PIN.
>> PIN Description	O	Human-readable description of the PIN, for example, the company name, location or the type of service.
>> PIN service	O	List of service that a PIN can provide, including the services provided by PINE or the service that can provided by application client on PINE: > PIN service Provider Identifier > PIN service type > PIN service Feature
>> PEMC information	O	Including the address or identifier of PEMC
Failure response	O (see NOTE)	Indicates that the PIN discovery request failed.
> Cause	M	Provides the cause for PIN discovery request failure.
NOTE: At least one of the IE shall be present.		

8.5.8 PINE management

8.5.8.1 General

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 the PIN elements with the necessary permission, for example, to be able to access to 5GS via the PEGC.

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.

8.5.8.2 Procedure

8.5.8.2.1 PIN client requests to join into a PIN

Figure 8.5.8.2.1-1 illustrates procedure of PIN client requests to join into a PIN, based on request/response model.

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 and already has application layer connection with PEMC;
4. The PIN client has already received the list of PIN ID, corresponding PEMC IP address and configuration information related to each PIN;

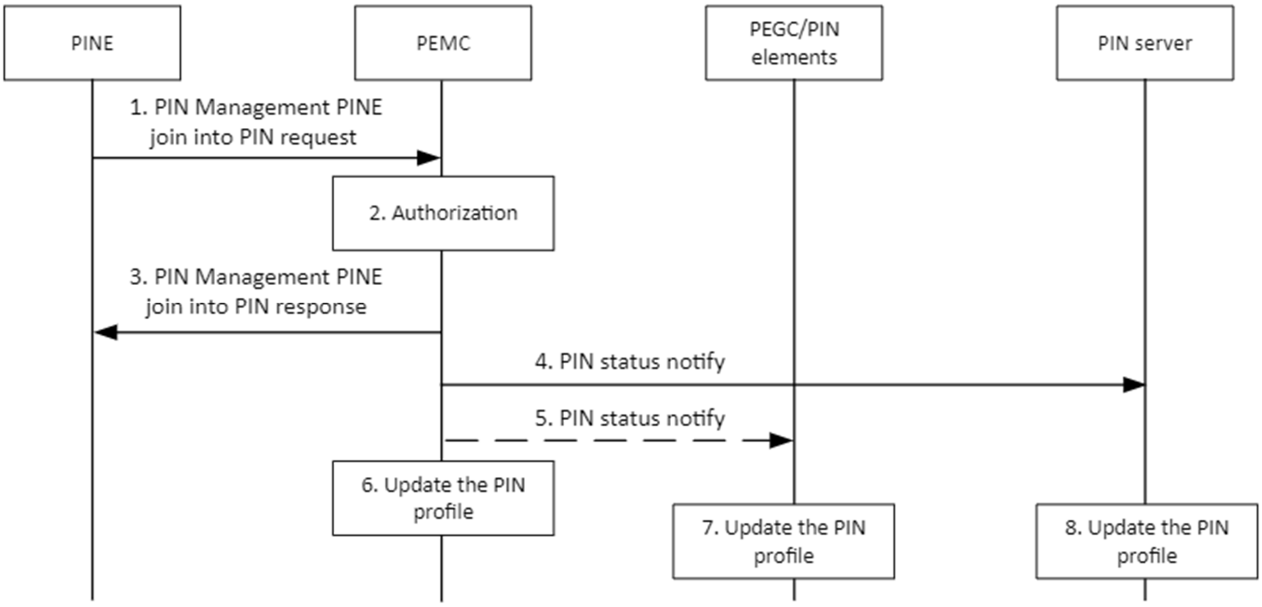
PINE
PEMC
PEGC/PIN elements
PIN server
1. PIN Management PINE join into PIN request
2. Authorization
3. PIN Management PINE join into PIN response
4. PIN status notify
5. PIN status notify
6. Update the PIN profile
7. Update the PIN profile
8. Update the PIN profile

Figure 8.5.8.2.1-1: PIN client requests to join into a PIN

1. The PIN client sends the PIN Management PINE join into PIN request to PEMC to join the PIN. The request includes the security credentials of the PIN client received during 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 defined in clause 8.5.8.3.2.

   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.

2. Upon receiving the request, the PEMC performs an authorization check to verify whether the PIN client has authorization to join the PIN. The authorization procedure is defined in clause 8.10.

3. The PEMC sends a successful PIN Management PINE join into PIN 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 in PIN to access 5G or access the network provided by PEGC. 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.

4. The PEMC sends PIN status notify to the PIN server containing the details of the new PIN client that joined the PIN, including PIN client ID, GPSI and etc.

5. The PEMC sends PIN status notify to the PEGC and other PIN elements that subscribed for PIN status notification which contains the details of the new PIN client that joined the PIN. And the PEGC decides to enables the PINE to access 5GS.

6-8. The PEMC/PEGC/PINE updates PIN profile with the details of the new PIN client that joined the PIN and the service that the PINE can provide.

8.5.8.2.2 Procedure of PIN elements decides to leave the PIN

The following procedure defines 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 and already has the application layer connection with the PEMC;

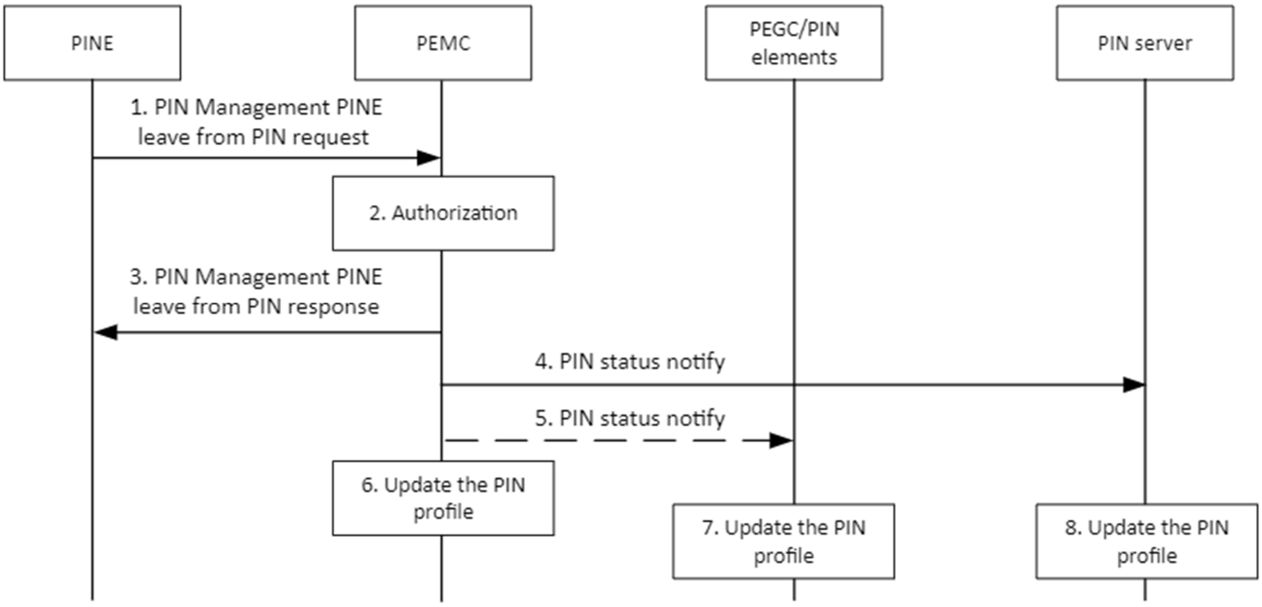
PINE
PEMC
PEGC/PIN elements
PIN server
1. PIN Management PINE leave from PIN request
2. Authorization
3. PIN Management PINE leave from PIN response
4. PIN status notify
5. PIN status notify
6. Update the PIN profile
7. Update the PIN profile
8. Update the PIN profile

Figure 8.5.8.2.2-1: PIN client decides to leave a PIN

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

2. The PEMC authorizes the request, and decides to remove a PIN client from a PIN which indicated by PIN client ID or UE GPSI. The authorization procedure is defined in clause 8.10.

3. The PEMC sends the PIN Management PINE leave from PIN response to PINE to notify that the PIN client is not the member of the PIN anymore.

4-5. The PEMC sends the PIN status notify Request to the PEGC, PIN server and PIN elements that subscribed for PIN status notification which contains the details of the PIN client that requested to leave the PIN. The details of the PINE include PIN client ID, GPSI and etc.

6-8. The PEMC/PEGC/PIN server updates the dynamic profile information of the PIN to remove the details of the PIN client that requested to leave the PIN. The PEGC disables the access control information for this PINE. The PEGC stops relaying traffic to the PINE.

8.5.8.2.3 Procedure of PEMC removes the PIN elements from a PIN

The following procedure defines 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 and already has the application layer connection with PEMC;

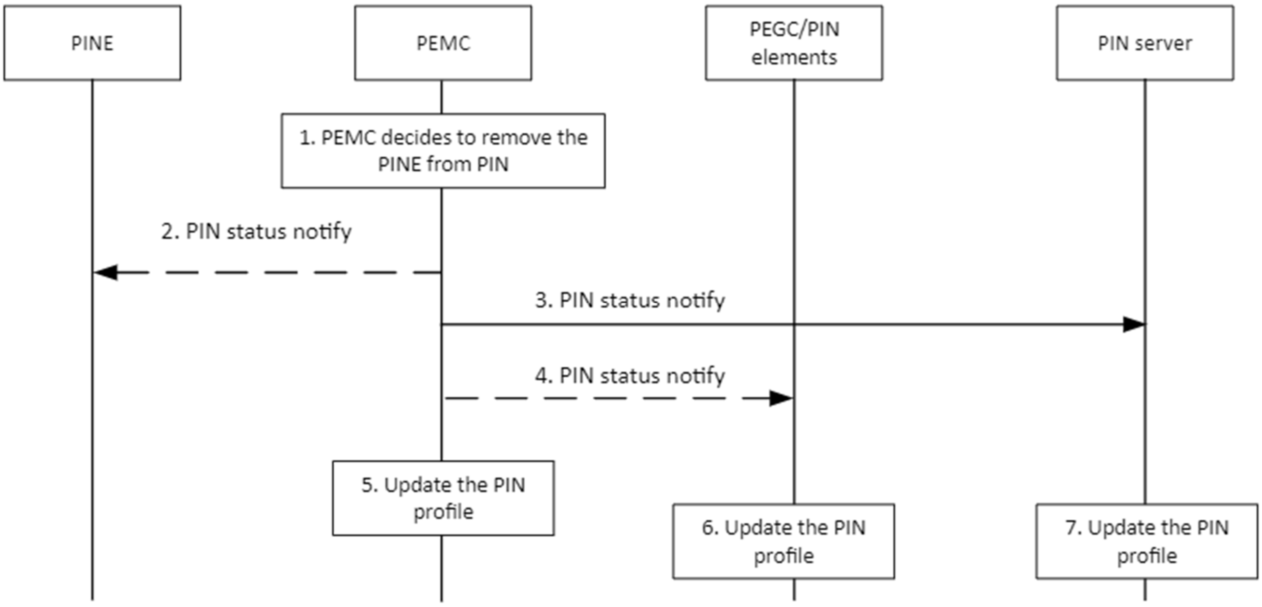
PINE
PEMC
PEGC/PIN elements
PIN server
1. PEMC decides to remove the PINE from PIN
2. PIN status notify
3. PIN status notify
4. PIN status notify
5. Update the PIN profile
6. Update the PIN profile
7. Update the PIN profile

Figure 8.5.8.2.3-1: Remove a PIN element from a PIN by PEMC

1. The PEMC decides to remove the PINE (identified by GPSI, PIN client ID and in certain PIN identified by PIN ID).
2. The PEMC sends the PIN status notify to the PINE that this PINE has been removed from the PIN that identified by PIN ID.

3-4. The PEMC sends the PIN status notify to the PEGC, PIN elements subscribed for PIN status notification and PIN server containing the details of the PIN client that is removed from the PIN. The details of the PINE include PIN client ID, GPSI and etc.

5-7. The PEMC/PEGC/PIN server updates the dynamic profile information of the PIN to remove the details of the PIN client that is removed from the PIN. The PEGC disables the access control information for this PINE. The PEGC stops relaying traffic to the PINE.

8.5.8.2.4 PINE join into PIN via PEGC

The PINE joins the PIN via the PEGC is depicted in Figure 8.5.8.2.4-1.

Pre-conditions:

1. The PINE has been pre-configured or has discovered the address (e.g. IP address, FQDN, URI) of the PEMC;
2. The PINE already establishes the connection with PEGC;
3. The PIN information to join is available at the PINE via e.g., PIN discovery procedure.

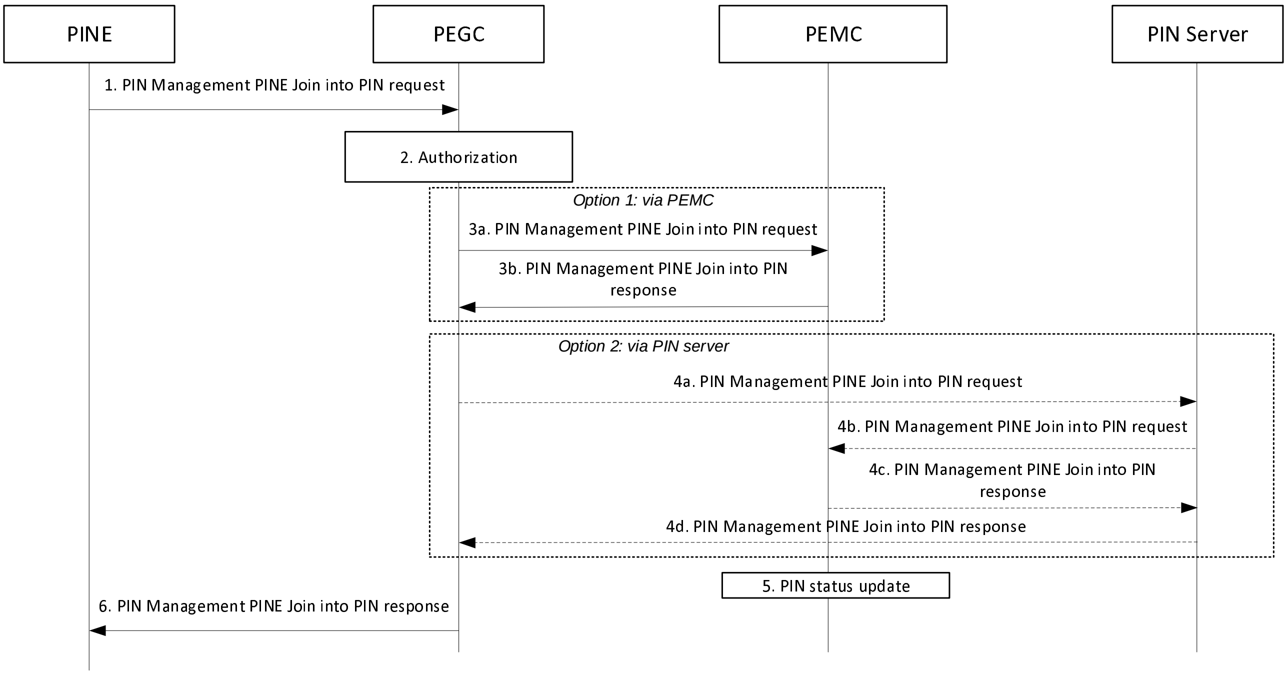
PINE
PEGC
PEMC
PIN Server
1. PIN Management PINE Join into PIN request
2. Authorization
Option 1: via PEMC
3a. PIN Management PINE Join into PIN request
3b. PIN Management PINE Join into PIN response
Option 2: via PIN server
4a. PIN Management PINE Join into PIN request
4b. PIN Management PINE Join into PIN request
4c. PIN Management PINE Join into PIN response
4d. PIN Management PINE Join into PIN response
5. PIN status update
6. PIN Management PINE Join into PIN response

Figure 8.5.8.2.4-1: PINE join into PIN via PEGC

1. The PINE sends PIN Management PINE join into PIN request to the PEGC. The PIN Management PINE join into PIN request contains the PIN ID which identifies the PIN to join, PINE client ID and credentials if available, PEMC identity/PIN server address.

   The request also includes service that PINE can provide.

2. The PEGC identifies the received message is the PIN Management PINE join into PIN request and perform the authorization. If authorized, the PEGC determines to forward the PIN Management PINE join into PIN request to the PEMC or the PIN server.

   If authorization in PEGC is failed, directly skip to step 6.

   The PEGC can decide to perform either Option 1 (from step 3a to step 3b) or Option 2 (from step 4a to step 4d). If direct communication between PEGC and PEMC always available, the PEGC performs Option 1.

3. (Option 1, step 3a and step 3b) The PEGC forwards the PIN Management PINE join into PIN request to the PEMC in step 3a, based on the PEMC identity in step 1 or by resolving the PIN ID. The PEMC authorized the PINE to join the PIN, and returns the PIN Management PINE join into PIN response to the PEGC in step 3b.

4. (Option 2, from step 4a to step 4d) The PEGC forwards the PIN Management PINE join into PIN request to the PIN server in step 4a based on the PIN server address in step 1 or by resolving the PIN ID. The PIN server forwards the PIN Management PINE join into PIN request to the PEMC in step 4b, and the PEMC authorized the PINE to join the PIN, and returns the PIN Management PINE join into PIN response to the PIN server in step 4c. Further the PIN server return the PIN server to the PEGC in step 4d.

5. After the join, the PEMC update the PIN and may notify other entities (e.g., existing joined members, PIN server). The PEMC triggers the PIN status notify to PEGC/PINE as indicated in step 5-6 of procedure Figure 8.5.8.2.2-1.

6. The PEGC return the PIN Management PINE join into PIN response to the PINE.

   If authorization in PEGC is failed, PEGC generates the PIN Management PINE join into PIN response to the PINE for the authorization failure.

8.5.8.2.5 PINE leave via PEGC

The PINE leaves the PIN via the PEGC is depicted in figure 8.5.8.2.5-1.

Pre-conditions:

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

2. The PINE already establishes the connection with PEGC;

3. The PEGC acts as the application layer relay as defined in 6.3.4

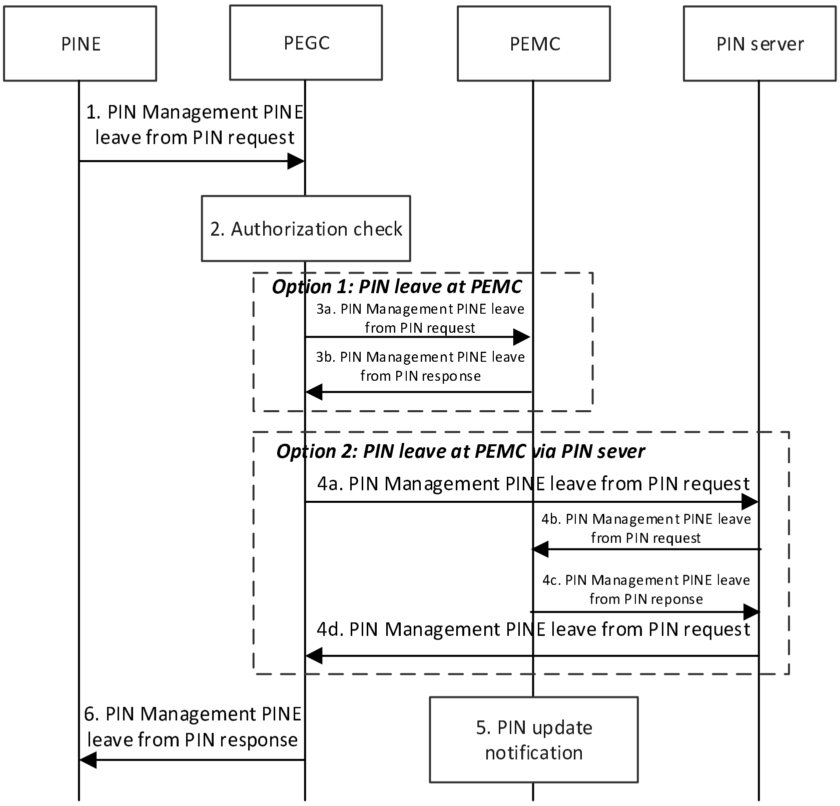
PINE
PEGC
PEMC
PIN server
1. PIN Management PINE leave from PIN request
2. Authorization check
Option 1: PIN leave at PEMC
3a. PIN Management PINE leave from PIN request
3b. PIN Management PINE leave from PIN response
Option 2: PIN leave at PEMC via PIN sever
4a. PIN Management PINE leave from PIN request
4b. PIN Management PINE leave from PIN request
4c. PIN Management PINE leave from PIN reponse
4d. PIN Management PINE leave from PIN request
6. PIN Management PINE leave from PIN response
5. PIN update notification

Figure 8.5.8.2.5-1: PINE leave via the PEGC

1. The PINE determines to leave the PIN and sends PIN Management PINE leave from PIN request to the PEGC. The PIN Management PINE leave from PIN request contains the PIN ID which identifies the PIN to leave, PINE client ID and credentials if available, PEMC identify/PIN server address[optional].

2. The PEGC identifies the received message is the PIN Management PINE leave from PIN request and perform the authorization. If authorized, the PEGC determines to forward the PIN leave request to the PEMC or the PIN server.

   If authorization in PEGC is failed, directly skip to step 6.

   The PEGC can decide to perform either Option 1 (from step 3a to step 3b) or Option 2 (from step 4a to step 4d). If direct communication between PEGC and PEMC always available, the PEGC performs Option 1.

3. (Option 1, step 3a and step 3b) If PEGC determine to forward the PIN Management PINE leave from PIN request to the PEMC in step 2, PEGC forwards the PIN Management PINE leave from PIN request to the PEMC based on the PEMC identity in step 1 or by resolving the PIN ID.

   The PEMC authorized the PINE to leave the PIN, and returns the PIN Management PINE leave from PIN response to the PEGC.

4. (Option 2, step 4a and step 4d) If PEGC determine to forward the PIN Management PINE leave from PIN request to the PIN Sever in step2, the PEGC forwards the PIN Management PINE leave from PIN request to the PIN server based on the PIN server address in step 1 or by resolving the PIN ID. The PIN server forwards the PIN Management PINE leave from PIN request to the PEMC, and the PEMC authorized the PINE to leave the PIN, and returns the PIN Management PINE leave from PIN response to the PIN server. Further the PIN server return the PIN Management PINE leave from PIN response to the PEGC.

5. Further, the PEMC updates the PIN and may notify other entities (e.g., existing joined members, PIN server).

6. The PEGC returns the PIN Management PINE leave from PIN response to the PINE. The PEGC disables the access control information for this PINE. The PEGC stops relaying traffic to the PINE.

   If authorization in PEGC is failed, PEGC generates the PIN Management PINE leave from PIN response to the PINE for the authorization failure.

8.5.8.3 Information flows

8.5.8.3.1 General

The following information flows are specified for PIN creation:

- PIN Management PINE join into PIN request and response;
- PIN Management PINE leave from PIN request and response;

8.5.8.3.2 PIN Management PINE join into PIN request

Table 8.5.8.3.2-1 describes information elements in the PIN Management PINE join into PIN request from the PINE to PEMC, from PINE to PEGC, from PEGC to PEMC, from PIN server to PEMC.

Table 8.5.8.3.2-1: PIN Management PINE join into PIN request

Information element	Status	Description
PIN ID	M	Identifier of the PIN that wants to join in.
Security credentials	M	Security credentials resulting from a successful authorization for the PIN service.
PIN client ID	M	The PIN client ID of PINE
PEMC ID	O	Identifier of the PEMC that PEGC should send request to.
UE Identifier	M	The identifier of the hosting UE (i.e. GPSI or identity token) or the PIN client ID of PEMC
PIN client profile(s)	O	Profiles of PIN clients. The PIN client profiles are further described in Table 8.2.2.3.
PIN server endpoint information	O	Includes URI(s), FQDN(s), IP address(es)) of PIN server.
UE location	O	The location information of the UE. The UE location is described in clause 7.2.7.
Services that PINE provide	O	Indicate the service that PINE can provide.

8.5.8.3.3 PIN Management PINE join into PIN response

Table 8.5.8.3.3-1 describes information elements in the PIN Management PINE join into PIN response from the PEMC to PINE, from PEGC to PINE, from PEMC to PEGC, from PEMC to PIN server.

Table 8.5.8.3.3-1: PIN Management PINE join into PIN response

Information element	Status	Description
Successful response	O (see NOTE)	Indicates that the PIN Management PINE join into PIN request was successful.
> Updated PIN client profile	O	PIN client profile information updated by the PEMC (e.g., default and backup PEGCs assigned to PINE).
> Heartbeat Timer	M	Heartbeat timer value assigned to PINE
> Lifetime of the PIN	M	Indicates the lifetime of PIN.
> Identifier of PEGCs	O	Indicates the PINE identifier authorized to be the PEGCs of this PIN.
>> PEGC address	O	Assigned IP address or port number of PEGC
> PEGC information	O	Includes the PEGC information for example,
>> Access control information	O	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
Failure response	O (see NOTE)	Indicates that the PIN Management PINE join into PIN request failed.
> Cause	M	Provides the cause for PIN Management PINE join into PIN request failure.
NOTE: At least one of the IE shall be present.		

8.5.8.3.4 PIN Management PINE leave from PIN request

Table 8.5.8.3.4-1 describes information elements in the PIN Management PINE leave from PIN request from the PINE to PEMC.

Table 8.5.8.3.4-1: PIN Management PINE leave from PIN request

Information element	Status	Description
PIN ID	M	Identifier of the PIN that wants to leave from.
Security credentials	M	Security credentials resulting from a successful authorization for the PIN service.
PIN client ID	M	The PIN client ID of PINE
UE Identifier	M	The identifier of the hosting UE (i.e. GPSI or identity token) or the PIN client ID of PEMC

8.5.8.3.5 PIN Management PINE leave from PIN response

Table 8.5.8.3.5-1 describes information elements in the PIN Management PINE leave from PIN response from the PEMC to PINE.

Table 8.5.8.3.5-1: PIN Management PINE leave from PIN response

Information element	Status	Description
Successful response	O (see NOTE)	Indicates that the PIN Management PINE leave from PIN request was successful.
Failure response	O	Indicates that the PIN Management PINE leave from PIN request failed.
> Cause	M (see NOTE)	Provides the cause for PIN Management PINE leave from PIN request failure.
NOTE: At least one of the IE shall be present.		

8.5.9 PIN status subscription

8.5.9.1 General

The PIN status update is used by the PINE, PEGC and PIN server to be notified of PIN status information by the PEMC.

PIN status information includes the following information:

- PINE add/remove into/from the PIN;
- PEGC/PEMC relocation in the PIN;
- PIN profile update;
- PIN state changes;

8.5.9.2 Procedure

8.5.9.2.1 PIN status subscribe

Figure 8.5.9.2.1-1 illustrates the PIN status subscribe procedure.

Pre-conditions:

1. The PINE/PEGC/PIN server has already received the address of PEMC;
2. The PINE/PEGC/PIN server has been authorized to communicate with PEMC;

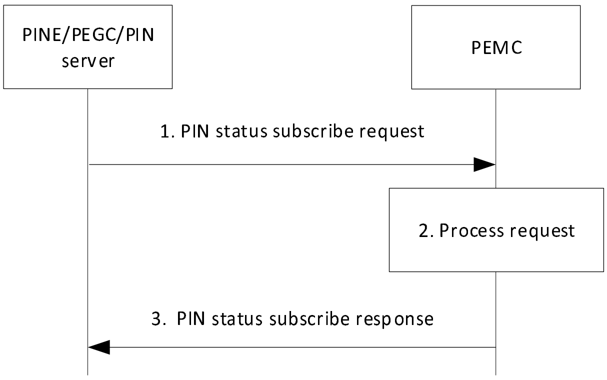
PINE/PEGC/PIN server
PEMC
1. PIN status subscribe request
2. Process request
3. PIN status subscribe response

Figure 8.5.9.2.1-1: PIN status subscribe

1. The PINE/PEGC/PIN server sends the PIN status subscribe request to the PEMC. The PIN status subscribe request includes the PIN client ID along with the security credentials, Event ID.
2. Upon receiving the request from the PINE/PEGC/PIN server, the PEMC checks if the PINE/PEGC/PIN server is authorized to subscribe for information of the requested PIN status information. The authorization check may apply to an individual PIN. If the request is authorized, the PEMC creates and stores the subscription for PIN.
3. If the processing of the request is successful, the PEMC sends a PIN status subscribe response to the PINE/PEGC/PIN server, which includes the subscription identifier and may include the expiration time, indicating when the subscription will automatically expire. To maintain the subscription, the PINE/PEGC/PIN server shall send a PIN status update request prior to the expiration time. If a new PIN status update request is not received prior to the expiration time, the PEMC shall treat the PINE/PEGC/PIN server as implicitly unsubscribed.

8.5.9.2.2 PIN status notify

Figure 8.5.9.2.2-1 illustrates the PIN status notify procedure.

Pre-conditions:

1. The PINE/PEGC/PIN has subscribed with the PEMC for the PIN status as specified in clause 8.5.9.2.1.

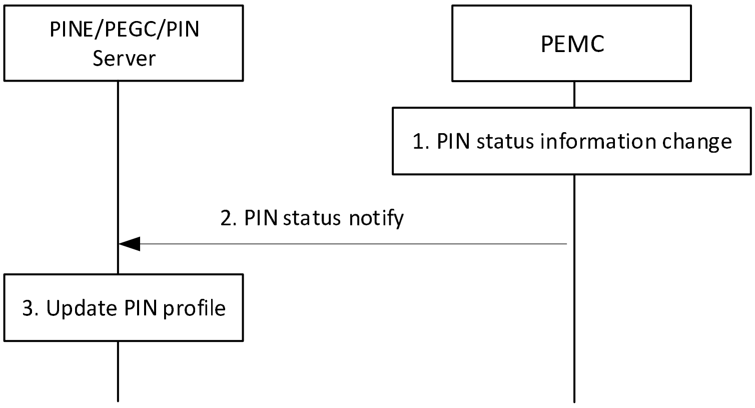

Figure 8.5.9.2.2-1: PIN status notify procedure

1. When an event occurs at the PEMC that satisfies trigger conditions for notifying (e.g. to provide updated PIN status, for example when a PINE joins into the PIN) a PINE/PEGC/PIN server.

   The status information of PIN is updated including the following cases:

   - PIN modification: The PIN modification includes the PEMC/PEGC relocation and the PINE joins into PIN or leaves the PIN;

   - PIN profile updates: The PIN profiles is referred to the section 8.2.2, and the updated PIN profile may be coordinated to other PINEs;

   - PIN state changes: Whenever the PIN state is changed from activated to de-activated or vice-versa;

2. The PEMC sends an PIN status notify to the PINE/PEGC/PIN server with the updated PIN status information.

   The PIN status information notification includes the following parameters:

   - PIN modification: If the PEMC decides the PEMC/PEGC relocation, the PEMC includes the parameters about the newly assigned PEMCs and PEGCs in the PIN status update request, for example, the PEMC/PEGC ID or address, the PEGC information in Table 8.5.2.3.3-1 about access control information and etc;

   - PINE management: If the PEMC decides the PINE to join or leave the PIN, the PEMC includes the parameters about the newly added/removed PINE in the PIN status update request, for example, the PIN client ID or address, the PIN client profile and etc. Also if the PINE is removed from the PIN, the parameters about the removed PINE should be included in the PIN status update request;

   - PIN profile update: If the PIN profile is updated, the PEMC includes the parameters about updated PIN profile in the PIN status update request;

   - PIN state changes: Whenever the PIN state is changed from activated to de-activated or vice-versa;

3. Upon receiving the notification, the PINE, PEGC or PIN server updates the PIN profile according to the information in the PIN status notify.

8.5.9.2.3 PIN status update

Figure 8.5.9.2.3-1 illustrates the PIN status update procedure.

Pre-conditions:

1. The PINE/PEGC/PIN server has subscribed with the PEMC for PIN status information as specified in 8.5.9.2.1;

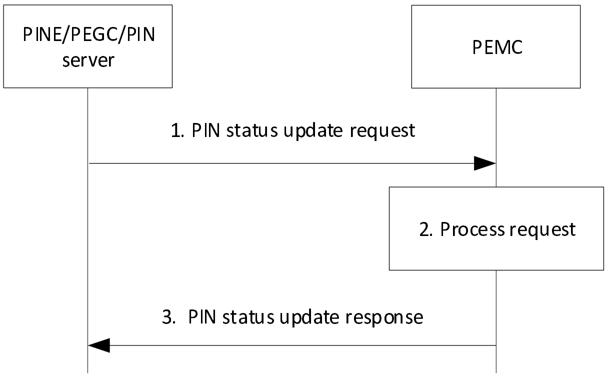

Figure 8.5.9.2.3-1: PIN status update

1. The PINE/PEGC/PIN server sends a PIN status update request to the PEMC. The PIN status update request includes the security credentials and the subscription identifier. It may also include subscribed events, notification target address and proposed expiration time.

2. Upon receiving the request from the PINE/PEGC/PIN server, the PEMC checks if the PINE/PEGC/PIN server is authorized to update the subscription information. If the request is authorized, the PEMC updates the stored subscription for PIN status information.

3. If the processing of the request is successful, the PEMC sends a PIN status update response to the PINE/PEGC/PIN server, which may include the expiration time, indicating when the subscription will automatically expire. To maintain the subscription, the PINE/PEGC/PIN server shall send an PIN status information subscription update request prior to the expiration time. If a PIN status update request is not received prior to the expiration time, the PEMC shall treat the PINE/PEGC/PIN server as implicitly unsubscribed.

8.5.9.2.4 PIN status unsubscribe

Figure 8.5.9.2.4-1 illustrates the PIN status unsubscribe procedure.

Pre-conditions:

1. The PINE/PEGC/PIN server has subscribed with the PEMC for PIN status information as specified in 8.5.9.2.1;

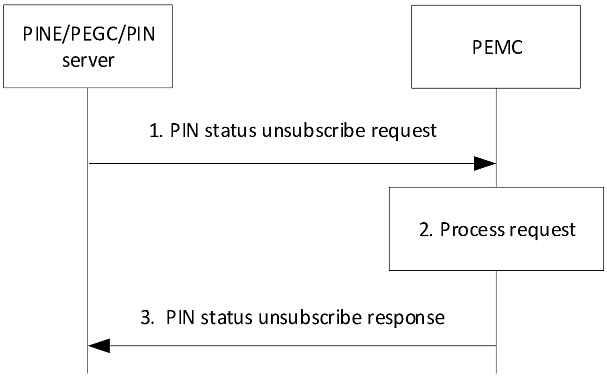
PINE/PEGC/PIN server
PEMC
1. PIN status unsubscribe request
2. Process request
3. PIN status unsubscribe response

Figure 8.5.9.2.4-1: PIN status unsubscribe

1. The PINE/PEGC/PIN server sends a PIN status unsubscribe request to the PEMC. The PIN status unsubscribe request includes the security credentials and the subscription identifier.

2. Upon receiving the request from the PINE/PEGC/PIN server, the PEMC checks if the PINE/PEGC/PIN server is authorized to unsubscribe. If the request is authorized, the PEMC cancels the subscription for PIN status information.

3. If the processing of the request is successful, the PEMC sends a PIN status unsubscribe response to the PINE/PEGC/PIN server.

8.5.9.3 Information flows

8.5.9.3.1 General

The following information flows are specified for PIN status:

- PIN status subscribe;
- PIN status notify;
- PIN status update;
- PIN status unsubscribe;

8.5.9.3.2 PIN status subscribe request

Table 8.5.9.3.2-1: PIN status subscribe request

Information element	Status	Description
PIN client ID	M	Unique identifier of the PINE/PEGC/PIN server.
Subscribed Events IDs	M	Identifies PIN status event for which the subscriber is notified, more than one PIN status event IDs can be provided. Event IDs: - PIN modification - PINE management (PINE join/leave) - PIN profile update - PIN state
Security credentials	M	Security credentials resulting from a successful authorization for the PIN service.
PIN ID	M	The identifier of PIN.
Notification Target Address	O	The Notification target address (e.g. URL) where the notifications destined for the PINE/PEGC/PIN server should be sent to.
Proposed expiration time	O	Proposed expiration time for the subscription

8.5.9.3.3 PIN status subscribe response

Table 8.5.9.3.3-1: PIN status subscribe response

Information element	Status	Description
Successful response	O	Indicates that the subscription request was successful.
> Subscription ID	M	Subscription identifier corresponding to the subscription.
> Expiration time	O	Indicates the expiration time of the subscription. To maintain an active subscription, a subscription update is required before the expiration time.
> Successfully subscribed event IDs	O	Indicates the successfully subscribed event IDs.
Failure response	O	Indicates that the subscription request failed.
> Cause	O	Indicates the cause of subscription request failure
> Unsuccessfully subscribed event IDs	O	Indicates the unsuccessfully subscribed event IDs.

NOTE: If some of the event ID is accepted to subscribe and others are rejected, the service provider should indicate the event ID that accepted and rejected individually to service consumer.

8.5.9.3.4 PIN status notify

Table 8.5.9.3.4-1 describes information elements in the PIN status notify from the PEMC to PEMC/PEGC/PINE/PIN server.

Table 8.5.9.3.4-1: PIN status notify

Information element	Status	Description
PIN Status event type	M	Identifies PIN status event types contained in the notification; more than one PIN status event type can be provided. PIN status event types - PIN modification - PINE management (PINE join/leave) - PIN profile update - PIN state (Activated or de-activated)
PIN ID	M	Indicate identifier of the PIN that status event related to
PINE management	O	Indicates the PINE join/leave the PIN and PINE removed, this IE is present if the PIN status event type is PINE management.
PIN modification	O	Indicates the modification of PIN as indicated in section 8.5.10 for example the PEMC/PEGC relocation, this IE is present if the PIN status event type is PIN modification.
PIN profiles update	O	Indicates a PIN profile update that indicated in section 8.2.2, this IE is present if the PIN status event type are PIN modification, PINE management, and is PIN profile update.
PIN state	O	Indicates the state of a PIN.

8.5.9.3.5 PIN status update request

Table 8.5.9.3.5-1: PIN status update request

Information element	Status	Description
Subscription ID	M	Subscription identifier corresponding to the subscription.
Security credentials	M	Security credentials resulting from a successful authorization for the PIN service.
PIN ID	M	The identifier of PIN.
Subscribed Events	O	Identifies PIN status event types for which the subscriber is notified, more than one PIN status event type can be provided. PIN status event types - PIN modification - PINE management (PINE join/leave) - PIN profile update - PIN state
Notification Target Address	O	The Notification target address (e.g. URL) where the notifications destined for the PINE/PEGC/PIN server should be sent to.
Proposed expiration time	O	Proposed expiration time for the subscription

8.5.9.3.6 PIN status update response

Table 8.5.9.3.6-1: PIN status update response

Information element	Status	Description
Successful response (see NOTE)	O	Indicates that the subscription update request was successful.
> Expiration time	O	Indicates the expiration time of the subscription. To maintain an active subscription, a subscription update is required before the expiration time.
Failure response (see NOTE)	O	Indicates that the subscription update request failed.
> Cause	M	Indicates the cause of subscription update request failure
NOTE: One IE is included in the response.		

8.5.9.3.7 PIN status unsubscribe request

Table 8.5.9.3.7-1: PIN status unsubscribe request

Information element	Status	Description
Subscription ID	M	Subscription identifier corresponding to the subscription.
Security credentials	M	Security credentials resulting from a successful authorization for the PIN service.

8.5.9.3.8 PIN status unsubscribe response

Table 8.5.9.3.8-1: PIN status unsubscribe response

Information element	Status	Description
Successful response (see NOTE)	O	Indicates that the unsubscribe request was successful.
Failure response (see NOTE)	O	Indicates that the unsubscribe request failed.
> Cause	M	Indicates the cause of unsubscribe request failure
NOTE: One IE is included in the response.		

8.5.10 PIN modification

8.5.10.1 General

This clause describes PIN modification functionality.

8.5.10.2 Procedures

8.5.10.2.1 General

8.5.10.2.2 PIN modification after local PEMC failure

Figure 8.5.10.2.2-1 describes the PIN modification procedure to perform a PEMC role change due to the failure of the PEMC. An authorised administrator is the owner of the PIN and accesses PIN configuration using an application on a UE, which is one of the PEMC for the PIN. The authorised administrator can manage the PIN locally or through the 5G network. This procedure describes a PEMC (e.g., an authorized administrator on a UE) managing the PIN remotely via the 5G network.

The procedure may be used e.g. when a PEMC is available on a UE for PIN management by an authorised administrator. When there is a local PEMC failure, the authorized administrator can be enabled to manage the PIN remotely, via the 5G network, using the following steps.

Pre-conditions:

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

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

3. The authorized administrator configures the active PEMC to provide PIN management for the PIN. UE/PEMC1 is the inactive PEMC.

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

5. The authorized 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. As a result, the authorized administrator is able to manage the PIN through the 5G network.

6. The UE/PEMC1 is subscribed to the PEGC for PIN connectivity notifications

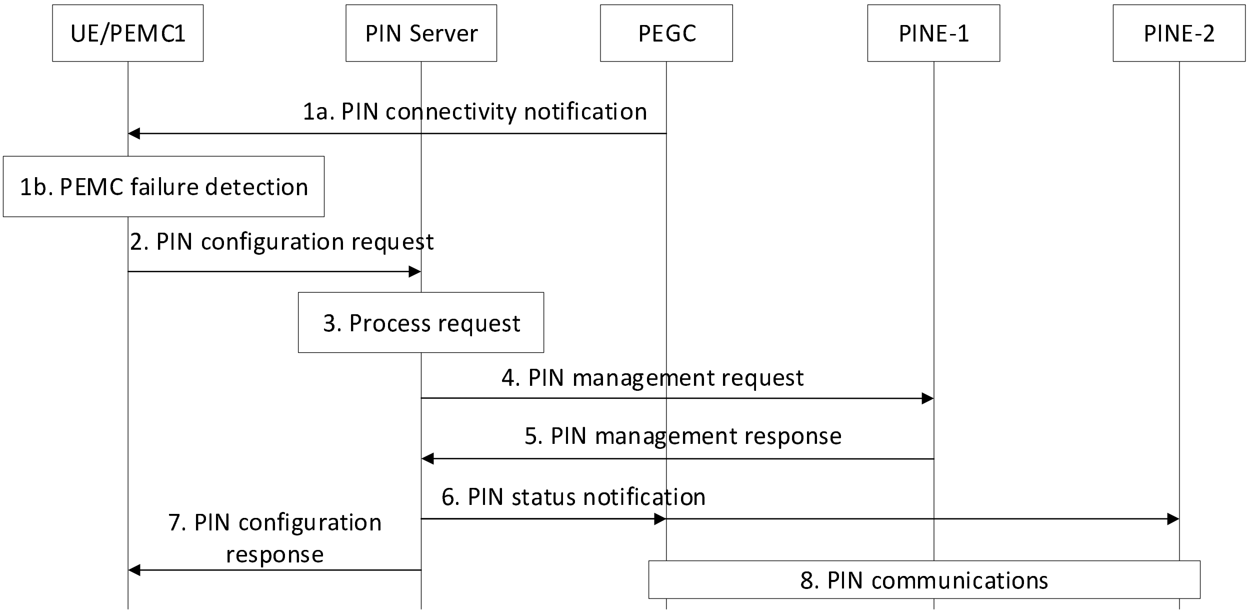
UE/PEMC1
PIN Server
PEGC
PINE-1
PINE-2
1a. PIN connectivity notification
1b. PEMC failure detection
2. PIN configuration request
3. Process request
4. PIN management request
5. PIN management response
6. PIN status notification
7. PIN configuration response
8. PIN communications

Figure 8.5.10.2.2-1: PIN Modification after local PEMC failure

1. The UE/PEMC1 may detect that PEMC2 is unavailable or failed. In step 1a, the UE/PEMC1 may receive a PIN connectivity notification from PEGC indicating that there is a communication failure with PEMC2. Otherwise, in step 1b, the UE/PEMC1 may detect that PEMC2 is unavailable by using the PIN heartbeat mechanism or if a communication timeout happens with PEMC2.

2. If UE/PEMC1 has detected that PEMC2 is unavailable or failed in step 1, an authorized administrator on UE/PEMC1 sends a PIN configuration request to the PIN server through the 5G network. The request includes the security credentials of the authorized administrator, the UE ID, the PIN ID, PIN member ID, authorization type indicating the role change (e.g., the request may indicate that PINE-1 be assigned the new PEMC).

3. If the PIN Server has received a PIN Configuration request in step 2, the PIN server processes the modification request and checks if the authorized administrator is allowed to modify the PIN. The PIN server verifies that PINE-1 has the capability to serve as a PEMC using information in the PIN profile.

4. If the authorized administrator is allowed to perform PIN modification or if the PIN Server has detected that PEMC2 is unavailable or failed and has determined that PINE-1 can be reassigned as the new PEMC, the PIN server sends a PIN management request to PINE-1 to assign PINE-1 as the new PEMC and provides PIN profile information to PINE-1.

5. PINE-1 processes the PIN management request indicating the PEMC assignment and a PIN management response to the PIN server indicating if the assignment was successful.

6. If the PIN management response in step 5 was successful, the PIN server notifies the other members of the PIN that PINE-1 will be the new PEMC for the PIN and updates PIN profile information.

7. If the PIN Server has received a PIN Configuration request in step 2, the PIN server sends a PIN configuration response to the UE/PEMC1, the response includes the updated PIN profile information if the PEGC assignment was successful; otherwise, the response indicates that the assignment failed.

8. If the PEGC assignment was successful, the PIN communications resume with PINE-1 serving as the new PEMC.

8.5.10.2.3 PIN modification with PEGC role change

Figure 8.5.10.2.3-1 describes a PIN modification procedure to perform a PEGC role change due to the unavailability of the PEGC. This procedure describes a PEMC detecting the unavailability of a PEGC (e.g. PEGC leaves the local service area of the PIN) and performing a PIN modification with the PIN Server to assign a new PEGC. As part of PIN management, a PEMC receives periodic PIN heartbeat messages from PEGCs to ensure PIN routing is available for members of the PIN at all times. If a PEMC does not receive the periodic PIN heartbeat messages from the PEGC, then the PEMC needs to assign a new PEGC or request the PIN server to assign the new PEGC.

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 on the capabilities of each PIN member.

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

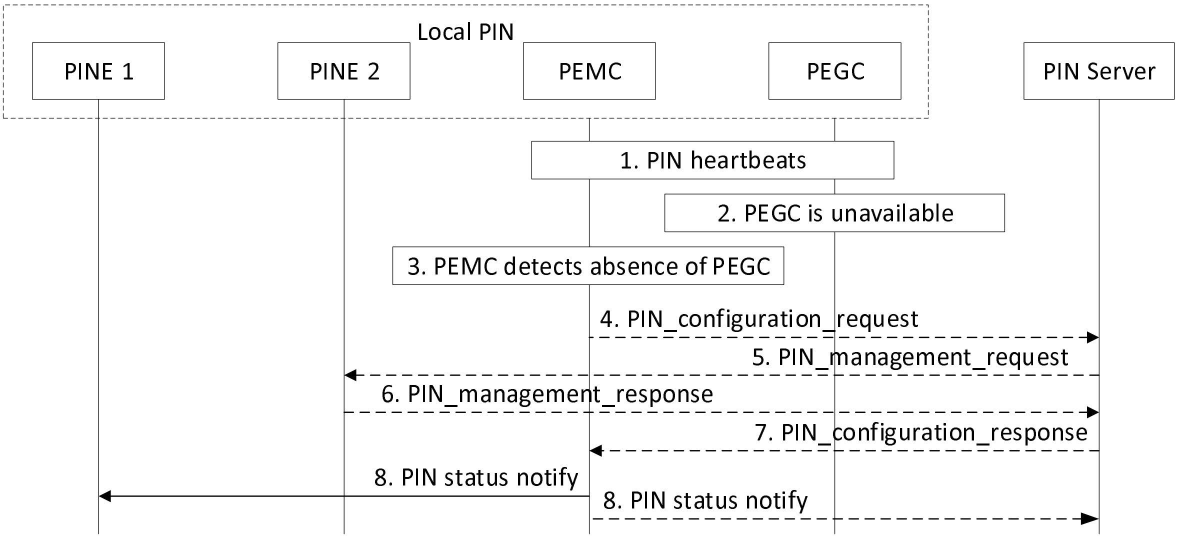
Local PIN
PINE 1
PINE 2
PEMC
PEGC
PIN Server
1. PIN heartbeats
2. PEGC is unavailable
3. PEMC detects absence of PEGC
4. PIN_configuration_request
5. PIN_management_request
6. PIN_management_response
7. PIN_configuration_response
8. PIN status notify
8. PIN status notify

Figure 8.5.10.2.3-1: PIN Modification due to PEGC unavailability

1. PEMC receives periodic PIN heartbeats from PEGC to monitor the availability of the PEGC.

2. PEGC leaves the local coverage area of the PIN, e.g., leaves the home, and is not available to route PIN communications.

3. PEMC does not receive a periodic PIN heartbeat from PEGC at the configured interval and determines that PEGC is no longer providing PIN routing capability.

   If secondary PEGC is available in PEMC, that the PEMC decides to configure this PEGC as the gateway of PIN, and skip the procedure from step 4 to step 7. And PEMC only notifies PIN server of newly selected PEGC in step 8.

   If secondary PEGC is unavailable in PEMC, that the PEMC decides to trigger the PIN server to discover the PEGC as the gateway of PIN from step 4 to step 7. And PEMC only notifies PINE in this PIN of newly selected PEGC in step 8.

4. PEMC sends a PIN configuration request to the PIN server to select a new PEGC. The request includes the PIN ID, the PEMC ID, the PEGC ID, authorization type indicating the role change, the ID of a PIN member that can serve as the new PEGC (e.g., PINE2), and a timestamp.

5. 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 PIN management request to PINE-2 with PIN profile and dynamic profile information. The dynamic profile information includes PIN traffic routing rules that PINE2 would need to make routing decisions.

6. PINE-2 sends a PIN management response accepting to serve as the new PEGC.

7. The PIN server sends a PIN configuration response with PIN profile and dynamic profile information to the PEMC with the status of the request, the ID of the new PEGC, and PIN traffic routing rules. The PIN server response triggers the PEMC to notify other PIN members of the PEGC role change.

8. PEMC notifies the PIN server or other members of the PIN that PINE2 will serve as the new PEGC. The PEMC includes PIN profile and dynamic profile information that includes traffic routing rules applicable to each member.

8.5.10.2.4 PEMC replacement triggered internally within the PIN

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 (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 8.5.2.10.2-4-1 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

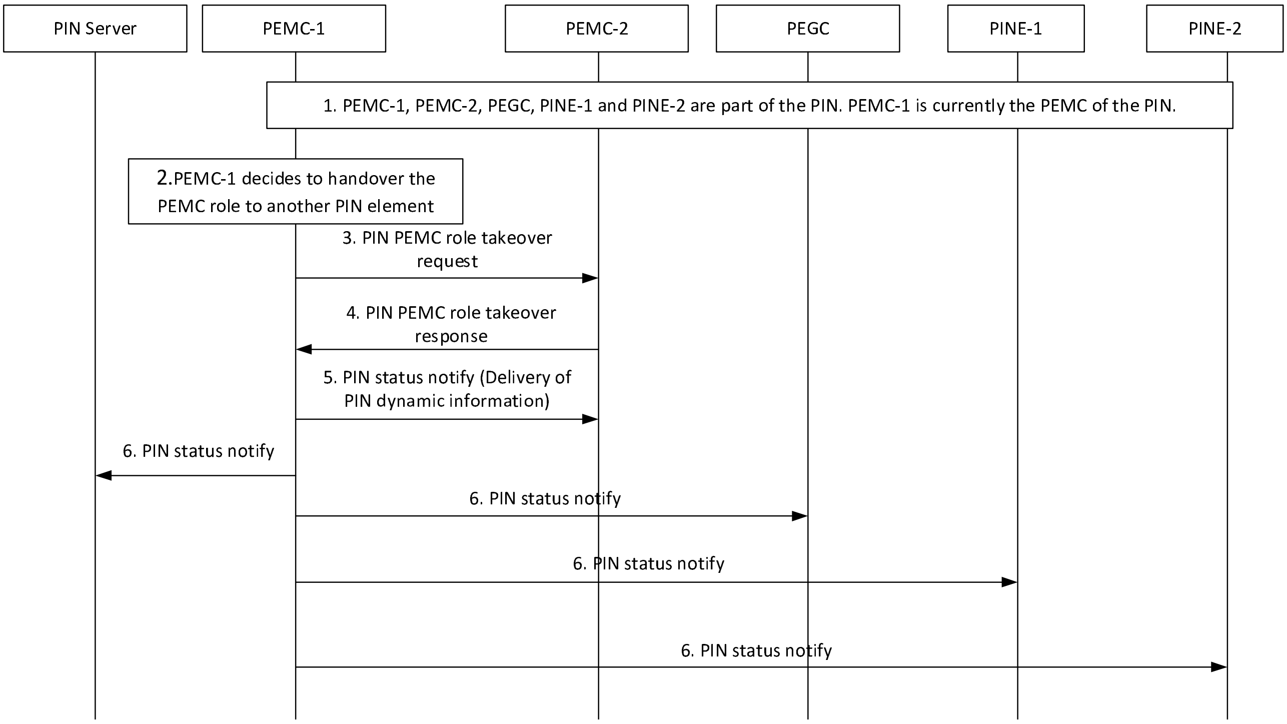
PIN Server
PEMC-1
PEMC-2
PEGC
PINE-1
PINE-2
1. PEMC-1, PEMC-2, PEGC, PINE-1 and PINE-2 are part of the PIN. PEMC-1 is currently the PEMC of the PIN.
2.PEMC-1 decides to handover the PEMC role to another PIN element
3. PIN PEMC role takeover request
4. PIN PEMC role takeover response
5. PIN status notify (Delivery of PIN dynamic information)
6. PIN status notify
6. PIN status notify
6. PIN status notify
6. PIN status notify

Figure 8.5.2.10.2.4-1: 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 by sending PIN PEMC role takeover request which includes the PIN identifier, PIN element identifier of PEMC-2.

4. If the PEMC-2 PINE decides to take up the role of PEMC it sends the PIN PEMC role takeover 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 by consuming PIN status notify message.

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 by sending PIN status notify message. On receiving this notification PIN server and PEGC updates the PIN dynamic profile information with the details of PEMC-2.

8.5.10.2.5 PEGC replacement triggered by PEMC

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 PEGC role to another PINE and deliver the PIN dynamic information to the new PEGC.

Figure 8.5.2.10.2-5-1 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.

3. PIN has only one PIN element configured with the role of PEGC.

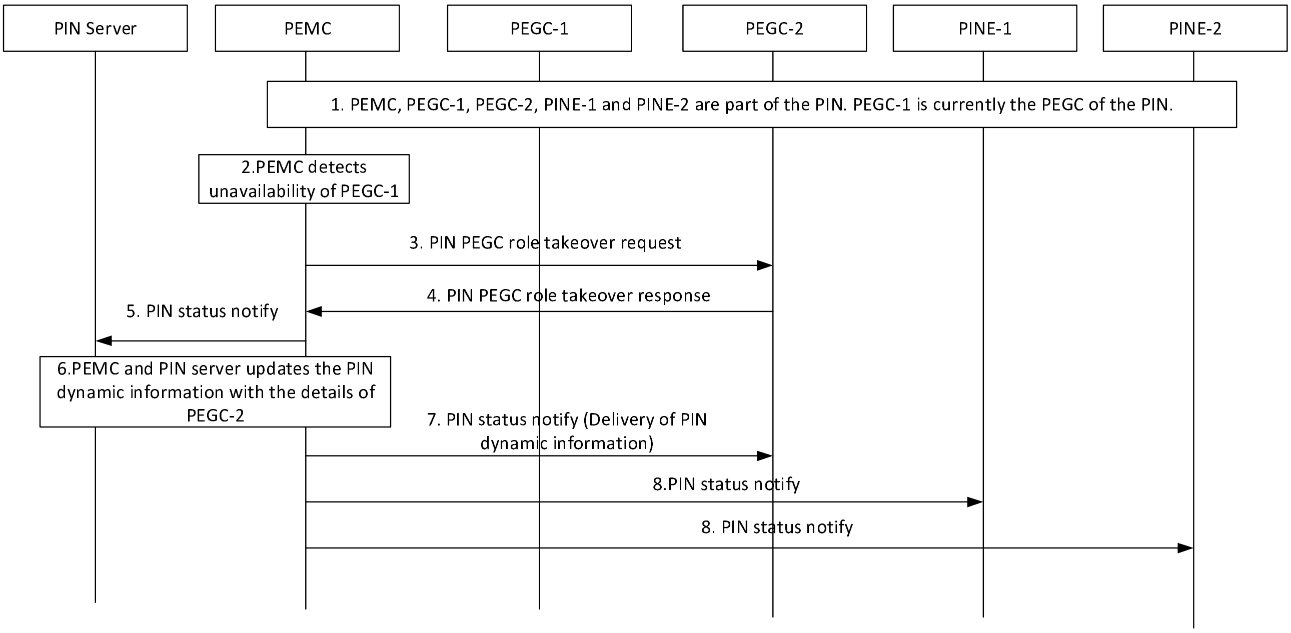
PIN Server
PEMC
PEGC-1
PEGC-2
PINE-1
PINE-2
1. PEMC, PEGC-1, PEGC-2, PINE-1 and PINE-2 are part of the PIN. PEGC-1 is currently the PEGC of the PIN.
2.PEMC detects unavailability of PEGC-1
3. PIN PEGC role takeover request
4. PIN PEGC role takeover response
5. PIN status notify
6.PEMC and PIN server updates the PIN dynamic information with the details of PEGC-2
7. PIN status notify (Delivery of PIN dynamic information)
8.PIN status notify
8. PIN status notify

Figure 8.5.2.10.2.5-1: 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 it is no longer receiving periodic PIN heartbeats from PEGC-1 or its duration to act as PEGC is ending.
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 by sending PIN PEGC role takeover request and this request includes the PIN Element ID of PEGC-2, PIN identifier and time duration to act as PEGC etc.
4. If the PEGC-2 PINE decides to take up the role of PEGC it sends the success PIN PEGC role takeover 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 by sending PIN status notification request containing the required details.
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 by consuming PIN status notify message.
8. The PEMC sends PIN status notify message to notify the relevant PINEs in the PIN about the change in the PIN element acting as PEGC and its reachability information.

8.5.10.3 Information flows.

8.5.10.3.1 General

8.5.10.3.2 PIN configuration request

Table 8.5.10.3.2-1 shows the informational elements of the PIN configuration request sent by a PIN Element to the PIN server to obtain authorization for the modification of a PIN.

Table 8.5.10.3.2-1: PIN configuration request

Information element	Status	Description
PIN ID	M	The identifier of the PIN
Requester PINE ID	M	The identifier of the PIN Element making the request
Authorization type	M	Request for the authorization to modify the configuration of a PIN: PEMC role change, PEGC role change
PINE ID of predecessor in the role	M	PINE ID of the element serving in the indicated role and needs to be changed e.g. due to being unavailable.
PINE ID of proposed successor in the role	O	PINE ID of the element proposed to assume the role
Additional PEMCs	O	Indicate additional PEMCs (with identifier of PEMC) that are requested to manage the PIN.

8.5.10.3.3 PIN configuration response

Table 8.5.10.3.3-1 shows the informational elements of the PIN configuration response provided by the PIN server to authorize the modification of a PIN.

Table 8.5.10.3.3-1: PIN configuration response

Information element	Status	Description
Response	M	The response (authorize or not authorize) from the PIN Server.
PIN profile information	M	The IEs from the PIN profile information that the PIN Server has updated for modifying the PIN
Dynamic PIN profile information	M	The IEs from the dynamic PIN profile information that the PIN Server has authorized for modifying the PIN
Additional PEMCs	O	Indicate additional PEMCs (with identifier of PEMC) that are allowed to manage the PIN.

8.5.10.3.4 PIN management request

Table 8.5.10.3.4-1 shows the informational elements of the PIN management request sent to PIN elements to make changes to the configuration of the PIN.

Table 8.5.10.3.4-1: PIN management request

Information element	Status	Description
PIN ID	M	The identifier of the PIN
Requestor ID	M	The identifier of the PIN Server or PIN Element making the request
Modification type	M	Request for the modification of the PIN: PEMC assignment, PEGC assignment
Dynamic PIN profile information	M	IEs from the dynamic PIN profile information that the PINE needs to operate in the new role

8.5.10.3.5 PIN management response

Table 8.5.10.3.5-1 shows the informational elements of the PIN management response received from the PIN element to the PIN modification request.

Table 8.5.10.3.5-1: PIN management response

Information element	Status	Description
Response	M	The response (accept or deny) from the PIN Element to the PIN management request.

8.5.10.3.6 PIN PEMC role takeover request

Table 8.5.10.3.6-1 shows the informational elements of the PIN PEMC role takeover request sent from current PEMC of the PIN to another PIN element with PEMC capability.

Table 8.5.10.3.6-1: PIN PEMC role takeover request

Information element	Status	Description
PIN ID	M	The identifier of the PIN
Current PEMC identifier	M	The identifier of the current PEMC making the request
New PEMC identifier	M	The identifier of the new PIN element requested to take the role of PEMC

8.5.10.3.7 PIN PEMC role takeover response

Table 8.5.10.3.7-1 shows the informational elements of the PIN PEMC role takeover response sent from requested PIN element to the current PEMC.

Table 8.5.10.3.7-1: PIN PEMC role takeover response

Information element	Status	Description
PIN ID	M	The identifier of the PIN
Success response (see NOTE)	O	Indicates that PEMC role takeover request is successful
Failure response (see NOTE)	O	Indicates that PEMC role takeover request is failure
> Cause	O	Indicates the reason for the failure
NOTE: Only one of the IE is included in the response		

8.5.10.3.8 PIN PEGC role takeover request

Table 8.5.10.3.8-1 shows the informational elements of the PIN PEGC role takeover request sent from current PEMC of the PIN to another PIN element with PEGC capability.

Table 8.5.10.3.8-1: PIN PEGC role takeover request

Information element	Status	Description
PIN ID	M	The identifier of the PIN
Current PEMC identifier	M	The identifier of the current PEMC making the request
New PEGC identifier	M	The identifier of the new PIN element requested to take the role of PEGC

8.5.10.3.9 PIN PEGC role takeover response

Table 8.5.10.3.9-1 shows the informational elements of the PIN PEGC role takeover response sent from requested PIN element to the current PEMC.

Table 8.5.10.3.9-1: PIN PEGC role takeover response

Information element	Status	Description
PIN ID	M	The identifier of the PIN
Success response (see NOTE)	O	Indicates that PEGC role takeover request is successful
Failure response (see NOTE)	O	Indicates that PEGC role takeover request is failure
> Cause	O	Indicates the reason for the failure
NOTE: Only one of the IE is included in the response		

8.5.11 PIN services management

8.5.11.1 General

PIN elements can indicate the list of services it is offering at the time of joining the PIN by listing them as part of the PIN client profile. here could be scenarios wherein the PIN element may not be able to continue to provide the service(s) it indicated while joining or there could be scenarios where the PIN element may want to offer some more new services which were not supported earlier at the time of joining the PIN. This clause describes the procedures for managing the PIN services enabling the PIN elements to register or de-register the services.

8.5.11.2 Procedures

8.5.11.2.1 PINE registering the services

Figure 8.5.11.2.1-1 illustrates procedure of PIN element registering the new service(s).

Pre-conditions:

1. PIN is already created and the PIN entities PEGC, PINE-1, PINE-2, PINE-3 and PINE-4 are all part of the same PIN;

2. The PINE-4 is the PEMC of the PIN;

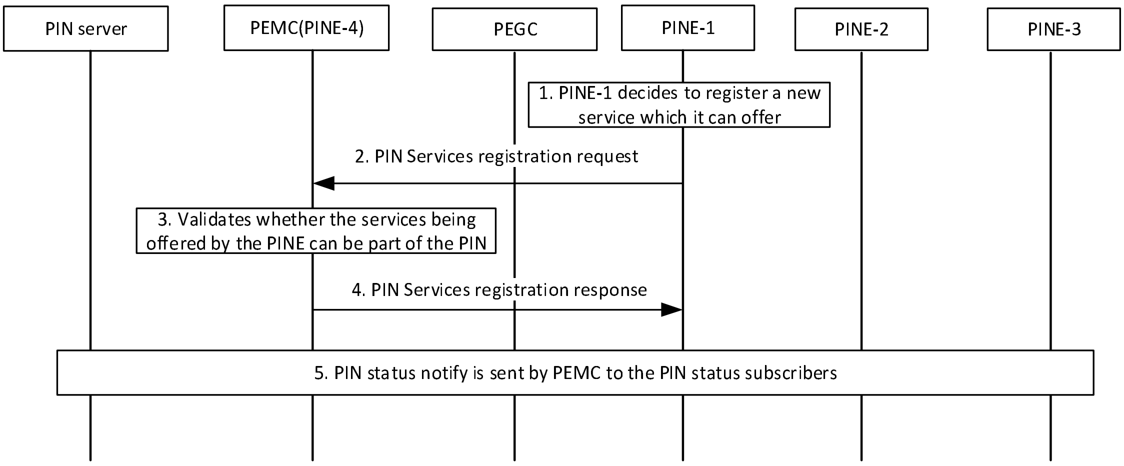
PIN server
PEMC(PINE-4)
PEGC
PINE-1
PINE-2
PINE-3
1. PINE-1 decides to register a new service which it can offer
2. PIN Services registration request
3. Validates whether the services being offered by the PINE can be part of the PIN
4. PIN Services registration response
5. PIN status notify is sent by PEMC to the PIN status subscribers

Figure 8.5.11.2.1-1: PINE registering the service(s)

1. PINE-1 decides to register a new service(s) that it can offer which it was not offering at the time of joining the PIN. This may happen because of the UE on which the PIN element is existing has been upgraded to offer extra services or for any other reason which could be implementation specific.

2. PINE-1 sends the PIN services registration request to the PEMC to register the new service(s). This request carries the PIN identifier, PIN element Identifier, list of new service(s) it is offering. The list of services can include a unique service id, human readable description of the service and may also contain time duration of when the service is available etc.

3. PEMC (PINE-4) on receiving the PIN services registration request checks whether the PINE-1 is allowed to register new service(s) and whether these services are allowed to be offered by the PIN by checking the PIN profile.

4. PEMC (PINE-4) sends the PIN services registration response which contains the status (success or failure) of the PIN services registration request.

5. PEMC notifies all the PIN entities including PIN server and PEGC about the details of the new services being offered and the details of the PINE offering the services. PIN server, PEMC and PEGC updates the PIN dynamic information with the details of the new service(s) being offered and the PINE which is offering it.

8.5.11.2.2 PINE de-registering the services

Figure 8.5.11.2.2-1 illustrates procedure of PIN element de-registering the service(s).

Pre-conditions:

1. PIN is already created and the PIN entities PEGC, PINE-1, PINE-2, PINE-3 and PINE-4 are all part of the same PIN;

2. The PINE-4 is the PEMC of the PIN;

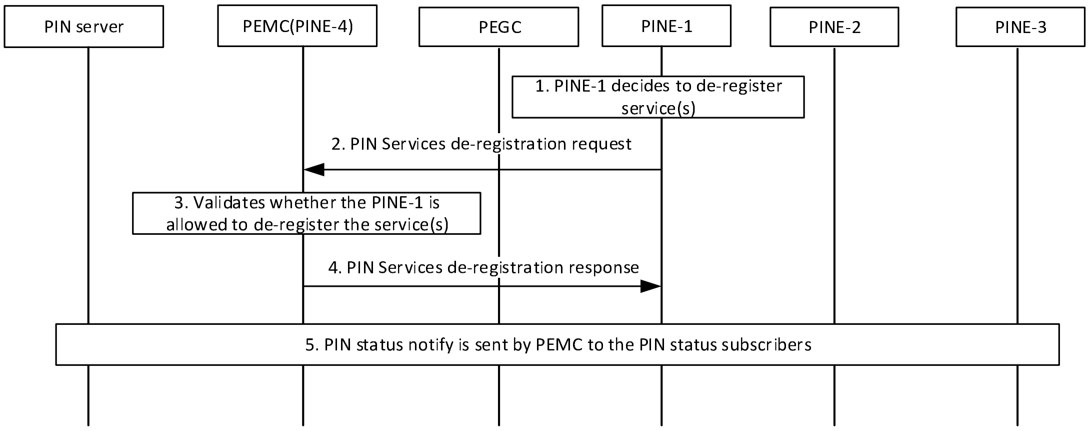
PIN server
PEMC(PINE-4)
PEGC
PINE-1
PINE-2
PINE-3
1. PINE-1 decides to de-register service(s)
2. PIN Services de-registration request
3. Validates whether the PINE-1 is allowed to de-register the service(s)
4. PIN Services de-registration response
5. PIN status notify is sent by PEMC to the PIN status subscribers

Figure 8.5.11.2.2-1: PINE de-registering the service(s)

1. PINE-1 decides to de-register a service(s) that it is currently offering and which it has indicated during the PIN registration or PIN join procedure. This may happen because the UE on which the PIN element is existing might face hardware failure, services might be scheduled to be offered for a certain time period/duration or for any other reason which could be implementation specific.

2. PINE-1 sends the PIN services de-registration request to the PEMC to de-register the service(s). This request carries the PIN identifier, PIN element Identifier, list of service(s) it is de-registering. The list of services can include a unique service id, human readable description of the service.

3. PEMC (PINE-4) on receiving the PIN services de-registration request checks whether the PINE-1 is allowed to de-register service(s) by checking the PIN profile.

4. PEMC (PINE-4) sends the PIN services de-registration response which contains the status (success or failure) of the PIN services de-registration request.

5. PEMC notifies all the PIN entities including PIN server and PEGC about the details of the services being de-registered. PIN server, PEMC and PEGC updates the PIN dynamic information to remove the details of the service(s) being de-registered.

8.5.11.3 Information flows.

8.5.11.3.1 General

8.5.11.3.2 PIN services registration request

Table 8.5.11.3.2-1 shows the informational elements of the PIN services registration request sent by a PIN Element to the PEMC to register for new services it is offering.

Table 8.5.11.3.2-1: PIN services registration request

Information element	Status	Description
PIN ID	M	The identifier of the PIN
Requester PINE ID	M	The identifier of the PIN Element making the request
List of services	M	List of services that a PINE wants to register
> Service type	O	Indication of service type
> Time duration	O	Availability period of service
> Service description	O	Description of the service
> Service Identifier	M	Identifier of the service

8.5.11.3.3 PIN services registration response

Table 8.5.11.3.3-1 shows the informational elements of the PIN services registration response sent by PEMC to the PIN element.

Table 8.5.11.3.3-1: PIN services registration response

Information element	Status	Description
PIN ID	M	The identifier of the PIN
Requester PINE ID	M	The identifier of the PIN Element making the request
Result	M	Indication of whether the service registration is success or failure.
> Successful response	O	Indicates the successfully registered PIN services.
> Failure response	O	Indicates the failure of registered PIN services.

8.5.11.3.4 PIN services de-registration request

Table 8.5.11.3.4-1 shows the informational elements of the PIN services de-registration request sent by a PIN Element to the PEMC.

Table 8.5.11.3.4-1: PIN services de-registration request

Information element	Status	Description
PIN ID	M	The identifier of the PIN
Requester PINE ID	M	The identifier of the PIN Element making the request
List of services	M	List of services that a PINE wants to de-register
> Service type	O	Indication of service type
> Service description	O	Description of the service
> Service identifier	M	Identifier of the service

8.5.11.3.5 PIN services de-registration response

Table 8.5.11.3.5-1 shows the informational elements of the PIN services de-registration response sent by PEMC to the PIN element.

Table 8.5.11.3.5-1: PIN services de-registration response

Information element	Status	Description
PIN ID	M	The identifier of the PIN
Requester PINE ID	M	The identifier of the PIN Element making the request
Result	M	Indication of whether the service de-registration is success of failure.

8.5.12 PIN heartbeat

8.5.12.1 General

Periodic PIN heartbeats are sent by PINE(s) and PEGC(s) to the PEMC. These heartbeats are used by the PEMC to keep track of the availability of PINE(s) and PEGC(s) and detect if/when they are no longer available within the PIN. Likewise, periodic heartbeats are also sent by the PEMC to the PIN server to allow the PIN server to detect if/when the PEMC is no longer available.

8.5.12.2 Procedure

8.5.12.2.1 PIN heartbeat

Figure 8.5.12.2.1-1 illustrates the PIN heartbeat procedure.

Pre-conditions:

1. The PIN is successfully created and in use.
2. The PIN Server/PEMC and each PINE/PEGC/PEMC have set periodic timers corresponding to the heartbeat timer values respectively sent or received.

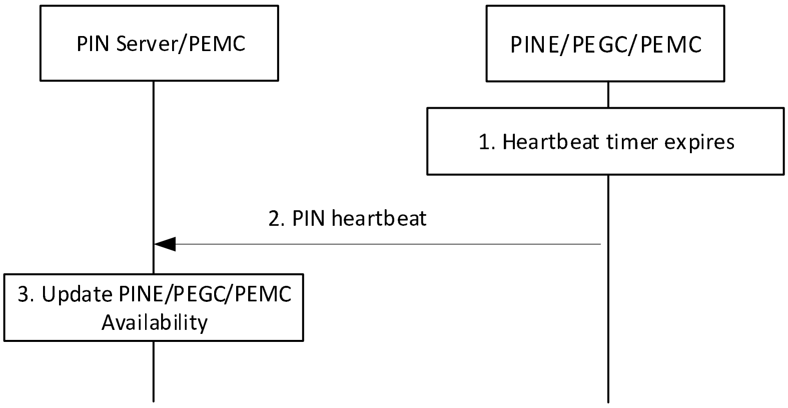
PIN Server/PEMC
PINE/PEGC/PEMC
1. Heartbeat timer expires
2. PIN heartbeat
3. Update PINE/PEGC/PEMC Availability

Figure 8.5.12.2.1-1: PIN heartbeat procedure

1. Before the periodic heartbeat timer at the PINE/PEGC/PEMC expires, the PINE/PEGC/PEMC triggers the sending of a PIN heartbeat.
2. The PINE/PEGC/PEMC sends a PIN heartbeat to either the PEMC (in the case of a PINE/PEGC) or PIN server (in the case of a PEMC). The PIN heartbeat includes the identifier of the PINE/PEGC/PEMC.
3. Upon receiving the PIN heartbeat, the PIN Server/PEMC updates the availability of the PINE/PEGC/PEMC.

If the periodic heartbeat timer expires at the PIN server/PEMC without receiving a PIN heartbeat message from the PINE/PEGC/PEMC, the PIN server/PEMC determines that PINE/PEGC/PEMC is not available.

8.5.12.3 Information flows

8.5.12.3.1 General

The PIN heartbeat information flow is specified for the PIN heartbeat.

8.5.12.3.2 PIN heartbeat

Table 8.5.12.3.2-1: PIN heartbeat

Information element	Status	Description
PIN client ID	M	Unique identifier of the PINE/PEGC/PEMC.
PIN ID	M	Identifier of the PIN.

8.5.13 PIN activation and deactivation

8.5.13.1 General

The procedures in this clause describes how a PEMC can activate and deactivate the PIN. PEMC being an authorized entity to manage the PIN can request to activate and deactivate the PIN. When the PIN is in deactivated state, services offered by the PIN are inaccessible and no PIN elements can join the PIN. Also PEGC closes all the communication channel it has created for the flow of application traffic from PIN elements via 5GS to the application server.

The PEMC deactivates the PIN when the expiration time obtained at PIN creation is reached and the PIN validity duration from the PIN profile is not expired (e.g., the PIN may be activated again in the future). The PEMC deletes the

PIN, according to the procedure specified in subclause 8.5.3.2, when the expiration time of the PIN obtained at PIN creation is reached and there is no PIN validity duration in the PIN profile.

8.5.13.2 Procedure

8.5.13.2.1 PIN activation

Figure 8.5.13.2.1-1 illustrates a procedure for activating the PIN by PEMC.

Pre-conditions:

1. PEMC(PINE-3), PEGC, PINE-1 and PINE-2 all are part of same PIN
2. The PIN being activated has already been created earlier and is in the deactivated state.
3. The PINE-3 is authorized as PEMC of the PIN.
4. PIN server, PEGC and PIN elements has active PIN status subscription with PEMC

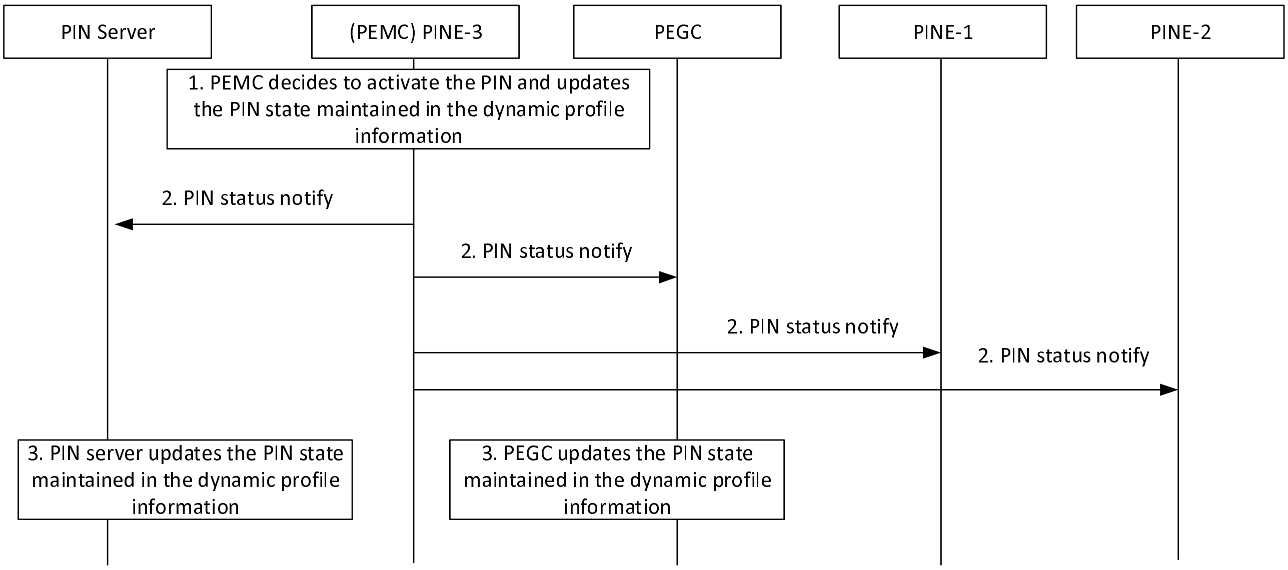
PIN Server
(PEMC) PINE-3
PEGC
PINE-1
PINE-2
1. PEMC decides to activate the PIN and updates the PIN state maintained in the dynamic profile information
2. PIN status notify
2. PIN status notify
2. PIN status notify
2. PIN status notify
3. PIN server updates the PIN state maintained in the dynamic profile information
3. PEGC updates the PIN state maintained in the dynamic profile information

Figure 8.5.13.2.1-1: Activation of PIN by PEMC

1. PEMC (PINE-3), PEGC, PINE-1, PINE-2, PINE-3 all are part of same PIN, which is created earlier and is now in deactivated state. PEMC decides to activate the PIN and updates the PIN state in the dynamic profile information of the PIN. Decision by PEMC to activate the PIN could be because of the PIN validity duration or based on the request from PIN owner/admin or any other implementation specific reasons.
2. PEMC notifies PIN server and all PIN elements including the PEGC that the PIN state is activated now by sending the PIN status notify.
3. PIN server and PEGC updates the dynamic PIN information to change the PIN state to active and PIN validity duration.

8.5.13.2.2 PIN de-activation

Figure 8.5.13.2.2-1 illustrates a procedure for de-activating the PIN by PEMC.

Pre-conditions:

1. PEGC, PINE-1, PINE-2 and PINE-3 are part of same PIN, which is created earlier and is now in activated state.
2. The PINE-3 is authorized as PEMC.

3. PEMC (PINE-3) decides to de-activate the PIN.

4. PIN server, PEGC and PINE has active PIN status subscription with PEMC

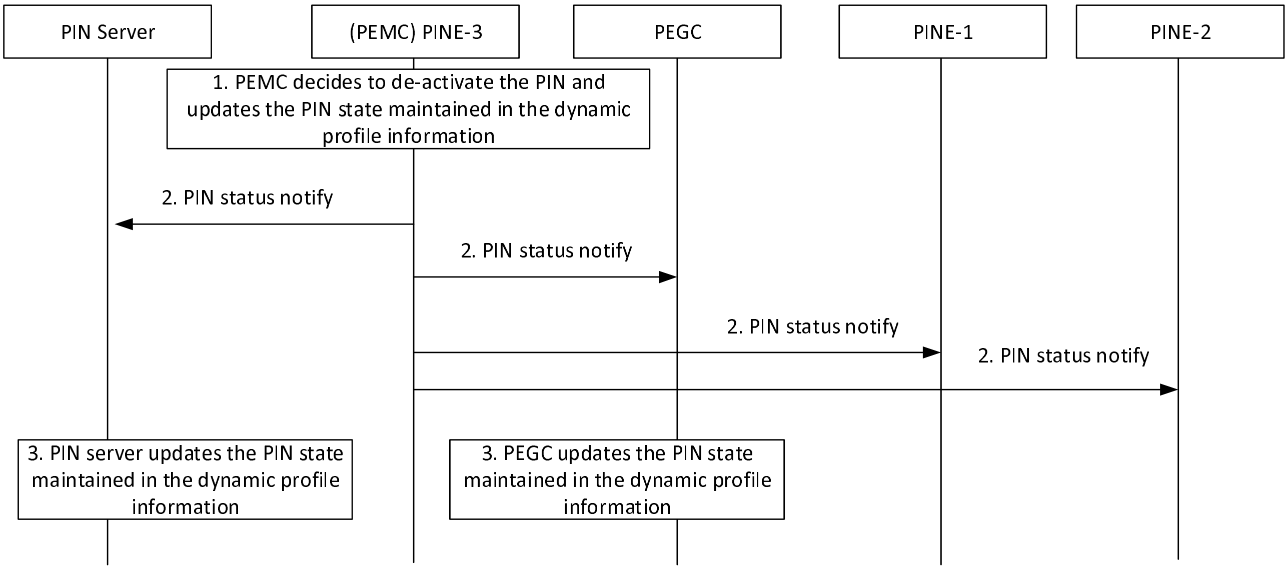
PIN Server
(PEMC) PINE-3
PEGC
PINE-1
PINE-2
1. PEMC decides to de-activate the PIN and updates the PIN state maintained in the dynamic profile information
2. PIN status notify
2. PIN status notify
2. PIN status notify
2. PIN status notify
3. PIN server updates the PIN state maintained in the dynamic profile information
3. PEGC updates the PIN state maintained in the dynamic profile information

Figure 8.5.13.2.2-1: Deactivation of PIN by PEMC

1. PEMC (PINE-3) decides to deactivate the PIN and updates the PIN state in the dynamic profile information of the PIN to de-activate. Decision reason by PEMC to deactivate the PIN could be PIN validity duration is expiring or all the PIN elements have left the PIN or on receiving the request from PIN owner/admin or for any other reasons which could be implementation specific.

2. PEMC notifies PIN server and all PIN elements including the PEGC that the PIN state is deactivated now by sending the PIN status notify

3. On receiving the PIN status notify, the PIN server and PEGC updates the PIN state to de-activate in the dynamic profile information. PEGC closes all the PIN communication with 5GS which it has created for the flow of application traffic of the PIN elements it is serving.

8.5.14 PIN connectivity subscription

8.5.14.1 General

The PIN connectivity subscription is used by the PINE/PEMC/PIN Server to be notified of PIN connectivity events by the PEGC.

PIN connectivity notification includes PIN connectivity information.

8.5.14.2 Procedure

8.5.14.2.1 PIN connectivity subscribe

Figure 8.5.14.2.1-1 illustrates the PIN connectivity subscribe procedure.

Pre-conditions:

1. The PINE/PEMC/PIN Server (e.g., subscriber) has already received the address of PEGC;

2. The subscriber has been authorized to communicate with PEGC;

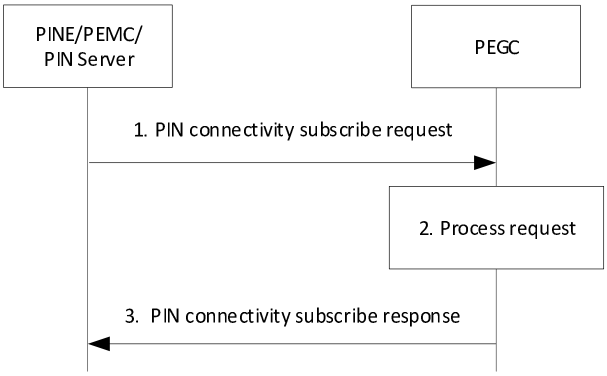
PINE/PEMC/
PIN Server
PEGC
1. PIN connectivity subscribe request
2. Process request
3. PIN connectivity subscribe response

Figure 8.5.14.2.1-1: PIN connectivity subscribe

1. The subscriber sends the PIN connectivity subscribe request to the PEGC. The PIN connectivity subscribe request includes the subscriber identifier along with the security credentials and the event identifier.
2. Upon receiving the request from the subscriber, the PEGC checks if the subscriber is authorized to subscribe for PIN connectivity information. The authorization check may apply to an individual PIN. If the request is authorized, the PEGC creates and stores the subscription for PIN.
3. If the processing of the request is successful, the PEGC sends a PIN connectivity subscribe response to the subscriber, which includes the subscription identifier and may include the expiration time, indicating when the subscription will automatically expire. To maintain the subscription, the subscriber shall send a PIN connectivity update request prior to the expiration time. If a new PIN connectivity update request is not received prior to the expiration time, the PEGC shall treat the subscriber as implicitly unsubscribed.

8.5.14.2.2 PIN connectivity notify

Figure 8.5.14.2.2-1 illustrates the PIN connectivity notify procedure.

Pre-conditions:

1. The PINE/PEMC/PIN Server (e.g., subscriber) has successfully subscribed with the PEGC for the PIN connectivity as specified in clause 8.5.14.2.1.

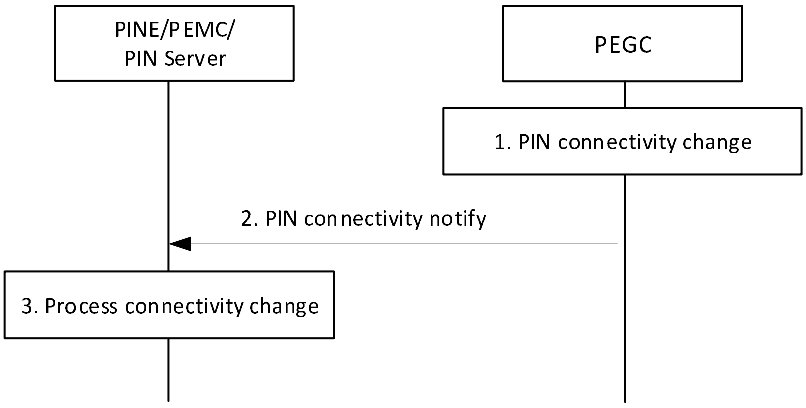
PINE/PEMC/
PIN Server
PEGC
1. PIN connectivity change
2. PIN connectivity notify
3. Process connectivity change

Figure 8.5.14.2.2-1: PIN connectivity notify procedure

1. When an event occurs at the PEGC that satisfies triggering conditions, the PEGC notifies the subscriber(s).
2. The PEGC sends an PIN connectivity notification to the subscribers related to the connectivity event and includes the PIN connectivity information.

   The PIN connectivity information includes the PEGC identifier, the PIN identifier, the PIN client identifier, and the event type (e.g., connectivity).
3. Upon receiving the notification, the subscriber processes the connectivity changes according to the information in the PIN connectivity notification.

8.5.14.2.3 PIN connectivity update

Figure 8.5.14.2.3-1 illustrates the PIN connectivity update procedure.

Pre-conditions:

1. The PINE/PEMC/PIN Server (e.g., subscriber) has subscribed with the PEGC for PIN connectivity information as specified in 8.5.14.2.1;

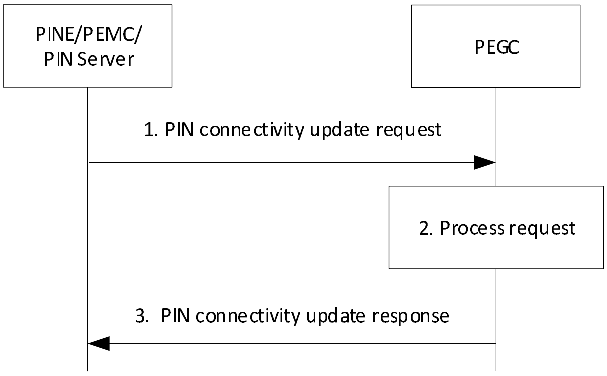
PINE/PEMC/
PIN Server
PEGC
1. PIN connectivity update request
2. Process request
3. PIN connectivity update response

Figure 8.5.14.2.3-1: PIN connectivity update

1. The subscriber sends a PIN connectivity update request to the PEGC. The PIN connectivity update request includes the security credentials and the subscription identifier. It may also include notification target address and proposed expiration time.
2. Upon receiving the request from the requestor, the PEGC checks if the subscriber is authorized to update the subscription information. If the request is authorized, the PEGC updates the stored subscription for PIN connectivity information.
3. If the processing of the request is successful, the PEGC sends a PIN connectivity update response to the subscriber, which may include the expiration time, indicating when the subscription will automatically expire. To maintain the subscription, the subscriber shall send an PIN connectivity update request prior to the expiration time. If a PIN connectivity update request is not received prior to the expiration time, the PEGC shall treat the subscriber as implicitly unsubscribed.

8.5.14.2.4 PIN connectivity unsubscribe

Figure 8.5.14.2.4-1 illustrates the PIN connectivity unsubscribe procedure.

Pre-conditions:

1. The PINE/PEMC/PIN Server (e.g., subscriber) has subscribed with the PEGC for PIN connectivity information as specified in 8.5.14.2.1;

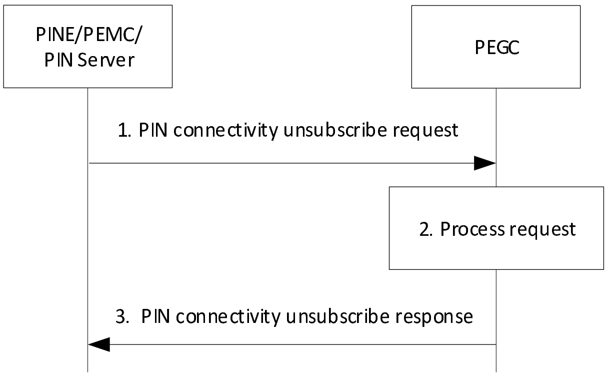
PINE/PEMC/
PIN Server
PEGC
1. PIN connectivity unsubscribe request
2. Process request
3. PIN connectivity unsubscribe response

Figure 8.5.14.2.4-1: PIN connectivity update

1. The subscriber sends a PIN connectivity unsubscribe request to the PEGC. The PIN connectivity unsubscribe request includes the security credentials and the subscription identifier.

2. Upon receiving the request from the subscriber, the PEGC checks if the requestor is authorized to unsubscribe. If the request is authorized, the PEGC cancels the subscription for PIN connectivity information.

3. If the processing of the request is successful, the PEGC sends a PIN connectivity unsubscribe response to the subscriber.

8.5.14.3 Information flows

8.5.14.3.1 General

The following information flows are specified for PIN connectivity subscription:

- PIN connectivity subscribe
- PIN connectivity notify
- PIN connectivity update
- PIN connectivity unsubscribe

8.5.14.3.2 PIN connectivity subscribe request

Table 8.5.14.3.2-1: PIN connectivity subscribe request

Information element	Status	Description
Subscriber identifier	M	Unique identifier of the PINE/PEMC/PIN server.
Security credentials	M	Security credentials resulting from a successful authorization for the PIN service.
PIN ID	M	The identifier of PIN.
Notification Target Address	M	The Notification target address (e.g. URL) where the notifications destined for the subscriber should be sent to.
Proposed expiration time	O	Proposed expiration time for the subscription

8.5.14.3.3 PIN connectivity subscribe response

Table 8.5.14.3.3-1: PIN connectivity subscribe response

Information element	Status	Description
Successful response	O	Indicates that the subscription request was successful.
> Subscription ID	M	Subscription identifier corresponding to the subscription.
> Expiration time	O	Indicates the expiration time of the subscription. To maintain an active subscription, a subscription update is required before the expiration time.
Failure response	O	Indicates that the subscription request failed.
> Cause	O	Indicates the cause of subscription request failure

8.5.14.3.4 PIN connectivity notify

Table 8.5.14.3.4-1 describes information elements in the PIN connectivity notification from the PEGC.

Table 8.5.14.3.4-1: PIN connectivity notification

Information element	Status	Description
PEGC identifier	M	Identifier of the PEGC
PIN identifier	M	Identifier of the PIN.
PIN client identifier	M	Unique identifier of the PINE/PEMC/PIN server related to the connectivity change
Event type	M	Type of event (e.g., connectivity)

8.5.14.3.5 PIN connectivity update request

Table 8.5.14.3.5-1: PIN connectivity update request

Information element	Status	Description
Subscription ID	M	Subscription identifier corresponding to the subscription.
Security credentials	M	Security credentials resulting from a successful authorization for the PIN service.
Notification Target Address	O	The Notification target address (e.g. URL) where the notifications destined for the subscriber should be sent to.
Proposed expiration time	O	Proposed expiration time for the subscription

8.5.14.3.6 PIN connectivity update response

Table 8.5.14.3.6-1: PIN connectivity update response

Information element	Status	Description
Successful response (see NOTE)	O	Indicates that the subscription update request was successful.
> Expiration time	O	Indicates the expiration time of the subscription. To maintain an active subscription, a subscription update is required before the expiration time.
Failure response (see NOTE)	O	Indicates that the subscription update request failed.
> Cause	M	Indicates the cause of subscription update request failure
NOTE: One IE is included in the response.		

8.5.14.3.7 PIN connectivity unsubscribe request

Table 8.5.14.3.7-1: PIN connectivity unsubscribe request

Information element	Status	Description
Subscription ID	M	Subscription identifier corresponding to the subscription.
Security credentials	M	Security credentials resulting from a successful authorization for the PIN service.

8.5.14.3.8 PIN connectivity unsubscribe response

Table 8.5.14.3.8-1: PIN connectivity unsubscribe response

Information element	Status	Description
Successful response (see NOTE)	O	Indicates that the unsubscribe request was successful.
Failure response (see NOTE)	O	Indicates that the unsubscribe request failed.
> Cause	M	Indicates the cause of unsubscribe request failure
NOTE: One IE is included in the response.		

8.6 PIN enable 5GS communication

8.6.1 General

For a certain PINE in PIN, the PEMC controls whether to allow or forbid the PINEs to communicate with other PINEs via PEGC directly or communicate with other PINEs via PEGC by 5GS. Also, the PEMC controls whether to allow or forbid the traffic from network sides to deliver to certain PINE.

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.

- 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.

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 PIN element sends PIN Communication Request to the PEMC and the PEMC checks whether to allow or forbid the PINEs to communicate with other PINEs via PEGC directly or communicate with other PINEs via PEGC by 5GS. If the alloewd, the PEMC sends Create/Update/Remove Communication Request (PIN ID, Packet filters, requested QoS) to the PEGC. Or,the PEMC directly send 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).

8.6.2 Procedure

8.6.2.1 AF trigger QoS establishment

For the AF related procedure, the AF trigger the QoS create/modification procedure as defined in Section 4.15.6.6 of TS 23.502[5] with parameters of Packet filters (that related to the PINEs needs communication), DN specific ID, to request the 5GS to arrange resource for PIN.

8.6.2.2 Procedures of PIN communication via 5GS triggered by PEGC

Pre-conditions:

1. The PINE already has application layer connection with PEGC;
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.

7. The PIN is in the activated state.

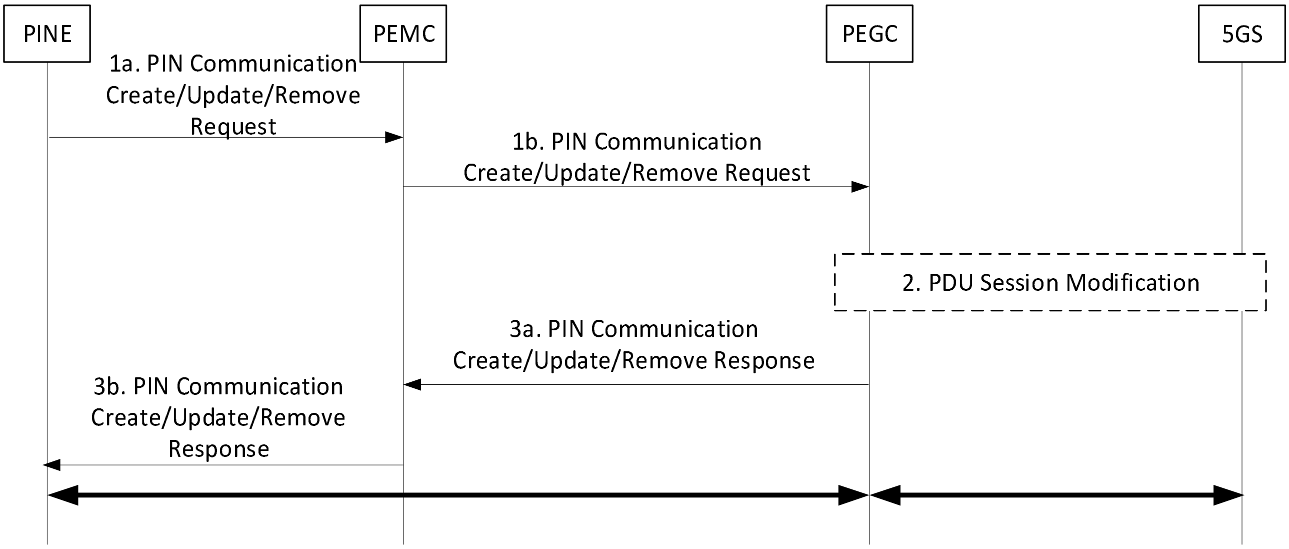
PINE
PEMC
PEGC
5GS
1a. PIN Communication Create/Update/Remove Request
1b. PIN Communication Create/Update/Remove Request
2. PDU Session Modification
3a. PIN Communication Create/Update/Remove Response
3b. PIN Communication Create/Update/Remove Response

Figure 8.6.2.2-1: Procedures of PIN communication via 5GS triggered by PEGC

The PINE may have the traffic to send via 5GS communication.

1a-1b. The PINE sends PIN Communication Create/Update/Remove Request (PIN ID, MAC address/IP address, Traffic descriptors, Packet filters, requested QoS) to the PEMC in step 1a, and the PEMC checks whether to allow or forbid the PINEs to communicate with other PINEs via PEGC directly or communicate with other PINEs via PEGC by 5GS. If permitted, PEMC sends PIN Communication Create/Update/Remove Request to PEGC in step 1b. If not permitted, PEMC directly performs step 3b to indicate failure in PIN Communication Create/Update/Remove response.

After the PEGC receives the PIN Communication Create/Update/Remove Request, the PEGC configures the local rule accordingly.

2. [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).

NOTE: How to the PEGC interacts with 5GS to initiate PDU Session Modification is referred to section 4.3.3.2 of TS 23.502[5].

3a. The PEGC sends PIN Communication Create/Update/Remove Response to the PEMC.

3b. If the request is triggered by PINE, step 3b is performed. The PEMC sends PIN Communication Create/Update/Remove Response to PINE.

After receiving successful response, the PINE sends data through the PEGC to the 5GS using the PDU session modified in step 2.

8.6.3 Information flows

8.6.3.1 General

The following information flows are specified for PIN communication:

- PIN Communication Create/Update/Remove Request and response;

8.6.3.2 PIN Communication Create Request

Table 8.6.3.2-1 shows the informational elements of the PIN Communication Create request sent by a PIN Element/PEMC to the PEGC to provide the PIN communication information.

Table 8.6.3.2-1: PIN Communication Create request

Information element	Status	Description
PIN ID	M	The identifier of the PIN
Requester PINE ID/PEMC	M	The identifier of the PIN Element/PEMC making the request
Security credentials	M	Security credentials resulting from a successful authorization for the PIN service.
MAC address/IP address	O	MAC address/IP address of PINE/PEMC
Traffic descriptors	M	Identify the target traffic to/from application server or to/from PINE, e.g.: IP 5 Tuple.
Packet filters	M	The Packet Filter is used in PEGC to identify one or more packet flow(s), and the PEGC can route the traffic to the target application server/PINEs.
Request QoS	O	The QoS (e.g.: packet delay or AMBR) of packet flow that requested by PINE.

8.6.3.3 PIN Communication Create Response

Table 8.6.3.3-1 shows the informational elements of the PIN Communication Create response sent by a PEGC to the PINE/PEMC.

Table 8.6.3.3-1: PIN Communication Create response

Information element	Status	Description
Successful response	O (see NOTE)	Indicates that the PIN communication creation request was successful.
> QoS information	M	Includes QoS information that agreed for this information flow.
> PIN communication flow ID	M	Includes the communication flow that successfully established by PEGC.
Failure response	O (see NOTE)	Indicates that the PIN communication creation request failed.
> Cause	M	Provides the cause for PIN communication creation request failure.
NOTE: At least one of the IE shall be present.		

8.6.3.4 PIN Communication Update Request

Table 8.6.3.4-1 shows the informational elements of the PIN Communication Update request sent by a PIN Element/PEMC to the PEGC to provide the updated PIN communication information.

Table 8.6.3.4-1: PIN Communication Update request

Information element	Status	Description
PIN ID	M	The identifier of the PIN
Requester PINE ID/PEMC	M	The identifier of the PIN Element/PEMC making the request
Security credentials	M	Security credentials resulting from a successful authorization for the PIN service.
MAC address/IP address	O	MAC address/IP address of PINE/PEMC
Traffic descriptors	M	Identify the updated target traffic to/from application server or to/from PINE, e.g.: IP 5 Tuple.
Packet filters	M	Updated packet filters that is used in PEGC to identify one or more packet flow(s), and the PEGC can route the traffic to the target application server/PINEs.
PIN communication flow ID	M	Includes the communication flow that has been successfully established by PEGC.
Request QoS	O	The updated QoS (e.g.: packet delay or AMBR) of packet flow that requested by PINE.

8.6.3.5 PIN Communication Update Response

Table 8.6.3.5-1 shows the informational elements of the PIN Communication Update response sent by a PEGC to the PINE/PEMC.

Table 8.6.3.5-1: PIN Communication Create response

Information element	Status	Description
Successful response	O (see NOTE)	Indicates that the PIN communication update request was successful.
> QoS information	M	Includes updated QoS information that agreed for this information flow.
> PIN communication flow ID	M	Includes the communication flow that successfully established by PEGC.
Failure response	O (see NOTE)	Indicates that the PIN communication update request failed.
> Cause	M	Provides the cause for PIN communication update request failure.
NOTE: At least one of the IE shall be present.		

8.6.3.6 PIN Communication Delete Request

Table 8.6.3.6-1 shows the informational elements of the PIN Communication Delete request sent by a PIN Element/PEMC to the PEGC to delete the PIN communication.

Table 8.6.3.4-1: PIN Communication Delete request

Information element	Status	Description
PIN ID	M	The identifier of the PIN
Requester PINE ID/PEMC	M	The identifier of the PIN Element/PEMC making the request
Security credentials	M	Security credentials resulting from a successful authorization for the PIN service.
PIN communication flow ID	M	Includes the communication flow that has been successfully established by PEGC.

8.6.3.7 PIN Communication Delete Response

Table 8.6.3.7-1 shows the informational elements of the PIN Communication Delete response sent by a PEGC to the PINE/PEMC.

Table 8.6.3.7-1: PIN Communication Delete response

Information element	Status	Description
Successful response	O (see NOTE)	Indicates that the PIN communication delete was successful.
Failure response	O (see NOTE)	Indicates that the PIN communication delete request failed.
> Cause	M	Provides the cause for PIN communication delete request failure.
NOTE: At least one of the IE shall be present.		

8.7 Service Switch

8.7.1 General

PIN service switch procedures enable a PIN Element participating in a PIN to transfer application session(s) to a different PIN Element participating in the same PIN. For example, a first PIN Element (e.g. a UE) can transfer a video streaming session to a second PIN Element (e.g. a television). PIN service switch can be triggered by a PIN Element when needed, for example when the first PIN Element joins a PIN and determines that an application flow can be switched to a second PIN Element present in that PIN.

Two scenarios are specified for PIN service switch:

- PIN service switch with PIN server support
- PIN service switch without PIN Server support (e.g. using only internal PIN communication).

8.7.2 Procedure

8.7.2.1 Service switch in a PIN with PIN server support

8.7.2.1.1 General

Following procedures are supported for service switch in a PIN with PIN server support:

- PIN Service Switch procedure;
- PIN Service Switch Configure procedure;

8.7.2.1.2 PIN Service Switch procedure

Pre-conditions:

1. The PIN Client established an application session with an Application Server;
2. The PIN Client joined a PIN.

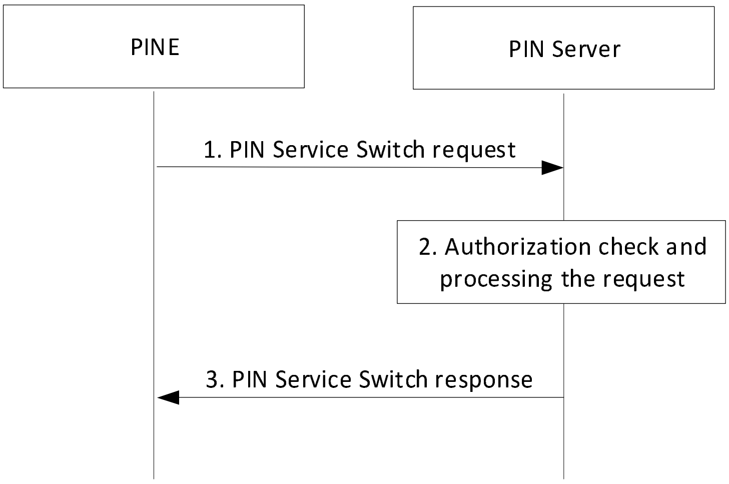
PINE
PIN Server
1. PIN Service Switch request
2. Authorization check and processing the request
3. PIN Service Switch response

Figure 8.7.2.1.2-1: PIN Service Switch procedure

1. The PIN Client sends a PIN Service Switch request to the PIN Server. The PIN Service Switch request includes the requestor identifier [PIN Client ID], security credential, a PIN identifier [PIN ID], an Application Client identifier [ACID], an Application Server identifier, an application session identifier, can include an IP 4 tuple that describes the traffic of the application session and can include a target PIN Client [PIN Client ID] if a target is known.

2. Upon receiving the request from the PIN Client, the PIN Server checks if the PIN Client is authorized to request service switching for the given Application Server and validates the request. If the request is authorized and valid, the PIN server can determine a target PIN Client if the target PIN Client was not included in the request. The PIN Server sends a PIN Configure Service Switch request to the PIN Management Client and the Application Server as in clause 8.7.2.1.2. The PIN Server can use the PIN ID to identify the PIN Management Client instance and the Application Server identifier, or IP 4 tuple, to identify the Application Server instance.

3. If the processing of the request was successful, the PIN Server sends a PIN Service Switch response to the PIN Client that indicates the Service Swich request was successfully processed and can include the target PIN Client information if it was decided by the PIN Server. Otherwise, the PIN Server sends a PIN Service Switch response to the PIN Client indicating that the request processing failed and can include appropriate reasons.

Upon reciving the PIN Service Switch response, the PIN Client validates if the request was succesful and can indicate the result to the Application Client; the PIN Client can transfer the application context to the target PIN Client. If the PIN Service Switch response indicated a failure, the PIN Client can attempt perform service switch again for the same or a different target PIN Client considering the failure reason.

8.7.2.1.3 PIN Service Switch Configure procedure

Pre-conditions:

1. The PIN Client successfully requested a service switch with the PIN Server

2. The AS is successfully subscribed for PIN service switch notifications with the PIN server.

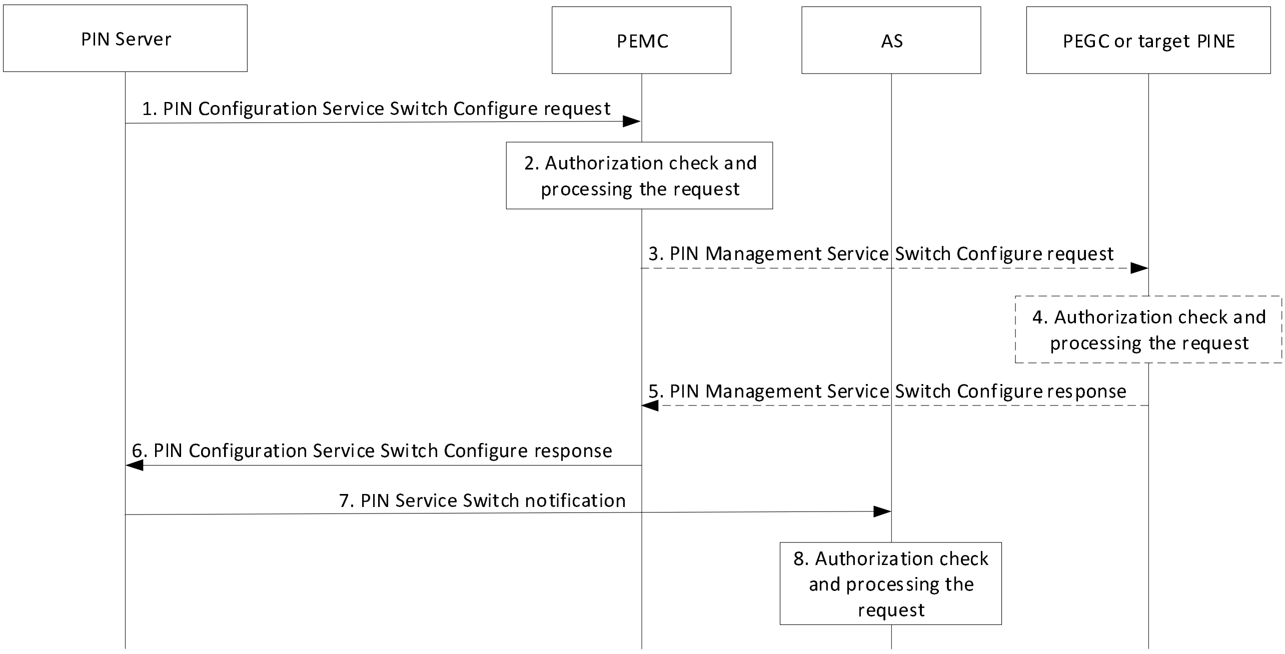
PIN Server
PEMC
AS
PEGC or target PINE
1. PIN Configuration Service Switch Configure request
2. Authorization check and processing the request
3. PIN Management Service Switch Configure request
4. Authorization check and processing the request
5. PIN Management Service Switch Configure response
6. PIN Configuration Service Switch Configure response
7. PIN Service Switch notification
8. Authorization check and processing the request

Figure 8.7.2.1.3-1: PIN Configure Service Switch procedure

1. The PIN Server sends the PIN Configuration Service Switch Configure request to the PIN Management Client. The PIN Configuration Service Switch Configure request includes the requestor identifier, security credential, Application Client identifier, Application Server identifier, target PIN Client, application session identifier and can include IP 4 tuple that descibes the traffic of the application session.

NOTE 1: The PIN Server first performs PIN Configure Service Switch procedure with the PIN Management Client, then if successful, notifies the Application Server.

2. Upon receiving the request from the PIN Server, the PIN Management Client checks if the PIN Server is authorized to request service switch configuration and validates the request.

   If the request is authorized and valid, the PIN Management Client prepares for sending PIN Configure Service Switch request to the PIN Gateway Client or the target PIN Client. The PIN Management Client can use the PIN ID to identify the PIN Gateway Client instance and the target PIN Client identifier to identify the target PIN Client.

3. The PIN Management Client sends the PIN Management Service Switch Configure request to the PIN Gateway Client or the target PIN Client including the information defined in step 1.

NOTE 2: The PIN Management Client first performs PIN Configure Service Switch procedure with the PIN Gateway Client, then if successful, with the target PIN Client.

4. Upon receiving the request from the PIN Management Client, the PIN Gateway Client or the target PIN Client checks if the PIN Managment Client is authorized to request service switch configuration and validates the request. If the PIN Management Client is authorized and the request is valid, the PIN Gateway Client or the target PIN Client use the information provided in the request to switch the application session to the target PIN Client.

NOTE 3: The target Application Client needs to receive the application context prior to re-establishing a switched application session with the Application Server.

NOTE 4: How the target Application Client recovers the switched application session is out of scope of this specification.

5. If the processing of the request was successful, the PIN Gateway Client or the target PIN Client send a PIN management Service Switch Configure response to the PIN Management Client indicating the processing was successful. Otherwise, the PIN Gateway Client or target PIN Client send a PIN Management Service Switch Configure response to the PIN Management Client indicating that processing the request failed and can include appropriate reasons.

6. If the processing of the request was successful, the PIN Management Client or Application Server send a PIN Configuration Service Switch Configure response to the PIN Server that indicates the request was successfully processed. Otherwise, the PIN Management Client or Application Server send a PIN Configuration Service Switch Configure response to the PIN Server indicating the processing the request failed and can include appropriate reasons.

7. The PIN Server sends the PIN service switch notification to the Application Server if the procedure with the PIN Management Client was successful in step 6. The PIN service switch notification includes the PIN server identifier, PIN identifier, Application Client identifier, target PIN Client, application session identifier and can include IP 4 tuple that descibes the traffic of the application session.

8. Upon receiving the PIN service switch notification, the Application Server uses the information provided in the notification to switch the application session to the target PIN client.

8.7.2.1.4 PIN Service Switch subscription

8.7.2.1.4.1 General

The PIN service switch subscription is used by the Application Server to be notified of PIN service switch events by the PIN Server.

The PIN service switch notification events includes PIN service switch configuration information.

8.7.2.1.4.2 Procedure

8.7.2.1.4.2.1 PIN service switch subscribe

Figure 8.7.2.1.4.2.1-1 illustrates the PIN service switch subscribe procedure.

Pre-conditions:

1. The application server has already received the address of the PIN server;

2. The application server is authorized to communicate with PIN server;

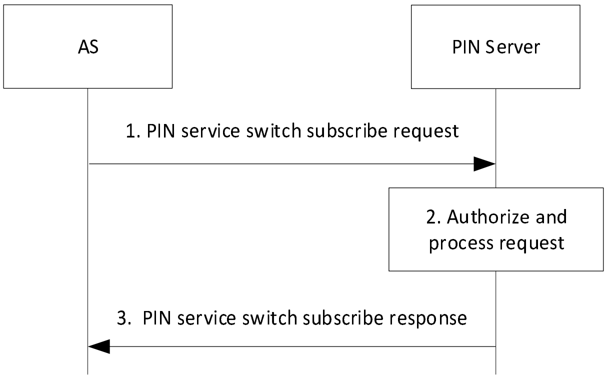
AS
PIN Server
1. PIN service switch subscribe request
2. Authorize and process request
3. PIN service switch subscribe response

Figure 8.7.2.1.4.2.1-1: PIN service switch subscribe

1. The application server sends the PIN service switch subscribe request to the PIN server. The PIN service switch subscribe request includes the application server identifier along with the security credentials, PIN ID, subscribed event, notification target address, and may include proposed expiration time.

2. Upon receiving the request from the application server, the PIN server checks if the application server is authorized to subscribe. The authorization check may apply to an individual PIN. If the request is authorized, the PIN server creates and stores the subscription for application server.

3. If the processing of the request is successful, the PIN server sends a PIN service switch subscribe response to the application server, which includes the subscription identifier and may include the expiration time, indicating when the subscription will automatically expire. To maintain the subscription, the application server shall send a

PIN service switch update request prior to the expiration time. If a new PIN service switch update request is not received prior to the expiration time, the PIN server shall treat the application server as implicitly unsubscribed.

8.7.2.1.4.2.2 PIN service switch notify

Figure 8.7.2.1.4.2.2-1 illustrates the PIN service switch notify procedure.

Pre-conditions:

1. The application server has subscribed with the PIN server as specified in clause 8.7.2.1.4.2.1.

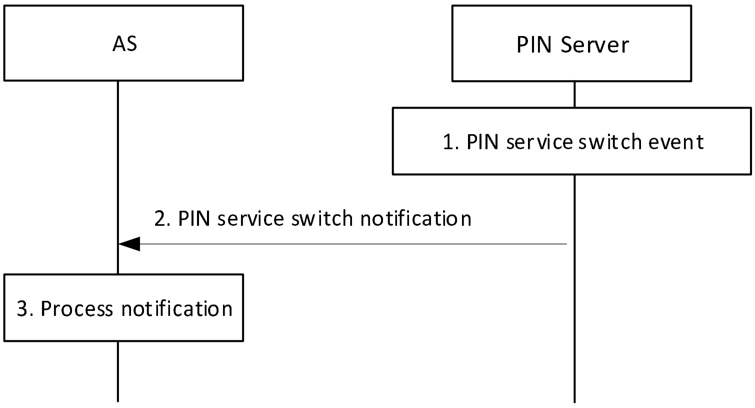
AS
PIN Server
1. PIN service switch event
2. PIN service switch notification
3. Process notification

Figure 8.7.2.1.4.2.2-1: PIN service switch notify procedure

1. When a service switch event occurs at the PIN server that satisfies triggering conditions, the PIN server sends a server switch notification to the subscribed application servers.
2. The PIN server sends an PIN service switch notification to the subscribed application server(s) related to the service switch event and includes the PIN service switch configuration information.

   The PIN service switch configuration information includes the PIN subscription identifier, subscribed event, PIN server identifier, PIN identifier, Application Client identifier, application session identifier, target PIN Client, application session identifier and can include IP 4 tuple that describes the traffic of the application session.
3. Upon receiving the notification, the application server uses the information provided in the notification to switch the application session to the target PIN client.

8.7.2.1.4.2.3 PIN service switch update

Figure 8.7.2.1.4.2.3-1 illustrates the PIN service switch update procedure.

Pre-conditions:

1. The application server has subscribed with the PIN server as specified in clause 8.7.2.1.4.2.1.

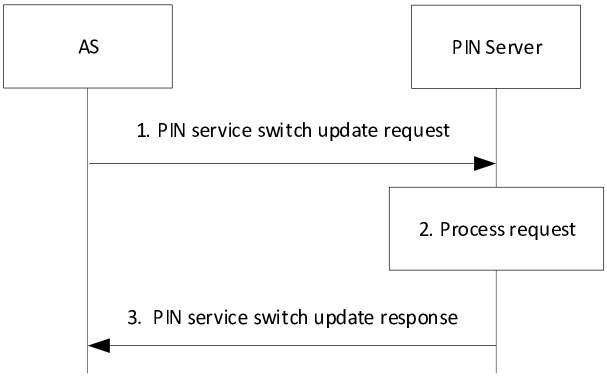
AS
PIN Server
1. PIN service switch update request
2. Process request
3. PIN service switch update response

Figure 8.7.2.1.4.2.3-1: PIN service switch update

1. The application server sends a PIN service switch update request to the PIN server. The PIN service switch update request includes the security credentials and the subscription identifier. It may also include notification target address and proposed expiration time.

2. Upon receiving the request from the application server, the PIN server checks if the application server is authorized to update the subscription information. If the request is authorized, the PIN server updates the stored subscription.

3. If the processing of the request is successful, the PIN server sends a PIN service switch update response to the application server, which may include the expiration time, indicating when the subscription will automatically expire. To maintain the subscription, the application server shall send a PIN service switch subscription update request prior to the expiration time. If a PIN service switch update request is not received prior to the expiration time, the PIN server shall treat the application server as implicitly unsubscribed.

8.7.2.1.4.2.4 PIN service switch unsubscribe

Figure 8.7.2.1.4.2.4-1 illustrates the PIN service switch unsubscribe procedure.

Pre-conditions:

1. The application server has subscribed with the PIN server as specified in clause 8.7.2.1.4.2.1.

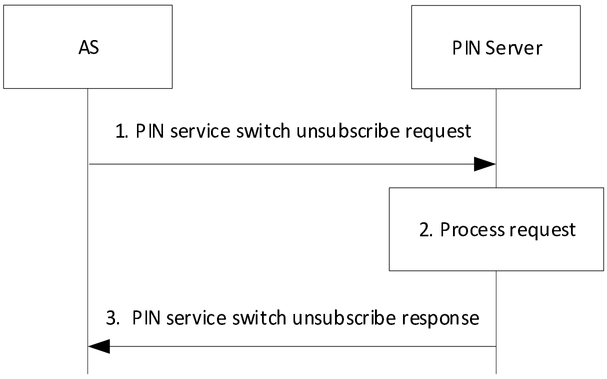
AS
PIN Server
1. PIN service switch unsubscribe request
2. Process request
3. PIN service switch unsubscribe response

Figure 8.7.2.1.4.2.4-1: PIN service switch unsubscribe

1. The application server sends a PIN service switch unsubscribe request to the PIN server. The PIN service switch unsubscribe request includes the security credentials and the subscription identifier.

2. Upon receiving the request from the application server, the PIN server checks if the application server is authorized to unsubscribe. If the request is authorized, the PIN server cancels the subscription indicated by the subscription identifier.

3. If the processing of the request is successful, the PIN server sends a PIN service switch unsubscribe response to the application server.

8.7.2.2 Service switch in a PIN without PIN server support

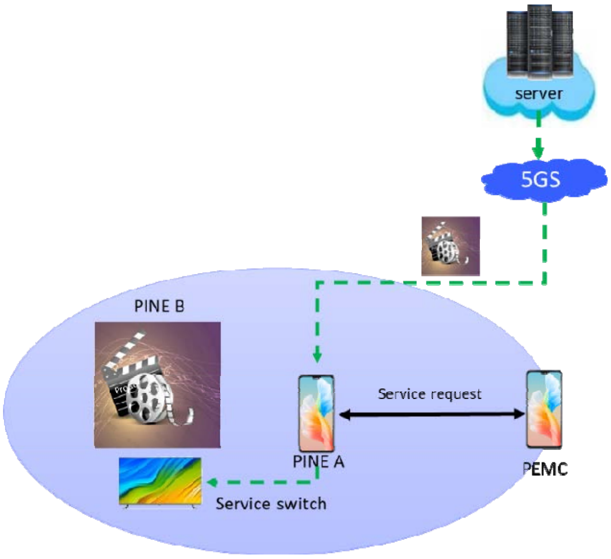

Figure 8.7.2.2-1: PIN Service Switch internal PIN

In Figure 8.7.2.2-1, it describes the service switch scenario supported internal PIN.

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.

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.

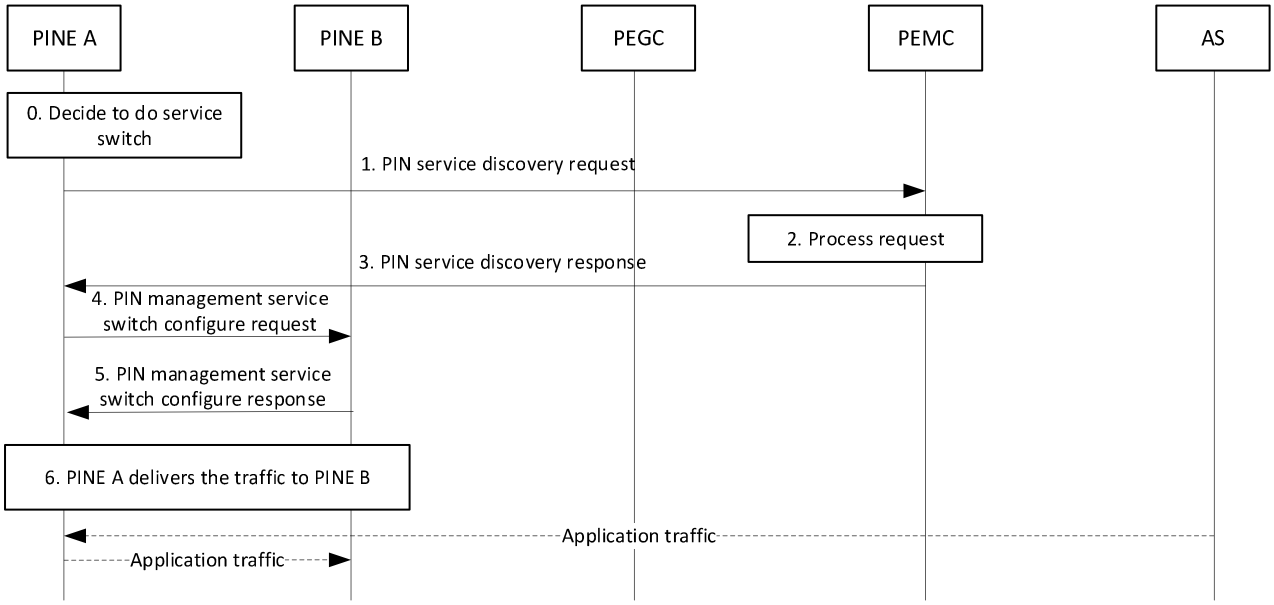
PINE A
PINE B
PEGC
PEMC
AS
0. Decide to do service switch
1. PIN service discovery request
2. Process request
3. PIN service discovery response
4. PIN management service switch configure request
5. PIN management service switch configure response
6. PINE A delivers the traffic to PINE B
Application traffic
Application traffic

Figure 8.7.2.2-2: 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 request towards PEMC. This request carries the list of services the PINE A 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.

3. The PEMC provides the list of PINE endpoint(s), application client endpoint(s) information that are offering the requested services to PINE A in PIN service discovery response. 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 selects PINE B from the list of PINEs provided in the PIN service discovery response.

   The PINE A sends the PIN Management Service Switch Configure request to the selected PINE B including: PIN ID, requestor ID, service information (e.g. PIN service type, PIN service feature) before performing service switch.

5. Upon receiving the request from PINE A, PINE B determines whether it can accept the service switch request and sends the PIN Management Service Switch Configure response to PINE A.

   If the PIN Management Service Switch Configure response indicates failure, the PINE A may consider other PINEs in the list of PINEs provided in the PIN service discovery response received in step 3 and may perform step 4 again.

   If the PIN Management Service Switch Configure response indicates success, the PINE A maintains the service towards AS and proceeds with switching the service traffic to PINE B.

6. The PINE A switches the traffic flow to PINE B via direct communication or via PEGC.

8.7.3 Information flows

8.7.3.1 General

The following information flows are specified for Service Switch:

- PIN service switch request and response
- PIN configuration service switch configure request and response

- PIN management service switch configure request and response
- PIN service discovery request and response
- PIN service switch subscribe
- PIN service switch notify
- PIN service switch update
- PIN service switch unsubscribe

8.7.3.2 PIN service switch request

Table 8.7.3.2-1 describes information elements for the PIN service switch request that is sent from the PIN client to the PIN server.

Table 8.7.3.2-1: PIN service switch request

Information element	Status	Description
PIN client identifier	M	Requestor identifier.
Security credentials	M	Security credentials of the PIN client.
PIN identifier	M	Identifier of the PIN.
Application client identifier	M	Identifier of the application client.
Application server identifier	M	Identifier of the application server
Application session identifier	M	Identifier of the application session
Application session descriptor	O	Descriptor of application traffic flows (e.g., IP 4 tuple)
Target PIN client identifier (see NOTE)	O	Target PIN client identifier.
NOTE: Only if target PIN client is known.		

8.7.3.3 PIN service switch response

Table 8.7.3.3-1 describes information elements for the PIN service switch response.

Table 8.7.3.3-1: PIN service switch response

Information element	Status	Description
Successful response (see NOTE 1)	O	Indicates that the request was successful.
> Target PIN client identifier (see NOTE 2)	O	Target PIN client identifier.
Failure response (see NOTE 1)	O	Indicates that the request failed.
> Cause	O	Indicates the cause of the request failure.
NOTE 1: Only one of the IE must be included in the response. NOTE 2: Only if target PIN client is not provided in the PIN service switch request.		

8.7.3.4 PIN configuration service switch configure request

Table 8.7.3.4-1 describes information elements for the PIN configuration service switch configure request that is sent from the PIN server to the PIN management client and the application server.

Table 8.7.3.4-1: PIN configuration service switch configure request

Information element	Status	Description
PIN server identifier	M	Requestor identifier.
Security credentials	M	Security credentials of the PIN server.
PIN identifier	M	Identifier of the PIN.
Application client identifier	M	Identifier of the application client.
Application server identifier (see NOTE 1)	O	Identifier of the application server.
Application session identifier	M	Identifier of the application session.
Application session descriptor	O	Descriptor of application traffic flows (e.g., IP 4 tuple)
Target PIN client identifier (see NOTE 2)	M	Target PIN client identifier.
NOTE 1: The IE is present if the request is sent to the PIN management client. NOTE 2: The IE is present if the request is sent to the application server.		

8.7.3.5 PIN configuration service switch configure response

Table 8.7.3.5-1 describes information elements for the PIN configuration service switch configure response.

Table 8.7.3.5-1: PIN configuration service switch configure response

Information element	Status	Description
Successful response (see NOTE)	O	Indicates that the request was successful.
Failure response (see NOTE)	O	Indicates that the request failed.
> Cause	O	Indicates the cause of the request failure.
NOTE: Only one of the IE must be included in the response.		

8.7.3.6 PIN management service switch configure request

Table 8.7.3.6-1 describes information elements for the PIN management service switch configure request that is sent from the PIN management client to the PIN gateway client and the target PIN client.

Table 8.7.3.6-1: PIN management service switch configure request

Information element	Status	Description
PINE identifier	M	Requestor identifier.
Security credentials	M	Security credentials of the PIN management client.
PIN identifier	M	Identifier of the PIN.
Application client identifier	M	Identifier of the application client.
Application server identifier	M	Identifier of the application server.
PIN gateway client identifier (see NOTE 1)	O	Identifier of the PIN gateway client.
Application session identifier	M	Identifier of the application session.
Application session descriptor	O	Descriptor of application traffic flows (e.g., IP 4 tuple)
Target PIN client identifier (see NOTE 2)	O	Target PIN client identifier.
Service information (see NOTE 3)	O	PIN service type and PIN service feature
NOTE 1: The IE is present if the request is sent to the target PIN client. NOTE 2: The IE is present if the request is sent to the PIN gateway client. NOTE 3: The IE is present if the request is sent to the PINE.		

8.7.3.7 PIN management service switch configure response

Table 8.7.3.7-1 describes information elements for the PIN management service switch configure response.

Table 8.7.3.7-1: PIN management service switch configure response

Information element	Status	Description
Successful response (see NOTE)	O	Indicates that the request was successful.
Failure response (see NOTE)	O	Indicates that the request failed.
> Cause	O	Indicates the cause of the request failure.
NOTE: Only one of the IE must be included in the response.		

8.7.3.8 PIN Service Discovery Request

Table 8.7.3.8-1 shows the informational elements of the PIN Service Discovery Request sent by a PIN Element to the PEMC to discover the candidate PINEs that can provide the certain PIN service.

Table 8.7.3.8-1: PIN Service Discovery Request

Information element	Status	Description
PIN ID	M	The identifier of the PIN
Requester PINE ID	M	The identifier of the PIN Element making the request
Security credentials	M	Security credentials resulting from a successful authorization for the PIN service.
MAC address/IP address	O	MAC address/IP address of PINE/PEMC
Request PIN service type	M	List the PIN service type that the PINE request to determine the targe PINE for service switch.

8.7.3.9 PIN Service Discovery Response

Table 8.7.3.9-1 shows the informational elements of the PIN Service Discovery Response sent by a PEMC to the PINE to list the candidate PINEs that can provide the target PIN service. The candidate PINEs that can provide the target PIN service may be multiple.

Table 8.7.3.9-1: PIN Service Discovery Response

Information element	Status	Description
Successful response	O	Indicates that the PIN Service Discovery request was successful.
> PINE ID(s)	M	The identifier of the PIN Elements that can provide the target PIN service
> MAC address(es)/IP address(es)	M	MAC address/IP address of PINEs that can provide the target PIN service.
Failure response	O	Indicates that the PIN Service Discovery request failed.
> Cause	M	Provides the cause for PIN Service Discovery request failure.

8.7.3.10 PIN service switch subscribe request

Table 8.7.3.10-1: PIN service switch subscribe request

Information element	Status	Description
Application server ID	M	Unique identifier of the application server.
Security credentials	M	Security credentials resulting from a successful authorization for the PIN service.
PIN ID	M	The identifier of PIN.
Subscribed event	M	Identifies event type for which the subscriber is notified. Event types: - Service Switch
Notification Target Address	M	The Notification target address (e.g., URL) where the notifications destined for the application server should be sent.
Proposed expiration time	O	Proposed expiration time for the subscription

8.7.3.11 PIN service switch subscribe response

Table 8.7.3.11-1: PIN service switch subscribe response

Information element	Status	Description
Successful response (see NOTE)	O	Indicates that the subscription request was successful.
> Subscription ID	M	Subscription identifier corresponding to the subscription.
> Expiration time	O	Indicates the expiration time of the subscription. To maintain an active subscription, a subscription update is required before the expiration time.
Failure response (see NOTE)	O	Indicates that the subscription request failed.
> Cause	O	Indicates the cause of subscription request failure
NOTE: One IE is included in the response.		

8.7.3.12 PIN service switch notify

Table 8.7.3.12-1 describes information elements in the PIN service switch notification from the PIN server to application server.

Table 8.7.3.12-1: PIN service switch notification

Information element	Status	Description
PIN subscription identifier	M	Identifier of the subscription
Subscribed event	M	Identifies the event type as described in table 8.7.3.10-1 for which the notification is sent.
PIN server identifier	M	Identifier of the PIN server sending the notification.
PIN identifier	M	Identifier of the PIN.
Application client identifier	M	Identifier of the application client.
Application session identifier	M	Identifier of the application session.
Application session descriptor	O	Descriptor of application traffic flows (e.g., IP 4 tuple)
Target PIN client identifier	M	Target PIN client identifier.

8.7.3.13 PIN service switch update request

Table 8.7.3.13-1: PIN service switch update request

Information element	Status	Description
Subscription ID	M	Subscription identifier corresponding to the subscription.
Security credentials	M	Security credentials resulting from a successful authorization for the PIN service.
PIN ID	O	PIN identifier
Subscribed event	O	Identifies the event type as described in table 8.7.3.10-1 for which the subscriber is notified.
Notification Target Address	O	The Notification target address (e.g., URL) where the notifications destined for the application server should be sent to.
Proposed expiration time	O	Proposed expiration time for the subscription

8.7.3.14 PIN service switch update response

Table 8.7.3.14-1: PIN service switch update response

Information element	Status	Description
Successful response (see NOTE)	O	Indicates that the subscription update request was successful.
> Expiration time	O	Indicates the expiration time of the subscription. To maintain an active subscription, a subscription update is required before the expiration time.
Failure response (see NOTE)	O	Indicates that the subscription update request failed.
> Cause	M	Indicates the cause of subscription update request failure
NOTE: One IE is included in the response.		

8.7.3.15 PIN service switch unsubscribe request

Table 8.7.3.15-1: PIN service switch unsubscribe request

Information element	Status	Description
Subscription ID	M	Subscription identifier corresponding to the subscription.
Security credentials	M	Security credentials resulting from a successful authorization for the PIN service.

8.7.3.16 PIN service switch unsubscribe response

Table 8.7.3.16-1: PIN service switch unsubscribe response

Information element	Status	Description
Successful response (see NOTE)	O	Indicates that the unsubscribe request was successful.
Failure response (see NOTE)	O	Indicates that the unsubscribe request failed.
> Cause	M	Indicates the cause of unsubscribe request failure
NOTE: One IE is included in the response.		

8.7.4 APIs

8.7.4.1 General

Table 8.7.4.1-1 illustrates the API for AS service switch subscription.

Table 8.7.4.1-1: Ppinserver_ASServiceSwitchSubscription API

API Name	API Operations	Operation Semantics	Consumer(s)
Ppinserver_ASServiceSwitch	Subscribe	Subscribe/Notify	AS
	Notify		
	Update		
	Unsubscribe		

8.7.4.2 Ppinserver_ ASServiceSwitch_Subscribe operation

API operation name: Ppinserver_ASServiceSwitch_Subscribe

Description: The consumer subscribes for service switch information.

Inputs: See clause 8.7.3.10.

Outputs: See clause 8.7.3.11.

See clause 8.7.2.1.4.2.1 for details of usage of this operation.

8.7.4.3 Ppinserver_ ASServiceSwitch_Notify operation

API operation name: Ppinserver_ASServiceSwitch_Notify

Description: The consumer is notified with service switch information.

Inputs: See clause 8.7.3.12.

Outputs: None.

See clause 8.7.2.1.4.2.2 for details of usage of this operation.

8.7.4.4 Ppinserver_ ASServiceSwitch_ Update operation

API operation name: Ppinserver_ASServiceSwitch_Update

Description: The consumer updates an existing subscription for service switch information.

Inputs: See clause 8.7.3.13.

Outputs: See clause 8.7.3.14.

See clause 8.7.2.1.4.2.3 for details of usage of this operation.

8.7.4.5 Ppinserver_ ASServiceSwitch_ Unsubscribe operation

API operation name: Ppinserver_ASServiceSwitch_Unsubscribe

Description: The consumer cancels an existing subscription for service switch information.

Inputs: See clause 8.7.3.15.

Outputs: See clause 8.7.3.16.

See clause 8.7.2.1.4.2.4 for details of usage of this operation.

8.8 Application server discovery and registration in PIN

8.8.1 General

The PEMC and PIN Server have capabilities for maintaining information related to application servers that may be available to the PINE(s) within a PIN. Application server information may be pre-provisioned in the PIN Server or the PEMC; the application server may also register with the PEMC or the PIN Server if it has such capability.

8.8.2 Procedure

8.8.2.1 General

The follosing procedures are specified for AS discovery in PIN:

- AS discovery;
- AS registration;
- AS registration update;
- AS de-registration;

8.8.2.2 AS discovery

Figure 8.8.2.2-1 illustrates the AS discovery procedure between the PINE and the PEMC and between the PEMC and the PIN Server. This procedure enables the PEMC to provide AS connectivity information to the PINE when requested by the PINE.

Pre-conditions:

1. The PINE has joined the PIN and is authorized to communicate with the PEMC;

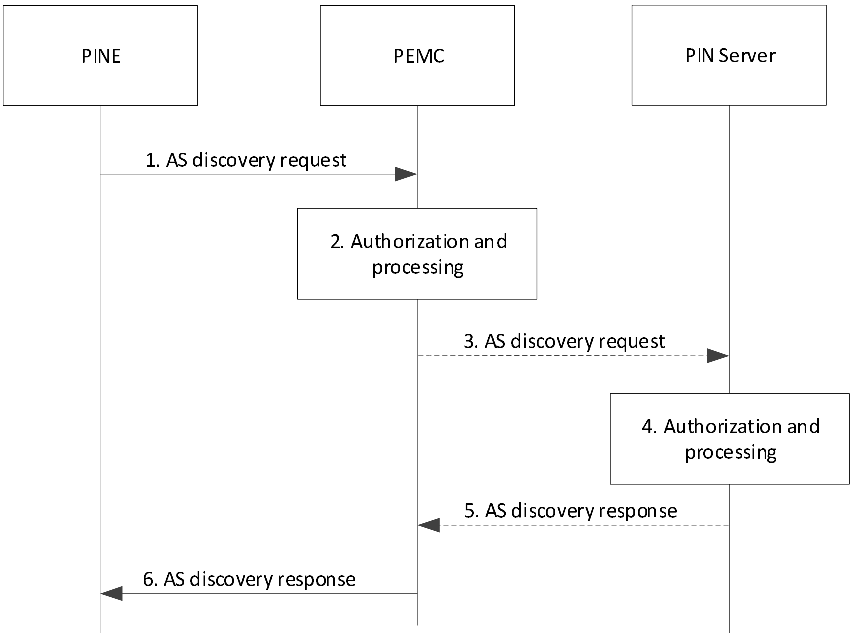

Figure 8.8.2.2-1: AS discovery procedure

1. The PINE sends an AS discovery request to the PEMC. The AS discovery request includes the requestor identifier, security credentials of the PINE and the AS service identifier of a service associated with an AS.
2. Upon receiving the request, the PEMC checks if the requestor is authorized to request AS discovery, and if the request is authorized, the PEMC verifies if it has information on an AS providing associated with the requested

AS service identifier. If the PEMC identifies information about an AS providing the requested service, the PEMC proceeds to step 6.

3. If the PEMC has not identified an AS in step 2, the PEMC sends an AS discovery request to the PIN Server. The AS discovery request includes the requestor identifier, security credentials of the PEMC and the AS service identifier associated with an AS.

4. Upon receiving the request, the PJN Server checks if the requestor is authorized to request AS discovery, and if the request is authorized, the PIN Server verifies if it has information on an AS providing associated with the requested AS service identifier.

5. If the processing of the request was successful, the PIN Server sends an AS discovery response to the requestor indicating successful processing and includes connectivity information to the AS. If the request processing failed, the PIN Server indicates failure and may provide a failure reason.

6. If the processing of the request was successful in step 2 or the PEMC has received a successful response from the PIN Server in step 5, the PEMC sends an AS discovery response to the requestor indicating successful processing and includes connectivity information to the discovered AS. If the request processing failed, the PEMC indicates failure and may provide a failure reason.

Upon receiving the AS discovery response from the PEMC, if the response indicates success, the PINE (e.g., PIN Client) may provide the AS connectivity information to the AC so the AC can access the AS. If the response indicates failure, the PINE may retry AS discovery considering the failure reason.

8.8.2.3 AS registration

Figure 8.8.2.3-1 illustrates the AS registration procedure between the AS and the PEMC or PIN Server. This procedure enables the AS to provide AS connectivity information to the PEMC or the PIN Server.

Pre-conditions:

1. The AS is authorized to communicate with the PEMC or the PIN Server;

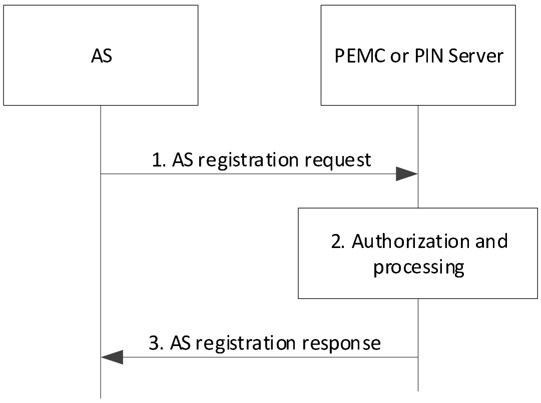
AS
PEMC or PIN Server
1. AS registration request
2. Authorization and processing
3. AS registration response

Figure 8.8.2.3-1: AS registration procedure

1. The AS sends an AS registration request to the PEMC or PIN Server. The AS registration request includes the requestor identifier, security credentials of the AS, the AS service identifier of the service associated with the AS, the connectivity information of the AS.

2. Upon receiving the request, the PEMC or PIN Server checks if the requestor is authorized to request AS registration, and if the request is authorized, the PEMC or PIN Server stores information associated with AS service.

3. If the processing of the request was successful, the PEMC or PIN Server sends an AS registration response to the requestor indicating successful processing and include the AS registration identifier; the response may include an expiration time to indicate to the AS when the registration will automatically expire. To maintain the registration, the AS shall send a registration update request prior to the expiration time. If a registration update request is not received prior to the expiration time, the PEMC or PIN Server shall treat the AS as implicitly de-

registered. If the request processing failed, the PEMC or PIN Server indicates failure and may provide a failure reason.

Upon receiving the AS registration response from the PEMC, if the response indicates success, the AS stores the registration identifier and may reuse it to update or delete its registration to the PEMC or PIN Server. If the response indicates failure, the AS may retry AS registration considering the failure reason.

8.8.2.4 AS registration update

Pre-conditions:

1. The AS has registered with the PEMC or PIN Server;
2. The AS has determined that its existing registration needs to be updated;

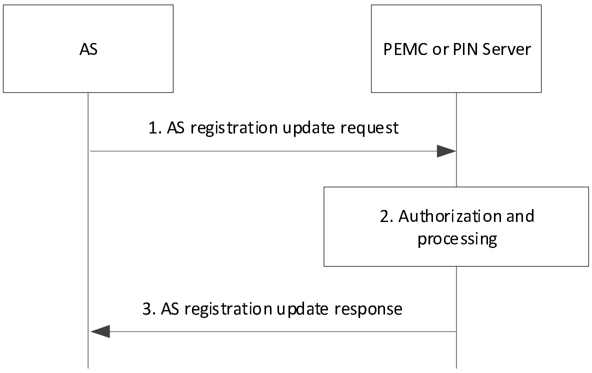
AS
PEMC or PIN Server
1. AS registration update request
2. Authorization and processing
3. AS registration update response

Figure 8.8.2.4-1: AS registration update procedure

1. The AS sends an AS registration update request to the PEMC or PIN Server where it registered. The request shall include the AS registration identifier and may include registration information such as the AS service identifier and AS connectivity information.
2. The PEMC or PIN Server performs an authorization check to verify whether the requestor is authorized to request AS registration update for the provided AS registration identifier; if the request is authorized and the AS registration identifier is valid, the PEMC or PIN Server update the registration information associated with the AS registration identifier.
3. If the request processing is successful, the PEMC or PIN Server replies to the AS with an AS registration update response and may include an updated expiration time to indicate to the AS when the updated registration will automatically expire. To maintain the registration, the AS shall send a registration update request prior to the expiration time. If a registration update request is not received prior to the expiration time, the PEMC or PIN Server shall treat the AS as implicitly de-registered. If the request processing failed, the PEMC or PIN Server indicates failure and may provide a failure reason.

8.8.2.5 AS de-registration

Pre-conditions:

1. The AS has registered with the PEMC or PIN Server;
2. The AS has determined that de-registration is required;

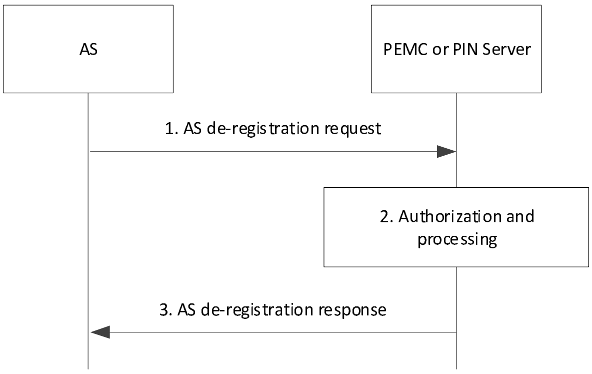
AS
PEMC or PIN Server
1. AS de-registration request
2. Authorization and processing
3. AS de-registration response

Figure 8.8.2.5-1: AS de-registration procedure

1. The AS sends an AS de-registration request to the PEMC or PIN Server where it registered. The request shall include the AS registration identifier.

2. The PEMC or PIN Server performs an authorization check to verify whether the requestor is authorized to request AS de-registration for the provided AS registration identifier; if the request is authorized and the AS registration identifier is valid, the PEMC or PIN Server removes the registration information associated with the AS registration identifier.

3. If the request processing is successful, the PEMC or PIN Server replies to the AS with an AS de-registration response. If the request processing failed, the PEMC or PIN Server indicates failure and may provide a failure reason.

8.8.3 Information flows

8.8.3.1 General

The following information flows are specified for AS discovery:

- AS discovery request and response;

- AS registration request and response;

8.8.3.2 AS discovery request

Table 8.8.3.2-1 describes information elements for the AS discovery request from the PINE to the PEMC or from the PEMC to the PIN Server.

Table 8.8.3.2-1: AS discovery request

Information element	Status	Description
Requestor identifier	M	The identifier of the requestor instance (e.g., PINE ID)
Security credentials	M	Security credentials of the PINE.
Service identifier	M	The identifier of a service provided by an AS (e.g., name)

8.8.3.3 AS discovery response

Table 8.8.3.3-1 describes information elements for the AS discovery response from the PEMC to the PINE or from the PIN Server to the PEMC.

Table 8.8.3.3-1: AS discovery response

Information element	Status	Description
Successful response	O	Indicates that the AS discovery request was successful.
> AS connectivity information	M	The connectivity information to the AS (e.g., IP address, FQDN, URI)
Failure response	O	Indicates that the AS discovery request failed.
> Cause	O	Indicates the cause of AS discovery request failure.

8.8.3.4 AS registration request

Table 8.8.3.4-1 describes information elements for the AS registration request from the AS to the PEMC or the PIN Server.

Table 8.8.3.4-1: AS registration request

Information element	Status	Description
Requestor identifier	M	The identifier of the requestor instance (e.g., AS ID)
Security credentials	M	Security credentials of the AS.
AS service identifier	M	The identifier of a service provided by an AS (e.g., name)
AS connectivity information	M	The connectivity information to the AS (e.g., IP address, FQDN, URI)

8.8.3.5 AS registration response

Table 8.8.3.5-1 describes information elements for the AS registration response from the PEMC or PIN Server to the AS.

Table 8.8.3.5-1: AS registration response

Information element	Status	Description
Successful response (see NOTE)	O	Indicates that the AS registration request was successful.
> AS registration identifier	M	The identifier of a registration
> Expiration time	O	Indicates the expiration time of the registration. To maintain an active registration status, a registration update is required before the expiration time. If the Expiration time IE is not included, it indicates that the registration never expires.
Failure response (see NOTE)	O	Indicates that the AS discovery request failed.
> Cause	O	Indicates the cause of AS discovery request failure.
NOTE: One IE is included in the response.		

8.8.3.6 AS registration update request

Table 8.8.3.6-1 describes information elements for the AS registration update request from the AS to the PEMC or the PIN Server.

Table 8.8.3.6-1: AS registration update request

Information element	Status	Description
Requestor identifier	M	The identifier of the requestor instance (e.g., AS ID)
AS registration identifier	M	The identifier of an AS registration
Security credentials	M	Security credentials of the AS.
AS service identifier	O	The identifier of a service provided by an AS (e.g., name)
AS connectivity information	O	The connectivity information to the AS (e.g., IP address, FQDN, URI)

8.8.3.7 AS registration update response

Table 8.8.3.7-1 describes information elements for the AS registration update response from the PEMC or PIN Server to the AS.

Table 8.8.3.7-1: AS registration update response

Information element	Status	Description
Successful response (see NOTE)	O	Indicates that the AS registration update request was successful.
> Expiration time	O	Indicates the expiration time of the registration. To maintain an active registration status, a registration update is required before the expiration time. If the Expiration time IE is not included, it indicates that the registration never expires.
Failure response (see NOTE)	O	Indicates that the AS discovery request failed.
> Cause	O	Indicates the cause of AS discovery request failure.
NOTE: One IE is included in the response.		

8.8.3.8 AS de-registration request

Table 8.8.3.8-1 describes information elements for the AS de-registration request from the AS to the PEMC or the PIN Server.

Table 8.8.3.8-1: AS de-registration request

Information element	Status	Description
Requestor identifier	M	The identifier of the requestor instance (e.g., AS ID)
AS registration identifier	M	The identifier of an AS registration
Security credentials	M	Security credentials of the AS.

8.8.3.9 AS de-registration response

Table 8.8.3.9-1 describes information elements for the AS de-registration response from the PEMC or PIN Server to the AS.

Table 8.8.3.9-1: AS de-registration response

Information element	Status	Description
Successful response (see NOTE)	O	Indicates that the AS de-registration request was successful.
Failure response (see NOTE)	O	Indicates that the AS discovery request failed.
> Cause	O	Indicates the cause of AS discovery request failure.
NOTE: One IE is included in the response.		

8.8.4 APIs

8.8.4.1 General

Table 8.8.4.1-1 illustrates the API for AS registration.

Table 8.8.4.1-1: Ppinserver_ASRegistration API

API Name	API Operations	Operation Semantics	Consumer(s)
Ppinserver_ASRegistration	Request	Request/Response	AS
	Update		
	Deregister		

8.4.4.2 Ppinserver_ASRegistration_Request operation

API operation name: Ppinserver_ASRegistration_Request

Description: The consumer requests to register the AS on the PIN server.

Inputs: See clause 8.8.3.4.

Outputs: See clause 8.8.3.5.

See clause 8.8.2.3 for details of usage of this operation.

8.4.4.3 Ppinserver_ASRegistration_Update operation

API operation name: Ppinserver_ASRegistration_Update

Description: The consumer requests to update the registered information of the AS on the PIN server.

Inputs: See clause 8.8.3.6.

Outputs: See clause 8.8.3.7.

See clause 8.8.2.4 for details of usage of this operation.

8.4.4.4 Ppinserver_ASRegistration_Deregister operation

API operation name: Ppinserver_ASRegistration_Deregister

Description: The consumer requests to deregister the AS from the PIN server.

Inputs: See clause 8.8.3.8.

Outputs: See clause 8.8.3.9.

See clause 8.8.2.5 for details of usage of this operation.

8.9 Service Continuity

8.9.1 General

PIN service continuity procedures enable an Application Client participating in a PIN to maintain service when PIN Elements enter or leave the PIN. The following examples illustrate scenarios where PIN service continuity is needed.

In a first scenario, a first PIN Element (e.g. a UE) receives data from a second PIN Element (e.g. a home sensor), both PIN Elements are participating in the same PIN. Service contnuity can be triggered when the UE leaves home in order to re-configure the connectivity between both PIN Elements.

In a second scenario, a PIN Element is communicating with an Application Server via a PIN Gateway Client.Service continuity can be triggered when the PIN Gateway Client becomes unreachable in order to find a replacement PIN Gateway Client and re-configure connectivity between the PIN Element, the replacement PIN Gateway and the Application Server.

Two scenarios are specified for PIN Service Continuity:

- PIN service continuity in PIN Gateway Client relocation;
- PIN service continuity in changing access to 5GS.

8.9.2 Procedure

8.9.2.1 Service continuity in PEGC relocation scenario

8.9.2.1.1 General

Following procedures are supported for service continuity in a PEGC relocation scenario:

- PIN Management PEGC Service Continuity procedure;
- PIN Management PEGC Configuration procedure;
- PIN Configuration Service Continuity Update procedure;
- PIN Management PEGC Discovery procedure;
- PIN Service Continuity subscription procedure.

8.9.2.1.2 PIN Management PEGC Service Continuity procedure

Pre-conditions:

1. PIN Element has an application session that goes through a PIN Gateway Client; and
2. PIN Gateway Client needs to be replaced (e.g., PEGC will become unavailable or PEGC is unreachable).

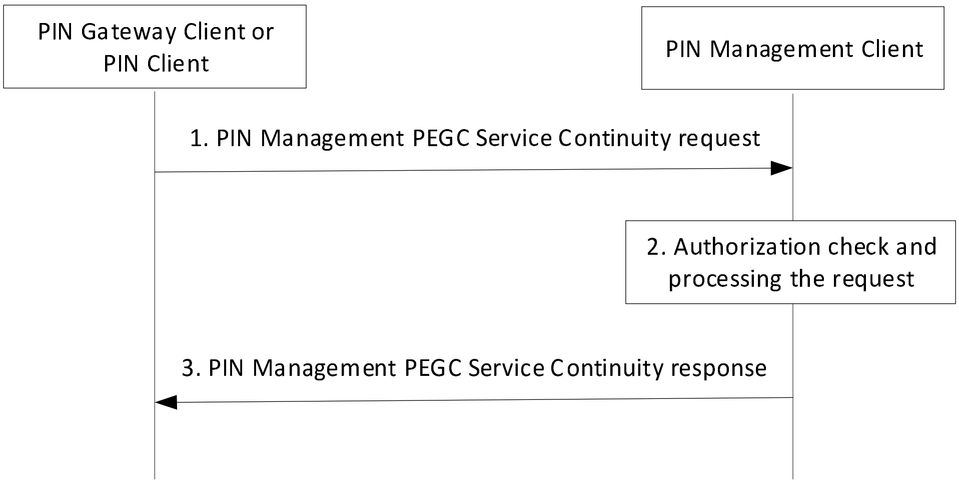
PIN Gateway Client or PIN Client
PIN Management Client
1. PIN Management PEGC Service Continuity request
2. Authorization check and processing the request
3. PIN Management PEGC Service Continuity response

Figure 8.9.2.1.2-1: PIN PEGC Service Continuity procedure

1. The PIN Gateway Client or the PIN Client sends a PIN Management PEGC Service Continuity request to the PIN Management Client for a specific service. The PIN Management PEGC Service Continuity request includes security credentials, PIN Client identifier(s), PIN Gateway identifier, and Service identifier.

2 Upon receiving the request, the PIN Management Client validates the request and checks if the request is authorized for the given PIN Client(s), PIN Gateway Client and service. If the request is authorized and valid,

the PIN Management Client determines if a target PIN Gateway Client meets the requirements for handling the application traffic for the provided service.

If the PIN Management Client identifes a target PIN Gateway Client that meets the requirements, the PIN Management Client sends PIN Management PEGC Configuration request to the target PIN Gateway Client to configure the target PIN Gateway for handling service traffic from the PIN Client(s) as in clause 8.9.2.1.3. If the service is provided by an Application Server, the PIN Management Client send a PIN Configuration Service Continuity Update request to the PIN Server if needed to inform of the service continuity changes in the PIN as in clause 8.9.2.1.4.

3. If the procesing of the request was successful, the PIN Management Client sends a PIN Management PEGC Service Continuity response to indicate that the request processing was successfull and includes target PIN Gateway Client information. Otherwise, the PIN Management Client sends a PIN PEGC Service Continuity response indicating that the request processing failed and can include appropriate reasons.

Upon receiving the PIN Management PEGC Service Continuity response, if the response was received by the PIN Client, the PIN Client validates if the request was successful and can inform the application client of the target PIN Gateway Client provided in the response to establish connectivity. If the response was received by the PIN Gateway Client, the PIN Gateway Client notifies each PIN Client included in the PIN Management PEGC Service Continuity request about the target PIN Gateway Client change as in clause 8.9.2.1.5.

8.9.2.1.3 PIN Management PEGC Configuration procedure

Pre-conditions:

1. The PIN Management Client has received a PIN Management PEGC Service Continuity request; and
2. The PIN Management client has identified a target PIN Gateway Client.

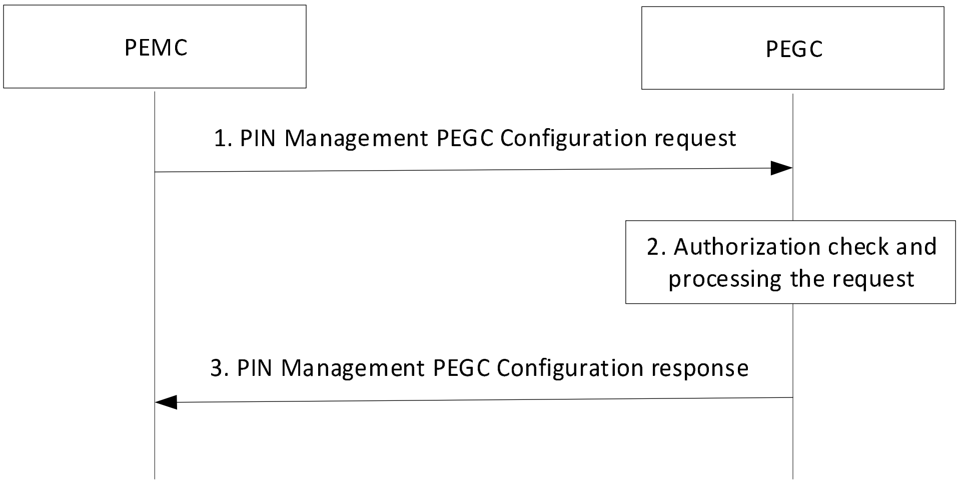
PEMC
PEGC
1. PIN Management PEGC Configuration request
2. Authorization check and processing the request
3. PIN Management PEGC Configuration response

Figure 8.9.2.1.3-1: PIN Management PEGC Configuration procedure

1. The PIN Management Client sends a PIN Management PEGC Configuration request to the target PIN Gateway Client. The PIN Management PEGC Configuration request includes security credentials, PIN Client identifier(s), PIN Gateway identifier, and Service identifier.
2. Upon receiving the request, the PIN Gateway Client validates the request and checks if the PIN Management Client is authorized to request PEGC Configuration. If the request is authorized and the request is valid, the PIN Gateway Client creates a new configuration for the PIN Client(s) and service that are indicated in the request.
3. If the processing of the request was successful, the target PIN Gateway Client sends a PIN Management PEGC Configuration response to the PIN Management Client to indicate that the request was successful and can include connectivity information to be used by the PIN Client(s). Otherwise, the target PIN Gateway sends a PIN Management PEGC Configuration response indicating that the request failed and can include appropriate reasons.

Upon receiving the PIN Management PEGC Configuration response, the PIN Management Client uses the information provided in the response to inform the PIN Client(s) or the PIN Gateway Client from which the service continuity request originated as in clause 8.9.2.1.2.

8.9.2.1.4 PIN Configuration Service Continuity Update procedure

The PIN Configuration Service Continuity Update procedure allows the PEMC to inform the PIN Server about a service continuity request received at the PEMC for a PINE, and it allows the PIN Server to inform the related AS of the same if such functionality is supported by the AS.

The PIN Server may provide, in the response, policy information to the PEMC about service continuity for the concerned PINE.

Pre-conditions:

1. PINE has an application session that goes through a PEGC; and
2. PEGC needs to be replaced (e.g., PEGC will become unavailable or PEGC is unreachable).
3. The AS is successfully subscribed for PIN service continuity notifications with the PIN Server.

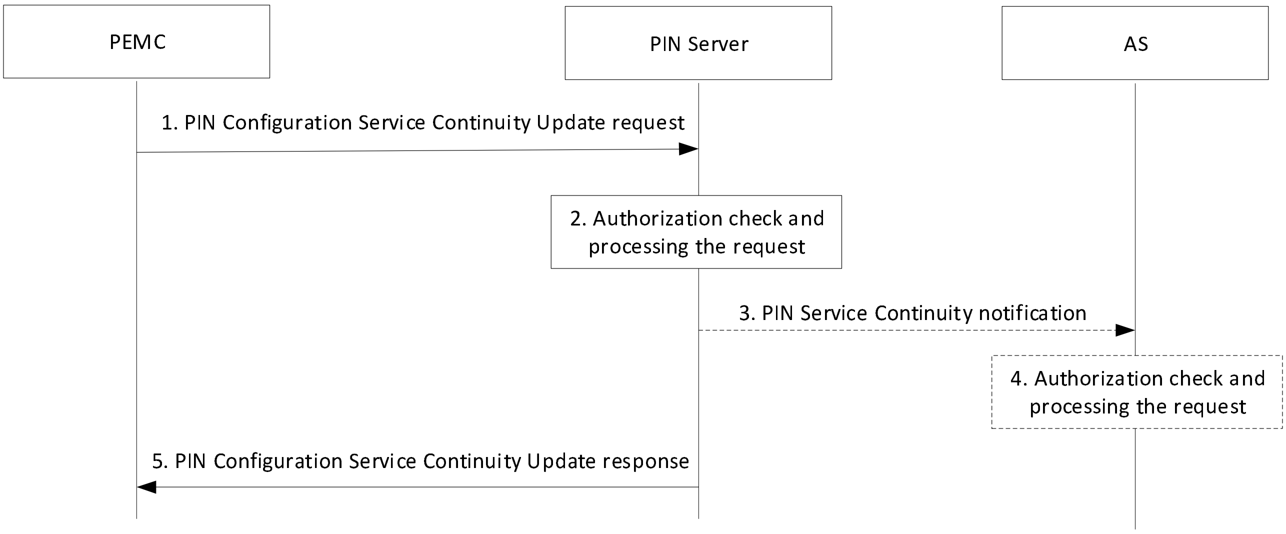
PEMC
PIN Server
AS
1. PIN Configuration Service Continuity Update request
2. Authorization check and processing the request
3. PIN Service Continuity notification
4. Authorization check and processing the request
5. PIN Configuration Service Continuity Update response

Figure 8.9.2.1.4-1: PIN Configuration Service Continuity Update procedure

1. The PEMC sends a PIN Configuration Service Continuity Update request to the PIN Server. The PIN Configuration Service Continuity Update request includes the requestor identifier, security credentials, PINE identifier(s), source and target PIN Gateway identifiers, and service identifier (e.g., application client identifier, application server identifier, application session identifier, application session identifier), and the PIN ID.
2. Upon receiving the request, the PIN Server validates the request and checks if the PEMC is authorized to request service continuity update. If the request is authorized and valid, if the PIN Server has not authorized the PINE for service continuity, the PIN Server validates if the PINE is authorized and determines policy information about service continuity for the PINE. If the PIN Server has already authorized the PINE for service continuity, the PIN Server updates the configuration for the PINE and service indicated in the request.
3. If the PIN Server needs to update the AS with service continuity information, the PIN Server sends a PIN Service Continuity notification to the AS. The PIN Service Continuity notification includes PIN identifier, PINE identifier(s), PEGC identifier, service identifier and may include an application session identifier and terminating endpoints on the PINE and PEGC.
4. Upon receiving the notification, the AS validates the notification. If the notification is valid, the AS updates the service continuity configuration related to the PINE and service indicated in the notification.
5. If the processing of the PIN Configuration Service Continuity Update request was successful, the PIN Server sends a PIN Configuration Service Continuity Update response to indicate that the request processing was successful and may include policy information about service continuity for the PINE. Otherwise, the PIN Server

sends a PIN Configuration Service Continuity Update response indicating that the request processing failed and can include appropriate reasons.

Upon receiving the PIN Configuration Service Continuity Update response, the PEMC uses the information provided in the response to inform the PINE(s) or the PEGC from which the service continuity request originated as in clause 8.9.2.1.2.

8.9.2.1.5 PIN Management PEGC Discovery procedure

PEMC performs PIN Management PEGC discovery procedure to discover which PEGC are available at the PINE when the PEMC does not have that information; for example, the PEMC may ignore if a PEGC is available at the PINE or PEGC information may not have been provided to the PEMC in the service provisioning request.

Pre-conditions:

1. The PEMC has been triggered for service continuity;
2. The target PEGC is not known by the PEMC.

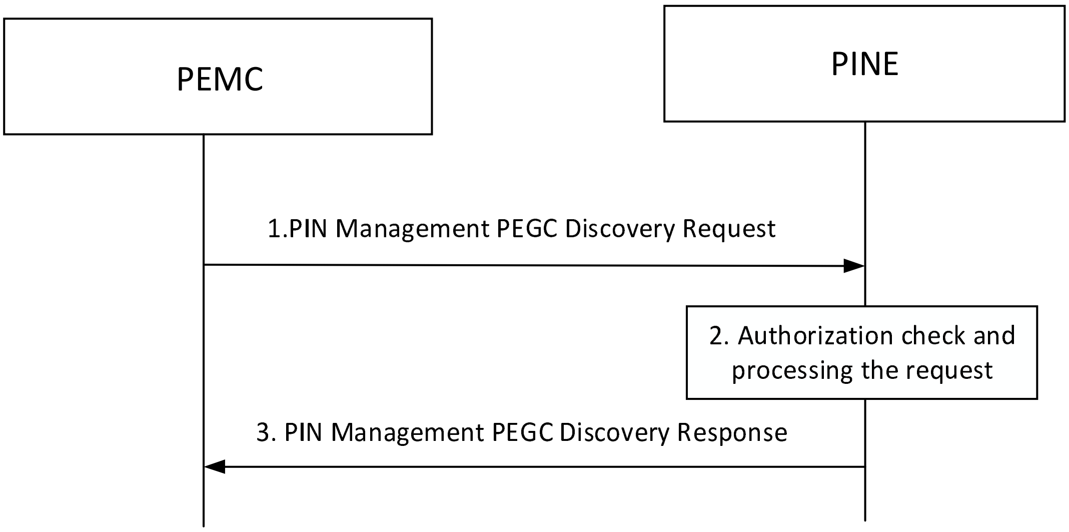
PEMC
PINE
1.PIN Management PEGC Discovery Request
2. Authorization check and processing the request
3. PIN Management PEGC Discovery Response

Figure 8.9.2.1.5-1: PIN Management PEGC Discovery procedure

1. The PEMC sends a PIN Management PEGC Discovery request to the PINE involved in the service continuity procedure. The PIN Management PEGC Discovery request includes security credentials, requestor identifier, PIN identifier, PINE identifier and list of PEGC information.
2. Upon receiving the request, the PINE validates the request and checks if the request is authorized. If the request is authorized and valid, the PINE uses the PEGC information provided in the request to identify PEGC(s) that are reachable and creates a list of PEGC identifier(s) that are available at the PINE.
3. If the procesing of the request was successful, the PINE sends a PIN Management PEGC Discovery response to indicate that the request processing is successfull and includes the list of PEGC identifier(s) available at the PINE. Otherwise, the PINE sends a PIN Management PEGC Discovery response indicating that the request processing failed and can include appropriate reasons.

Upon receiving the response, the PEMC selects the target PEGC based on the list of available PEGC received and the PIN policy.

8.9.2.1.6 PIN Service Continuity subscription

8.9.2.1.6.1 General

The PIN service continuity subscription is used by the Application Server to be notified of PIN service continuity events by the PIN Server.

The PIN service continuity notification includes PIN service continuity information.

8.9.2.1.6.2 Procedure

8.9.2.1.6.2.1 PIN service continuity subscribe

Figure 8.9.2.1.6.2.1-1 illustrates the PIN service continuity subscribe procedure.

Pre-conditions:

1. The application server has already received the address of the PIN server;
2. The application server is authorized to communicate with PIN server;

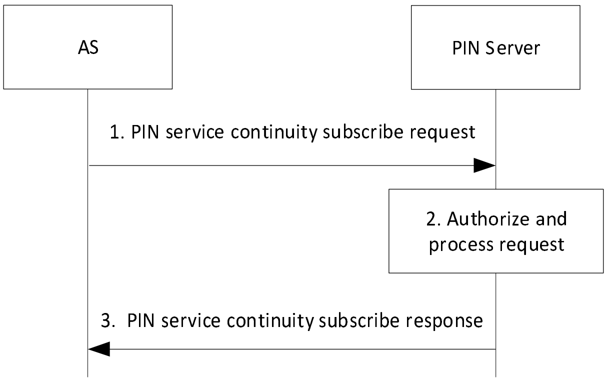
AS
PIN Server
1. PIN service continuity subscribe request
2. Authorize and process request
3. PIN service continuity subscribe response

Figure 8.9.2.1.6.2.1-1: PIN service continuity subscribe

1. The application server sends the PIN service continuity subscribe request to the PIN server. The PIN service continuity subscribe request includes the application server identifier along with the security credentials, PIN ID, subscribed event, notification target address and proposed expiration time.
2. Upon receiving the request from the application server, the PIN server checks if the application server is authorized to subscribe. The authorization check may apply to an individual PIN. If the request is authorized, the PIN server creates and stores the subscription for application server.
3. If the processing of the request is successful, the PIN server sends a PIN service continuity subscribe response to the application server, which includes the subscription identifier and may include the expiration time, indicating when the subscription will automatically expire. To maintain the subscription, the application server shall send a PIN service continuity update request prior to the expiration time. If a new PIN service continuity update request is not received prior to the expiration time, the PIN server shall treat the application server as implicitly unsubscribed.

8.9.2.1.6.2.2 PIN service continuity notify

Figure 8.9.2.1.6.2.2-1 illustrates the PIN service continuity notify procedure.

Pre-conditions:

1. The application server has subscribed with the PIN server as specified in clause 8.9.2.1.6.2.1.

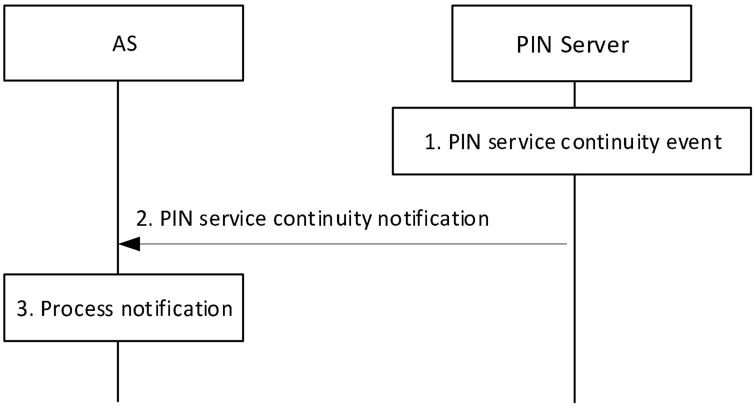
AS
PIN Server
1. PIN service continuity event
2. PIN service continuity notification
3. Process notification

Figure 8.9.2.1.6.2.2-1: PIN service continuity notify procedure

1. When a service continuity event occurs at the PIN server that satisfies triggering conditions, the PIN server sends a service continuity notification to the subscribed application servers.
2. The PIN server sends an PIN service continuity notification to the subscribed application server(s) related to the service continuity event and includes the PIN service continuity information.

   The PIN service continuity information includes the PIN subscription identifier, subscribed event, PIN server identifier, PIN identifier, PINE identifier(s), PEGC identifier, service identifier, application session identifier and may include terminating endpoints on the PINE and PEGC.
3. Upon receiving the notification, the application server uses the information provided in the notification to update the service continuity configuration related to the PINE and service indicated in the notification.

8.9.2.1.6.2.3 PIN service continuity update

Figure 8.9.2.1.6.2.3-1 illustrates the PIN service continuity update procedure.

Pre-conditions:

1. The application server has subscribed with the PIN server as specified in clause 8.9.2.1.6.2.1.

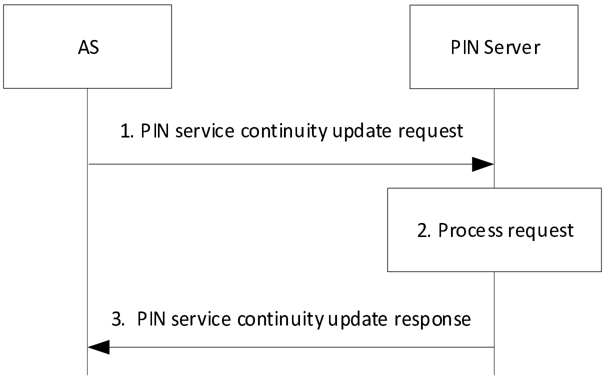
AS
PIN Server
1. PIN service continuity update request
2. Process request
3. PIN service continuity update response

Figure 8.9.2.1.6.2.3-1: PIN service continuity update

1. The application server sends a PIN service continuity update request to the PIN server. The PIN service continuity update request includes the security credentials and the subscription identifier. It may also include notification target address, PIN ID, event ID and proposed expiration time.
2. Upon receiving the request from the application server, the PIN server checks if the application server is authorized to update the subscription information. If the request is authorized, the PIN server updates the stored subscription.
3. If the processing of the request is successful, the PIN server sends a PIN service continuity update response to the application server, which may include the expiration time, indicating when the subscription will automatically expire. To maintain the subscription, the application server shall send a PIN service continuity

update request prior to the expiration time. If a PIN service continuity update request is not received prior to the expiration time, the PIN server shall treat the application server as implicitly unsubscribed.

8.9.2.1.6.2.4 PIN service continuity unsubscribe

Figure 8.9.2.1.6.2.4-1 illustrates the PIN service continuity unsubscribe procedure.

Pre-conditions:

1. The application server has subscribed with the PIN server as specified in clause 8.9.2.1.6.2.1.

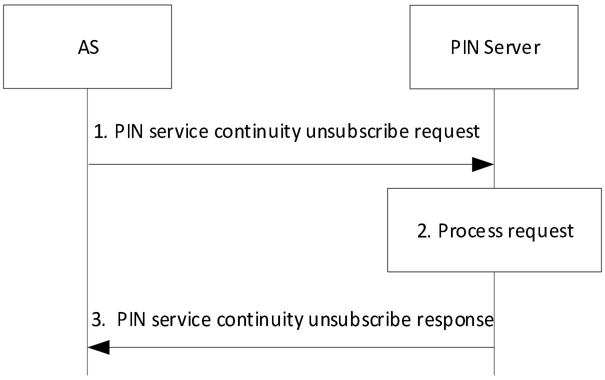
AS
PIN Server
1. PIN service continuity unsubscribe request
2. Process request
3. PIN service continuity unsubscribe response

Figure 8.9.2.1.6.2.4-1: PIN service continuity unsubscribe

1. The application server sends a PIN service continuity unsubscribe request to the PIN server. The PIN service continuity unsubscribe request includes the security credentials and the subscription identifier.
2. Upon receiving the request from the application server, the PIN server checks if the application server is authorized to unsubscribe. If the request is authorized, the PIN server cancels the subscription indicated by the subscription identifier.
3. If the processing of the request is successful, the PIN server sends a PIN service continuity unsubscribe response to the application server.

8.9.2.2 Service continuity in changing access to 5GS

This procedure solves the situation, that PINE 1 has application layer communication with PINE 2 via PEGC 1. But when the communication via PEGC 1 is not viable, for example, the PINE 2 moves out of the coverage of PEGC 1, only PINE 2 triggers to establish the 5GS communication to connect to PINE 1 via PEGC 2is the potential way.

Figure 8.9.2.2-1 illustrates the service continuity to change application layer communication via PEGC only to application layer communication via PEGC + 5GS or 5GS + 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 PINE 1 has the subscription that can communicate with PINE 2 via 5GS;
4. The PINE 2 does not have the 3GPP capability and require support of a PEGC to access the 3GPP network.

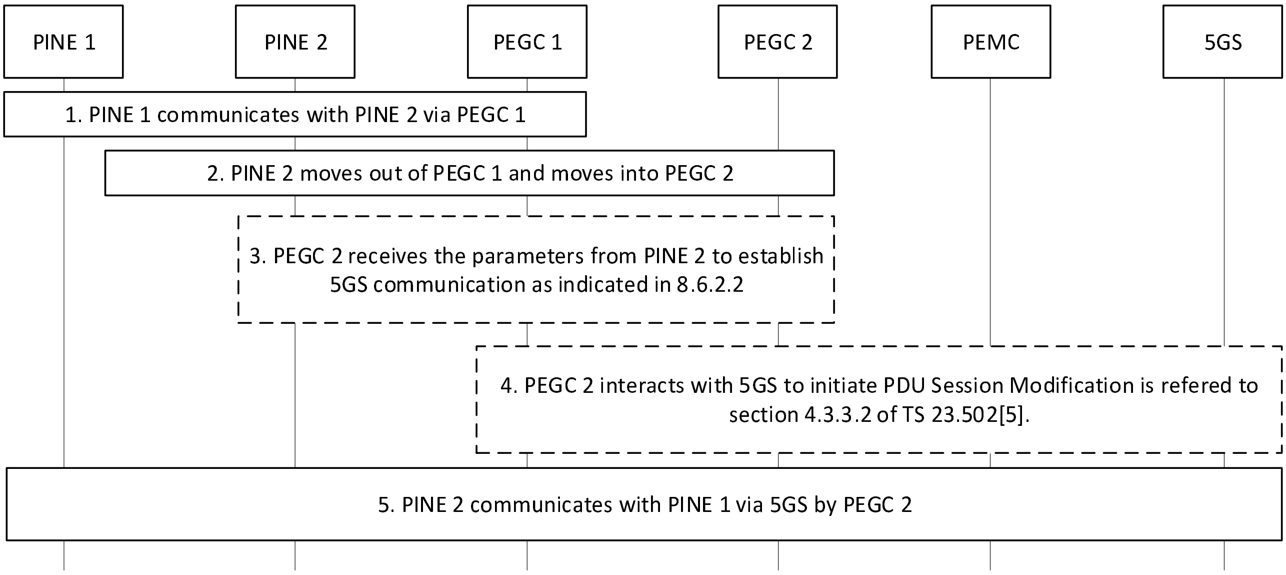
PINE 1
PINE 2
PEGC 1
PEGC 2
PEMC
5GS
1. PINE 1 communicates with PINE 2 via PEGC 1
2. PINE 2 moves out of PEGC 1 and moves into PEGC 2
3. PEGC 2 receives the parameters from PINE 2 to establish 5GS communication as indicated in 8.6.2.2
4. PEGC 2 interacts with 5GS to initiate PDU Session Modification is refered to section 4.3.3.2 of TS 23.502[5].
5. PINE 2 communicates with PINE 1 via 5GS by PEGC 2

Figure 8.9.2.2-1: Change application layer communication to communication via 5GS

1. The PINE 1 has application layer communication with PINE 2 via PEGC 1.
2. The PINE 2 moves out of PEGC 1 and moves into the coverage of PEGC 2. The PINE 2 connects to the network that provided by PEGC 2 via access control information.
3. The PEGC 2 receives the related parameter (PIN ID, MAC address/IP address, Traffic descriptors, Packet filters, requested QoS) as indicated in section 8.6.2.2 from PINE 2 or PEMC.
4. According to the Packet filters, the PEGC 2 may initiate PDU Session Modification as indicated in section 4.3.3.2 of TS 23.502[5] with the Packet filters and requested QoS towards 5G system in order to make 5GC configure the N4 rules for UPF(s), referred to section 8.6.2.2.
5. The PINE 2 communicates with PINE 1 via 5GS by PEGC 2. To enable this communication via PEGC + 5GS or 5GS + PEGC, each PINE includes the PINE ID of the destination PINE in its communication.

8.9.3 Information flows

8.9.3.1 General

The following information flows are specified for Service Continuity:

- PIN Management PEGC Service Continuity request and response
- PIN Management PEGC Configuration request and response
- PIN Configuration Service Continuity Update request and response
- PIN Management PEGC Discovery request and response
- PIN service continuity subscribe
- PIN service continuity notify
- PIN service continuity update
- PIN service continuity unsubscribe

8.9.3.2 PIN Management PEGC Service Continuity request

Table 8.9.3.2-1 describes information elements for the PIN Management PEGC Service Continuity request that is sent from the PIN Gateway client to the PIN Management client.

Table 8.9.3.2-1: PIN Management PEGC Service Continuity request

Information element	Status	Description
Requestor identifier	M	Requestor identifier
Security credentials	M	Security credentials of the requestor
PIN identifier	M	Identifier of the PIN
PINE identifier	M	Identifier of the PINE
Source PEGC identifier	M	Identifier of the source PEGC
Application client identifier	M	Identifier of the application client.
Application server identifier	M	Identifier of the application server.
Application session identifier	M	Identifier of the application session.
Application session descriptor	O	Descriptor of application traffic flows (e.g., IP 4 tuple)

8.9.3.3 PIN Management PEGC Service Continuity response

Table 8.9.3.3-1 describes information elements for the PIN Management PEGC Service Continuity response.

Table 8.9.3.3-1: PIN Management PEGC Service Continuity response

Information element	Status	Description
Successful response (see NOTE)	O	Indicates that the request was successful.
> Target PEGC identifier	O	Identifier of the target PEGC
Failure response (see NOTE)	O	Indicates that the request failed.
> Cause	O	Indicates the cause of the request failure.
NOTE: Only one of the IE must be included in the response.		

8.9.3.4 PIN Management PEGC Configuration request

Table 8.9.3.4-1 describes information elements for the PIN Management PEGC Configuration request that is sent from the PEMC to the PEGC.

Table 8.9.3.4-1: PIN Management PEGC Configuration request

Information element	Status	Description
Requestor identifier	M	Requestor identifier.
Security credentials	M	Security credentials of the requestor.
PIN identifier	M	Identifier of the PIN
PINE identifier	M	Identifier of the PINE
Application client identifier	M	Identifier of the application client.
Application server identifier	M	Identifier of the application server.
Application session identifier	M	Identifier of the application session.
Application session descriptor	O	Descriptor of application traffic flows (e.g., IP 4 tuple)

8.9.3.5 PIN Management PEGC Configuration response

Table 8.9.3.5-1 describes information elements for the PIN Management PEGC Configuration response.

Table 8.9.3.5-1: PIN Management PEGC Configuration response

Information element	Status	Description
Successful response (see NOTE)	O	Indicates that the request was successful.
> PEGC connectivity information	O	Information about the configured PEGC connectivity to be used by the PINE.
Failure response (see NOTE)	O	Indicates that the request failed.
> Cause	O	Indicates the cause of the request failure.
NOTE: Only one of the IE must be included in the response.		

8.9.3.6 PIN Configuration Service Continuity Update request

Table 8.9.3.6-1 describes information elements for the PIN Configuration Service Continuity Update request that is sent from the PEMC to the PIN Server.

Table 8.9.3.6-1: PIN Configuration Service Continuity Update request

Information element	Status	Description
Requestor identifier	M	Requestor identifier.
Security credentials	M	Security credentials of the requestor.
PIN identifier	M	Identifier of the PIN
PINE identifier	M	Identifier of the PINE
Source PEGC identifier	M	Identifier of the source PEGC
Target PEGC identifier	M	Identifier of the target PEGC
Application client identifier	M	Identifier of the application client.
Application server identifier	M	Identifier of the application server.
Application session identifier	M	Identifier of the application session.
Application session descriptor	O	Descriptor of application traffic flows (e.g., IP 4 tuple)

8.9.3.7 PIN Configuration Service Continuity Update response

Table 8.9.3.7-1 describes information elements for the PIN Configuration Service Continuity Update response.

Table 8.9.3.7-1: PIN Configuration Service Continuity Update response

Information element	Status	Description
Successful response (see NOTE)	O	Indicates that the request was successful.
> Service continuity policy information	O	Information about service continuity policy of the PINE.
Failure response (see NOTE)	O	Indicates that the request failed.
> Cause	O	Indicates the cause of the request failure.
NOTE: Only one of the IE must be included in the response.		

8.9.3.8 PIN Management PEGC discovery request

Table 8.9.3.8-1 describes information elements for the PIN Management PEGC discovery request that is sent from the PEMC to the PINE.

Table 8.9.3.8-1: PIN Management PEGC discovery request

Information element	Status	Description
Requestor identifier	M	Requestor identifier
Security credentials	M	Security credentials of the requestor
PIN identifier	M	Identifier of the PIN
PINE identifier	M	Identifier of the PINE
List of PEGC information	M	The information of PEGC(s) available in the PIN per the PEGC List of clause 8.2.2.2.

8.9.3.9 PIN Management PEGC discovery response

Table 8.9.3.9-1 describes information elements for the PIN Management PEGC discovery response.

Table 8.9.3.3-1: PIN Management PEGC discovery response

Information element	Status	Description
Successful response (see NOTE)	O	Indicates that the request was successful.
> List of PEGC identifiers	O	List of PEGC identifiers available at the PINE
Failure response (see NOTE)	O	Indicates that the request failed.
> Cause	O	Indicates the cause of the request failure.
NOTE: Only one of the IE must be included in the response.		

8.9.3.10 PIN service continuity subscribe request

Table 8.9.3.10-1: PIN service continuity subscribe request

Information element	Status	Description
Application server ID	M	Unique identifier of the application server.
Security credentials	M	Security credentials resulting from a successful authorization for the PIN service.
PIN ID	M	The identifier of PIN.
Subscribed event	M	Identifies event type for which the subscriber is notified. Event types: - Service Continuity
Notification Target Address	M	The Notification target address (e.g., URL) where the notifications destined for the application server should be sent.
Proposed expiration time	O	Proposed expiration time for the subscription

8.9.3.11 PIN service continuity subscribe response

Table 8.9.3.11-1: PIN service continuity subscribe response

Information element	Status	Description
Successful response (see NOTE)	O	Indicates that the subscription request was successful.
> Subscription ID	M	Subscription identifier corresponding to the subscription.
> Expiration time	O	Indicates the expiration time of the subscription. To maintain an active subscription, a subscription update is required before the expiration time.
Failure response (see NOTE)	O	Indicates that the subscription request failed.
> Cause	O	Indicates the cause of subscription request failure
NOTE: One IE is included in the response.		

8.9.3.12 PIN service continuity notify

Table 8.9.3.12-1 describes information elements in the PIN service continuity notification from the PIN server to application server.

Table 8.7.3.12-1: PIN service continuity notification

Information element	Status	Description
PIN subscription identifier	M	Identifier of the subscription
Subscribed event	M	Identifies the event type as described in table 8.9.3.10-1 for which the notification is sent.
PIN server identifier	M	Identifier of the PIN server sending the notification.
PIN identifier	M	Identifier of the PIN.
PINE identifier(s)	M	Identifier(s) of PINE(s)
PEGC identifier	M	Identifier of the PEGC
Service identifier	M	Identifier of a service
Application session identifier	M	Identifier of the application session.
Application session descriptor	O	Descriptor of application traffic flows (e.g., IP 4 tuple) on the PINE and PEGC

8.9.3.13 PIN service continuity update request

Table 8.9.3.13-1: PIN service continuity update request

Information element	Status	Description
Subscription ID	M	Subscription identifier corresponding to the subscription.
Security credentials	M	Security credentials resulting from a successful authorization for the PIN service.
PIN ID	O	PIN identifier
Subscribed event	O	Identifies the event type as described in table 8.9.3.10-1 for which the subscriber is notified.
Notification Target Address	O	The Notification target address (e.g., URL) where the notifications destined for the application server should be sent.
Proposed expiration time	O	Proposed expiration time for the subscription

8.9.3.14 PIN service continuity update response

Table 8.9.3.14-1: PIN service continuity update response

Information element	Status	Description
Successful response (see NOTE)	O	Indicates that the subscription update request was successful.
> Expiration time	O	Indicates the expiration time of the subscription. To maintain an active subscription, a subscription update is required before the expiration time.
Failure response (see NOTE)	O	Indicates that the subscription update request failed.
> Cause	M	Indicates the cause of subscription update request failure
NOTE: One IE is included in the response.		

8.9.3.15 PIN service continuity unsubscribe request

Table 8.9.3.15-1: PIN service continuity unsubscribe request

Information element	Status	Description
Subscription ID	M	Subscription identifier corresponding to the subscription.
Security credentials	M	Security credentials resulting from a successful authorization for the PIN service.

8.9.3.16 PIN service continuity unsubscribe response

Table 8.7.3.16-1: PIN service continuity unsubscribe response

Information element	Status	Description
Successful response (see NOTE)	O	Indicates that the unsubscribe request was successful.
Failure response (see NOTE)	O	Indicates that the unsubscribe request failed.
> Cause	M	Indicates the cause of unsubscribe request failure
NOTE: One IE is included in the response.		

8.9.4 APIs

8.9.4.1 General

Table 8.9.4.1-1 illustrates the API for AS service continuity subscription.

Table 8.9.4.1-1: Ppinserver_ASServiceContinuitySubscription API

API Name	API Operations	Operation Semantics	Consumer(s)
Ppinserver_ASServiceContinuity	Subscribe	Subscribe/Notify	AS
	Notify		
	Update		
	Unsubscribe		

8.9.4.2 Ppinserver_ ASServiceContinuity_Subscribe operation

API operation name: Ppinserver_ASServiceContinuity_Subscribe

Description: The consumer subscribes for service continuity information.

Inputs: See clause 8.9.3.10.

Outputs: See clause 8.9.3.11.

See clause 8.9.2.1.6.2.1 for details of usage of this operation.

8.9.4.3 Ppinserver_ ASServiceContinuity_Notify operation

API operation name: Ppinserver_ASServiceContinuity_Notify

Description: The consumer is notified with service continuity information.

Inputs: See clause 8.9.3.12.

Outputs: None.

See clause 8.9.2.1.6.2.2 for details of usage of this operation.

8.9.4.4 Ppinserver_ ASServiceContinuity_ Update operation

API operation name: Ppinserver_ASServiceContinuity_Update

Description: The consumer updates an existing subscription for service continuity information.

Inputs: See clause 8.9.3.13.

Outputs: See clause 8.9.3.14.

See clause 8.9.2.1.6.2.3 for details of usage of this operation.

8.9.4.5 Ppinserver_ ASServiceContinuity_ Unsubscribe operation

API operation name: Ppinserver_ASServiceContinuity_Unsubscribe

Description: The consumer cancels an existing subscription for service continuity information.

Inputs: See clause 8.9.3.15.

Outputs: See clause 8.9.3.16.

See clause 8.9.2.1.6.2.4 for details of usage of this operation.

8.10 PIN Authorization

8.10.1 General

The PIN authorization procedure is used by a PINE, PEGC or PEMC to acquire security information needed to perform procedures with other functional entities (e.g., PIN Server, PEMC, PEGC) of the PIN. The security information is used by a PINE, PEGC or PEMC (e.g., a requestor) when performing procedures of clause 8 that require security credentials for request authorization. A PINE, PEGC or PEMC performs the PIN authorization procedure with the PIN server.

NOTE: How security credentials are provisioned on the PIN server is implementation dependent.

For deployments where a PIN server has CAPIF core function capabilities, and a PINE, PEGC, PEMC or AS have CAPIF API invoker capabilities, as defined in 3GPP TS 23.222 [7], security information may be obtained via CAPIF mechanisms as specified in 3GPP TS 33.122 [8].

8.10.2 Procedure

8.10.2.1 General

PIN authorization procedure is either performed directly with the PIN server or indirectly via the PEGC for PINE(s) that require support of the PEGC to access the PIN server; the PEGC can deliver the PIN authorization request of the PINE to the PIN server when needed.

8.10.2.2 PIN authorization with PIN server

Figure 8.10.2.2-1 illustrates PIN authorization procedure based on request/response model.

Pre-conditions:

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

2. The PINE/PEGC/PEMC has been pre-configured with the PIN identifier;

3. The PIN server has been configured with the PIN profile;

4. The requestor has been authenticated.

NOTE: In the current release, requestor authentication relies on pre-provisioned information and is implementation dependent.

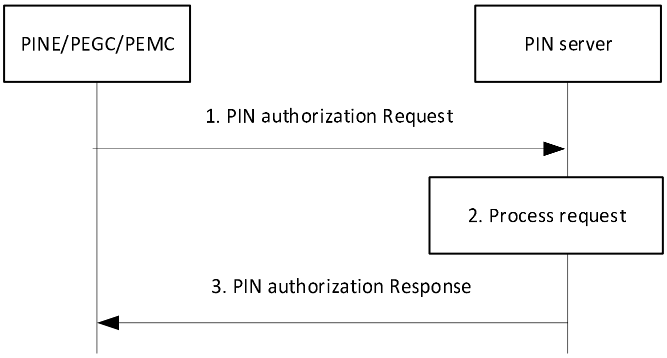

Figure 8.10.2.2-1: PIN authorization with PIN server

1. The PINE sends a PIN authorization request to the PIN server. The request includes the PIN identifier, and the requestor identifiers, name, description, and address.

2. Upon receiving the request, the PIN server validates if the requestor is allowed to access the requested PIN using the information provided in the request and the PIN configuration information from the PIN profile.

3. The PIN server sends a PIN authorization response to the requestor. If the PIN server successfully determines that the requestor is allowed to access the PIN, the PIN server includes security information for the requestor to use within the PIN. If the PIN server fails to authorize the requestor, the PIN server indicates failure in the response and includes a failure reason.

8.10.3 Information flows

8.10.3.1 General

The following information flows are specified for PIN authorization:

- PIN authorization request and response;

8.10.3.2 PIN authorization request

Table 8.10.3.2-1 describes information elements in the PIN authorization request sent from the PINE or AS to the PIN server.

Table 8.10.3.2-1: PIN authorization request

Information element	Status	Description
Requestor identifiers	M	The identifiers of the requestor (i.e., GPSI of the PINE, and PINE identifier or AS identifier). See NOTE.
PIN identifier	M	Identifier of the PIN.
Requestor IP Address	O	The IP address of PINE or AS.
NOTE: If the PINE registration is accepted by PIN server, the PIN Server may use the PIN client ID provided in the PINE registration for authorization.		

NOTE: The AS is pre-configured with the security credentials.

8.10.3.3 PIN authorization response

Table 8.10.3.3-1 describes information elements in the PIN authorization response sent to the PINE.

Table 8.10.3.3-1: PIN authorization response

Information element	Status	Description
Successful response	O (see NOTE)	Indicates that the PIN authorization request was successful.
> Security information	M	The security information to be used by the requestor in PIN procedures.
Failure response	O (see NOTE)	Indicates that the PIN authorization request failed.
> Cause	M	Provides the cause for PIN authorization request failure.
NOTE: At least one of the IE shall be present.		

Annex A (Informative): Authorization

A.1 General Principles

This clause defines the general principles used for defining the PIN authorization procedure:

- the solution can be based on HTTPS and focus on protection of reference points;
- security information can be pre-provisioned on the PINE/PEMC/PEGC/PIN Server/AS for authentication and authorization; pre-provisioning of security information is up to implementation;
- security information format can be defined for interoperability between PINE/PEMC/PEGC/PIN Server/AS;
- the PIN server can be authorized to generate and distribute the security information.

Annex B (informative):
Change history

Change history

Date	Meeting	TDoc	CR	Rev	Cat	Subject/Comment	New version
2023-01	SA6#52bis-e					TS skeleton (version 0.0.0) approved in S6-230388.	0.0.0
2023-01	SA6#52bis-e					Implementation of the following pCRs approved by SA6: S6-230081, S6-230082, S6-230083, S6-230118, S6-230121, S6-230124, S6-230126, S6-230184, S6-230185, S6-230300, S6-230369, S6-230370, S6-230381, S6-230384, S6-230386, S6-230387, S6-230388, S6-230487, S6-230488, S6-230489, S6-230490, S6-230491, S6-230492,	0.1.0
2023-02	SA6#53					Implementation of the following pCRs approved by SA6: S6-230554, S6-230577, S6-230648, S6-230896, S6-230900, S6-230901, S6-230902, S6-230904, S6-230905, S6-230906, S6-230940, S6-230941, S6-230942, S6-230948, S6-230949, S6-230950, S6-230952, S6-231017, S6-231057, S6-231083	0.2.0
2023-04	SA6#54e					Implementation of the following pCRs approved by SA6: S6-231154, S6-231156, S6-231157, S6-231179, S6-231182, S6-231188, S6-231206, S6-231207, S6-231233, S6-231235, S6-231237, S6-231433, S6-231438, S6-231439, S6-231440, S6-231441, S6-231442, S6-231443, S6-231444, S6-231567, S6-231568, S6-231569, S6-231594	0.3.0
2023-05	SA6#55					Implementation of the following pCRs approved by SA6: S6-231745, S6-231746, S6-231748, S6-231749, S6-231861, S6-231909, S6-231912, S6-231913, S6-231914, S6-231927, S6-232054, S6-232055, S6-232056, S6-232057, S6-232058, S6-232059, S6-232060, S6-232061, S6-232062	0.4.0
2023-06	SA#100	SP-230688				Submitted to SA#100 for information and approval	1.0.0
2023-06	SA#100	SP-230688				MCC Editorial update for publication after TSG SA approval (SA#100)	18.0.0
2023-09	SA#101	SP-231008	0001	1	F	Add missing information elements to information flow of PINE join into PIN request/response	18.1.0
2023-09	SA#101	SP-231008	0002	2	F	Alignment of information flow in PIN service registration	18.1.0
2023-09	SA#101	SP-231008	0003	2	F	Clarification of whether delete or deactivate PIN when expiration time comes	18.1.0
2023-09	SA#101	SP-231008	0004	1	F	Correction of heartbeat	18.1.0
2023-09	SA#101	SP-231008	0007	2	F	Correction of PIN modification due to PEGC unavailability	18.1.0
2023-09	SA#101	SP-231008	0008	1	F	Correction of PIN service registration	18.1.0
2023-09	SA#101	SP-231008	0009	2	F	Correction of PIN status service	18.1.0
2023-09	SA#101	SP-231008	0010	1	F	Correction of PINE remove request	18.1.0
2023-09	SA#101	SP-231008	0011	1	F	Correction of PINE update for port number	18.1.0
2023-09	SA#101	SP-231008	0012	1	F	Correction of PINE update registration to PIN server	18.1.0
2023-09	SA#101	SP-231008	0013	1	F	PEGC authorization failure and select proper route for PINE join/leave request	18.1.0
2023-09	SA#101	SP-231008	0014	1	F	PEMC represents the PINE to register	18.1.0
2023-09	SA#101	SP-231008	0015	1	F	Use PIN status notify to deliver dynamic PIN profile	18.1.0
2023-09	SA#101	SP-231008	0016		F	Editorial corrections	18.1.0
2023-09	SA#101	SP-231008	0017		F	General corrections to clause 8.7.3	18.1.0
2023-09	SA#101	SP-231008	0018	1	F	PIN Service Switch subscription	18.1.0
2023-09	SA#101	SP-231008	0020	1	F	PIN Service Continuity subscription	18.1.0
2023-12	SA#102	SP-231563	0019	3	F	Resolve issues related to PIN modification after local PEMC failure	18.2.0
2023-12	SA#102	SP-231563	0021	2	F	Clarification of PIN profile and dynamic PIN profile	18.2.0
2023-12	SA#102	SP-231563	0022	1	F	Clarification of PIN profile generation during PIN create	18.2.0
2023-12	SA#102	SP-231563	0023	1	F	Correction of information flow of PIN status notify	18.2.0
2023-12	SA#102	SP-231563	0024	1	F	Correction of PIN communication	18.2.0
2023-12	SA#102	SP-231563	0026	1	F	Correction of PINE registration indirectly to PIN server	18.2.0
2023-12	SA#102	SP-231563	0028	1	F	Correction of service continuity	18.2.0
2023-12	SA#102	SP-231563	0029	2	F	Correction of Service Switch	18.2.0
2023-12	SA#102	SP-231563	0030	1	F	Get the PINE service	18.2.0
2023-12	SA#102	SP-231563	0031	3	F	PIN-Notify-Correction	18.2.0
2023-12	SA#102	SP-231563	0032	2	F	PIN-Removal-Behaviour	18.2.0
2023-12	SA#102	SP-231563	0036	1	F	Clarification of PEMC represents multiple PINEs or PEGCs to register	18.2.0
2023-12	SA#102	SP-231563	0037	1	F	Clarification on PIN management operations by secondary PEMC	18.2.0
2023-12	SA#102	SP-231563	0038		F	Corrections to scope and introduction	18.2.0
2023-12	SA#102	SP-231563	0039	1	F	Corrections to general architecture	18.2.0
2023-12	SA#102	SP-231563	0040		F	Corrections to terminology	18.2.0
2023-12	SA#102	SP-231563	0040		F	Corrections to PIN-9	18.2.0
2023-12	SA#102	SP-231563	0042	1	F	Corrections to PIN-8	18.2.0
2023-12	SA#102	SP-231563	0043		F	Corrections to cardinality from UE perspective	18.2.0
2023-12	SA#102	SP-231563	0044	1	F	Corrections to Identities	18.2.0

2023-12	SA#102	SP-231563	0045		F	Corrections on use of “Application Layer” term	18.2.0
2023-12	SA#102	SP-231563	0046	1	F	PINE Communication via 5GS+PEGC	18.2.0
2023-12	SA#102	SP-231563	0047	2	F	PINAPP security clarifications	18.2.0
2024-03	SA#103	SP-240308	0048	1	F	Resolving EN on PEGC/PEMC authorization	18.3.0
2024-03	SA#103	SP-240308	0049	1	F	Resolving EN on CAPIF usage	18.3.0
2024-03	SA#103	SP-240308	0050	1	F	Resolving EN on enhanced PIN security aspects	18.3.0
2024-03	SA#103	SP-240308	0051	1	F	Resolving EN on Annex A.1	18.3.0
2024-03	SA#103	SP-240308	0052	1	F	Correction of authorization	18.3.0
2024-03	SA#103	SP-240308	0053	1	F	Correction of Additional PEMCs	18.3.0
2024-06	SA#104	SP-240761	0054	1	F	Correction of credentials provision in PINAPP	18.4.0
2024-06	SA#104	SP-240761	0056	2	F	Notifying the PIN elements about backup PEGC	18.4.0
2024-06	SA#104	SP-240761	0057		F	Correction of PINE management	18.4.0
2024-06	SA#104	SP-240761	0058	2	F	Correction of Service Continuity	18.4.0
2024-06	SA#104	SP-240761	0059		F	EN resolutions	18.4.0

History

Document history		
V18.3.0	April 2024	Publication
V18.4.0	July 2024	Publication