Converged Personal Network Service Core Technical Specification

Candidate Version 1.0 – 03 May 2011

Open Mobile Alliance

OMA-TS-CPNS_Core-V1_0-20110305-C

Contents

Figures

Tables

1. Scope

This document specifies the functions, interfaces and behaviour of CPNS entities, then protocols and CPNS System concept together with syntax and semantics of CPNS messages.

2. References

2.1 Normative References

[CPNS-AD] "Converged Personal Network Service Architecture", Open Mobile Alliance™, OMA-AD-CPNS-V1_0, URL:http://www.openmobilealliance.org/

[CPNS-RD] "Converged Personal Network Service Requirements", Open Mobile Alliance™, OMA-RD-CPNS-V1_0, URL:http://www.openmobilealliance.org/

[RFC2119] "Key words for use in RFCs to Indicate Requirement Levels", S. Bradner, March 1997, URL:http://www.ietf.org/rfc/rfc2119.txt

[RFC4234] "Augmented BNF for Syntax Specifications: ABNF". D. Crocker, Ed., P. Overell. October 2005, URL:http://www.ietf.org/rfc/rfc4234.txt

[SCRRULES] "SCR Rules and Procedures", Open Mobile Alliance™, OMA-ORG-SCR_Rules_and_Procedures, URL:http://www.openmobilealliance.org/

2.2 Informative References

[OMADICT] "Dictionary for OMA Specifications", Version 2.8, Open Mobile Alliance™, OMA-ORG-Dictionary-Vx_y, URL:http://www.openmobilealliance.org/

[PUCC-ARCH] "PUCC Architecture", pucc_architecture_20070930_rev2, URL:http://www.mo.puc.jp/spec/

[PUCC-BASIC] "PUCC Basic Protocol", pucc_basic_protocol_20080328, URL:http://www.mo.puc.jp/spec/

[PUCC-DDSI] "PUCC Device Discovery and Service Invocation Protocol", pucc_device_discovery_and_service_invocation_protocol_20080328, URL:http://www.mo.puc.jp/spec/

[PUCC-META] "PUCC Metadata Template Specification", pucc_metadata_template_20080328, URL:http://www.mo.puc.jp/spec/

3. Terminology and Conventions

3.1 Conventions

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in [RFC2119].

All sections and appendixes, except “Scope” and “Introduction”, are normative, unless they are explicitly indicated to be informative.

3.2 Definitions

CPNS Device	See [CPNS-RD]
CPNS Entity	There are three identified logical entities: PNE, PN GW and CPNS Server. In the CPNS v1.0, the CPNS Server entity resides in the core network and the PNE and/or PN GW entity resides in the CPNS device.
External Entity	See [CPNS-RD]
Group Key Encryption Key (GKEK)	Key used by PN GW to encrypt Group Key when using broadcast based Group Key delivery from PN GW to PNE.
Group Key Decryption Key (GKDK)	Key used by PNE to decrypt Group Key when using broadcast based Group Key delivery from PN GW to PNE.
Operator Policy	Policy provided by Network Operator or CPNS Service Provider.
Remote PNE	A PNE which does not belong to the same PN as the requesting PNE does and communicates with that requesting PNE through the CPNS Server
SG Owner	A PNE which requests creation of the Service Group or is granted ownership of the Service Group by CPNS Server or former SG Owner. It is authorized to expel member PNE from a Service Group, delete a Service Group and pass the ownership to another PNE. Terms ‘SG’ and ‘Service Group’ are used interchangeably in this specification. They represent exactly the same concept.
Mode	See [CPNS-RD]
PN Inventory	See [CPNS-RD]
Secure PAN	PAN which has security mechanism to protect authenticity, confidentiality and integrity of CPNS message. That is, if PNE/PN GW uses security mechanism of Secure PAN, it is guaranteed that source ID of CPNS message is not falsified (i.e. authenticity protection), payload of CPNS message can not be read by CPNS Entity other than receiver CPNS Entity designated by destination ID of the message (i.e., confidentiality protection), and CPNS message is not changed during transmission (i.e., integrity protection).
Secure Storage	A storage that stores the key material (e.g., Entity User Key (EUKey), Group Key, protected Password,…) to protect against unauthorized access
SG Inventory	A list of Service Group(s) and the information of Service Group which includes information of group members.
Temporary Key (TK)	Key used by CPNS Entity to encrypt and decrypt EUKey when EUKey is delivered from PN GW to PNE in case that PNE does not have enough UI capabilities and the PAN between PN GW and PNE is not secure.

3.3 Abbreviations

OMA	Open Mobile Alliance
PSK	Pre-Shared Key
SG	Service Group

SHA-1	Secure Hash Algorithm 1
UI	User Interface

4. Introduction

This document defines signalling procedure of CPNS entities and syntax and semantics of CPNS messages based on CPNS requirement document [CPNS-RD] and CPNS architecture document [CPNS-AD].

Section 5 describes the CPNS system concept

Section 6 describes the high level procedure

Section 7 describes the signalling procedures of CPNS entities with CPNS messages.

Section 8 describes syntax and semantics of CPNS messages.

Section 9 describes CPNS Transport Protocol binding specification.

4.1 Version 1.0

This specification release covers all the requirements from [CPNS-RD] assigned for this Release 1.0.

5. CPNS System Description

5.1 Identification

The following identifiers are used in the CPNS Enabler:

- The UserID allows to uniquely identify a CPNS User
- The PNID allows to uniquely identify a PN
- The EntityID allows to uniquely identify an CPNS Entity
- ServiceID, which identifies uniquely the CPNS services
- The SGID allows to uniquely identify a Service Group

5.1.1 UserID

A CPNS User is identified by his/her CPNS UserID.

A CPNS UserID can be used for authentication, authorization and charging, etc.

A CPNS UserID is in the form of:

- A MSISDN which is uniquely and globally identifying a mobile service subscription; or,
- An Email Address, in the case that a CPNS User does not own his/her MSISDN; or,
- An operator SHALL assign a UserID, if any of above two UserIDs is not appropriate.

An example of a MSISDN is “82212345678” and also an example of an Email Address is jeonghoon@mail.co.kr.

5.1.2 PNID

A PN in the CPNS Enabler is identified by its PNID.

A PNID is composed of 2 parts:

- The first part is the EntityID of the PN GW pertaining to the PN
- The second part is number. This part allows to identify which PN it is if the PN GW manages several PNs.

For example:

- A PN GW has the ID: 00-17-C4-E1-A0-Q2.PNGW.

  The ID of the first PN is:

  00-17-C4-E1-A0-Q2.PNGW.1

- If the PN GW has a second PN:

  00-17-C4-E1-A0-Q2.PNGW.2

5.1.3 EntityID

The EntityID of CPNS Server is identified by their existing ID such as domain name, etc.

For the PN GW and PNE, the EntityID is composed of two parts: the first part is a device ID for identifying a physical device and the second part is a type of Entity.

- A device ID may have the following formats:
  - a physical address given by the manufacturer, such as Mac addresses for Ethernet, Bluetooth, Wi-Fi, ZigBee, etc ; and/or
  - a device name combined with a UserID : a device name is allocated by a user and the allocated device name is unique among devices owned by the user. Since a UserID is globally unique, the combination of a device name and a UserID is an identifier of a device.

  NOTE: The device ID expressed with physical address is persistent, whereas a device name combined with a UserID is not always persistent. If there are two or more physical addresses in the device, the CPNS enabler SHALL choose one. How to choose and when to choose is up to the implementation matter.
- A type of Entity can be either of
  - PN GW
  - PNE

For example, if a CPNS Device has two capable Modes, PN GW and PNE, then the CPNS Device has two EntityIDs: one for PN GW and the other for PNE such as “00-17-C4-E1-A0-Q2.PNGW” and “00-17-C4-E1-A0-Q2.PNE”.

5.1.4 ServiceID

ServiceID is an identifier used to identify a specific service over the CPNS Enabler.

ServiceID is a unique identifier for active services..

It is important that the format of the ServiceID is associated with an EntityID and/or domain name of the service provider and a number to differentiate from other services in the same category. This makes it easier to distinguish the service and also associate it with the provider e.g. BBC sport channel (bbc.co.uk/sport/snooker_1).

A ServiceID is made of 2 parts:

- Source ID: In the case of an External Entity , it could be URL or other forms, while in the case of a PNE, it should be the PNEID
- Service name

For example:

- URL (PNEID)_service name

ServiceID can be created by PNE or the CPNS Server when providing a service and is included in the service description. ServiceID is also used when populating a Service Group Inventory, to manage the service or a service group, and also is used for service discovery functionality.

5.1.5 SGID

A SG in the CPNS Enabler is identified by its SGID.

A SGID is used in SG management.

A SGID is composed of 3 parts:

- The first part is a prefix “SG”.
- The second part is the EntityID of PNE or PN GW which requests SG creation.
- The third part is number. This part allows to identify which SG it is if the PNE or PN GW creates several SGs.

For example:

- A PNE has the ID: 00-17-C4-E1-B0-Q2.PNE.

  The ID of the first SG is:

  SG.00-17-C4-E1-B0-Q2.PNE.1

- If the PNE creates a second SG:

  SG.00-17-C4-E1-B0-Q2.PNE.2

5.2 CPNS Entity Mode

In the CPNS Enabler v1.0, CPNS Device can support three identified Modes, PN GW, PNE and BOTH. The Mode can be detected by CPNS Entity Discovery function, among CPNS Devices. Because a PN consists at a minimum of a device acting in PN GW Mode and another or same device acting in PNE Mode, devices should know the mode of the other devices to create or join PN. The PN GW SHALL be able to recognize the PNE(s) in order to make it as a member of PN. PNE SHALL be able to recognize the PN GW to request to join or create PN.

If a device supports the only PNE functionalities (e.g. MP3 player, Smart meter), the device operates only on PNE mode. If a device supports only PN GW functionalities (e.g. Home Network Router), the device operates only on PN GW mode.

If a device supports both of PN GW and PNE functionalities (e.g. mobile phone), the Mode of device should be set initially and can be changed according to user’s preference or Operator Policy. For example, when the CPNS user initiates to create or joins a Personal Network the user can set the Mode manually or the Operator Policy can be applied automatically for the Mode. (e.g. depending on the Operator Policy considering the device capabilities, network capabilities)

5.3 Security Consideration

5.3.1 EUKey Management

CPNS Server assigns EUKey to PNE and PN GW after authenticating CPNS User based on UserID and password. Assigned EUKey is stored securely in CPNS Server together with EntityID, UserID and password.

Before assigning EUKey to PNE or PN GW, UserID and password of the CPNS User who owns PNE or PN GW SHALL be registered with CPNS Server.

EUKey assignment to PNE SHALL be performed after the PNE discovers PN GW by Entity Discovery and before PNE attempts to connect to PN (i.e., before establishing PN, joining PN or being invited to PN)

EUKey assignment to PN GW SHALL be performed before mutual authentication between PN GW and CPNS Server.

If there is EUKey in the PNE or PN GW already assigned, EUKey assignment SHALL NOT happen.

Section 7.4 describes the different approaches of EUKey assignment depending on UI capability and PAN security

5.3.2 Group Key Management

Group Key is a security key which all member entities in the same Service Group share and is used to ensure security (e.g., confidentiality and integrity etc.) of messages destined to Service Group. For Group Key management, CPNS supports the following operations:

- create Group Key

When Service Group is created, CPNS Server creates Group Key.

- delete Group Key

When Service Group is deleted, CPNS Server and SG member PNEs delete Group Key.

- update Group Key

Update of Group Key is performed in two ways;

  - When SG member PNE leaves or is expelled from Service Group, CPNS Server updates Group Key.
  - CPNS Server itself can update Group Key. (e.g. for periodic updates).

- deliver Group Key

When Group Key is created or updated, CPNS Server delivers a Group Key to PN GW(s). Then, each PN GW delivers a Group Key to Service Group member PNE(s) pertaining to the same PN of the PN GW.

Delivery of Group Key from PN GW to PNE can be performed in three different ways: unicast based Group Key delivery, broadcast based Group Key delivery or hybrid of the two (Section 7.8.5). PN GW and PNE SHALL support unicast based Group Key delivery. If a device in which PN GW/PNE is deployed supports underlying network broadcast mechanism, PN GW/PNE SHOULD support broadcast based Group Key delivery

5.3.3 Authentication, Confidentiality and Integrity

5.3.3.1 CPNS messages to CPNS Entity

Authenticity, confidentiality and integrity of CPNS messages to CPNS Entity are ensured by the secure session established between CPNS Server and PNE, CPNS Server and PN GW and PN GW and PNE.

Regarding message protection between PN GW and CPNS Server, if fixed or removable module keeping identity information and credential (e.g., a SIM/USIM/ISIM) is installed on PN GW, PN GW and CPNS Server can utilize that credential (e.g., a SIM/USIM/ISIM) for security

Regarding message protection between PN GW and PNE, if PN GW and PNE connect to Secure PAN, PN GW and PNE can utilize security mechanism of Secure PAN to protect security of CPNS message.

Otherwise, secure session needs to be established between PN GW and PNE.

Secure session used to protect CPNS message is chosen based on its SourceID and DestID.

- For CPNS message whose SourceID and DestID are CPNS Server/PNE and PNE/CPNS Server respectively
  - Secure session is achieved between CPNS Server and PNE
- For CPNS message whose SourceID and DestID are CPNS Server/PN GW and PN GW/CPNS Server respectively
  - Secure session is achieved between CPNS Server and PN GW
- For CPNS message whose SourceID and DestID are PN GW/PNE and PNE/PN GW respectively
  - Secure session is achieved between PN GW and PNE

5.3.3.1.1 Secure Session in CPNS Enabler

- Secure session establishment

Secure session between CPNS Entities is established by PSK-based approach.

As for session establishment between CPNS Server and PNE/PN GW, EUKey is used as PSK.

As for session establishment between PNE and PN GW, another key is used as PSK, since EUKey is not necessarily shared between PNE and PN GW. The key (hereinafter, LocalEUKey) is created in CPNS Server and sent to PNE and PN GW after encrypted by EUKey of each entity. Before assigning LocalEUKey, EUKey is assigned to PNE and PN GW.

By using EUKey or LocalEUKey as PSK, secure session is established by the two operations: mutual authentication and session key sharing

- Mutual authentication

Two CPNS Entities authenticate each other by using PSK based authentication outlined in section 7.5.

- Session key sharing

Session key sharing is also performed by using PSK. Two CPNS Entities create session key by calculating hash value from random number and PSK (i.e., EUKey or LocalEUKey). Since both sides use the same random number and the same PSK, the same session keys are created at both sides. Same random numbers exchanged during mutual authentication are used here.

- Message protection by secure session

  - Authenticity and integrity

  Message sender calculates hash value of message by session key, and adds the hash value to the message as MAC (message authentication code). Message recipient can verify message authenticity and integrity by verifying MAC using session key.

  - Confidentiality

  Message is encrypted by session key. For some messages, encryption can be skipped. CPNS Entities MAY have predefined policy on which message they can skip encryption. How to set the policy is out of scope of CPNS Enabler 1.0.

  Note: Whether or not to skip encryption can be chosen on a message by message basis. That is, if a certain message is chosen to be encrypted, all the elements and attributes except for common parameter (8.1.1) of that message should be encrypted.

5.3.3.2 CPNS messages to Service Group

When sending out a message to Service Group, CPNS Entities SHALL use Group Key to guarantee security of message delivery to member PNEs. However, to those member PNEs which satisfy both of the following two conditions, CPNS Entities can send the message without protection by using Group Key.

1. PNE connects to its PN GW via Secure PAN which ensures message authenticity, integrity and confidentiality
2. its PN GW has fixed or removable module keeping identity information and credential (e.g., a SIM/USIM/ISIM) and uses the module for secure communication with CPNS Server

When using Group Key, security of CPNS messages is protected as follows:

- Authenticity and integrity

  Message sender calculates hash value of message by Group Key, and adds the hash value to the message as MAC (message authentication code). By verifying MAC using Group key, message recipient can verify message authenticity (i.e., can verify if the message is sent from SG member PNE or CPNS Server). Also, message recipient can verify message integrity.

- Confidentiality

CPNS message destined to Service Group is encrypted by Group Key.

5.3.4 Authorization

Since CPNS Server stores EUKey with EntityID of PNE or PN GW and UserID of CPNS User who owns PNE or PN GW, CPNS Server can know correct EntityID and UserID after authenticating PNE or PN GW. Thus, CPNS Server can perform authorization using EntityID and UserID.

5.4 PN Management and SG Management

5.4.1 PN Management

PN Management covers PN Establishment, PN Update as a result of PNE joining/invitation/leaving/expulsion and PN Release.

PN SHALL be established with only one PN GW and one or more PNE(s) in PAN and the PN create request can be done by both PNE and PNGW. After creating PN, PN Inventory (see section 5.8) is created in PNE, PNGW and CPNS Server. CPNS User can allow sharing of PNE information among member PNEs. The PN Inventory SHALL be kept in PNE, PN GW and CPNS Server even though member PNEs are disconnected with PN GW temporary because CPNS Enabler supports stable information related with PN, which is sustained PN (e.g. PN Inventory, continuous Content/Service Delivery per Service in PN, and Usage statistic history per PNID). However, CPNS User can configure the temporary PN so that it is released immediately and removed from PN Inventory after physical disconnection of PAN, which means PNE is disconnected from PN GW (e.g. PN for Zone based service).

In zone based service scenario, PN consists of one PNE and one PN GW which can belong to different users.

Member PNE Update can be requested by PNE and PN GW. PNE can invite or request to expel the other PNE and PNE can join or leave itself. PN GW also can invite or expel the other PNE. If the User wants to share the information of member PNE's each other, the member PNE get the notification about member update.

PN Release can be requested by PNE, PN GW or CPNS Server.

5.4.2 SG Management

SG Management covers SG Establishment, SG Update as a result of PNE joining/invitation/leaving/expulsion and SG Release.

SG SHALL be established with one or more PNE(s). The SGCreateRequest can be initiated either by PNE or by PNGW. After SG creation, the output is SG Inventory in PNE, PNGW and CPNS Server (see section 5.8). If the CPNS User wants to share the information of member PNEs each other, the CPNS User can set member sharing.

The SG Inventory SHALL be kept in PNE, PN GW and CPNS Server even in the case when member PNEs are disconnected from PN GW. SG member Update can be requested by PNE and PN GW. Any PNE SHALL be able to send requests to join, and member PNE shall be able to leave and invite other PNEs to join an SG, but only the SG owner can initiate expulsion of other PNEs. SG Owner can invite or expel the other PNE. If the User wants to share the information of member PNE's each other, the member PNE get the notification about member update.

SG Release can be requested by SG Owner or CPNS Server.

5.5 Service / Content Delivery

5.5.1 General

The Service/Content delivery procedure provides function to deliver Services and Content between:

- Different PNEs

- PNEs and External Entity;

The Service/Content Delivery can be performed after CPNS Entity Discovery, PN Management and PN Registration.

The PNE invoke service or content of another PNE or External Entity via CPNS Server.

Each operation is application specific and out of scope of CPNS Enabler. As example, the operations of service are;

- "Play" : the service requester of e.g., media streaming service initiates the consumption of the requested service
- "Stop": the service requester of e.g., media streaming service stops the consumption of the requested service.
- "Pause": the service requester of e.g., media streaming service stops for a while the consumption of the service.
- "Resume": the service requester of e.g., media streaming service reactivates the consumption of the service

5.5.1.1 PNE and external entities

PNE SHALL be able to invoke the Service / Content Delivery.

PNE can send and receive Content to and from External Entity.

PNE can send and receive Content to and from PNE.

5.5.1.2 CPNS Server

CPNS Server sends and/or forwards messages and Content for Service/Content Delivery to and from PN GW and external entities.

The CPNS Server controls the Service / Content Delivery:

- Initialization
- Management of the services
- Management of the Content

5.5.1.3 PN GW

PN GW forwards:

- messages needed for Service / Content Delivery,
- contents to and from PNE,
- contents to and from CPNS Server.

5.6 Device Capability

Based on Devices capabilities, CPNS Server SHALL be able to determine resources allocation and utilization

5.7 Non CPNS Device Proxy

The PN GW supports Non CPNS Device Proxy function, which translates CPNS message to the corresponding method of external Personal Networks, not implementing CPNS standards, e.g., UPNP, DLNA and Bluetooth and vice versa. The Non CPNS Device Proxy forwards the translated message between CPNS Entity and Non CPNS Device. The Non CPNS Device Proxy acts on behalf of non CPNS Device as PNE. The Non CPNS Device Proxy can manage the information of external Personal Networks.

The Non CPNS Device Proxy supports;

- Non CPNS Device registration
- Service Advertisement and Discovery
- Service / Content Delivery

NOTE: Detailed implementation guidance will be done in the future release.

5.8 PN Inventory

PN Inventory contains the information about PN(s).

PN Inventory SHALL be created or updated when a PN is established or when a PN is changed. PN Inventory SHALL be deleted when a PN is released.

CPNS Server SHALL store PN Inventory registered to CPNS Server. PN GW SHALL store PN Inventory upon the receipt of of successful PN registration notification from CPNS Server.

PNE SHALL store PN Inventory upon the receipt of successful PN setup notification from PN GW.

PN Inventory SHALL be used when a CPNS Entity manages the PN, or when device capability needs to be acknowledged, or in case that PNE asks about PN information of other CPNS Users or PN information in a remote PN of CPNS user via service discovery.

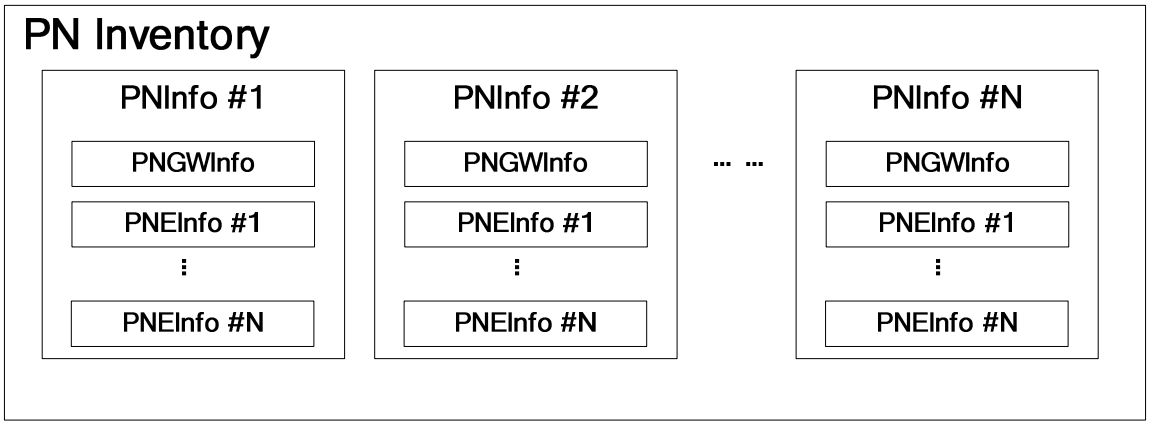


Figure 1 PN Inventory Diagram

T: Type, S: CPNS Server, G: PN GW, P: PNE.

Element	Cardinality	T	Data Type	Description	S	G	P
PNInfo	1..n	E		PN Information. Its sub attributes are • PNID • Description	M	M	M

				• TempPN • Active • Sharing • Disclosure • OwnershipEntityID Its sub elements are • PNGWInfo • PNEInfo			
PNID	1	A	String	PN Identification.	M	M	M
Description	0..1	A	String	PN Description.	O	O	O
TempPN	0..1	A	Boolean	If this PN is temporary PN, this is "TRUE". If the physical connection between PNGW and all of PNEs is broken, this PN should be released automatically. If this PN is sustained PN, this TempPN attribute is empty or "FALSE".	O	O	O
Active	1	A	Boolean	The active status of PN. TRUE – This PN is active because at least one more member PNEs are physically connected. FALSE – This PN is not active because all of member PNEs are disconnected.	M	M	M
Sharing	1	A	Integer	The level of PN Inventory sharing in PNE side 1 – Shared, both PNGWInfo and PNEInfo in PNInfo are shared in PNE 2 – Protected, only PNGWInfo in PNInfo is shared in PNE.	M	M	M
Disclosure	1	A	Integer	The willingness of openness of PN Information, in case Service Discovery is requested after PN Setup 1 - Blocked; PN information should not be unveiled. 2 - Open; PN information will be unveiled, when other CPNS Entities asks service discovery. 3 - Selective: PN can be unveiled, only when the authorized CPNS entity allows in case Sservice dDiscovery request contains PNID, PNEID or UserID	M	M	M
OwnershipEntityID	0..1	A	String	The ID of authorized CPNS Entity which has authorization to allow PN Information open, in case Service Discovery is requested.	O		
PNGWInfo	1	E		PN GW Information	M	M	M

				Its sub attributes are • PNGWID • PNGWName • Mode • Zonebasedservicesupport • Broadcastgroupkeydeliverysupport			
PNGWID	1	A	String	PN GW Identification.	M	M	M
PNGWName	0..1	A	String	PN GW Name (e.g. assigned nickname)		O	O
Mode	1	A	Integer	The mode of current device 2 – PNGW, If the mode of device is PN GW, the value should be "PN GW". 3 – BOTH, If the mode of device is both of PNE and PN GW, the value should be "BOTH" (e.g. mobile phone)		M	M
Zonebasedservicesupport	0..1	A	Boolean	If this CPNS entity is a capable PN GW of Zone Based Service, this value should be "TRUE".	O	O	O
Broadcastgroupkeydeliverysupport	0..1	A	Boolean	TRUE: PN GW supports broadcast Group Key delivery FALSE: PN GW does not support broadcast Group Key delivery.	O	M	M
PNEInfo	1..n	E		PNE Information Its sub attributes are • PNEID • PNEName • Active • Mode Its sub elements are • UserInfo • DeviceCapa • ServiceProfile	M	M	C
PNEID	1	A	String	PNE Identification.	M	M	C
Name	0..1	A	String	PNE Name (e.g. mp3 player)	O	O	O
Active	1	A	Boolean	The active status of PNE. TRUE – This PNE is active because PNE is physically connected. FALSE – This PNE is not active because PNE is physically disconnected.	M	M	C
Mode	1	A	Integer	The mode of current device		M	C

				1 – PNE, If the mode of device is PNE, the value should be "PNE". 3 – BOTH, If the mode of device is both of PNE and PN GW, the value should be "BOTH" (e.g. mobile phone)			
UserInfo	0..1	E	-	Its attributes are • UserID • UserName	O	O	O
UserID	1	A	String	CPNS UserID	O	O	O
UserName	0..1	A	String	CPNS User Name	O	O	O
DeviceCapa	0..1	E		Capability information of device embedding PNE Its sub attributes are • UICapa Its sub element is • ExternalCapa	O	O	O
UICapa	0..1	A	Boolean	If this device doesn't support UI functionalities, this value SHALL be set with "TRUE". TRUE: PN GW needs to support confirmation and/or Key assignment functionalities instead of PNE.	O	O	O
ExternalCapa	0..1	E	-	XML fragment contains information such as DeviceType, VideoCodec, etc. CPNS V1.0 can make use of the format of device capabilities from DPE Enabler specification.	O	O	O
ServiceProfile	0..1	E		CPNS enabled application information to support certain service and status. Its sub elements are • Service (See section 5.10.2) • ContentInfo (See section 5.10.2)	O	O	O

Table 1 Information elements in PN Inventory

5.9 SG Inventory

SG Inventory contains the information about Service Group(s). SG Inventory SHALL be created or modified when a Service Group is established or when a Service Group is changed. SG Inventory SHALL be deleted when Service Group is released. CPNS Server SHALL store the SG Inventory of Service Groups registered with the CPNS Server. PN GW SHALL store the SG Inventory of Service Groups to which PNE(s) of the same PN belong to. PNE SHALL store the SG Inventory of Service Groups to which the PNE belongs to

This is the format of SG Inventory in CPNS Server, PN GW and PNE.

Element	Cardinality	T	Data Type	Description
SGInfo	1..n	E		Service Group Information. Its sub attributes are • SGID • SGDescription • Sharing • MaxPNE • MaxUser • SGOwner Its sub elements are • ServiceID • MemberInfo
SGID	1	A	String	Service Group Identification.
SGDescription	0..1	A	String	Service Group description. This is human readable description and helpful to understand or search Service Group.
Sharing	1	A	Integer	The level of SG Inventory sharing 1- Open, every PNE can have access to SG Inventory 2- Selective, open to SG member PNEs only 3- Closed, no PNE will have access to SG Inventory. In this case only the SG owner can have access to the SG Inventory
MaxPNE	0..1	A	Integer	The maximum number of member PNE in Service Group. If this value is empty, it follows the policies of Operator and/or Service Provider.
MaxUser	0..1	A	Integer	The maximum number of user in Service Group. If this value is empty, it follows the policies of Operator and/or Service Provider.
SGOwner	1	A	String	EntityIDentification of SGOwner.
ServiceID	0..n	E	String	Service Identifications.
MemberInfo	1..n	E		The Service Group member PNE Information. Its sub attributes are • PNEID • PNGWID • Name Its sub elements are

				• UserInfo • DeviceCapa • ServiceProfile
PNEID	1	A	String	PNE Identification.
PNGWID	1	A	String	PNGW Identification. The PN GW belongs to the same PN as PNE.
Name	0..1	A	String	PNE Name (e.g. mp3 player, assigned nickname)
UserInfo	0..1	E	-	User Information. Its attributes are • UserID • Name
UserID	0..1	A	String	UserIDentification
Name	0..1	A	String	User Name
DeviceCapa	0..1	E		Capability information of device embedding PNE Its sub attribute is • UIcapa Its sub element is • ExternalCapa
UICapa	0..1	A	Boolean	If this device doesn't support UI functionalities, this value SHALL be set with "TRUE". TRUE: PN GW needs to support confirmation and/or Key assignment functionalities instead of PNE.
ExternalCapa	0..1	E	-	XML fragment contains information such as DeviceType, VideoCodec, etc. CPNS V1.0 can make use of the format of device capabilities from DPE Enabler specification.
ServiceProfile	0..1	E		CPNS enabled application information to support certain service and status.Its sub-elements are • Service (See section 5.10.2) • ContentInfo (See section 5.10.2)

Table 2 Information elements in SG Inventory

5.10 CPNS metadata

5.10.1 CPNS profile

Following shows the conceptual image of CPNS profile

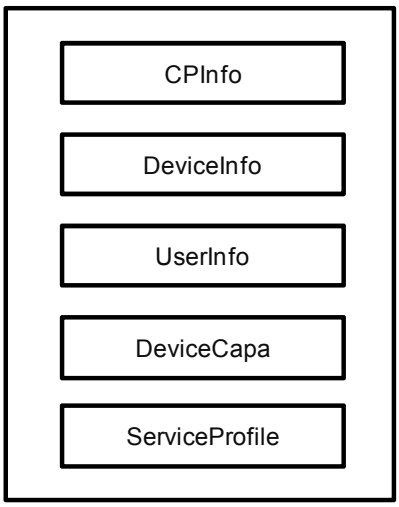


Figure 2 Conceptual image of CPNS profile

CPNS profile is metadata for the CPNS Device, and the external entities. The CPNS Server contains CPNS Profiles of external entities. When creating CPNS messages, CPNS Entity utilizes information in CPNS profile, such as user information and device information.

CPNS profile may be pre-configured (e.g., shipped with PNE or PN GW software) or configured dynamically when PNE or PN GW boots up or with user interaction. When and how to create and update CPNS profile is out of scope of CPNS Enabler. The CPNS profile of external entities in CPNS Server is created based on information published by external entities and can be updated through Service Discovery function.

Following is the brief description related to CPNS profile.

- The CPNS profile contains several subsets such as user information, device information, application information, device capability, status information, and service metadata.
- CPNS Entity SHOULD know the Service part of CPNS profile supplied by CPNS enabled application. The device metadata of CPNS profile is preconfigured or with some other means known to CPNS Entity. Hence PNE acts as local proxy for CPNS enabled application. For CPNS Enabler V1.0, how the CPNS enabled application is realized by CPNS entity and configuration interaction of the CPNS enabled application is out of scope.
- The namespace definition for CPNS profile is implementation matter for CPNS Enabler V1.0.

Following is the overview description of CPNS enabled application profile elements.

- **CPInfo** is the information of external content provider such as CPID, the name of external content provider.
- **DeviceInfo** contains the information of CPNS Device such as device ID, the name of PNE or PN GW.
- **UserInfo** is the UserID and additional information for user depending on the Operator Policy.
- **DeviceCapa** is the device capability of the device.
- **ServiceProfile** is the common description for the CPNS enabled application. This has the sub service or content information.
    - **Service Element** is the metadata that describes services provided using CPNS enabled application
    - **ContentInfo Element** is the metadata that describes Information of Content available to the CPNS enabled application

5.10.2 CPNS Profile Format

Element	Cardinality	T	Data type	Description
Profile	1	E	-	Its sub-elements are • CPInfo • DeviceInfo • UserInfo • DeviceCapa • ServiceProfile
CPInfo	0..1	E		External Content Provider information Its sub attributes are • CPID • CPName
CPID	0..1	A	String	Identifier of external content provider.
CPName	0..1	A	String	Name of external content provider.
DeviceInfo	0..1	E		Device information Its attributes are • DeviceID • PNEName • PNGWName • Mode • InactiveMode
DeviceID	1	A	String	Device identifier, e.g. device maker / model / serial number, UUID.
PNEName	0..1	A	String	Assigned nickname for PNE. Even if the PNE is not active, this name should be set in profile in case device has PNE functionalities. This name is used in Entity Discovery procedure and Service Discovery procedure.
PNGWName	0..1	A	String	Assigned nickname for PNGW. Even if the PN GW is not active, this name should be set in profile in case device has PN GW functionalities. This name is used in Entity Discovery procedure and Service Discovery procedure.
Mode	0..1	A	Integer	The acting mode of device. If the active mode is PNE, the value should be “1”(PNE). If the active mode is PN GW, the value should be “2”(PN GW). If the active mode is both of PNE and PN GW, the value should be “3”(BOTH) (e.g. mobile phone) 1 – PNE, If the mode of device is PNE, the value should be “PNE”. 2 – PNGW, If the mode of device is PN GW, the value should be “PN GW”.

				3 – BOTH, If the mode of device is both of PNE and PN GW, the value should be "BOTH" (e.g. mobile phone)
InactiveMode	0..1	A	Integer	If the current value of Mode is "1"(PNE) or "2"(PN GW) in a device and there are functionalities of PNE and PN GW in a device, the other function is inactive. (e.g. If the value of Mode is "PNE" and its functionalities are PNE and PN GW in a mobile phone, InactiveMode is set "PN GW" and this means inactive mode is "PN GW". e.g. If the value of Mode is "PN GW" and its functionalities are PNE and PN GW in a mobile phone, InactiveMode is set "PNE" and this means inactive mode is "PNE".) 1 – PNE 2 – PNGW
UserInfo	0..1	E	-	User Information for device. Its attributes are • UserID • UserName Its element is • ExtraUserInfo
UserID	0..1	A	String	CPNS UserID (See section 5.1.1)
UserName	1	A	String	CPNS User Name This value MAY be filled with input from user and/or application. If there is no specific input, it SHOULD be as same as UserID.
ExtraUserInfo	0..1	E	-	ExtraUseInfo element contains user information(e.g. Age to check this PNE's User is the allowed person for certain content.). For CPNS V1.0 additional format definition is out of scope and implementation matter.
DeviceCapa	0..1	E	-	Capability information of device embedding PNE Its sub attributes are • UICapa Its sub element is • ExternalCapa
UICapa	0..1	A	Boolean	If this device doesn't support UI functionalities, this value SHALL be set with "TRUE". TRUE: PN GW needs to support confirmation and/or Key assignment functionalities instead of PNE.
ExternalCapa	0..1	E	-	XML fragment contains information such as DeviceType, VideoCodec, etc. CPNS V1.0 can make use of the format of device capabilities from DPE Enabler specification.
ServiceProfile	0..1	E	-	CPNS enabled application information to support certain service and status in device or from external content provider. Its sub-elements are • Service

				• ContentInfo
Service	1..n	E	-	Service metadata is the metadata describes service of CPNS enabled application, which Service Discovery and possibly Service/Content Delivery function uses for operation. Its attributes are • ServiceID • Name Its sub-elements are • Operation • StatusVariable
ServiceID	1	A	String	Service identification. Namespace for the service, which is implementation matter for CPNS V1.0
Name	1	A	String	User-friendly representation of service e.g., application specific service name
Operation	1..n			Its attribute is • Name Its sub-elements are • InputParameterList • OutputParameterList
Name	1	A	String	User-friendly representation of service e.g., application specific operation name
InputParameterList	0..1	E	-	The input parameter (argument) for the service Its sub-elements are • Parameter (See Table 4)
OutputParameterList	0..1	E	-	The output parameter (returned parameter) for the service Its sub-elements are • Parameter (See Table 4)
StatusVariable	0..n	E	-	Status variable the application supports. Its sub attributes are • StatusName • DataType • SendEvents Its sub element is

				• AllowedValueList (see Table 5)
StatusName	1	A	String	Name of status parameter
DataType	1	A	String	Variable data type
SendEvents	1	A	Boolean	TRUE means “yes” FALSE means “no” When “yes” and the value associated to StatusVariable changes, StatusPublicationRequest message SHALL be generated
DefaultValue	0..1	A	String	Initial value
ContentInfo	0..n	E	-	Description of content information. XML fragment which structure is out of scope of CNPS1.0.

Table 3 CPNS Profile metadata

Following table shows the Parameter metadata format.

Element	Cardinality	T	Data type	Description
Parameter	1..n	E	-	Its attributes are • Name • DataType • RelatedStateVariable • DefaultValue Its sub-element is • AllowedValueList (see Table 5)
Name	1	A	String	Name of the parameter
DataType	0..1	A	String	Parameter valuable data type. Required if RelatedStateVariable is not set.
RelatedStateVariable	0..1	A	String	Related state valuable name. Required if DataType is not defined and referenced for parameter valuable.
DefaultValue	0..1	A	String	Not required if RelatedStateVariable is set

Table 4 CPNS Profile-Parameter

Following table shows the AllowedValueList metadata format.

Element	Cardinality	T	Data type	Description
AllowedValueList	0..n	E	-	List of allowed value Its sub-elements are • AllowedValueRange • AllowedValue
AllowedValueRange	0..1	E	String	Allowed value for the certain parent element

				Its sub attributes are • Minimum • Maximum
Minimum	1	A	Integer / Float / Double	Minimum value of the range
Maximum	1	A	Integer / Float / Double	Maximum value of the range
AllowedValue	1..n	E	String	Allowed Value

Table 5 CPNS Profile-AllowedValueList

6. High level procedures (informative)

The information flow in the following subsections describes flow of information between CPNS entities and include the abstract messages or information elements but do not necessarily fully conform to all the messages or information element. Normative specifications are found in section 8.

6.1 CPNS Typical Flow

The CPNS typical flow shows general sequences of CPNS functions to perform CPNS Service as general. This flow includes CPNS Entity Discovery & PN Registration, Service Publication & Discovery, Service/Content Delivery with Device Capability and Usage Statistics Collecting & Reporting.

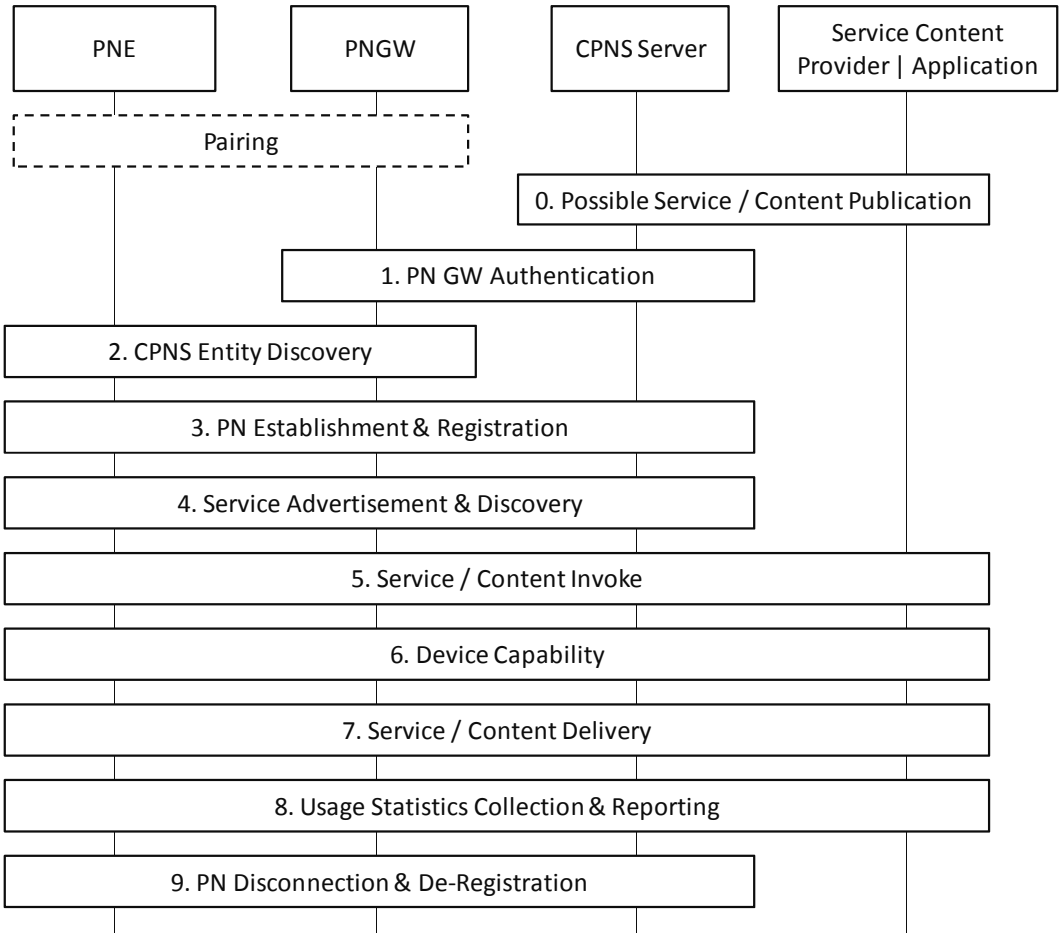


Figure 3 CPNS typical flow

A physical connection (pairing) with PAN technologies between the PNE and the PN GW should be established before CPNS message is sent. It assumes that the PNE in the above diagram and text below is the first PNE which participates in the PN.

0. The Service/Content Provider or application publishes the Service Description to the CPNS Server whenever the service and content is available.

1. The PN GW is authenticated by the CPNS Server. This process can be done before or after the pairing between PN GW and PNE.

2. The PNE or the PN GW initiates CPNS Entity Discovery. This enables discovery of the current operational CPNS Mode (PNE or PN GW) in a CPNS device.

3. PNE and PN GW connect toeach other through a PN. The PN GW creates the information about the corresponding PN that is sent to the CPNS Server and stored in its PN Inventory.. Part of this PN information is sent by CPNS Server to the associated PN GW

4. The CPNS Server advertises Service Description to the PNE or the PNE queries Service Description to the CPNS Server.

5. The PNE invokes service based on the Service Description provided by the CPNS Server.

6. The information of device capability of the PNE, which consumes service or content, may be shared with the CPNS Server and/or Service/Content Provider for delivery of service and content.

7. The service or content is delivered to the PNE from the Service/Content Provider.

8. The PNE reports all the information on the service usage from the CPNS device based on user preference or Operator Policy. The CPNS Server collects the report from the PNE(s) with the related user information.

9. The PNE or the PN GW requests disconnection with the PN. Then, the PN GW de-registers to the CPNS Server on behalf of the PNE.

6.2 Zone Based Service Flow

This section describes general flows for Zone Based Service, which is mainly provided through the public PN GW

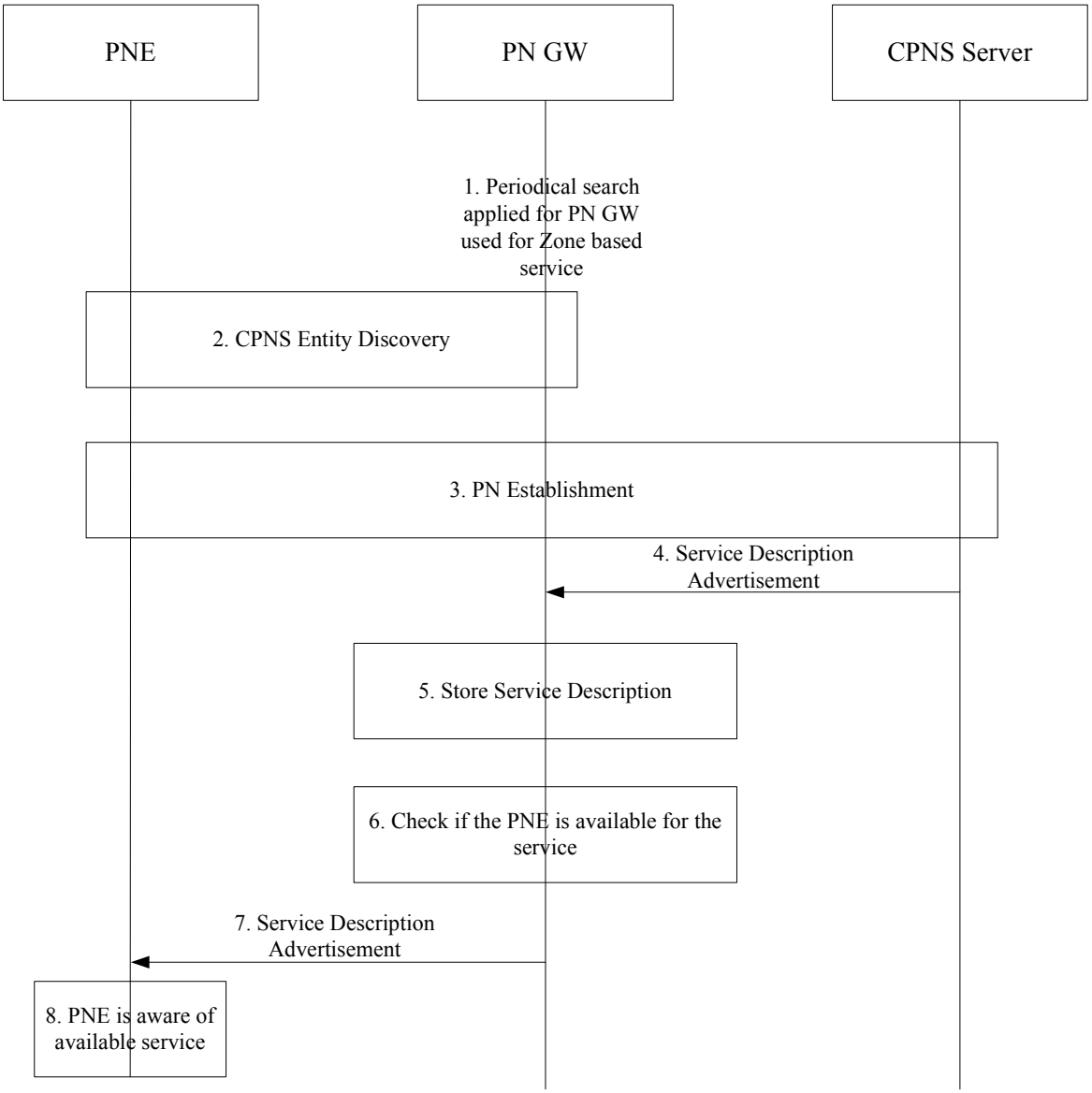


Figure 4 Flow of Zone Based Service

0. The CPNS Server delivers the ServiceDescriptionAdvertise message to the PN GW. This is a presumed step for the Zone Based Service, and can be happed again during the following steps.
1. Periodical search performed.by PN GW for Zone based Service is executed.
2. CPNS entity discovery is executed between PNE and PN GW when there is a newly found PNE entering its zone.
3. PN establishment is executed between the newly-found PNE, PN GW, and CPNS Server.
4. If there's no Service Description Advertise sent from CPNS Server beforehand or the new ServiceDescriptionAdvertise message was made, the CPNS Sever sends the ServiceDescriptionAdvertise message to the PN GW
5. After receiving the ServiceDescriptionAdvertise message, the PN GW stores the Service Description.
6. The PN GW checks if the PNE is available for the service based on PN Inventory.
7. The PN GW delivers the ServiceDescriptionAdvertise message to the PNE

8. Based on ServiceDescriptionAdvertise message, PNE is aware of available services to consume in the Zone. During the period above, the PN GW shall continuously perform periodic search to find another new PNE(s) entering its zone.

6.3 EUKey Assignment

6.3.1 EUKey Assignment for PNE with UI capabilities

Figure 5 shows high level flow of EUKey assignment for a PNE running on a CPNS Device which provides enough UI for CPNS User to insert UserID and password.

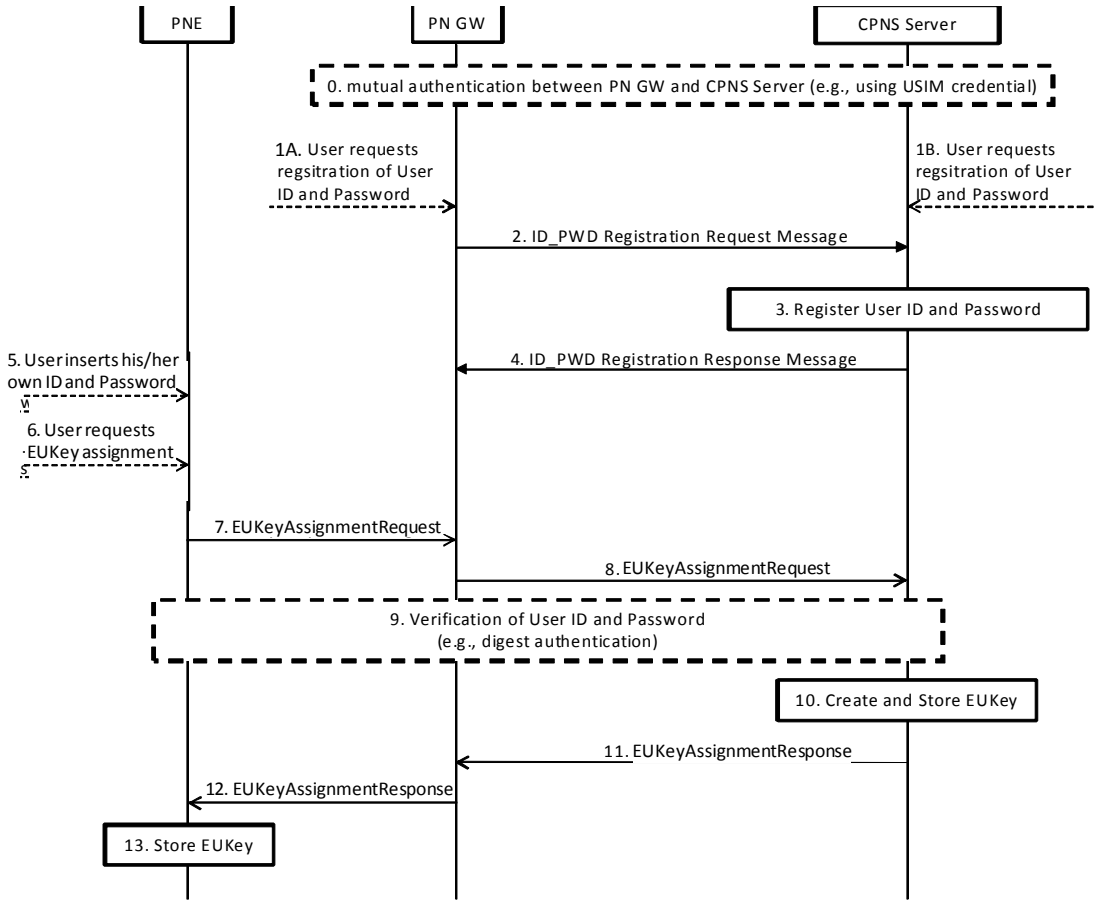


Figure 5 Flow of EUKey Assignment for PNE with UI

0. PNGW and CPNS Server authenticate each other with various ways (e.g., using USIM-creadentials)

1. CPNS User requests to register his/her own UserID and password with CPNS Server. CPNS User can request the registration from PN GW (1A.). CPNS User can also request the registration directly to CPNS Server (1B.) in a way provided outside of the CPNS enabler, such as through a website. If the user has registered the ID and password via the external way (1B), steps from 2 to 4 are not necessary.

2. If CPNS User requests the UserID and password registration from the PN GW, PN GW sends ID_PWDRegistrationRequest Message to the CPNS Server in the case where PN GW and CPNS Server authenticate each other beforehand (e.g., using USIM-credentials).

3. CPNS Server registers UserID and password with itself

4. If registration of UserID and password is triggered by ID_PWDRegistrationRequest message, CPNS Server sends ID_PWDRegistrationResponse message to the PN GW.

   If the ID and password of CPNS User are already registered with the CPNS Server before, steps from 0 to 4 will be skipped.

5. CPNS User turns on a CPNS Device which runs in PNE mode, and inserts UserID and password

6. CPNS User triggers PNE to request EUKey assignment.

7. The PNE sends EUKeyAssignmentRequest Message to a PN GW.

8. The PN GW relays EUKeyAssignmentRequest Message to CPNS Server.

9. Upon receiving the EUKeyAssignmentRequest Message, the CPNS Server verifies the UserID and password (e.g., using digest authentication)

10. If authentication succeeds, CPNS Server creates EUKey. CPNS Server also stores EUKey with the PNE's ID (i.e., EntityID) and UserID of CPNS User who owns the PNE.

11. CPNS Server encrypts EUKey by a secure material calculated from password (e.g., hashed password), and sends the encrypted EUKey via EUKeyAssignmentResponse Message to the PN GW.

12. The PN GW forwards EUKeyAssignmentResponse Message to the PNE.

13. Upon receiving EUKeyAssignmentResponse Message from PNGW, PNE decrypts and stores EUKey.

6.3.2 EUKey Assignment for PNE without UI capabilities

This section describes general EUKey assignment flows for PNE without UI.

6.3.2.1 EUKey Assignment when PAN is secure

The following procedure will happen when the PNE does not have UI capabilities and the underlying network between the PNGW and PNE is the Secure PAN and PNE and PN GW are owned by the same CPNS User.

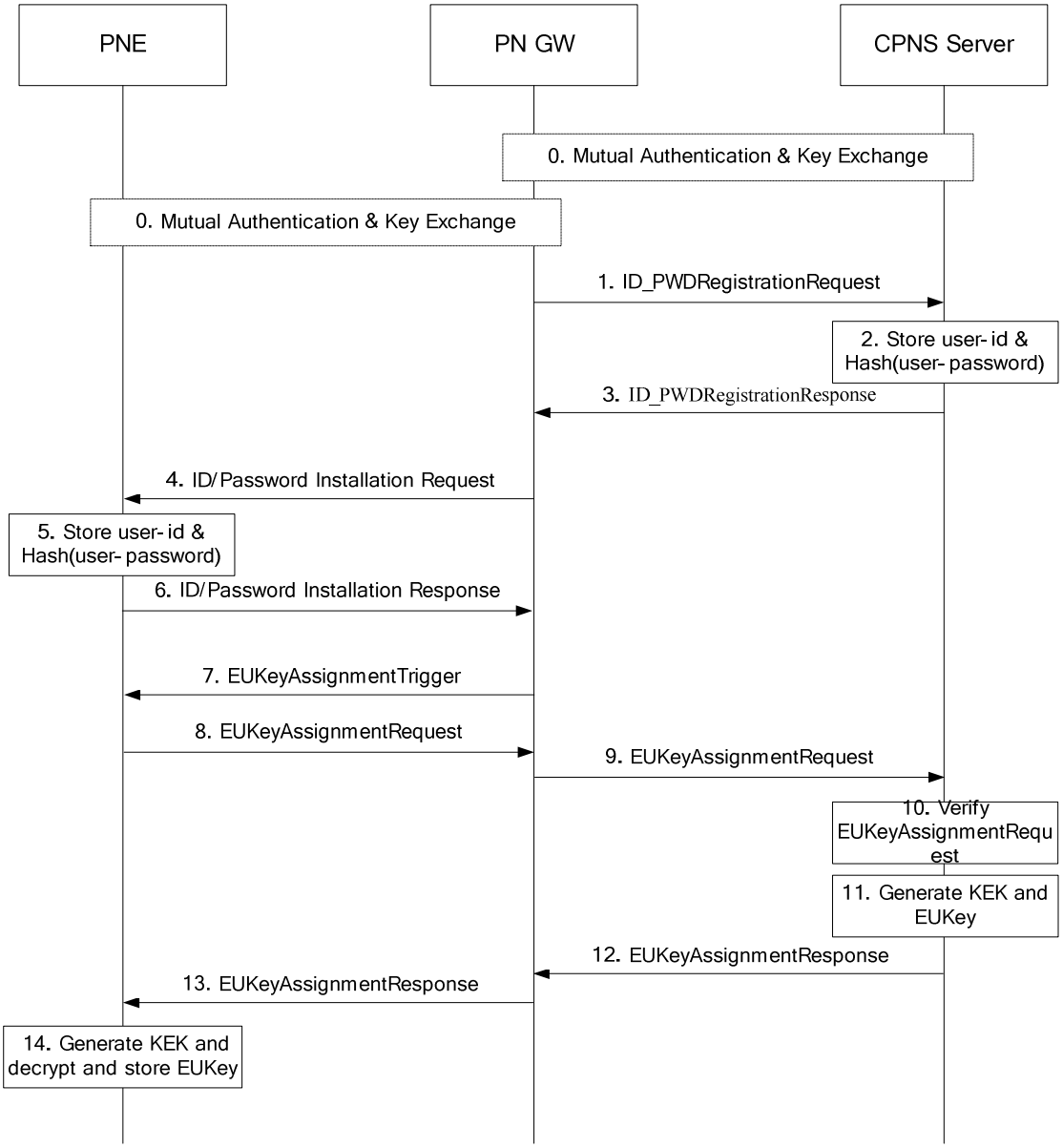


Figure 6 Key Assignment for PNE without UI

0. Before EUKey assignment for PNE without UI, a CPNS Server and a PNGW perform the mutual authentication & key exchange using the existing mechanism (e.g., 3GPP GBA). Also the PNGW and a PNE perform the mutual authentication & key exchange using the existing PAN technologies.

1. The PN GW sends the ID_PWD Registration_Request message to the CPNS Server. The message includes UserID, encrypted user-password and subscription information.

2. Upon receiving the ID_PWD Registration Request message, the CPNS Server stores the received UserID and hash of user-password to the Secure Storage in the CPNS Server.

3. The CPNS Server sends the ID_PWD Registration Response message to the PN GW. The message includes status of handling the Subscription & Registration Request message.

4. The PN GW sends the ID & Password Installation Request message to the PNE. The message includes UserID and encrypted user-password.

5. Upon receiving the ID & Password Installation Request message, the PNE stores the received UserID and hash of user-password to the Secure Storage in the PNE.

6. The PNE sends the ID & Password Installation Response message to the PN GW. The message includes status of handling of the ID & Password Installation Request message.

7. The PN GW sends the EUKeyAssignmentTrigger message to the PNE.

8. Upon receiving the EUKeyAssignmentTrigger message, the PNE verify the trigger is sent by the user of the PNE. If the verification is success, the PNE sends the EUKeyAssignmentRequest message to the PN GW. The message includes UserID and security material for EUKeyAssignmentRequest.

9. The PN GW relays the EUKeyAssignmentRequest message to the CPNS Server.

10. Upon receiving the EUKeyAssignmentRequest message, the CPNS Server verifies the request using the security material for EUKey assignment.

11. If the verification of the request is success, the CPNS Server generates the KEK (i.e. Key Encryption Key) based on the user-password, the received security material from the PNE and the CPNS Server generated security material. Also the CPNS Server randomly generates the PNE EUKey.

12. The CPNS Server sends the EUKeyAssignmentResponse message to the PN GW. The message includes status of handling the EUKeyAssignmentRequest message, the CPNS Server generated security material and the encrypted EUKey with the KEK.

13. The PN GW relays the EUKeyAssignmentResponse message to the CPNS Server.

14. The PNE generates the KEK based on the user-password, the received security material from the CPNS Server and the PNE generated security material. After generating the KEK, the PNE decrypts the PNE EUKey with the KEK, stores the EUKey in the Secure Storage of the PNE.

6.3.2.2 EUKey Assignment when PAN is not secure

The following procedure will happen, if the PNE does not have UI and the underlying network between the PNGW and PNE is not the Secure PAN

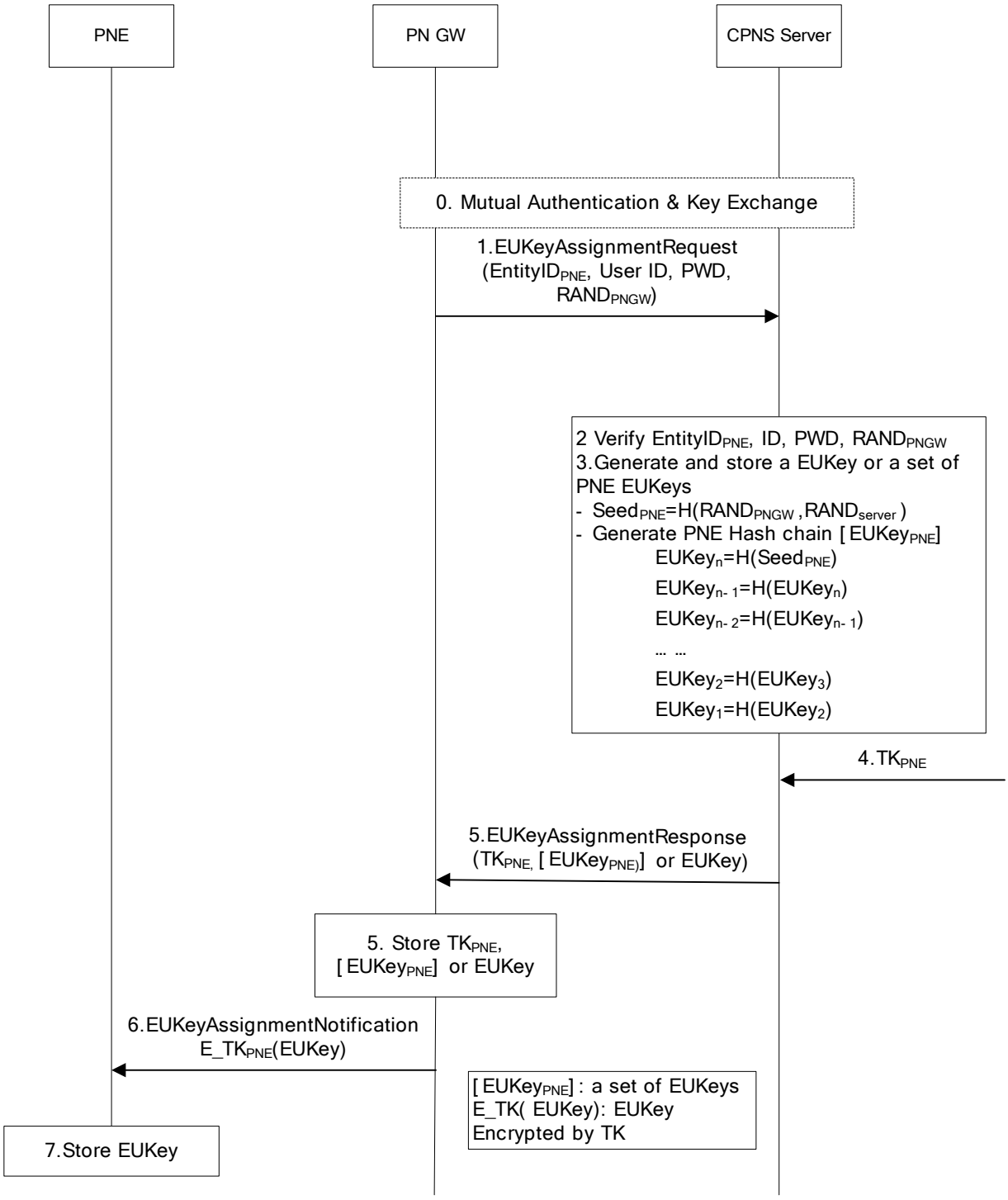


Figure 7 EUKey Assignment for PNE without UI capabilities

In the description below, PNGW and PNE are owned by the same CPNS User. In addition, PNE has secret passphrase, "Temporary Key", which is preconfigured by manufacturer. Temporary Key is stored inside of PNE.

0. Before EUKey assignment for PNE without UI, a CPNS Server and a PNGW perform the mutual authentication &key exchange using the existing mechanism (e.g., 3GPP GBA).

1. The PN GW sends the EUKeyAssignmentRequest message to the CPNS Server upon CPNS User request. The message includes the CPNS UserID and PNE EntityID. In addition, to enable CPNS Server to verify CPNS UserID in the message, the message includes hashed user password.

2. Upon receiving the EUKeyAssignmentRequest message, the CPNS Server authenticates CPNS User of PNE by verifying hashed user password. .

3. The CPNS Server generates and stores a PNE EUKey or a set of PNE's EUKeys together with CPNS UserID and PNE EntityID to Secure Storage.

4. The CPNS Server receives the Temporary Key corresponding to the received EntityID.

5. The CPNS Server sends the EUKeyAssignmentResponse message to the PN GW. The message includes the Temporary Key and a PNE EUKey or a set of PNE's EUKeys. Upon receiving the EUKeyAssignmentResponse message, the PN GW stores the received Temporary Key and a PNE EUKey or a set of PNE's EUKeys in the Secure Storage in the PN GW.

6. The PN GW sends EUKeyAssignmentNotification message to the PNE. The message includes PNE's EUKey encrypted by PNE's Temporary Key.

7. Upon receiving the EUKeyAssignmentNotification message, the PNE decrypts the PNE's EUKey with the Temporary Key and stores the PNE's EUKey securely.

6.3.3 Flow of EUKey Assignment for PN GW

6.3.3.1 Flow of EUKey Assignment for PN GW with UI

Figure 8 shows high level flow of EUKey assignment for a PN GW running on a CPNS Device which provides enough UI for CPNS User to insert UserID and password. If fixed or removable module keeping identity information and credential (i.e. a SIM/USIM/ISIM) is installed and used for secure communication on PN GW, following procedure is not performed..

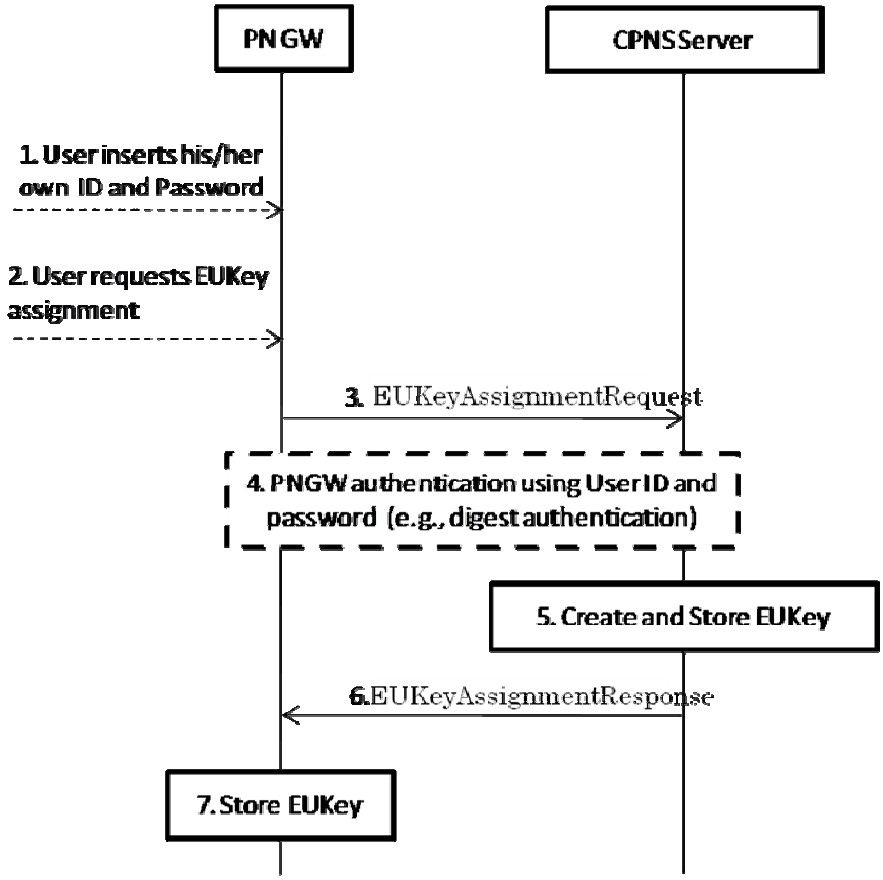


Figure 8 Flow of EUKey Assignment for PN GW with UI

1. CPNS User turns on a CPNS Device which runs in PN GW or PNE+PN GW mode, and inserts UserID and password
2. Previous step for Inserting User ID and password triggers PN GW to request EUKey assignment.
3. The PN GW sends EUKeyAssignmentRequest Message to a CPNS Server.
4. Upon receiving the EUKeyAssignmentRequest Message, the CPNS Server authenticates the PN GW using UserID and password of CPNS User who owns the PN GW. For example, digest authentication mechanism is applied for this authentication.

Note: CPNS Enabler does not specify flow of digest authentication, since existing standard covers it.

5. If authentication succeeds, CPNS Server creates EUKey. CPNS Server also stores EUKey with the PN GW's ID (i.e., EntityID) and UserID of CPNS User who owns the PN GW.
6. CPNS Server encrypts EUKey by a secure material calculated from password (e.g., hashed password), and sends the encrypted EUKey by EUKeyAssignmentResponse Message to the PN GW.
7. Upon receiving EUKeyAssignmentResponseMessage from CPNS Server, PN GW decrypts and stores EUKey securely.

6.4 CPNS Entity Discovery

This section describes the flow of CPNS Entity Discovery.

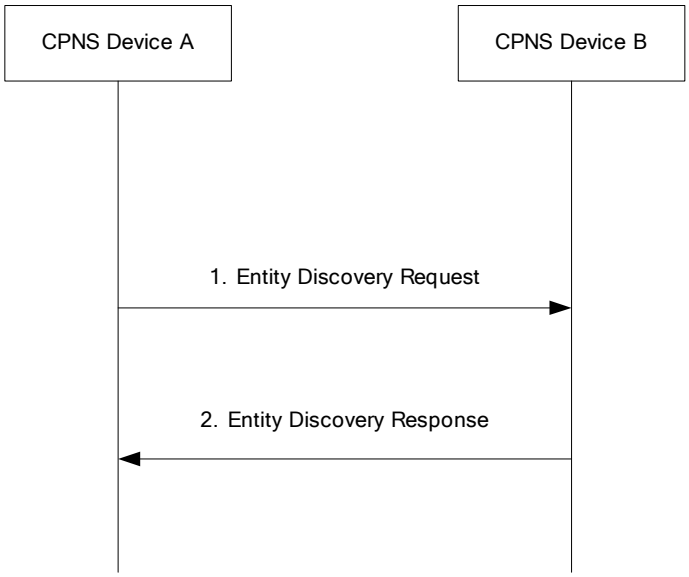


Figure 9 CPNS Entity Discovery

Note 1: when the device detects the other devices physically, it has no information about Entity in device.

Note 2: If the CPNS device is a Zone based PN GW, this CPNS device should inform of this zone based support information

1. CPNS Device A sends Entity Discovery Request to CPNS Device B. This EntityDiscoveryRequest message includes the information such as;
   - The mode of CPNS Device A
   - The CPNS Entity ID (PNEID, PNGWID)
2. CPNS Device B sends Entity Discovery Response to CPNS Device A. This Entity Discovery Response message includes the information such as;
   - The mode of CPNS Device B
   - The CPNS EntityID (PNEID, PNGWID)

6.5 PN GW Authentication

Figure 10 shows the high level flow of PN GW Authentication. In the flow, PN GW and CPNS Server perform mutual authentication and session key sharing. If fixed or removable module keeping identity information and credential (i.e., a SIM/USIM/ISIM) is installed and used for secure communication on PN GW, following flow is not performed.

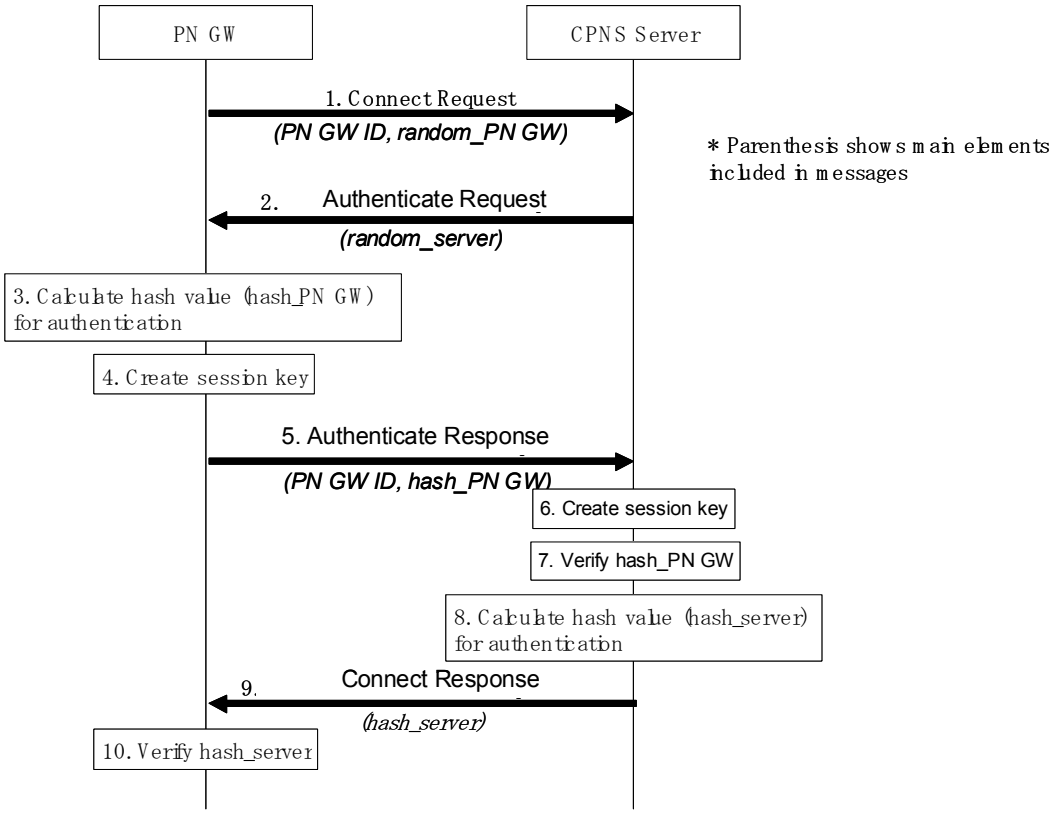


Figure 10 PN GW Authentication

1. PN GW sends ConnectRequest message to CPNS Server. The message includes CPNS EntityID of the PN GW and random number created by PN GW (random_PN GW).
2. CPNS Server sends AuthenticateRequest message to the PN GW. The message includes random number created by CPNS Server (random_server).
3. PN GW calculates hash value from message 1 & 2 by using its own EUKey (hash_PN GW).
4. PN GW creates session key from random_PN GW, random_server and its own EUKey.
5. PN GW sends AuthenticateResponse message to CPNS Server. The message includes CPNS EntityID of the PN GW and hash_PN GW calculated in step 3.
6. CPNS Server creates session key from random_PN GW, random_server and EUKey of the PN GW.
7. CPNS Server authenticates PN GW. That is, CPNS Server verifies hash_PN GW by checking if the same hash value can be calculated by itself.
8. CPNS Server calculates hash value (hash_server) from message 1, 2 & 5 by using EUKey of the PN GW.
9. CPNS Server sends ConnectResponse message to the PN GW. The message includes hash_server
10. PN GW authenticates CPNS Server. That is, the PN GW verifies hash_server by checking if the same hash value can be calculated by itself.

6.6 PN Management

This section provides a flow of PN Establishment which enables PNE to connect to CPNS Server through PN GW for consuming/providing services or contents. PN Establishment can be initiated by PNE or PN GW, based on circumstances or some user preferences.

6.6.1 PN Establishment

This section differentiates PNE initiated and PN GW initiated PN Establishment for easy understanding and readability.

6.6.1.1 PNE initiated

This flow shows the PNE initiated procedure of PN Establishment. In the flow, it is assumed that PNE 1, 2 and PN GW have physical pairing among themselves with PAN technologies.

The PN may consist of one PN GW and one PNE or multiple PNEs. This section covers both cases in Figure 11 and description.

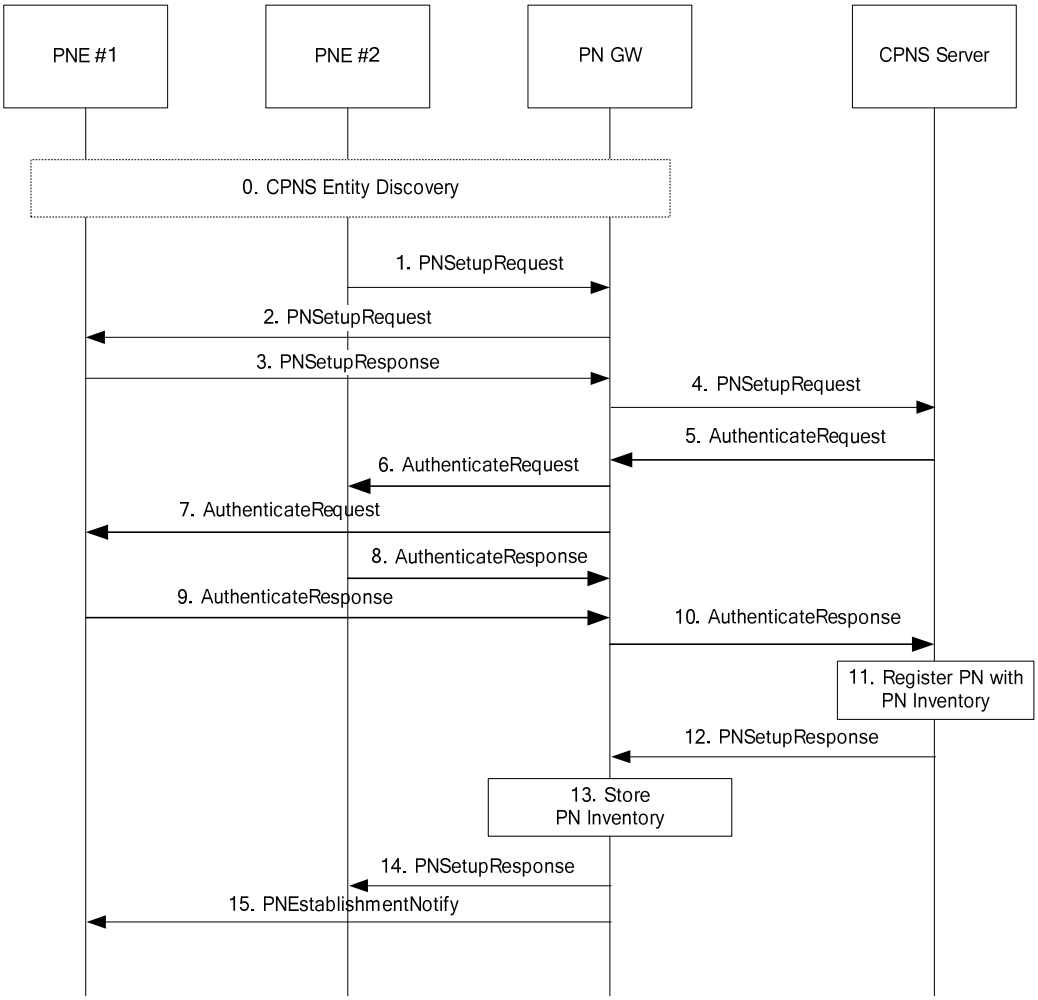


Figure 11 Flow of PN Establishment initiated by PNE

Figure 11 shows a flow of PN Establishment. The flow depicts the scenario where PNE initiates PN establishment.

0. Before PN Establishment, the PNE 1, 2 and PN GW perform CPNS Entity Discovery among themselves respectively. Detailed flow is shown in section 6.4

1. The PNE 2 sends a PNSetupRequest message to PNGW.

   The PNSetupRequest message contains;

   - Device Capabilities of device the PNE belongs to
   - Optionally Content(s) information which the device has
   - Type of PN Setup
     - A '1-1' case which enable the PNE to establish a PN with the PN GW only; or
     - B 'All' case which enable the PNE to establish a PN with all CPNS devices connected to the PN GW; or
     - C PNEIDs to be invited
   - Random number created by PNE2 (hereinafter, rand_PNE2) to be used for mutual authentication between PNE2 and CPNS Server
   - Indication to request LocalEUKey assignment if both of the following two conditions are met. Otherwise, the indication is not included in the message:
     - PNE2 has enough UI
     - PAN between PNE2 and PN GW does not provide sufficient security mechanism to protect authenticity, confidentiality and integrity of CPNS message,

NOTE: In case of 1-1, the only procedure related to PNE 2 with PN GW and CPNS Server should be performed in Figure 11.

2. The PN GW sends the PNSetupRequest message to the PNE 1.

   The PNSetupRequest message contains;

   - The initiator of PN Setup
   - PNID

3. The PNE 1 sends the PNSetupResponse to the PN GW in order to confirm participation in PN. The PNSetupResponse message contains;

   - Random number created by PNE1 (hereinafter, rand_PNE1) to be used for mutual authentication between PNE1 and CPNS Server
   - Indication to request LocalEUKey assignment if both of the following two conditions are met. Otherwise, the indication is not included in the message:
     - PNE1 has enough UI
     - PAN between PNE1 and PN GW does not provide sufficient security mechanism to protect authenticity, confidentiality and integrity of CPNS message

4. When receiving a PNSetupRequest message, the PN GW creates the information for PN Inventory for the corresponding Personal Network, creates and maintains routing table for the routing of inside Personal Network, which is made out of PN Inventory.

   PN GW sends PNSetupRequest message to CPNS Server.

   The PNSetupRequest message may contain the information;

- PN GW Info.
  - Capability information of device which PN GW is deployed
  - Subscription information
- PNE Info.
  - Capability information of device which PNE is deployed
  - Optionally Contents information which the device has
  - PNEID
- PNID
- rand_PNE1 and rand_PNE2

5. The CPNS Server creates two LocalEUKeys to be shared between PNE1 and PN GW (hereinafter, LocalEUKey_PNE1), and between PNE2 and PN GW (hereinafter, LocalEUKey_PNE2), if there is indication to request LocalEUKey assignment. For each LocalEUKey, two copies are created, one for PNE and the other for PN GW, and each copy is encrypted by PNE's EUKey and PN GW's EUKey.

   Then, the CPNS Server sends AuthenticationRequest message for the PNEs to the PN GW.

   The AuthenticateRequest message contains;

   - Random number created by CPNS Server (hereinafter, rand_server) to be used for mutual authentication between CPNS Server and PNE1 and PNE2
   - Encrypted LocalEUKey_PNE1 and encrypted LocalEUKey_PNE2 (two encrypted copies for each LocalEUKey, one encrypted by PNE's EUKey and the other encrypted by PN GW's EUKey)
   - PNID

6. Upon receiving AuthenticateRequest message, PN GW decrypts LocalEUKey_PNE1 and LocalEUKey_PNE2 by its own EUKey, and stores the LocalEUKey_PNE1 and LocalEUKey_PNE2 Then, the PN GW relays the AuthenticateRequest message to the PNE 2 based on routing table identified with PNID.

   The AuthenticateRequest message contains;

   - Encrypted LocalEUKey_PNE2 (copy of LocalEUKey_PNE2 encrypted by PNE2's EUKey)
   - rand_server

Upon receiving AuthenticateRequest message, PNE2 decrypts LocalEUKey_PNE2 and stores the LocalEUKey_PNE2.

Then, if PAN between PNE2 and PN GW does not provide sufficient security mechanism to protect authenticity, confidentiality and integrity of CPNS message, PNE2 and PN GW perform mutual authentication and session key sharing by using LocalEUKey_PNE2 in the same way as described in 7.5.5 "PN GW Authentication"

7. The PN GW also relays the AuthenticateRequest message to the PNE 1 based on routing table identified with PNID.

   The AuthenticateRequest message contains;

   - Encrypted LocalEUKey_PNE1 (copy of LocalEUKey_PNE1 encrypted by PNE1's EUKey)
   - rand_server

Upon receiving AuthenticateRequest message, PNE1 decrypts LocalEUKey_PNE1 and stores the LocalEUKey_PNE1.

Then, if PAN between PNE1 and PN GW does not provide sufficient security mechanism to protect authenticity, confidentiality and integrity of CPNS message,PNE1 and PN GW perform mutual authentication and session key sharing by using LocalEUKey_PNE1 in the same way as described in 7.5.5 “PN GW Authentication”

8. The PNE2 calculates hash value for authentication (hereinafter, hash_PNE2) and session key to be shared with CPNS Server (hereinafter, SK_PNE2). SK_PNE2 is calculated from rand_PNE2, rand_server and EUKey of PNE2. hash_PNE2 is calculated from rand_PNE2, rand_server, EUKey of PNE2 and SK_PNE2. Then, the PNE 2 sends the AuthenticateResponse message to the PN GW.

   The AuthenticateResponse message contains;

   - hash_PNE 2

9. The PNE1 calculates hash value for authentication (hereinafter, hash_PNE1) and session key to be shared with CPNS Server (hereinafter, SK_PNE1). The calculation is performed in the same way as in the above step. Then, the PNE 1 sends the AuthenticateResponse message to the PN GW.

   The Authentication response contains;

   - hash_PNE 1

10. The PN GW relays the AuthenticateResponse message to the CPNS Server.

    The AuthenticateResponse message contains;

    - hash_PNE 1 and hash_PNE 2

11. Upon receiving the AuthenticateResponse message, the CPNS Server authenticates PNE1 and PNE2 by verifying hash_PNE1 and hash_PNE2, respectively. The CPNS Server registers the PN with PN Inventory, when at least one of the PNEs is authenticated.

12. CPNS Server calculates session key and hash value for authentication for each PNE (hereinafter hash_server_PNE1 and hash_server_PNE2).

    Session keys are calculated in the same way as in the step 8 and 9 (Thus, the same session key, SK_PNE1 and SK_PNE2 are calculated, if CPNS Server and PNE have the same EUKey).

    hash_server_PNE1 and hash_server_PNE2 are also calculated in the similar way as in the step 8 and 9, but additionally use another value, hash_PNE1 for hash_server_PNE1 and hash_PNE2 for hash_server_PNE2, respectively.

    Then, CPNS Server sends PN Registration Response message to PN GW.

    The PNSetupRequest message contains;

    - hash_server_PNE 1 and hash_server_PNE 2

13. PN GW stores the PN Inventory locally.

14. PN GW sends PNSetupResponse message to PNE 2.

    The PNSetupResponse message contains;

    - PN Inventory
    - hash_server_PNE2

Upon receiving PNSetupResponse message, PNE2 authenticates CPNS Server by verifying hash_server_PNE2 and create PN Inventory.

15. The PN GW sends the PNEstablishmentNotify to the PNE 1.

    The PNEstablishmentNotify message contains;

- PN Inventory
- hash_server_PNE1

Upon receiving PNEstablishmentNotify message, PNE1 authenticates CPNS Server by verifying hash_server_PNE1 and create PN Inventory

If PNE1 and PNE2 fail to verify hash_server_PNE1 and hash_server_PNE2, they do not store PN information and give up to connect to the PN.

6.6.1.2 PN GW initiated

This flow shows the PN GW initiated procedure of PN Establishment, in case PN GW establishes a PN with one PNE or multiple PNEs. In the flow, it is assumed that PNE 1, 2 and PN GW among themselves have physical pairing with PAN technologies.

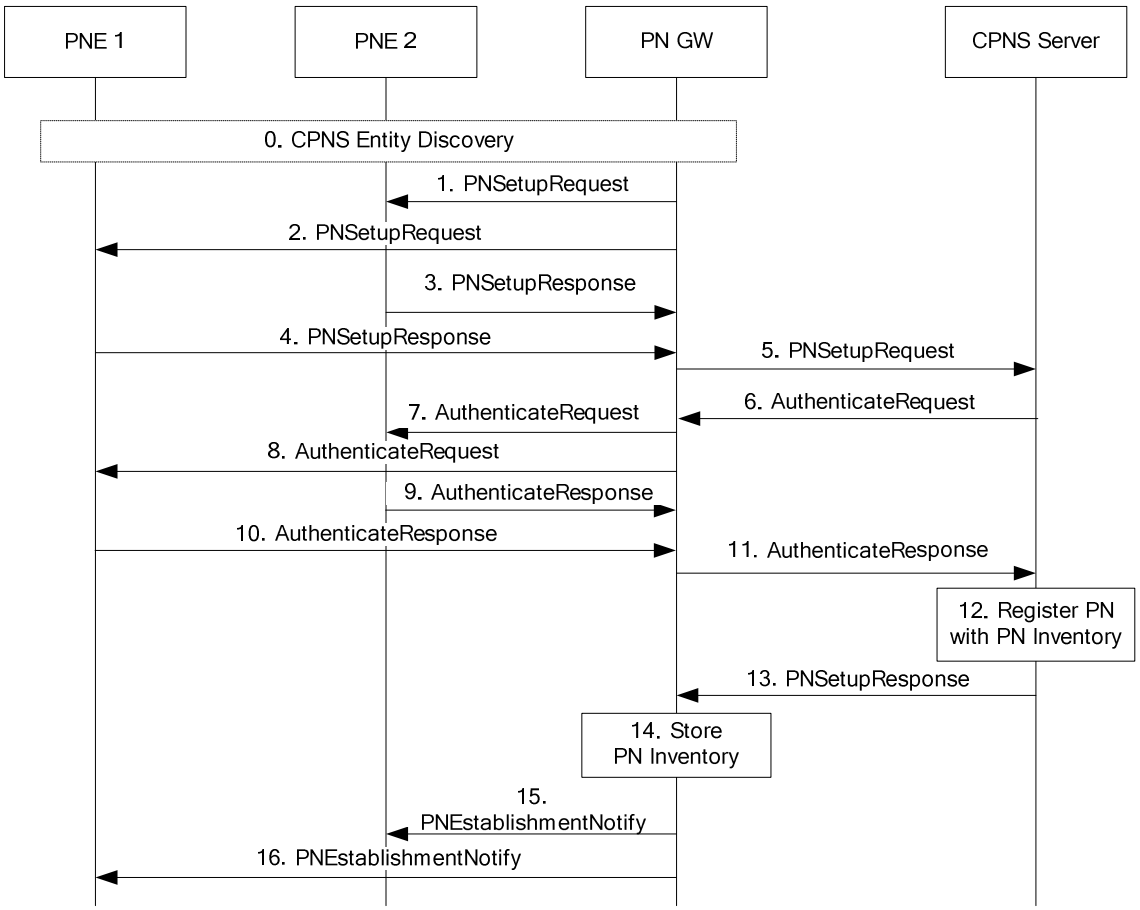


Figure 12 PN GW initiated PN Establishment

0. Before PN Establishment, PNEs and PN GW perform CPNS Entity Discovery as described in section 6.4
1. The PN GW sends a PNSetupRequest message to PNE 2.
2. The PN GW sends a PNSetupRequest message to PNE 1.
3. Upon receiving the PNSetupRequest message from the PN GW, the PNE 2 sends PNSetupResponse message to confirm whether it participates in the PN or not.

   The PNSetupResponse message contains;

- Device Capabilities of device the PNE belonging to
- Optionally, Contents information which the device has
- PNEID
- Random number created by PNE2 (hereinafter, rand_PNE2) to be used for mutual authentication between PNE2 and CPNS Server
- Indication to request LocalEUKey assignment if both of the following two conditions are met. Otherwise, the indication is not included in the message:
    - PNE2 has enough UI
    - PAN between PNE2 and PN GW is not Secure PAN,

4. Upon receiving the PNSetupRequest message from the PN GW, the PNE 1 sends PNSetupResponse message to confirm whether it participates in the PN or not.

   The PNSetupResponse message contains;

   - Capability information of device which PNE is deployed
   - Optionally, Contents information which the device has
   - PNEID
   - Random number created by PNE1 (hereinafter, rand_PNE1) to be used for mutual authentication between PNE1 and CPNS Server
   - Indication to request LocalEUKey assignment if both of the following two conditions are met. Otherwise, the indication is not included in the message:
       - PNE1 has enough UI
       - PAN between PNE1 and PN GW is not Secure PAN.

5. When receiving a PNSetupResponse message with the confirmation of participation in the PN, the PN GW creates the information for PN Inventory for the corresponding Personal Network, creates and maintains the routing table for the routing of inside the Personal Network.

   The PN GW sends PNSetupRequest message to CPNS Server.

   The PNSetupRequest message contains;

   - PN WG Info.
       - Capability information of device which PN GW is deployed
       - Subscription information
   - PNE Info.
       - Capability information of device which PNE is deployed
       - Optionally Contents which the device has
       - Optionally, PNEID which is embedded in factory or the user creates
   - PNID
   - rand_PNE1 and rand_PNE2

6. The CPNS Server creates two LocalEUKeys to be shared between PNE1 and PN GW (hereinafter, LocalEUKey_PNE1), and between PNE2 and PN GW (hereinafter, LocalEUKey_PNE2). For each LocalEUKey, two copies are created, one for PNE and the other for PN GW, and each copy is encrypted by PNE's EUKey and PN GW's EUKey.

   Then, the CPNS Server sends AuthenticationRequest message for the PNEs to the PN GW.

   The AuthenticationRequest message contains;

   - Random number created by CPNS Server (hereinafter, rand_server) to be used for mutual authentication between CPNS Server and PNE1 and PNE2
   - Encrypted LocalEUKey_PNE1 and encrypted LocalEUKey_PNE2 (two encrypted copies for each LocalEUKey, one encrypted by PNE's EUKey and the other encrypted by PN GW's EUKey)
   - PNID

7. Upon receiving AuthenticationRequest message, PN GW decrypts LocalEUKey_PNE1 and LocalEUKey_PNE2 by its own EUKey, and stores the LocalEUKey_PNE1 and LocalEUKey_PNE2. Then, the PN GW relays the AuthenticationRequest message to the PNE 2 based on routing table identified with PNID.

   The AuthenticationRequest message contains;

   - Encrypted LocalEUKey_PNE2 (copy of LocalEUKey_PNE2 encrypted by PNE2's EUKey)
   - rand_server

Upon receiving AuthenticationRequest message, PNE2 decrypts LocalEUKey_PNE2 and stores the LocalEUKey_PNE2.

Then, if PAN between PNE2 and PN GW is not Secure PAN,PNE2 and PN GW perform mutual authentication and session key sharing by using LocalEUKey_PNE2 in the same way as described in 7.5.5 "PN GW Authentication"

8. The PN GW also relays the AuthenticationRequest message to the PNE 1 based on routing table identified with PNID.

   The AuthenticationRequest message contains;

   - Encrypted LocalEUKey_PNE1 (copy of LocalEUKey_PNE1 encrypted by PNE1's EUKey)
   - rand_server

Upon receiving AuthenticationRequest message, PNE1 decrypts LocalEUKey_PNE1 and stores the LocalEUKey_PNE1.

Then, if PAN between PNE1 and PN GW is not Secure PAN,PNE1 and PN GW perform mutual authentication and session key sharing by using LocalEUKey_PNE1 in the same way as described in 7.5.5 "PN GW Authentication"

9. The PNE2 calculates hash value for authentication (hereinafter, hash_PNE2) and session key to be shared with CPNS Server (hereinafter, SK_PNE2). SK_PNE2 is calculated from rand_PNE2, rand_server and EUKey of PNE2. hash_PNE2 is calculated from rand_PNE2, rand_server, EUKey of PNE2 and SK_PNE2. Then, the PNE 2 sends the AuthenticationResponse message to the PN GW.

   The AuthenticationResponse message contains;

   - hash_PNE 2

10. The PNE1 calculates hash value for authentication (hereinafter, hash_PNE1) and session key to be shared with CPNS Server (hereinafter, SK_PNE1). The calculation is performed in the same way as in the above step. Then, the PNE 1 sends the Authentication response to the PN GW.

    The AuthenticationResponse message contains;

    - hash_PNE 1

11. The PN GW relays the AuthenticationResponses message to the CPNS Server.

The AuthenticationResponse message contains;

- hash_PNE 1 and hash_PNE 2

12. Upon receiving the AuthenticationResponses message, the CPNS Server authenticates PNE1 and PNE2 by verifying hash_PNE1 and hash_PNE2, respectively. The CPNS Server registers the PN with PN Inventory, when at least one of the PNEs is authenticated.

13. The CPNS Server calculates session key and hash value for authentication for each PNE (hereinafter hash_server_PNE1 and hash_server_PNE2).

    Session keys are calculated in the same way as in the step 8 and 9 (Thus, the same session key, SK_PNE1 and SK_PNE2 are calculated, if CPNS Server and PNE have the same EUKey).

    hash_server_PNE1 and hash_server_PNE2 are also calculated in the similar way as in the step 8 and 9, but additionally use another value, hash_PNE1 for hash_server_PNE1 and hash_PNE2 for hash_server_PNE2, respectively.

    Then, CPNS Server sends PNSetupResponse message to the PN GW.

    The PN Registration Response message contains;

    - hash_server_PNE 1 and hash_server_PNE 2

14. The PN GW stores the PN Inventory locally.

15. The PN GW sends PNEstablishmentNotify message to PNE 2.

    The PNEstablishmentNotify message contains;

    - PN ID
    - hash_server_PNE2

Upon receiving PNEstablishmentNotify message, PNE2 authenticates CPNS Server by verifying hash_server_PNE2 and create PN Inventory.

16. The PN GW sends PNEstablishmentNotify message to PNE 1.

    The PNEstablishmentNotify message contains;

    - PN ID
    - hash_server_PNE1

Upon receiving PNEstablishmentNotify message, PNE1 authenticates CPNS Server by verifying hash_server_PNE1 and create PN Inventory.

If PNE1 and PNE2 fail to verify hash_server_PNE1 and hash_server_PNE2, they do not store PN information and give up to connect to the PN.

6.6.2 PNE Management

6.6.2.1 PN GW Inviting

This section describes general PN GW invite flow in a PN. Basic assumption is that the PNE1 is a member of PN and PN GW wants to invite PNE2 as a member of PN.

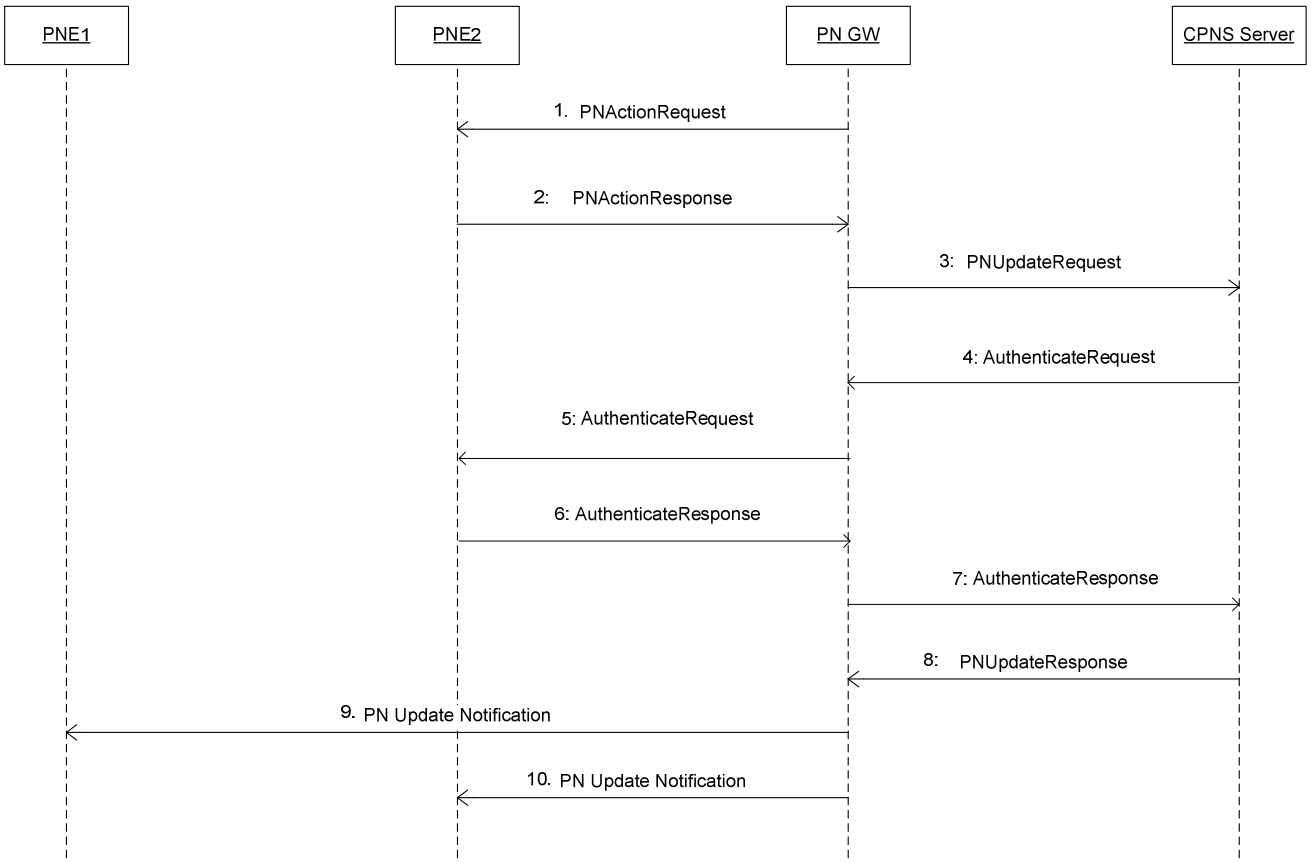


Figure 13 PNE Invite initiated by PN GW

1. PN GW sends PNActionRequest message with Command 2 (i.e. 2 - Invite, the PNE or PN GW wants to invite other PNE(s)) to PNE2, which means PN GW invites PNE2 to be a member of PN.
2. PNE2 sends PNActionResponse message to PN GW.
3. PN GW sends PNActionRequest message to CPNS Server.
4. CPNS Server sends AuthenticateRequest message to PN GW to authenticate invited PNE, PNE2.
5. PN GW forwards AuthenticateRequest message to PNE2.
6. PNE2 generates authentication data using its EUKey and send it by AuthenticateResponse message to CPNS Server via PN GW
7. PN GW forwards AuthenticateResponse message to CPNS Server.
8. After authenticating PNE2, CPNS Server updates PN Inventory and sends PNUpdateResponse message to PN GW.
9. If the PN GW shares the member information with the member of PN, PN GW sends PNUpdateNotification message to the PNE1 including PNE2 information.
10. PN GW sends PNUpdateNotification message to the PNE2 to let PNE2 know it successfully connects to PN.

6.6.2.2 PNE inviting

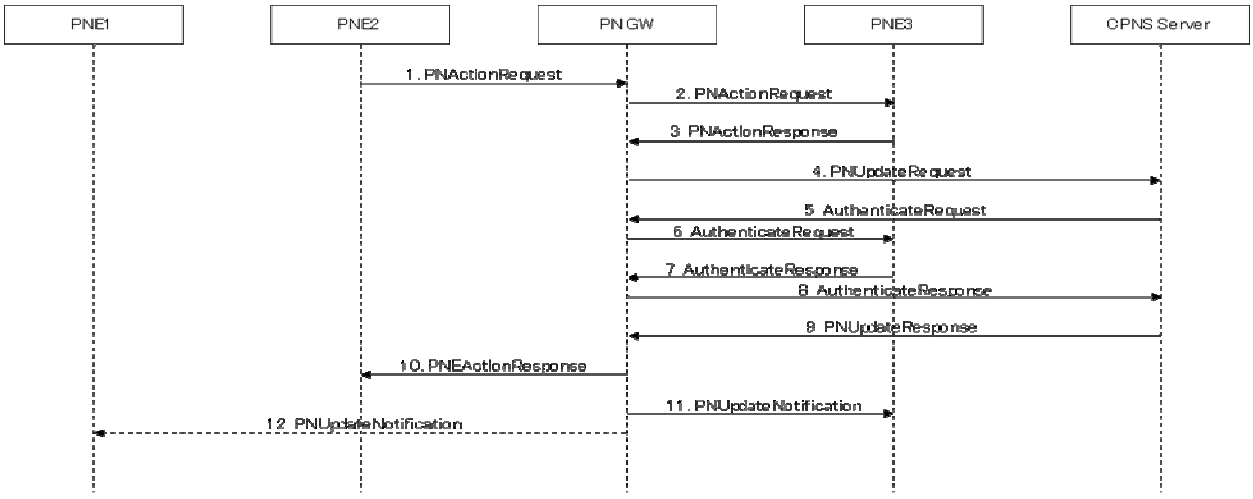


Figure 14 PNE Invite Initiated by PNE

1. PNE2 sends PNActionRequest message with Command 2 (i.e. 2 - Invite, the PNE or PN GW wants to invite other PNE(s)), which means PNE2 invites PNE3 to be a member of PN.
2. PN GW sends PNActionRequest message to PNE3.
3. PNE3 sends PNActionResponse message to PN GW.
4. PN GW sends PNUpdateRequest message to CPNS Server.
5. CPNS Server sends AuthenticateRequest message to PN GW to authenticate invited PNE, PNE3.
6. PN GW forwards AuthenticateRequest message to PNE3.
7. PNE3 generates authentication data using its EUKey and send it by AuthenticateResponse message to CPNS Server via PN GW
8. PN GW forwards AuthenticateResponse message to CPNS Server
9. After authenticating PNE3, CPNS Server updates PN Inventory and sends PNUpdateResponse message to PN GW.
10. PN GW sends PNActionResponse message to PNE2.
11. If the PN GW shares the member information with the member of PN, PN GW sends PNUpdateNotification message to the PNE1 including PNE3 information.
12. The PN GW sends PNUpdateNotification message to the PNE3 to let PNE3 know it successfully connects to PN..

6.6.2.3 PNE Joining

Figure 15 shows a flow of PNE joins a PN which is initiated by PNE.

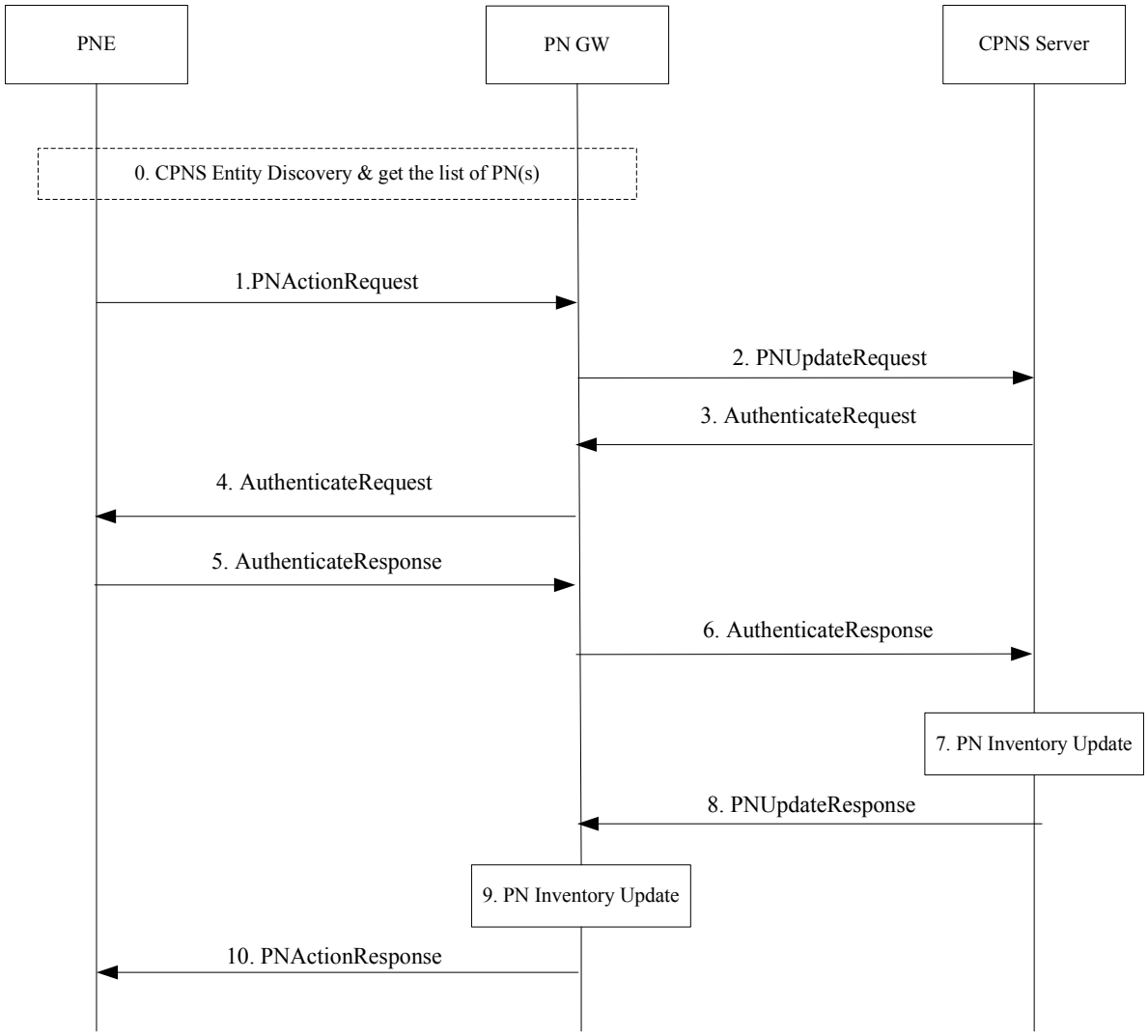


Figure 15 Flow of PNE Joins a PN Initiated by PNE

0. PNE and PN GW discover each other, and PNE gets the list of PN(s) this PN GW belongs to.
1. The PNE sends PNActionRequest message with Command "1" (Join) to PN GW to join one of PN(s) in the list.
2. The PN GW sends PNUpdateRequest message to the CPNS Server.
3. CPNS Server sends AuthenticateRequest message to PN GW to authenticate PNE.
4. PN GW forwards AuthenticateRequest message to PNE.
5. PNE generates authentication data using its EUKey and send it by AuthenticateResponse message to CPNS Server via PN GW
6. PN GW forwards AuthenticateResponse message to CPNS Server
7. After authenticating PNE, The CPNS Server updates the PN Inventory.
8. The CPNS Server sends PNUpdateResponse message to the PN GW.
9. The PN GW updates PN Inventory locally.
10. The PN GW sends PNActionResponse message to the PNE.

6.6.2.4 PNE Leaving

Figure 16 shows a flow of PNE leaves a PN which is initiated by PNE.

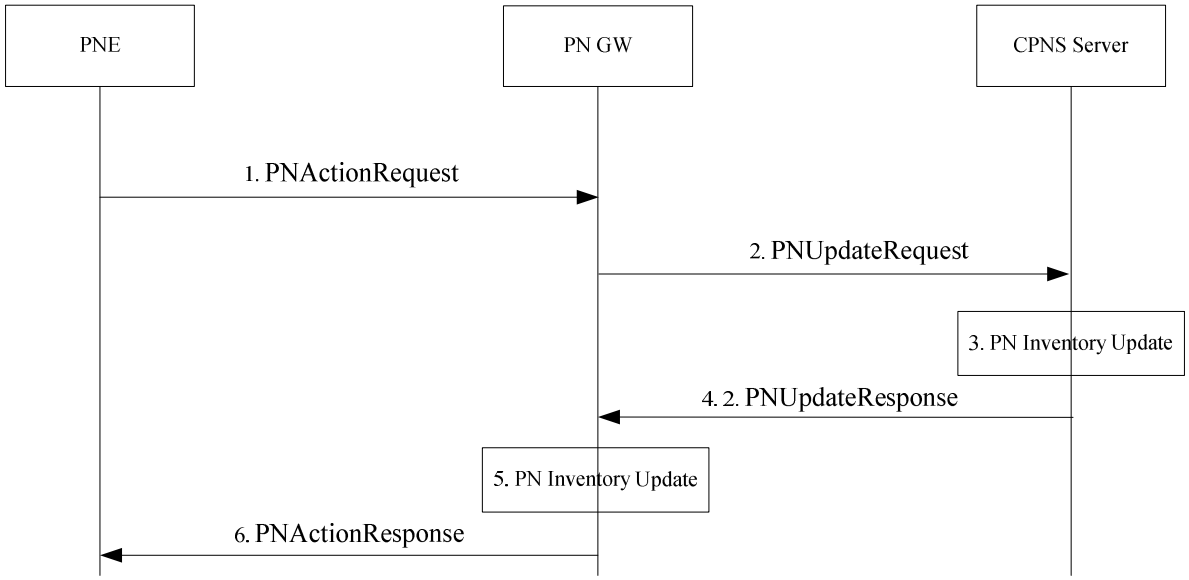


Figure 16 Flow of PNE Leaves a PN Initiated by PNE

1. The PNE sends PNActionRequest message with Command "3" (Leave) to PN GW for leaving the PN.
2. The PN GW sends PNUpdateRequest message to the CPNS Server.
3. The CPNS Server updates the PN Inventory.
4. The CPNS Server sends PNUpdateResponse message to the PN GW.
5. The PN GW updates PN Inventory locally.
6. The PN GW sends PNActionResponse message to the PNE.

6.6.2.5 PNE Expulsion

Figure 17 shows a flow of PNE leaves a PN which is initiated by PN GW.

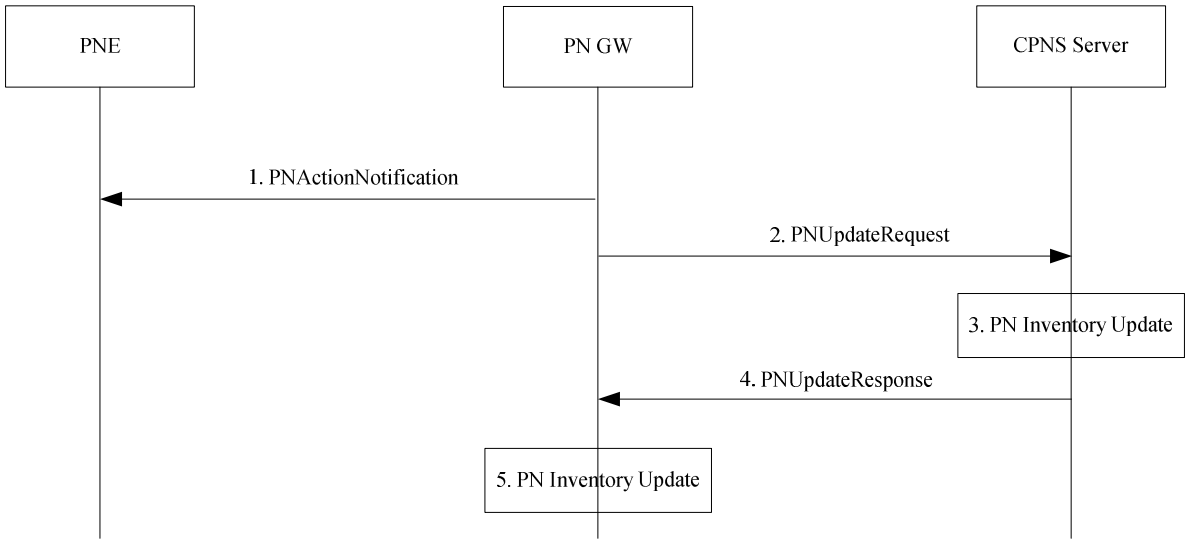


Figure 17 Flow of PNE Leaves a PN Initiated by PN GW

1. The PN GW sends PNActionNotification message with Command "1" to PNE, indicate the PNE will be removed from the PN.
2. The PN GW sends PNUpdateRequest message to the CPNS Server.
3. The CPNS Server updates the PN Inventory.
4. The CPNS Server sends PNUpdateResponse message to the PN GW.
5. The PN GW updates PN Inventory locally.

6.6.3 PN Release

This section describes PN Release flow. The PN Release can be done by PNE or PN GW.

Basic assumption is the PNE1 and PNE2 are members of PN and PN GW decides to remove PN.

6.6.3.1 Initiated by PN GW

Figure 19 shows a flow of PN Release which is initiated by PNE.

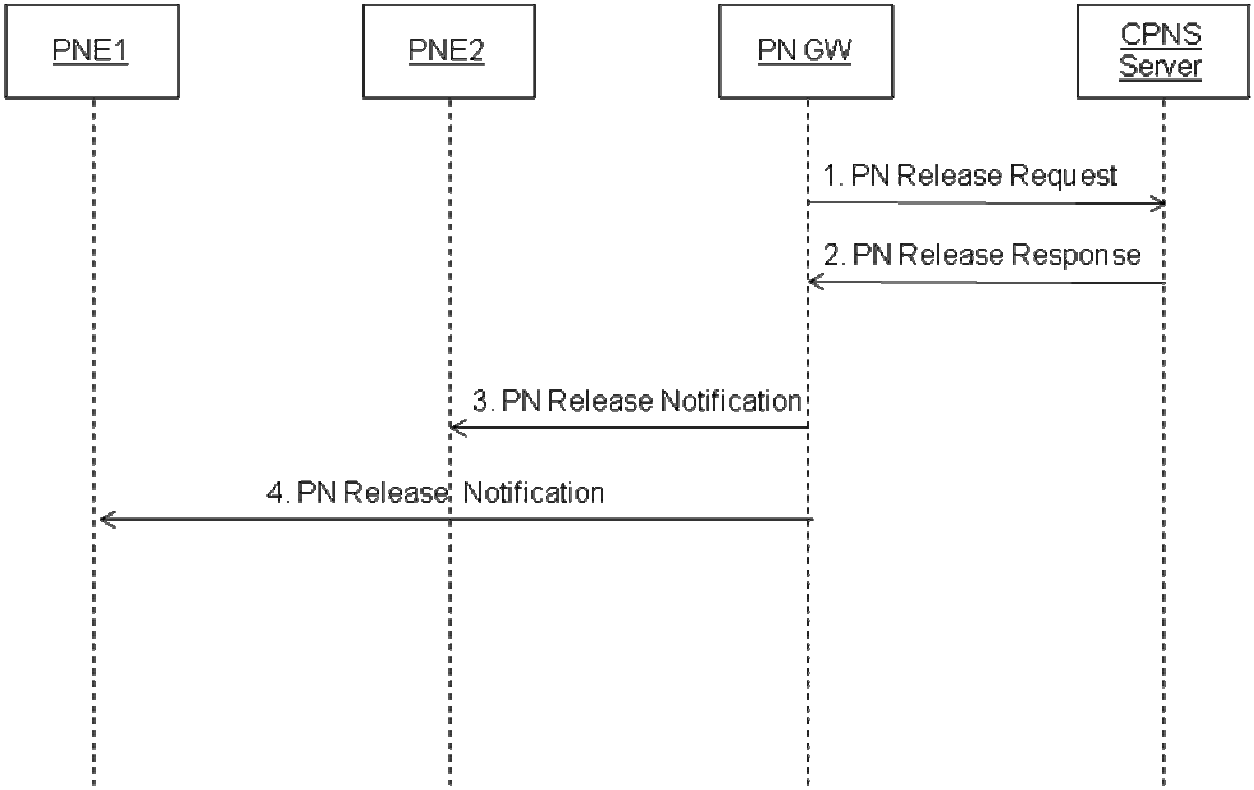


Figure 18 PN Release initiated by PN GW

1. PN GW sends PN Release Request to CPNS Server.
2. CPNS Server removes local PN Inventory and then sends PN Release Response to PN GW.
3. PN GW sends PN Release Notification to the PNE2.
4. PN GW sends PN Release Notification to the PNE1.

6.6.3.2 Initiated by PNE

Figure 19 shows a flow of PN Release which is initiated by PNE.

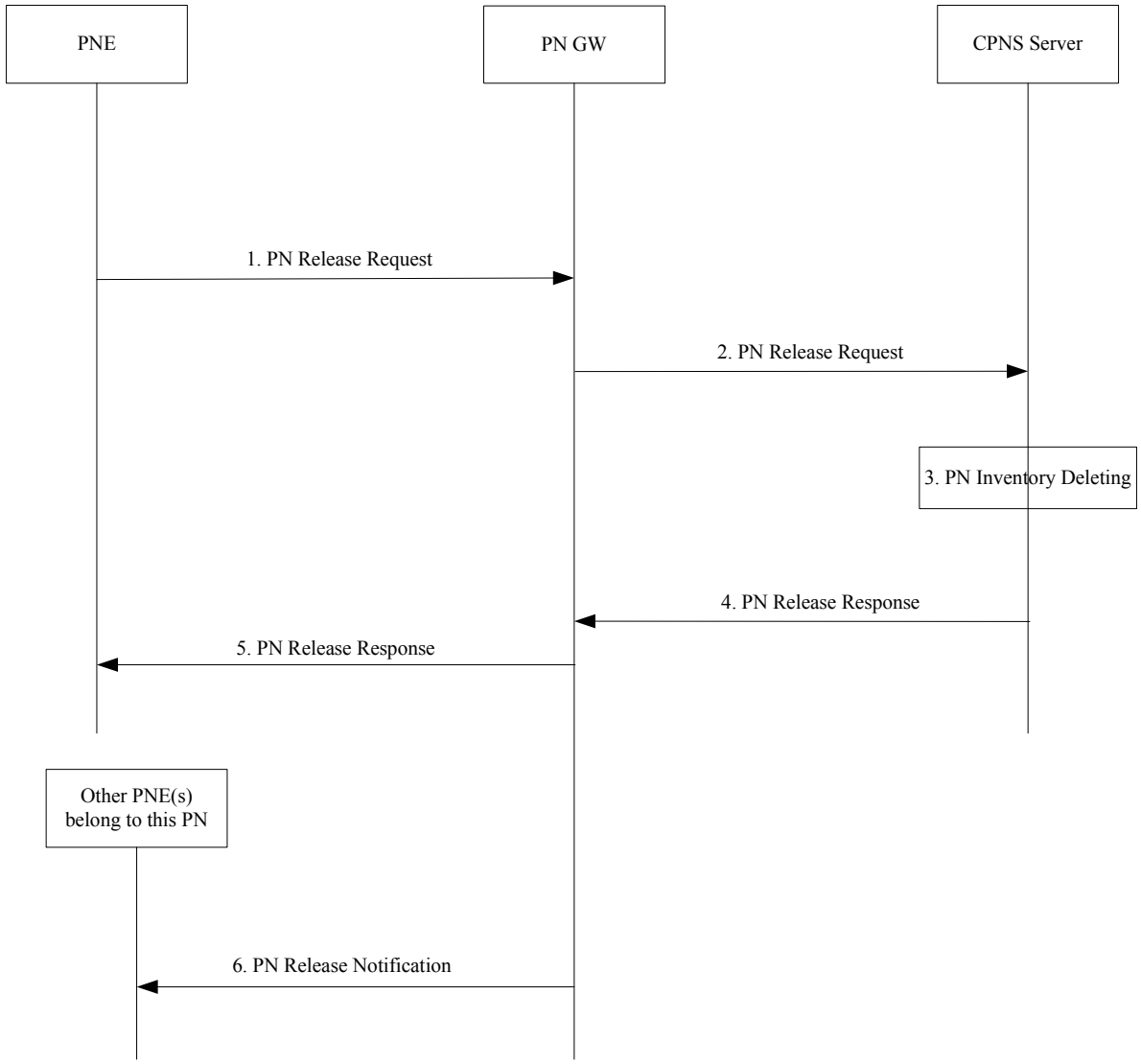


Figure 19 Flow of PN Release Initiated by PNE

1. The PNE sends PNReleaseRequest message to the PN GW.
2. The PN GW sends PNReleaseRequest message to the CPNS Server.
3. The CPNS Server deletes the PN Inventory which the PN GW requests.
4. The CPNS Server sends the PNReleaseResponse message to the PN GW.
5. The PN GW sends the PNReleaseResponse message to the PNE.
6. The PN GW notifies PN is released to other PNE(s) belong to this PN.

6.7 Service Publication & Discovery

6.7.1 ServiceDescriptionRegistration flow

Following figure shows high level ServiceDescriptionRegistration flow.

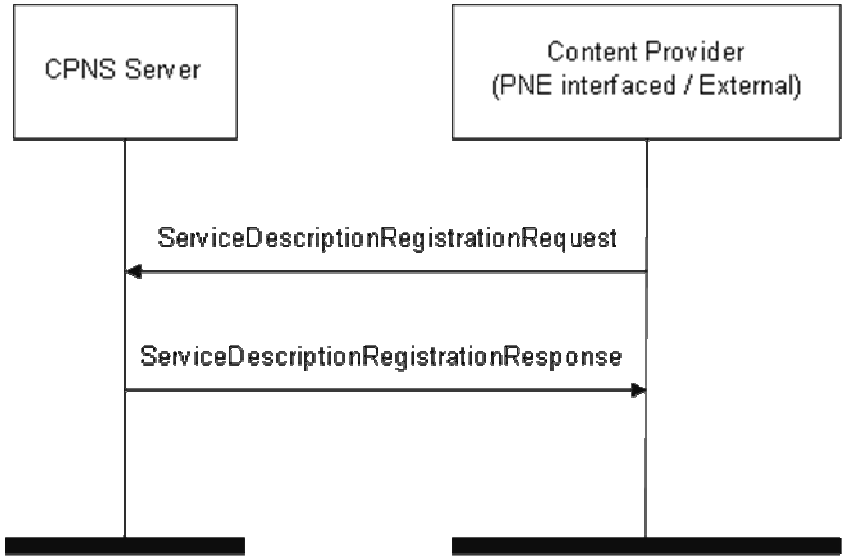


Figure 20 ServiceDescriptionRegistration flow

1. The Content Provider sends ServiceDescriptionRegistrationRequest message with Service Description to CPNS Server to publish the Service Description.
2. The CPNS Server stores the received Service Description and sends back the ServiceDescriptionRegistrationResponse to the content provider with result (e.g., success or failure).

6.7.2 ServiceDiscoveryRequest/Response flow

Following figure presents high level ServiceDiscoveryRequest / Response flow.

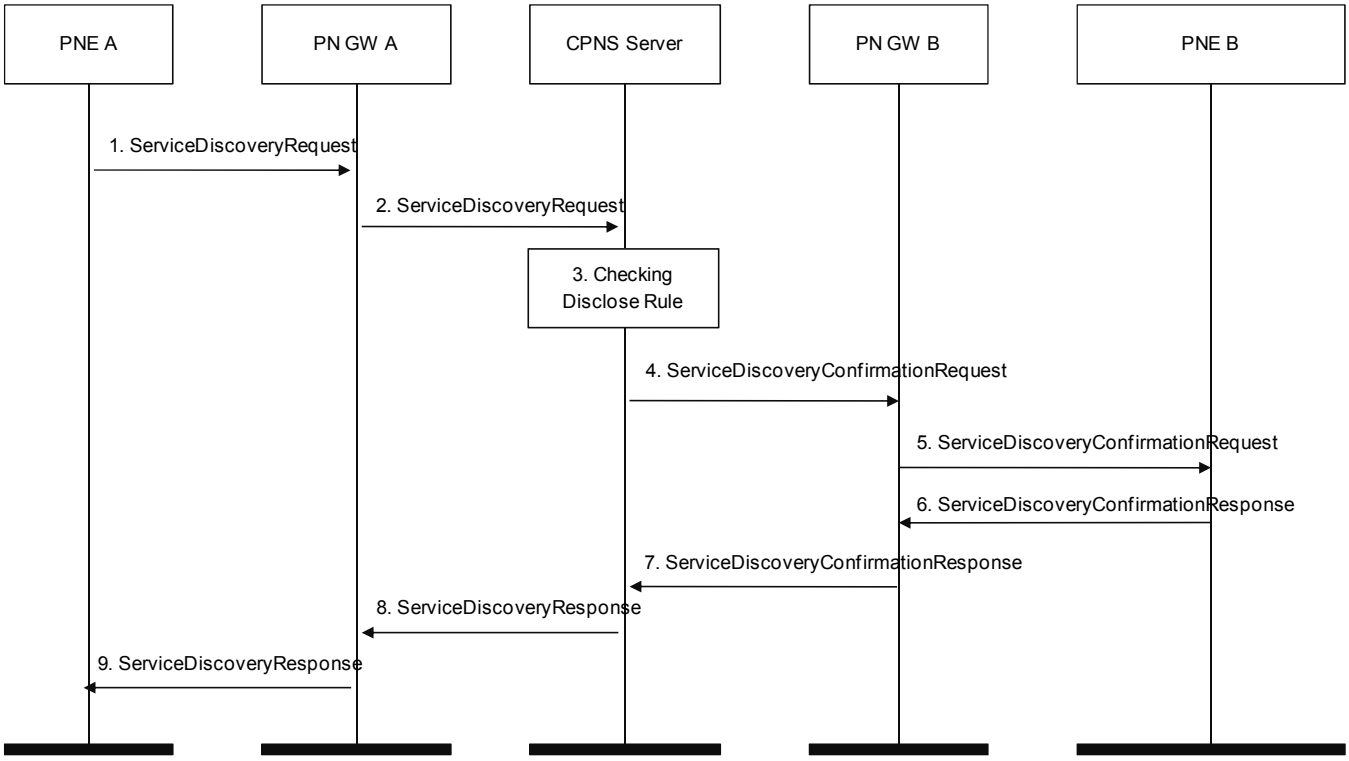


Figure 21 ServiceDiscoveryRequest/Response flow

1. The PNE A sends a ServiceDiscoveryRequest to the PN GW A with or without searching condition, Keyword or PNEID.

2. The PN GW A relays the ServiceDiscoveryRequest to the CPNS Server.

3. The CPNS Server checks the configuration of willingness to open Service / Conten Info in of PN Inventory corresponding to the PNEID. If the configuration sets open to deliver Service/Content information in PN Inventory, the CPNS Server may send ServiceDiscoveryResponse to the PN GW A.

   When the ServiceDiscoveryRequest contains searching condition and there are no Operator Policies, the CPNS Server performs searching based on the request and composes search results and sends the ServiceDiscoveryResponse with composed Service Description to the PN GW. If no match is found, then the CPNS Server sends the ServiceDiscoveryResponse with no Service Description to the PN GW.

   When the ServiceDiscoveryRequest contains searching condition and there are Operator Policies, the CPNS Server finds the Service Description based on the search and on policies (e.g., Operator Policy) and sends the ServiceDiscoveryResponse to the PN GW with the Service Description

   When the ServiceDiscoveryRequest contains no searching condition, but there are Operator Policies, the CPNS Server finds the Service Description based on policies (e.g., Operator Policy) and sends the ServiceDiscoveryResponse to the PN GW with the Service Description.

   Note: The definition and procedure of managing (e.g., registering, updating, and so on) the Operator Policy is out of scope of CPNS Enabler.

   When the ServiceDiscoveryRequest contains no searching condition and there are no Operator Policies, but the request is for all available services, the CPNS Server identifies all the available Service Descriptions and sends them through the ServiceDiscoveryResponse to the PN GW.

   In all other cases, the CPNS Server sends ServiceDiscoveryResponse with no Service Description. In this case, the step 4 – 7 will be skipped. In addition, if the source of discovered service/content is an external Service/Content Provider, the step 4-7 will be skipped.

   If the configuration sets block to deliver Service/Content information in PN Inventory, the CPNS Server sends ServiceDiscoveryResponse with no Service Description to the PN GW.

   If the configuration sets necessity of confirmation, then CPNS Server sends the ServiceDiscoveryConfirmationRequest to the authorized CPNS Entity, which the CPNS User configured.

4. The CPNS Server sends ServiceDiscoveryConfirmationRequest to the PN GW B.

5. If the OwnershipEntityID is PN GW B, then step 6 and 7 are skipped. Otherwise, PN GW B relays Service DiscoveryConfirmationRequest to the PNE B.

6. The PNE B sends ServiceDiscoveryConfirmationResponse to the PN GW B.

7. The PN GW B sends ServiceDiscoveryConfirmationResponse to the CPNS Server.

8. The CPNS Server sends the ServiceDiscoveryResponse to the Service Discovery request to PN GW A.

9. The PN GW A relays the ServiceDiscoveryResponse to the PNE A.

6.7.3 ServiceDescriptionAdvertise flow

Following figure presents high level ServiceDescriptionAdvertise flow.

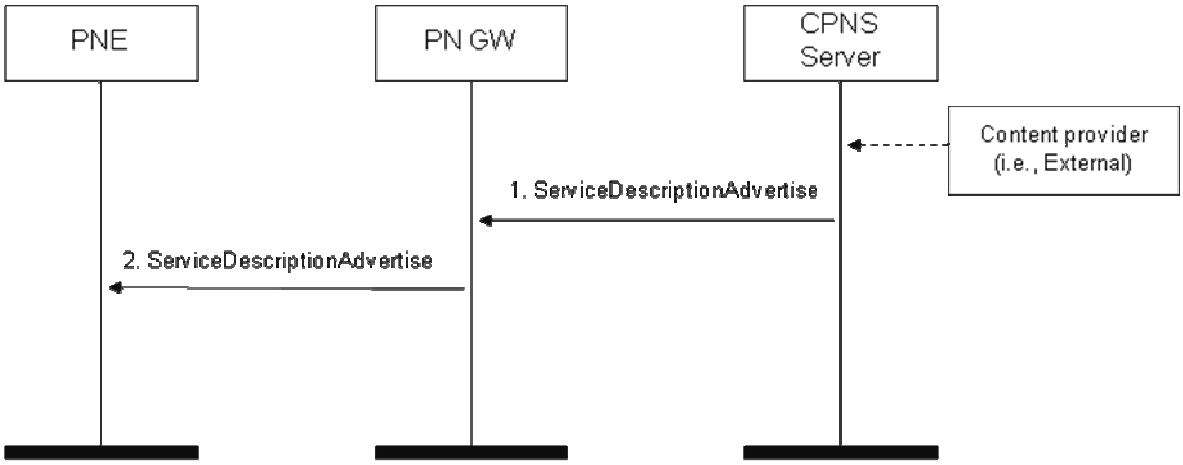


Figure 22 ServiceDescriptionAdvertise flow

1. The CPNS Server sends ServiceDescriptionAdvertise to the PNE via PN GW.
2. The PN GW relays the ServiceDescriptionAdvertise to the PNE.

6.8 Service Group Management

6.8.1 Create Service Group

This section describes general flows of Service Group management.

PNE creating a Service Group initially becomes a SG Owner.

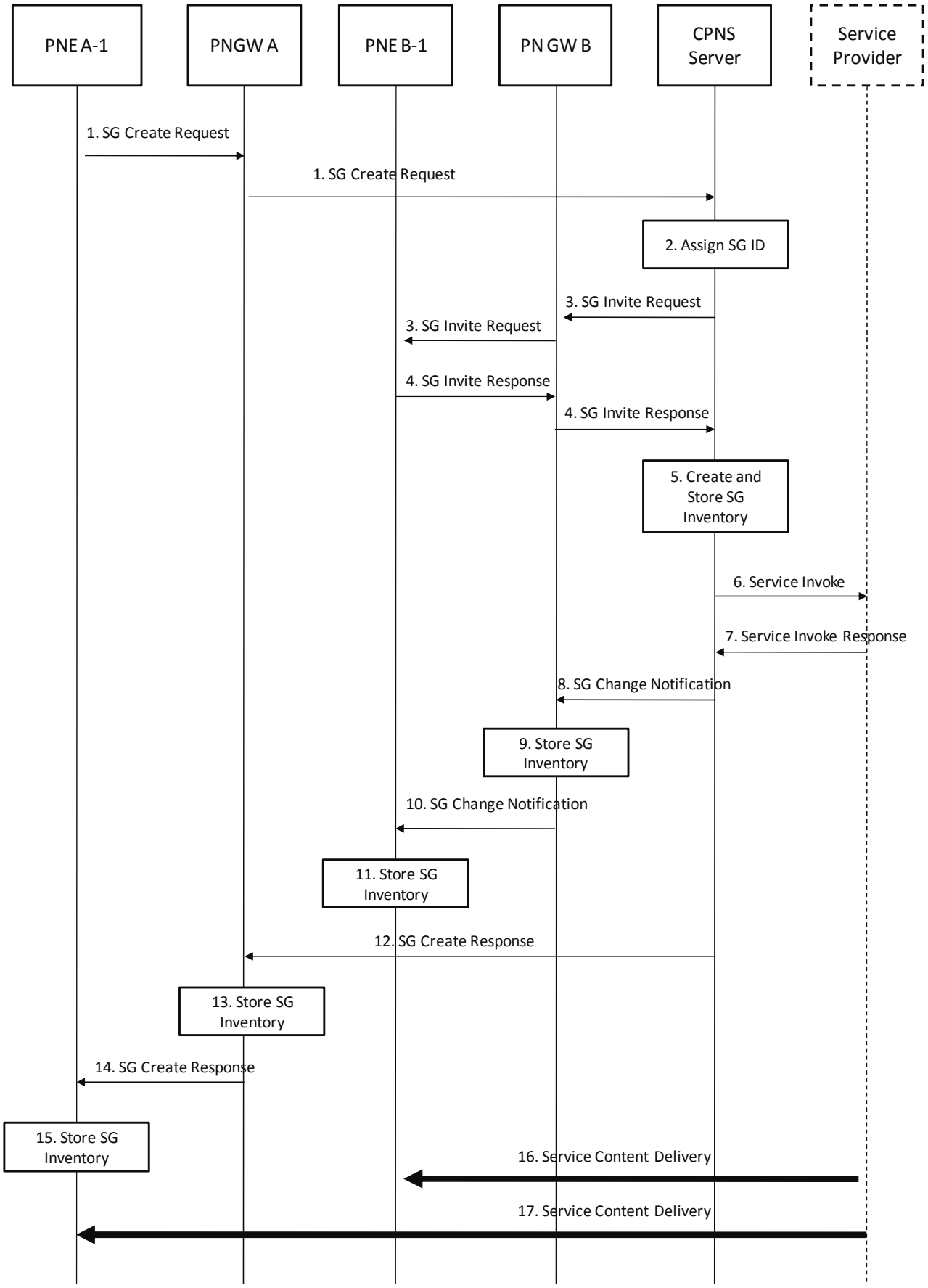


Figure 23 Flow of Service Group creation

Figure 23 shows a flow of Service Group (SG) creation.

In this figure, PNE A-1 initiates to create a new Service Group.

In order to create Service Group, the PNE A-1 needs to choose a specific service among list of services from received Service Group Advertisement.

1. PNE A-1 sends a SG Create Request message to PN GW A with information of PNE A-1's PNEID, SG description and PNE B-1's PNEID(s) as invitee PNE. PN GW A forwards the request to CPNS Server.

   The SG Creation Request message contains;

   - Service indication to be shared with other service group members
   - Optionally, PNEID(s)

   NOTE: If the SG Creation Request does NOT include PNEID(s), then steps from 3 to 9 are skipped.

2. CPNS Server assigns SGID.
3. CPNS Server sends SG invite request to PN GW B which forwards the request to PNE B-1.

   The SG Invite Request message contains;

   - Service indication to be shared with other service group members

4. PNE B-1 sends SG invite response to PN GW B which forwards the response to CPNS Server.
5. CPNS Server creates and stores SG Inventory which may include SGID, SG description, Service indication and PNEID(s) registered in Step.1 etc. If steps 3 and 4 are performed, CPNS Server adds information of PNE B-1 in SG Inventory. Then, CPNS Server creates Group Key and delivers the Group Key to PNE A-1 and PNE B-1 (7.8.1).
6. The CPNS Server verifies Service indication, requests the service and notifies to Service Provider to be chosen based on the Service indicationand shared, that a Service group is created.

   SG Creation NotificationService Invoke message contains;

   - Service Group Member information

7. The CPNS Server receives the response from 3rd Party Service Provider.
8. CPNS Server sends a SG Change Notification to PN GW B.
9. PN GW B stores a list of PNEs, which join the Service Group and managed by this PN GW in PN, according to SG Inventory (i.e., in this case PNE B-1).
10. PN GW B forwards the SG Change Notification to PNE B-1.
11. PNE B-1 stores SG Inventory locally
12. CPNS Server sends a SG Create Response message to PN GW A.
13. PN GW A stores a list of PNEs, which join the Service Group and managed by this PN GW in PN, according to SG Inventory.
14. PN GW A forwards the SG Create Response message to PNE A-1.
15. PNE A-1 stores SG Inventory locally.
16. PNE B-1 receives the service or content provisioned by Service Provider.

17. PNE A-1 receives the service or content provisioned by Service Provider.

6.8.2 Invite Service Group member by PNE

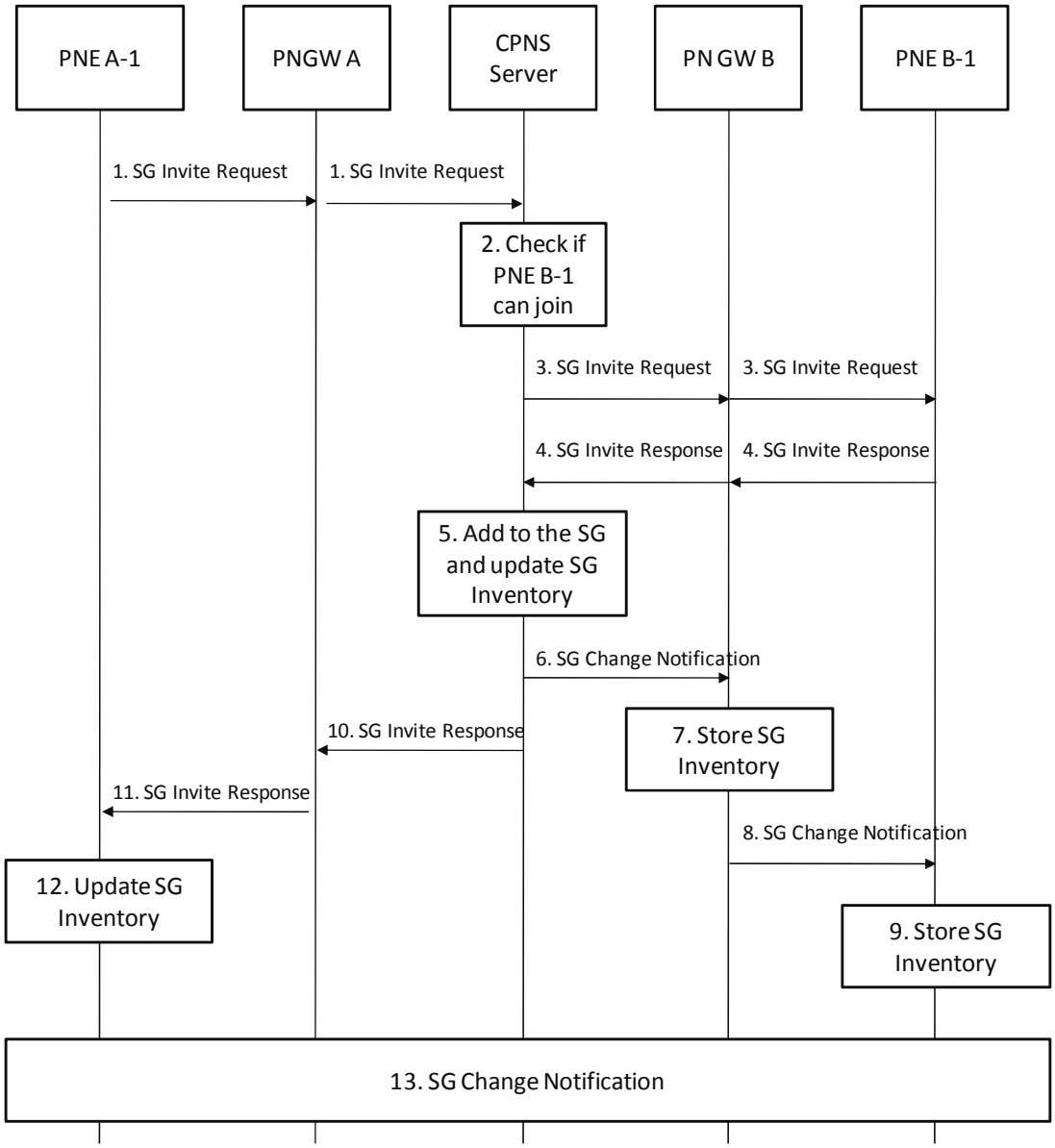


Figure 24 Flow of member invite by PNE

Figure 24 shows a flow of member invite. In this figure, PNE A-1 invites PNE B-1 to an exisiting Service Group.

1. PNE A-1 sends a SG invite request to PN GW A which forwards the request to CPNS Server.
2. CPNS Server checks if PNE B-1 can join the SG according to PNEID of PNE B-1 under PNEID(s) registered in SG creation.
3. If PNE B-1 is permitted to join SG, CPNS Server sends the SG invite request to PN GW B which forwards the request to PNE B-1.

4. PNE B-1 sends a SG invite response to PN GW B which forward the response to CPNS Server.
5. CPNS Server adds information of PNE B-1 in SG Inventory. Then, CPNS Server delivers Group Key to PNE B-1. (7.8.5).
6. CPNS Server sends a SG Change Notification to PN GW B.
7. PN GW B stores a list of PNEs, which join the Service Group and managed by this PN GW in PN, according to SG Inventory (i.e., in this case PNE B-1).
8. PN GW B forwards the SG Change Notification to PNE B-1.
9. PNE B-1 stores SG Inventory locally.
10. CPNS Server sends the SG invite response to PN GW A.
11. PN GW A forwards the SG invite response to PNE A-1.
12. PNE A-1 updates SG Inventory locally.
13. CPNS Server delivers the SG Change Notification to member PNEs. This flow is provided as another flow.

6.8.3 Expel Service Group Member

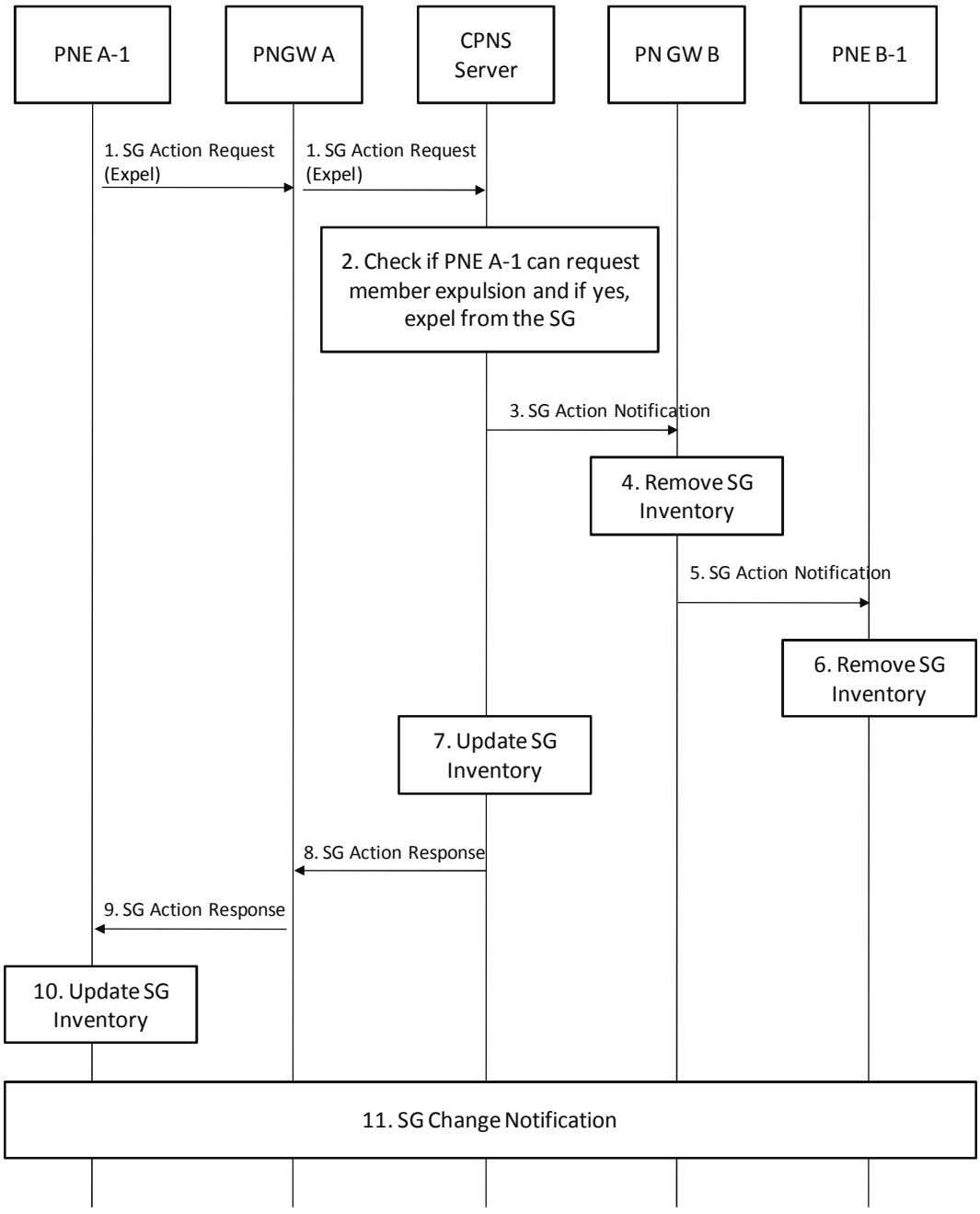


Figure 25 Flow of member expulsion

Figure 25 shows a flow of member expulsion. In this figure, if PNE A-1 is a SG Owner of Service Group, it can request expulsion of PNE B-1 from the Service Group.

1. PNE A-1 sends a SG Action Request (Expel) for PNE B-1 to PN GW A which forwards the request to CPNS Server.
2. CPNS Server checks if PNE A-1 (e.g. SG Owner) has the authority to request member expulsion of SG
3. If the PNE A-1 is permitted to expel the PNE B-1, CPNS Server sends the SG Action Notification to PN GW B. Then, CPNS Server updates Group Key and delivers the Group Key to PNE A-1 (7.8.2)

4. PN GW B removes a list of PNEs which join the Service Group and managed by this PN GW in PN since PNE B-1, which is only one member of Service Group in PN, is expelled from Service Group.
5. PN GW B forwards the SG Action Notification to PNE B-1.
6. PNE B-1 removes SG Inventory and deletes Group Key (7.8.3) locally.
7. After step 3, CPNS Server deletes information of PNE B-1 from SG Inventory.
8. CPNS Server sends the SG Action Response to PN GW A.
9. PN GW A forwards the SG Action Response to PNE A-1.
10. PNE A-1 updates SG Inventory locally.
11. CPNS Server delivers the SG Change Notification to member PNEs. This flow is provided as another flow.

6.8.4 Join Service Group

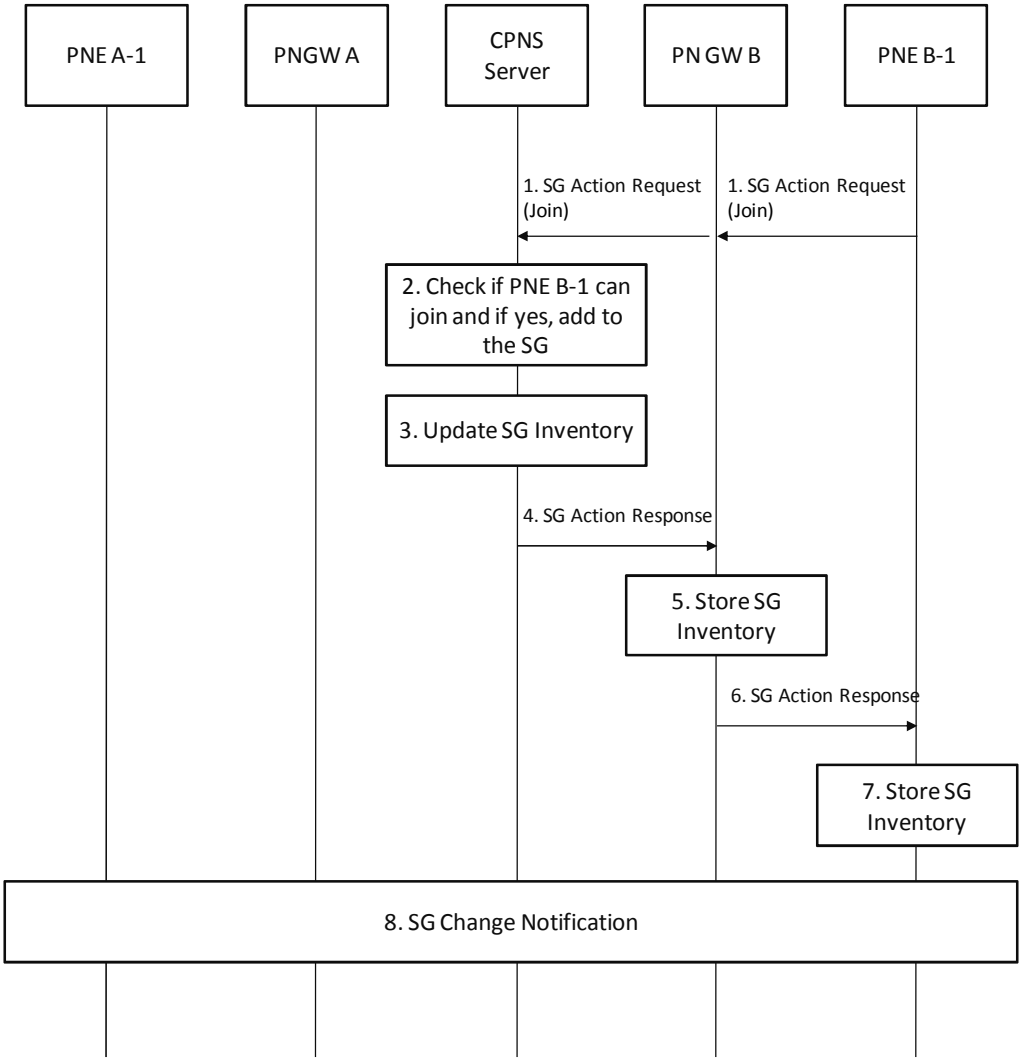


Figure 26 Flow of member join

Figure 26 shows a flow of member join. In this figure, PNE B-1 joins Service Group to which PNE A-1 belongs.

1. PNE B-1 sends a SG Action Request (Join) to PN GW B which forwards the request to CPNS Server.

2. CPNS Server checks if PNE B-1 can join the SG according to PNEID of PNE B-1 under PNEID(s) registered in SG creation.

3. If PNE B-1 is permitted to join SG, CPNS Server adds information of PNE B-1 in SG Inventory. Then, CPNS Server delivers Group Key to PNE B-1 (7.8.5).

4. CPNS Server sends a SG Action Response to PN GW B.

5. PN GW B stores a list of PNEs, which join the Service Group and managed by this PN GW in PN, according to SG Inventory.

6. PN GW B forwards the SG Action Response to PNE B-1.

7. PNE B-1 stores SG Inventory locally.

8. CPNS Server delivers the SG Change Notification to member PNEs in this case PNE A-1. This flow is provided as another flow.

6.8.5 Leave Service Group

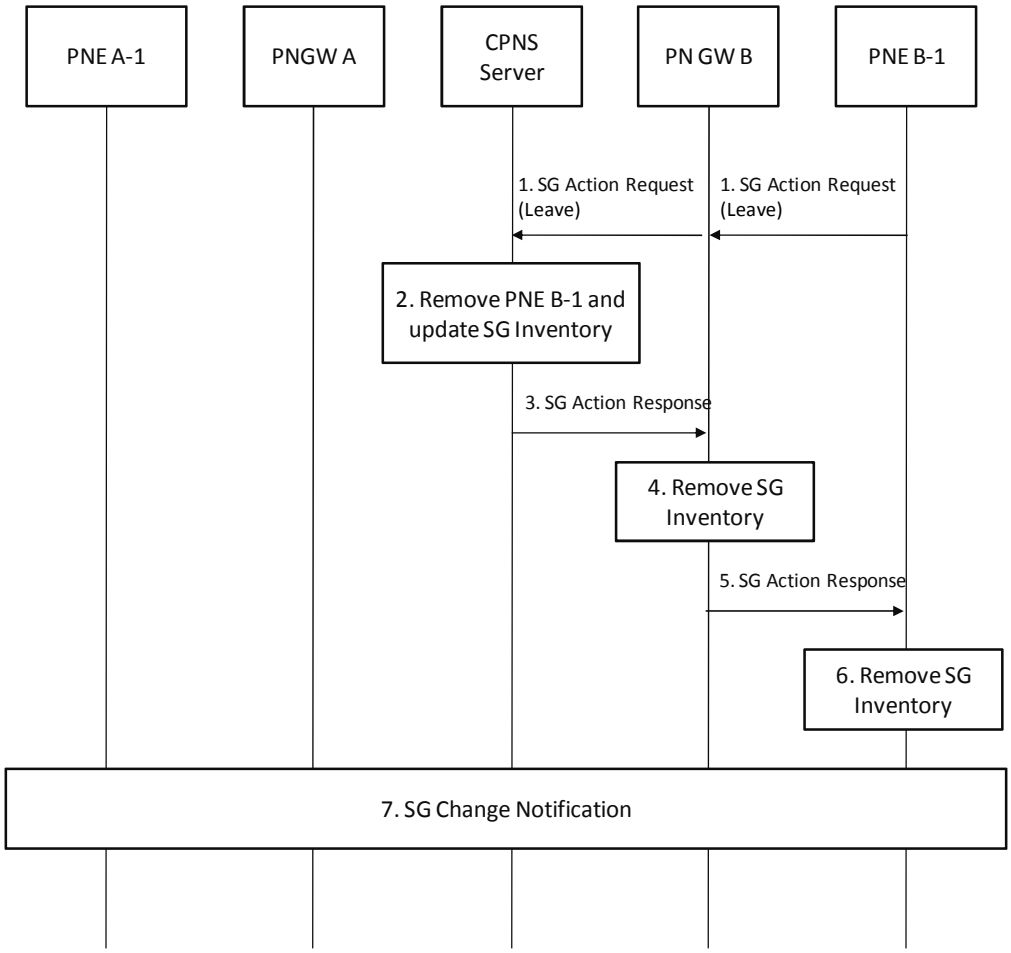


Figure 27 Flow of member leave

Figure 27 shows a flow of member leave. In this figure, PNE B-1 leaves Service Group to which PNE A-1 and PNE B-1 belongs.

1. PNE B-1 sends a SG Action Request (Leave) to PN GW B which forwards the request to CPNS Server.

2. CPNS Server deletes information of PNE B-1 from SG Inventory. Then, CPNS Server updates Group Key and delivers the Group Key to PNE A-1 (7.8.2).
3. CPNS Server sends a SG Action Response to PN GW B
4. PN GW B removes a list of PNEs which join the Service Group and managed by this PN GW in PN.
5. PN GW B forwards the SG Action Response to PNE B-1.
6. PNE B-1 removes SG Inventory and deletes Group Key (7.8.3) locally.
7. CPNS Server delivers the SG Change Notification to member PNEs in this case PNE A-1. This flow is provided as another flow.

6.8.6 Delete Service Group

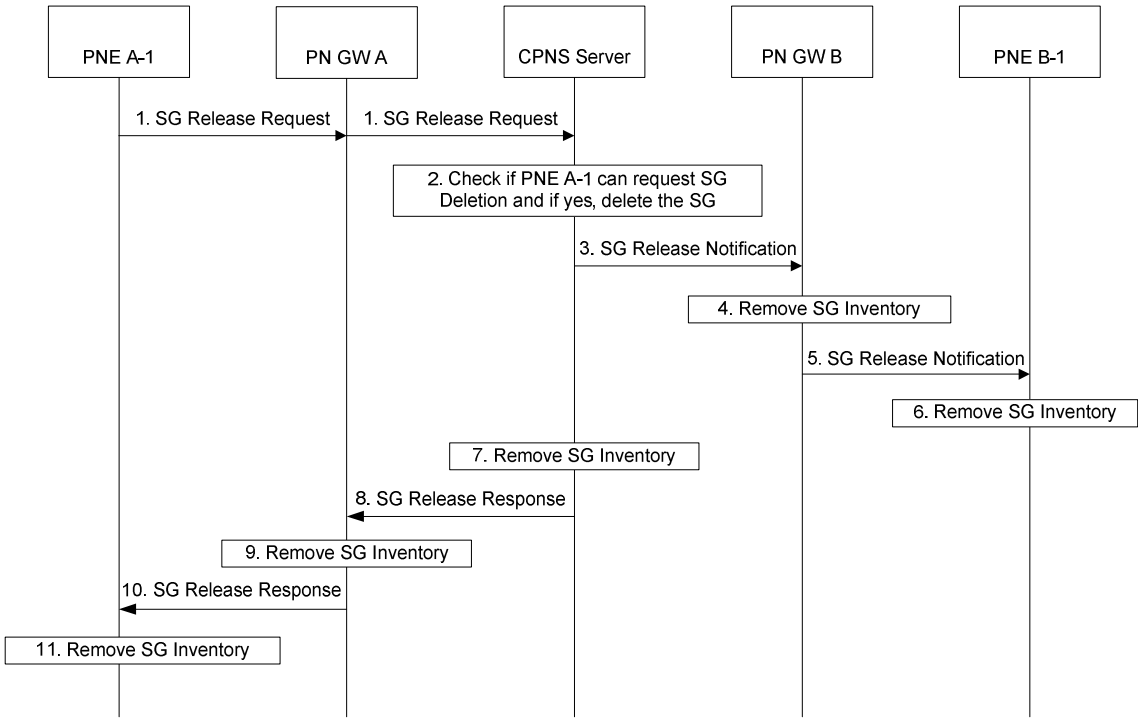


Figure 28 Flow of Service Group delete

Figure 28 shows a flow of Service Group deletion. In this figure, if PNE A-1 is a SG Owner of Service Group, it can delete the Service Group to which PNE A-1 and PNE B-1 belong.

1. PNE A-1 sends a SG Release Request to PN GW A which forwards the request to CPNS Server.
2. CPNS Server checks if PNE A-1 (e.g. SG Owner) has the authority to request Service Group deletion
3. If PNE A-1 is permitted to delete SG, CPNS Server sends a SG Release Notification to PN GW B. This flow should be done all PN GWs which connect to member PNEs in SG. Then, CPNS Server deletes Group Key (7.8.3).
4. PN GW B removes a list of PNEs which join the Service Group and managed by this PN GW in PN.
5. PN GW B forwards the SG Release Notification to PNE B-1.
6. PNE B-1 removes SG Inventory and deletes Group Key (7.8.3) locally.
7. After step 3, CPNS Server deletes SG Inventory.

8. CPNS Server sends a SG Release Response to PN GW A.
9. PN GW A removes a list of PNEs which join the Service Group and managed by this PN GW in PN.
10. PN GW A forwards the SG Release Response to PNE A-1.
11. PNE A-1 removes SG Inventory and deletes Group Key (7.8.3) locally

6.8.7 Notify membership change to member PNE(s)

When membership of SG changes, CPNS Server notifies it to member PNE(s). This flow may be performed at the events of member invite/expel and member join/leave.

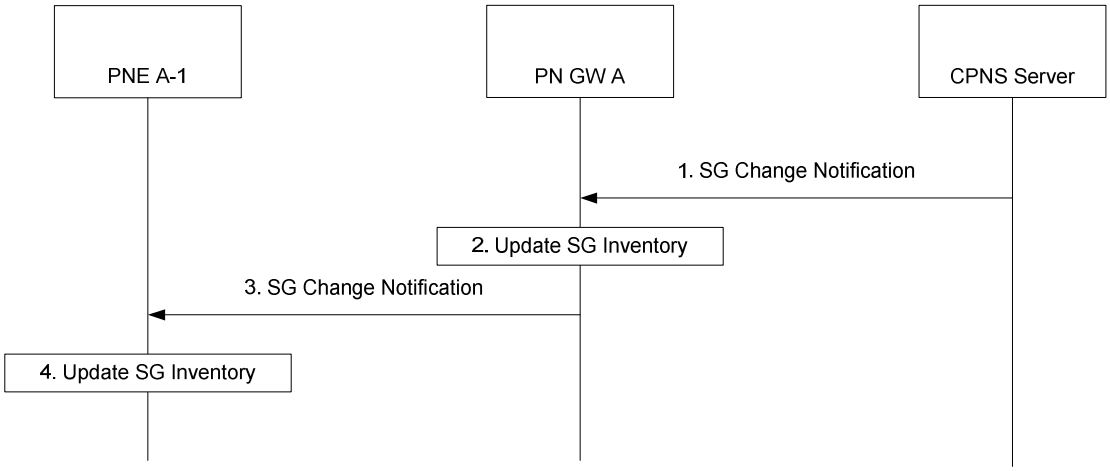


Figure 29 Flow of SG member change notification

Figure 29 shows a flow of SG member change notification. In this figure, CPNS Server notifies SG member change notification to PNE A-1.

1. When membership of SG changes, CPNS Server sends a SG Change Notification to PN GW A.
2. PN GW A updates a list of PNEs which join the Service Group and managed by this PN GW in PN if the SG member change notification indicates that PNE residing in PN join or leaves the Service Group.
3. PN GW A delivers the SG Change Notification to member PNEs connected to PN GW A in this case PNE A-1.
4. PNE A-1 updates SG Inventory locally.

6.8.8 Transfer of Service SG Owner

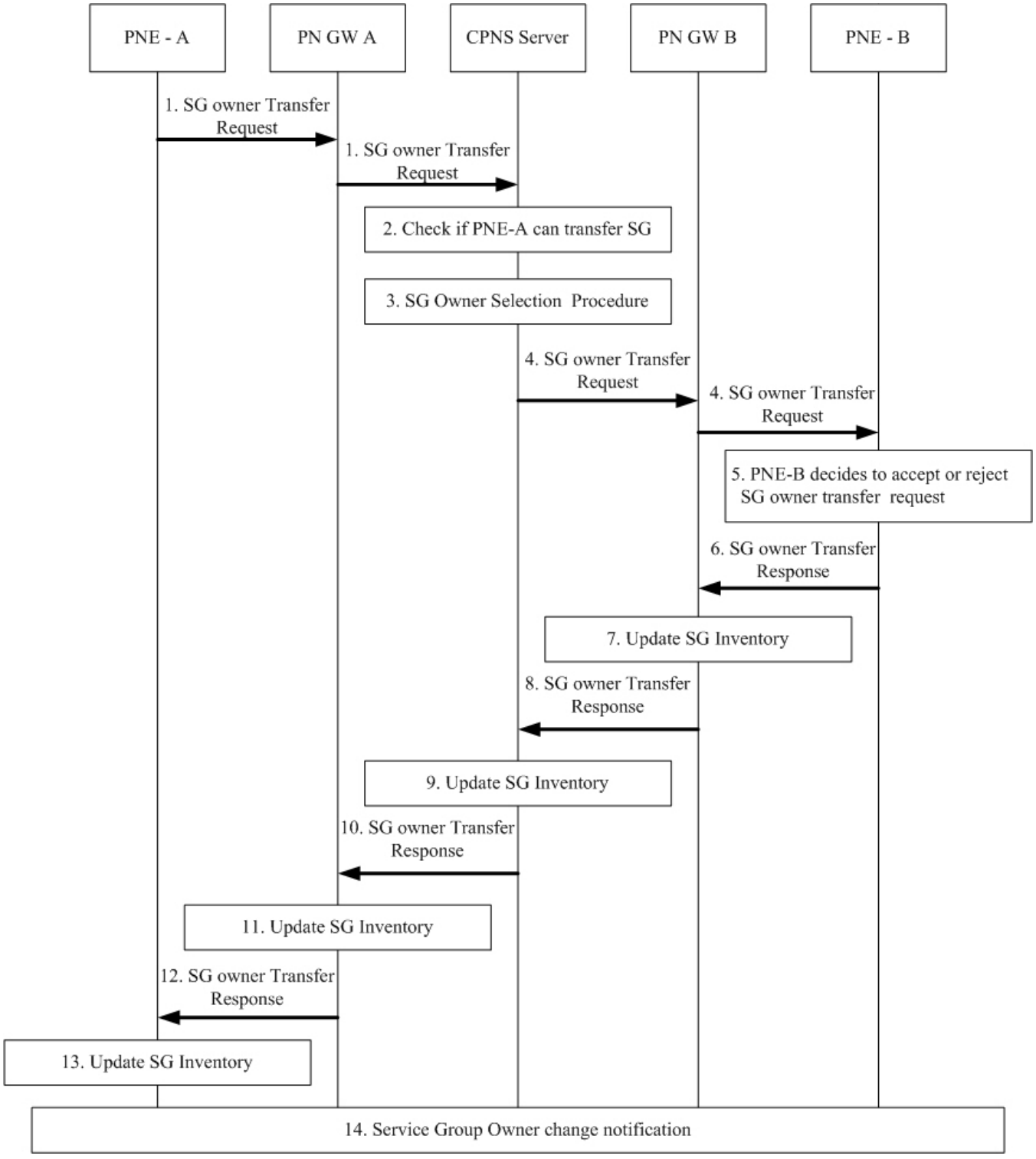


Figure 30 Flow of Service SG Owner Transfer

Figure 30 shows a flow of SG Owner Transfer. In this figure, if PNE A-1 is a SG Owner of SG, it can transfer SG Owner to PNE B-1 from the SG.

1. PNE A-1 sends a SG Owner Transfer request to PN GW A which forwards the request to CPNS Server.
2. CPNS Server checks if PNE A-1 has the authority to transfer SG Owner (e.g. SG Owner).If Yes, then continue to step 3.
3. Based on device capabilities, service description, Operator Policy of CPNS Server or the request (or suggestion) of the original SG owner (PNE A-1), PNE-B1 is selected as the new SG Owner, and the ownership is transferred from PNEA-1 to PNE B-1.
4. CPNS Server sends the SG Owner Transfer Request to PN GW B and forwards SG Owner Transfer Request to PNE B-1
5. PNE B-1 can decide to accept or reject the SG Owner Transfer Request.
6. If PNE B-1 accepts it, PNE B-1 sends SG Owner Transfer Response with positive confirmation to PN- GW B. If PNE B-1 rejects it, PNE B-1 sends SG Owner Transfer Response with negative confirmation to PN- GW B

NOTE: In step5 if PNE-B rejects to be a SG owner, all the following steps 7, 9, 11 and 13 of "Update SG Inventory" will not be performed. And PNE-A will remain as a SG owner.

7. With the SG Owner Transfer Response with positive confirmation from step6, PN GW B updates SG Inventory locally to indicate new Owner is PNE-B1 instead of PNE A-1.
8. PN GW B forwards the SG Owner Transfer Response to CPNS Server.
9. CPNS Server updates SG Inventory to indicate new Owner is PNE-B1 instead of PNE A-1.
10. CPNS Server forwards the SG Owner Transfer response to PNE GW A.
11. PNE GW A updates SG Inventory locally to indicate new Owner is PNE-B1 instead of PNE A-1.
12. PN GW A sends the SG Owner Transfer response to PNE A-1.
13. PNE A-1 updates SG Inventory to indicate new Owner is PNE-B1 instead of PNE A-1.
14. CPNS Server delivers the SG Owner change notification to member PNEs.

6.8.9 Service Group Query

This section describes general flows of Service Group Query. Service Group List Query procedure is executed to avoid certain circumstances of redundant SG creation and also can be applied when PNE tries to join other SG.

NOTE: If the PNE doesn't know the existence of other SGs, there will be a lot of redundant SGs created, even there are existing SGs available to provide the service that PNE wants to consume.

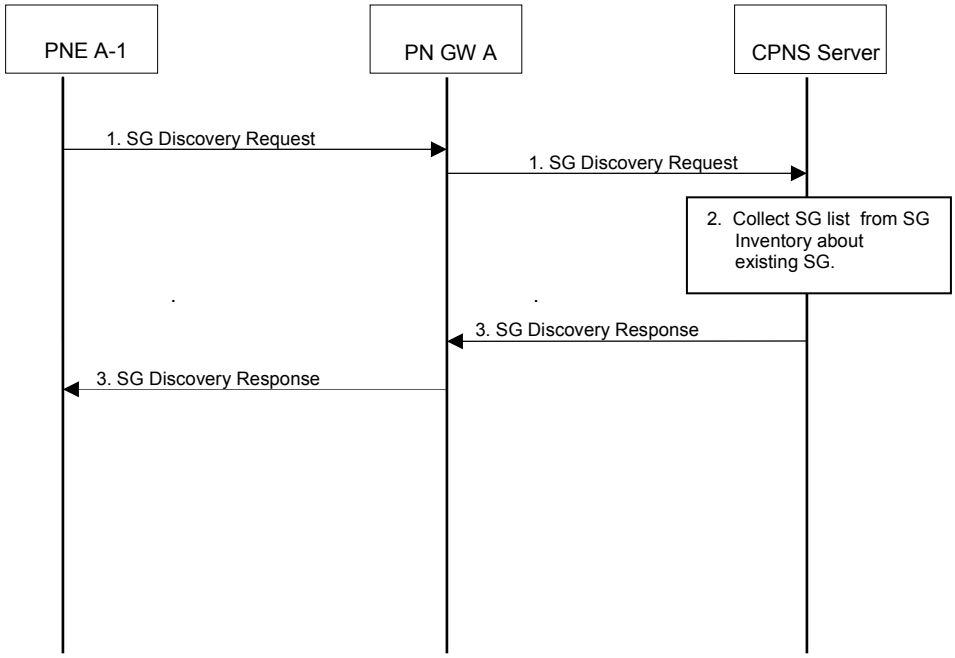


Figure 31 Flow of Service Group List Query

Figure 31 shows a flow of Service Group (SG) List Query procedure.

1. PNE A-1 queries information of current SGs stored in PN-GW or CPNS Server with certain query constraints and parameters, such as specific services, or UserID; or no criteria.

2. CPNS Sever collects SG list from SG Inventory information about existing SG. If there are some private SG and some related information invisible to other PNEs, privacy concern needs to be considered at CPNS Server.

3. CPNS Server responds with the current SG and PN GW forwards this to the PNE.

6.8.10 Service Group Owner Change Notification

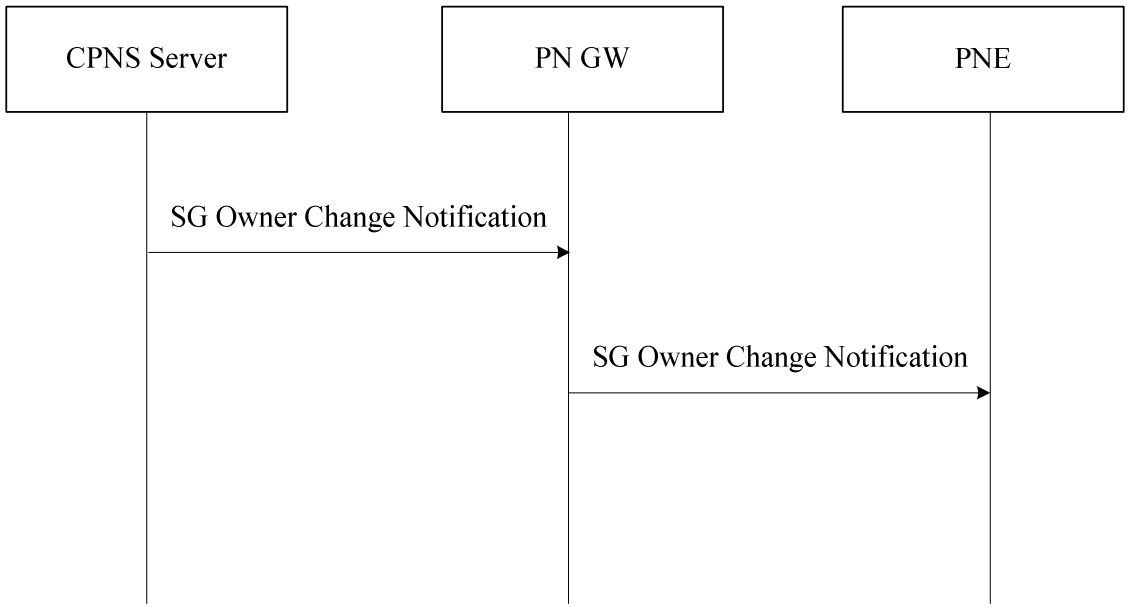


Figure 32 Flow of SG Owner Change Notification

1. CPNS Server sends SG Owner Change Notification to PN GW inside the service group to update
2. PN GW sends SG Owner Change Notification to all PNEs inside the service group to update the latest SG owner.

6.9 Group Key Management

6.9.1 GKDK request

Figure 33 shows a flow of GKDK request, in which a PN GW assigns GKDK to a PNE in the same PN.

This flow is initiated by PNE when the PNE wants to create Service Group or join Service Group or is invited to Service Group. This flow is not performed if GKDK has been already assigned from the PN GW. This flow is performed when PNE detects PN GW supports broadcast group key delivery.

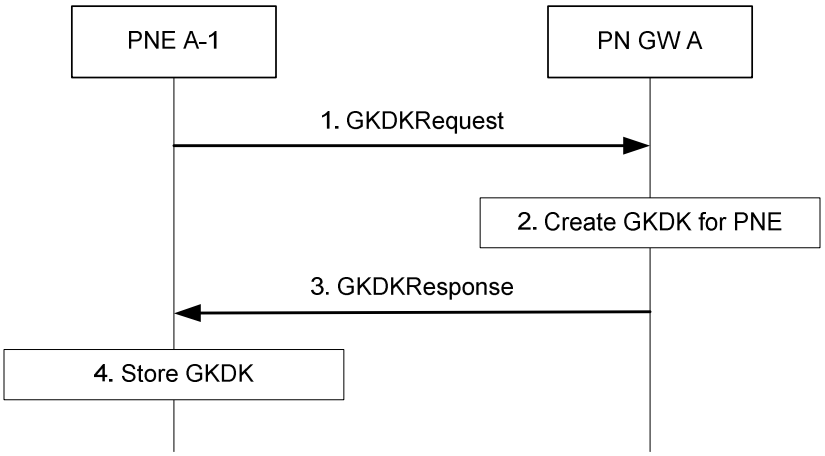
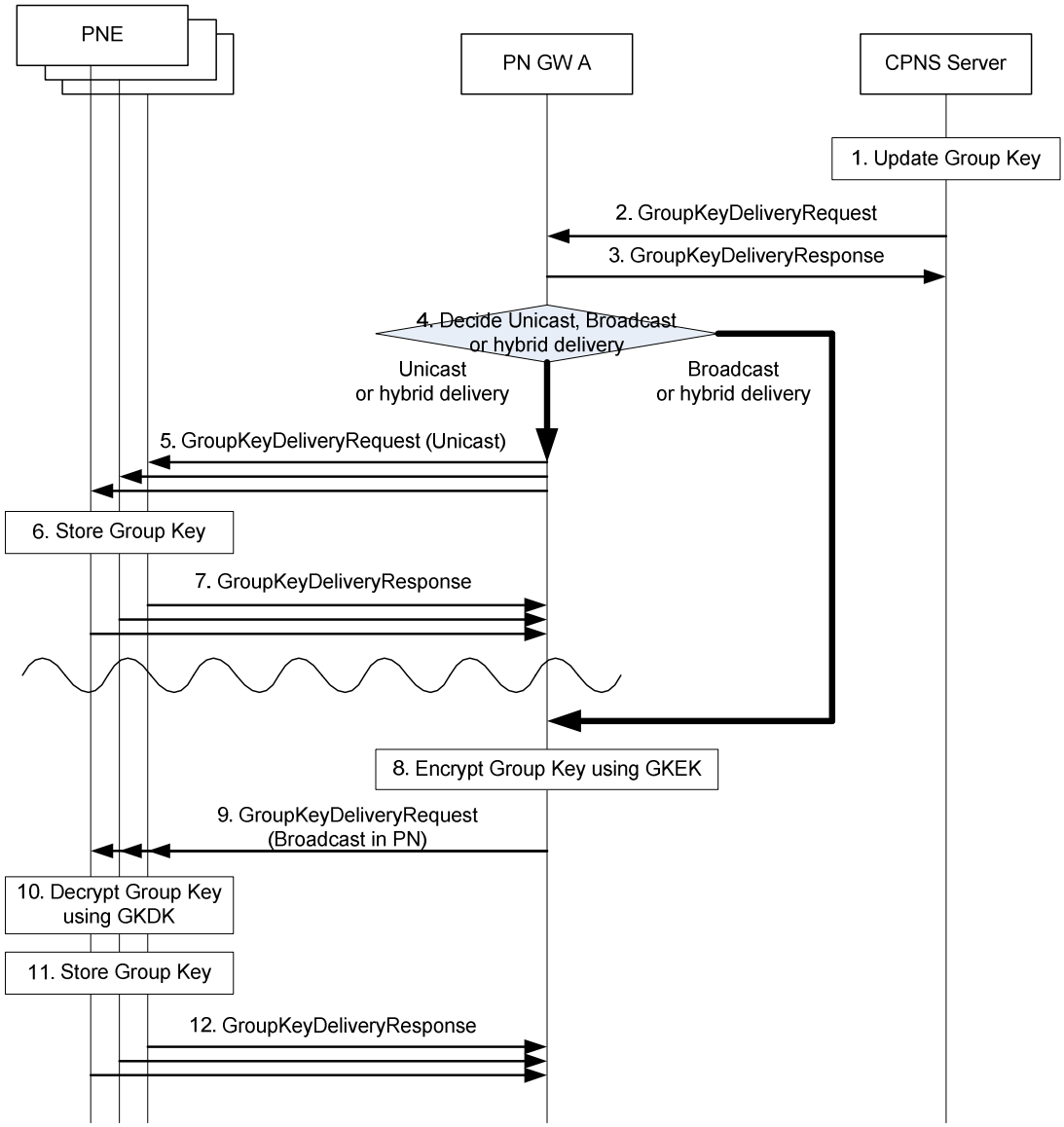


Figure 33 Flow of GKDK request

1. PNE A-1 sends a GKDKRequest message to PN GW A.
2. Upon receiving the GKDKRequest message, PN GW A creates GKDK for PNE A-1.
3. PN GW A sends a GKDKResponse message to PNE A-1 with the created GKDK and stores PNEID of PNE A-1.
4. Upon receiving GKDKResponse message, PNE A-1 stores GKDK.

6.9.2 Group Key delivery

Figure 34 shows a flow of Group Key delivery initiated by update of Group Key. In this figure, Service Group consists of three SG member PNEs which are connected to the same PN GW.



Note that if PN GW selects hybrid delivery in Step 4, Group Key is delivered by Unicast to some PNEs (from Step 6 to 7) and is delivered by Broadcast to other PNEs (from Step 8 to 12).

Figure 34 Flow of Group Key delivery

1. CPNS Server updates a Group Key.
2. After updating a Group Key, CPNS Server sends a GroupKeyDeliveryRequest message to PN GW A with Group Key.
3. Upon receiving the GroupKeyDeliveryRequest message from CPNS Server, PN GW A sends a GroupKeyDeliveryResponse message to CPNS Server.
4. PN GW A chooses a transmission method to deliver Group Key to SG member PNE(s) (i.e., Unicast, Broadcast or hybrid delivery).
   - PN GW A chooses Unicast, Broadcast or hybrid delivery based on certain criteria such as used media as underlying PN, the number of SG member PNE(s) in PN and capability of SG member PNE(s) in PN. In the hybrid delivery, Group Key is delivered to some SG member PNE(s) by Unicast and is delivered to other SG member PNE(s) by Broadcast.

5. If PN GW A chooses Unicast or hybrid delivery in Step 4, PN GW A sends a GroupKeyDeliveryRequest message with Group Key to each SG member PNE by Unicast.
6. Upon receiving the GroupKeyDeliveryRequest message, each PNE stores Group Key.
7. Each PNE sends a GroupKeyDeliveryReponse message to PN GW A.
8. If PN GW A chooses Broadcast or hybrid delivery in Step 4, PN GW A encrypts Group Key using the GKEK.
9. PN GW A broadcasts a GroupKeyDeliveryRequest message in PN with the encrypted Group Key.
10. Upon receiving the GroupKeyDeliveryRequest message, each PNE decrypts Group Key using pre-assigned GKDK.
11. Each PNE stores Group Key.
12. Each PNE sends a GroupKeyDeliveryResponse message to PN GW A.

6.10 Service/Content Delivery

6.10.1 Service/Content Delivery

Following Service/Content Delivery scenarios are identified.

- Service/Content Delivery when content provider is External Entity
- Service/Content Delivery when content provider is PNE, known as Remote PNE connection use-case

6.10.2 Service/Content Delivery flow

Following figure presents high level Service/Content Delivery flow for the scenario where content provider is External Entity.

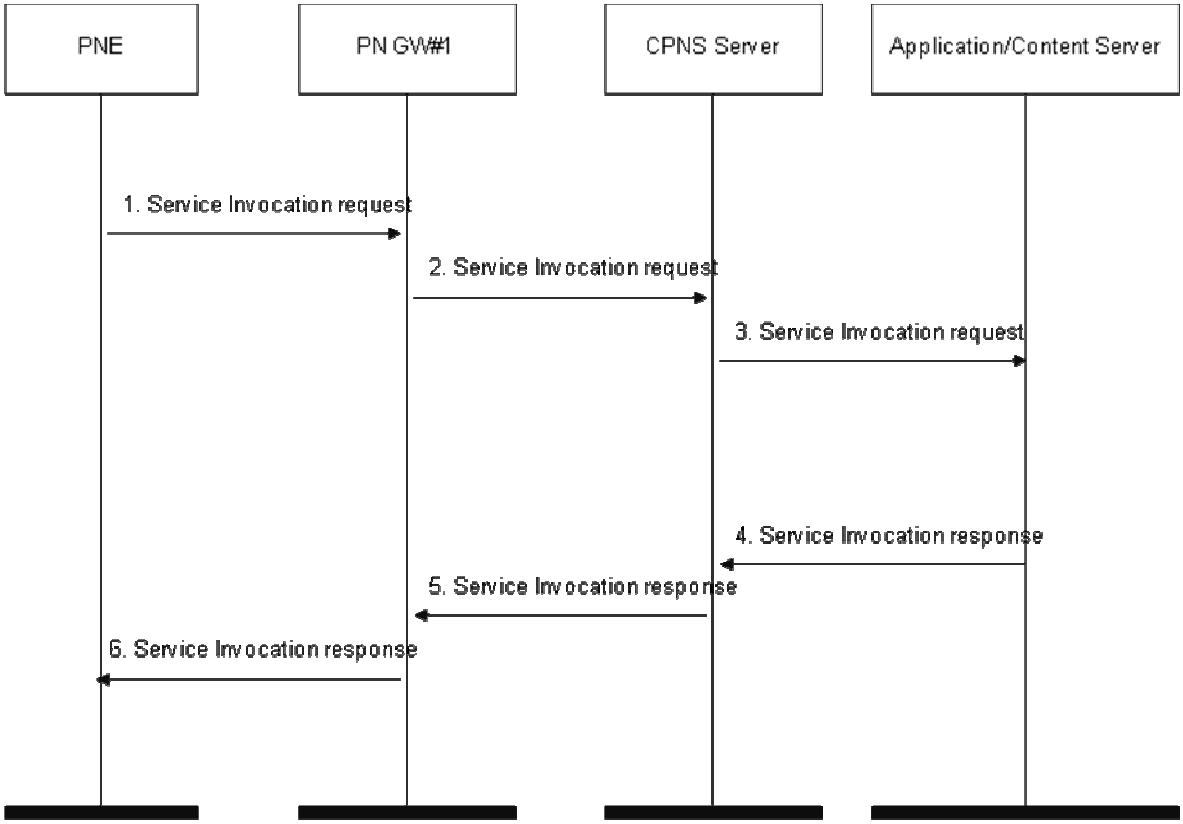


Figure 35 Flow of Service/Content delivery

1. The PNE sends the service invocation request to the PN GW#1 to invoke the service.
2. The PN GW#1 relays the request to the CPNS Server.
3. The CPNS Server relays the request to the Application/Content Server
4. Application/Content Server relays back the response to the CPNS Server
5. The CPNS Server relays back the response to the PN GW#1.
6. The PN GW#1 relays the response to the PNE.

6.10.3 Service/Content Delivery flow-Remote PNE connection

Following figure presents high level Service/Content Delivery flow through CPNS Server for the scenario where content provider is PNE. PN GW#1 is the gateway for service consumer PNE and both reside in same PN. PN GW#2 is the gateway for content provider PNE and both reside in same PN but different from the one PN GW#1 resides in.

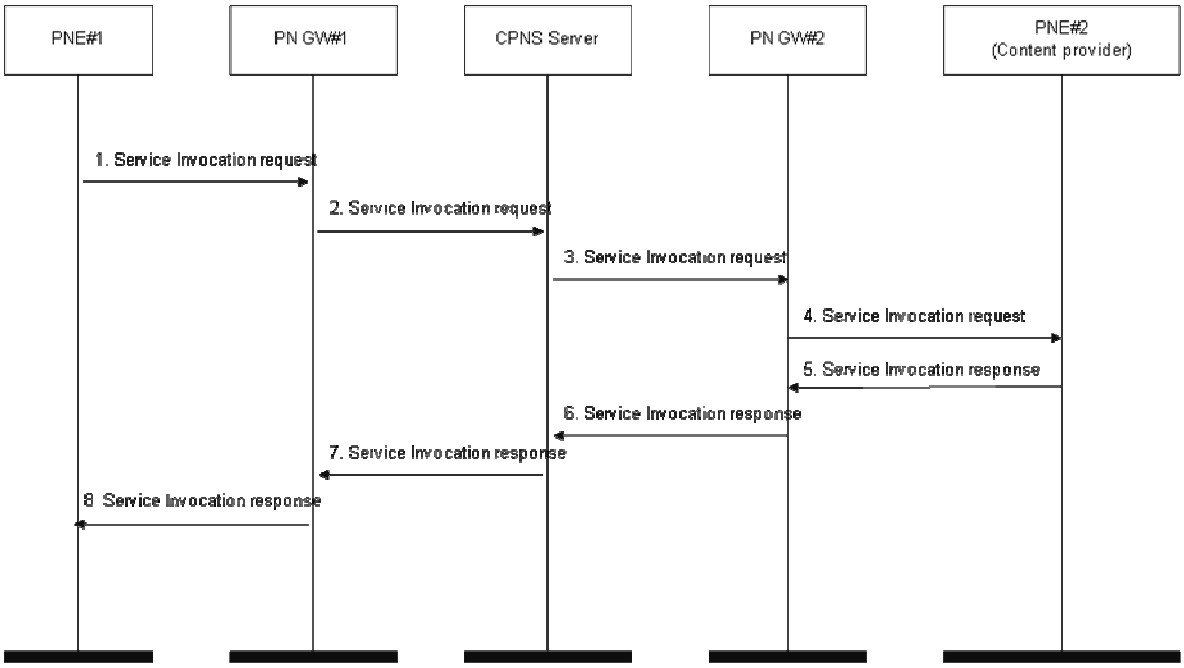


Figure 36 Service/Content Delivery flow-Remote PNE connection through CPNS Server

1. The PNE#1 sends the service invocation request to the PN GW#1 to invoke the service. The request contains information element such as ID of entity hosting service and operation.
2. The PN GW#1 relays the request to the CPNS Server.
3. The CPNS Server relays the request to the PN GW#2.
4. The PN GW#2 relays the request to PNE#2.
5. The PNE#2 sends the response with result of the request and reason of the result (e.g., success or failure) if available to the PN GW#2.
6. The PN GW#2 relays the response to the CPNS Server.
7. The CPNS Server relays the response to the PN GW#1.
8. The PN GW#1 relays the response to the PNE#1.

6.11 Device Capabilities Request and Response

This section describes general flows of Device Capabilities query when applied.

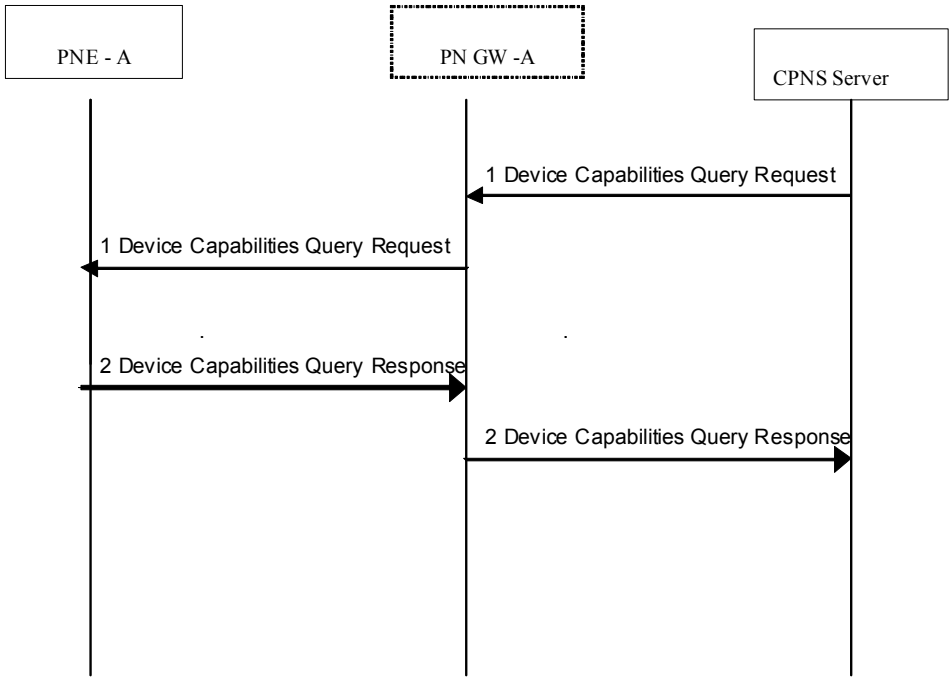


Figure 37 Flow of Device Capabilities Query of PNE -A

Figure 37 shows a flow of Device Capabilities Query Procedure

1. When CPNS Server wants to know the Device Capabilities of PNE-A, Device Capabilities Query Request is sent from CPNS Server to PNE-A through PN GW-A. PN GW-A forwards this message to PNE-A.
2. Device Capabilities Query Response is sent from PNE-A to CPNS Server through PN GW-A. PN GW-A forwards this message to CPNS Server.

In Figure 37, dotted box means PN GW only forwards/ relays the message received and sent. It doesn't process the message.

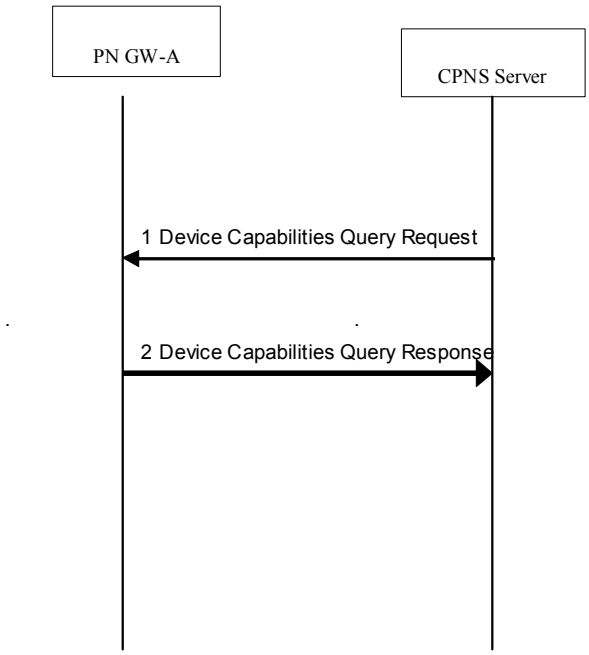


Figure 38 Flow of Device Capabilities Query Procedure of PN GW -A

Figure 38 shows a flow of Device Capabilities Query of PN GW-A.

1. When CPNS Server wants to know the Device Capabilities of PN GW –A, Device Capabilities Query Request is sent from CPNS Server to PN GW-A.
2. PN GW-A responds with Device Capabilities Query Response

6.12 Device Capabilities Change Notification

This function is used for delivering and managing the information of CPNS device capabilities, e.g. hardware and software characteristics of each device in the PN.

NOTE: A Service Provider and/or CPNS User can decide to opt in and opt out for this service. An entity can decide to retrieve the device capabilities information and opt out for automatic/dynamic device capability notification.

6.12.1 Device Capabilities Change Notification

This section describes general flows of Device Capabilities Change Notification.

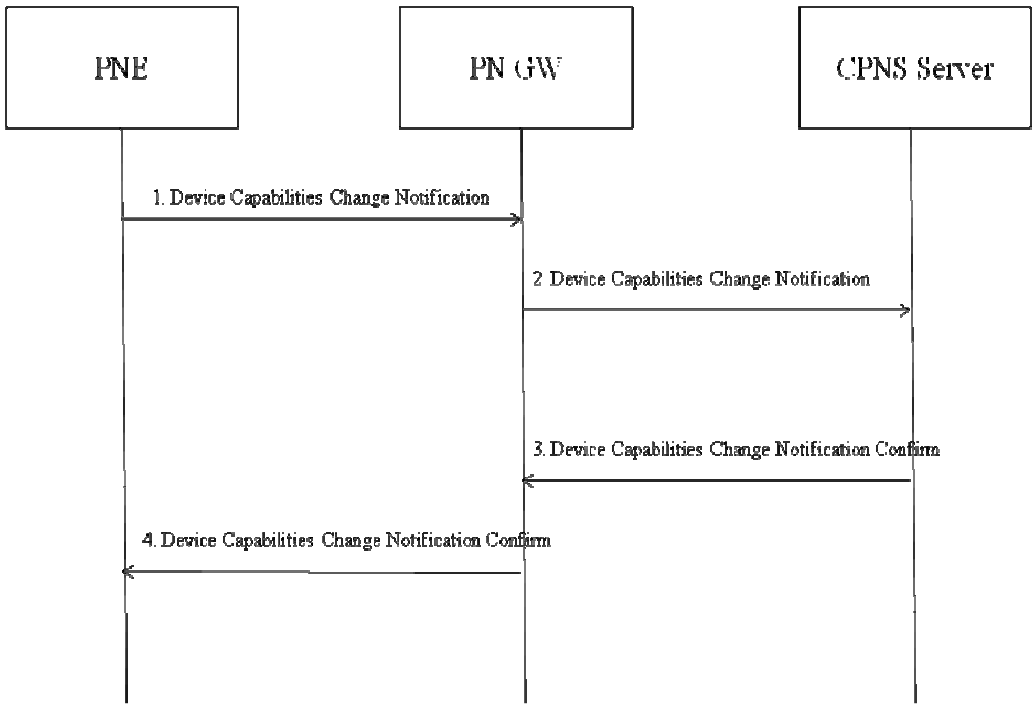


Figure 39 Flow of Device Capabilities Change Notification of PNE

Figure 39 shows a flow of Device Capabilities Notification Procedure

1. When a PNE is connected to a PN GW in a PN, device capability information of the PNE is sent to PN GW. Any subsequent change of these device capabilities will also be notified to the PN GW and CPNS Server
2. PN GW forwards this information to CPNS Server.
3. Device Capabilities Change Notification Confirm is sent from CPNS Server to PN GW
4. PN GW forwards this message to PNE

In Figure 39, PN GW only forwards/ relays the received message and sent. It doesn't process the message.

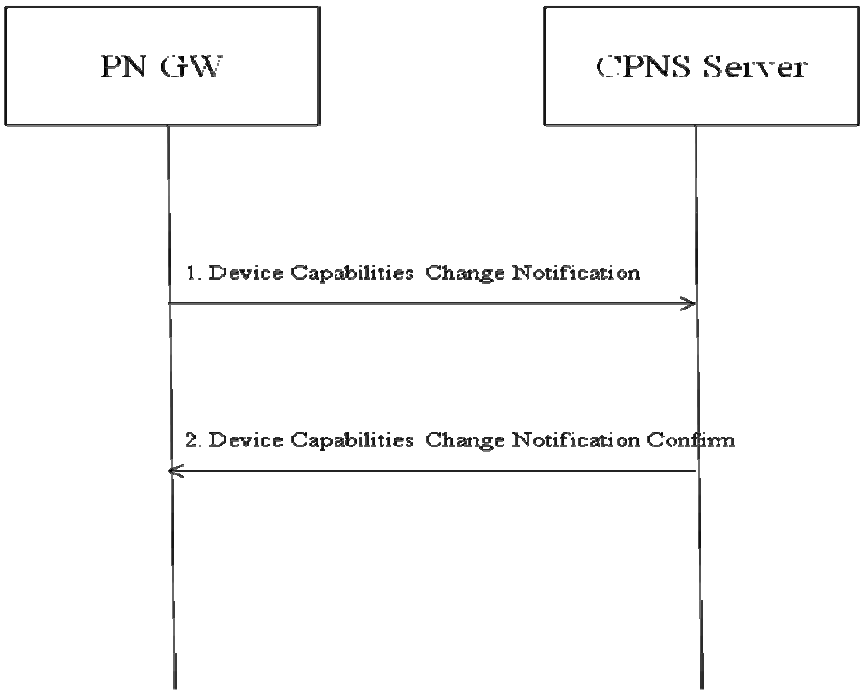


Figure 40 Flow of Device Capabilities Change Notification Procedure of PN GW

Figure 40 shows a flow of Device Capabilities Change Notification of PN GW.

1. When there is an update of Device Capabilities on PN GW, Device Capabilities Change Notification is sent from PN GW to CPNS Server.
2. CPNS Server responds with Device Capabilities Change Notification Confirm.

6.12.2 Device Capabilities Request and Response

This section describes general flows of Device Capabilities query and response when applicable.

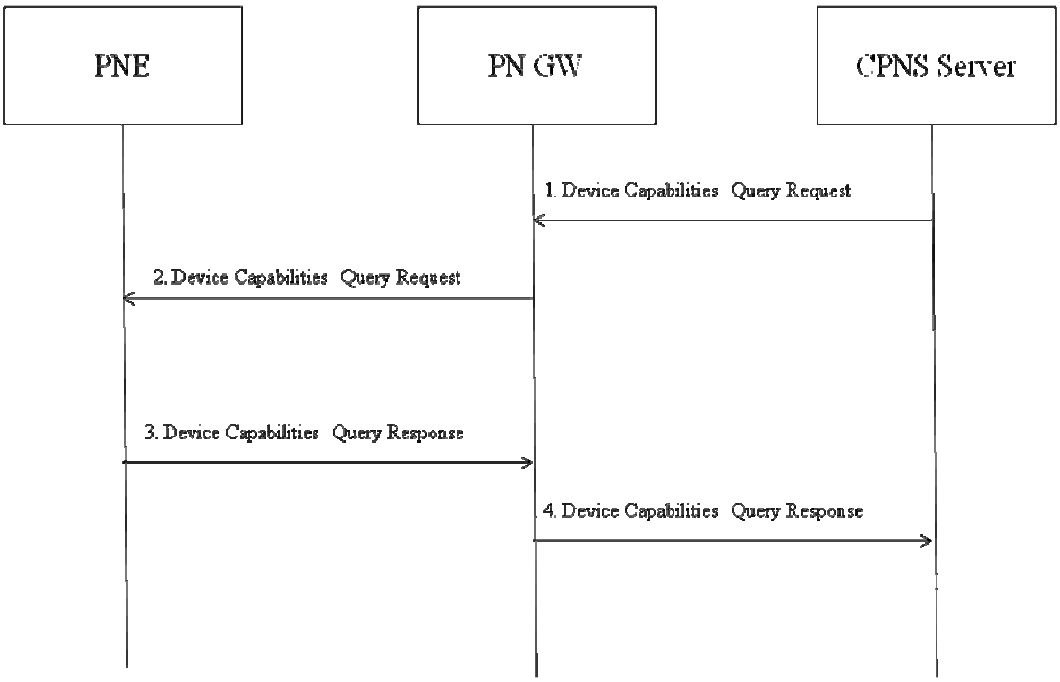


Figure 41 Flow of Device Capabilities Query of PNE

Figure 41 shows a flow of Device Capabilities Query Procedure

1. When CPNS Server wants to know the Device Capabilities of a PNE, Device Capabilities Query Request is sent from CPNS Server to the PN GW
2. PN GW forwards this message to PNE.
3. Device Capabilities Query Response is sent from PNE to PN GW.
4. PN GW forwards this message to CPNS Server.

In Figure 41, PN GW only forwards/ relays the message received and sent. It doesn't process the message.

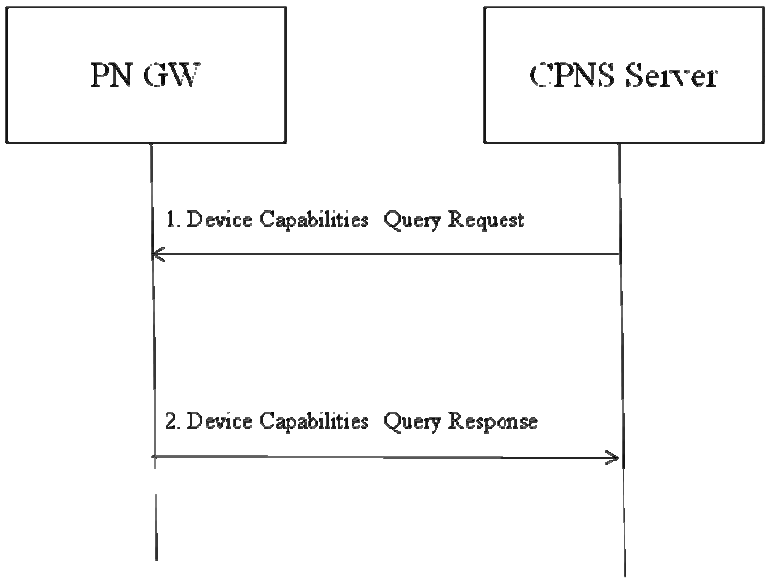


Figure 42 Flow of Device Capabilities Query Procedure of PN GW

Figure 42 shows a flow of Device Capabilities Query of PN GW.

1. When CPNS Server wants to know the Device Capabilities of PN GW, Device Capabilities Query Request is sent from CPNS Server to PN GW
2. PN GW responds with Device Capabilities Query Response.

6.13 Status Management

6.13.1 Introduction

The Status Management provides a mechanism to publish, collect, subscribe and notify the status of PNE and PN GW.

Each message in Status Management is formatted as CPNS Messages. The format of each message can be found in section 8.11.

Following status management procedures are identified.

- Publishing status information
- Subscribe and notify

6.13.2 Publishing status information

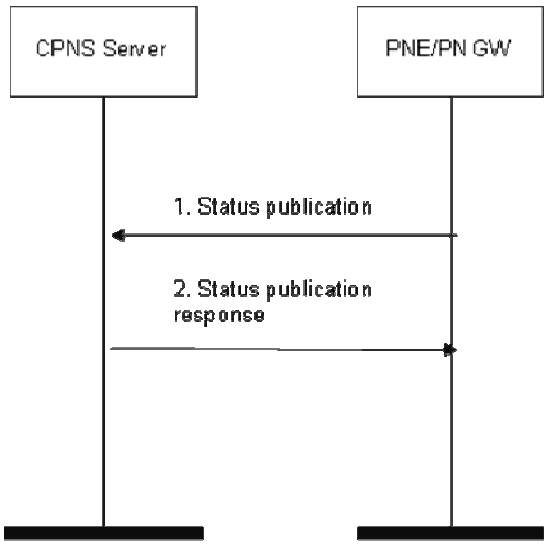


Figure 43 Publishing status information

1. When status changes, the PNE/PNGW publishes the status information to CPNS Server. In case PNE publishing the status information, the PNE publishes the status information via adjacent PNGW.

2. Receiving the status information, the CPNS Server stores the status information and sends back the response with result (e.g., success or failure), reason of the result and so on.

6.13.3 Subscribe and Notify

Following figure presents high level flow of subscribe and notify.

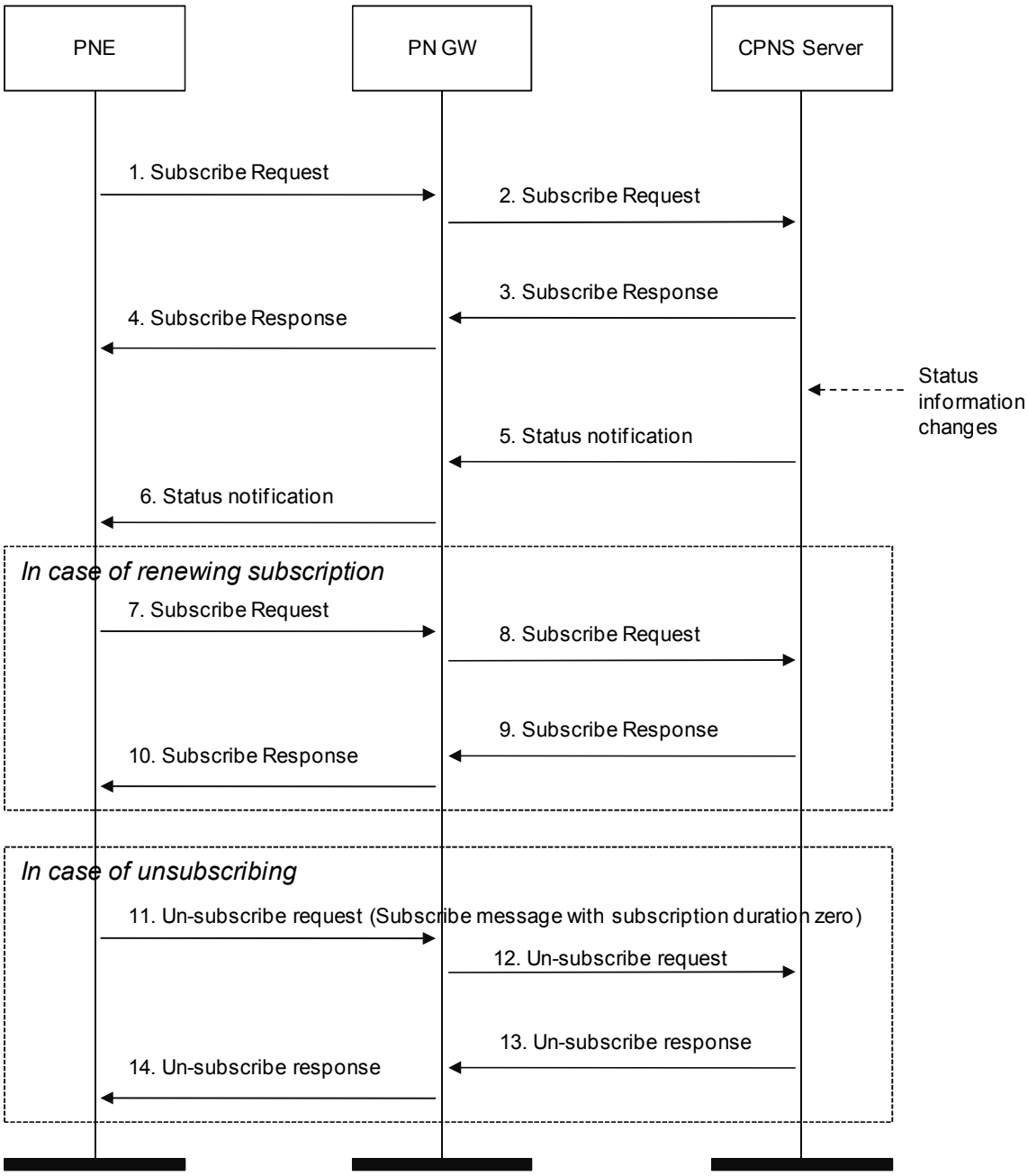


Figure 44 Subscribe and notify flow

1. The PNE sends Subscribe Request with ID of the entity hosting the service and duration of subscription to the CPNS Server via PN GW. Since the request is initial subscription, subscription ID is not included.

2. The PN GW relays the request to the CPNS Server.

3. The CPNS Server registers the event in accordance of the request and allocates unique subscription ID and send the Subscribe Response with result of subscription (e.g., “success” or “failure”) and reason of the result if any to the PNE via PN GW.

4. The PN GW relays the request to the PNE.

5. In accordance of registered event, the CPNS Server sends a status notification with subscription ID to the PNE via PN GW. The flow for status information change, publishing status information can be found in section 8.11.

6. The PN GW relays the request to the PNE.

7. Before subscription duration expires, the PNE MAY sends Subscribe Request to the PN GW with subscription ID to renew the subscription and extend the subscription duration.

8. The PN GW relays the request to the CPNS Server.

9. The CPNS Server updates the event registration in accordance of the request and sends a response with result of subscription (e.g., "success" or "failure") and reason of the result if any to the PNE via PN GW.

10. The PN GW relays the request to the PNE.

11. The PNE MAY unsubscribe from the event explicitly by sending Subscribe Request with subscription duration zero to the CPNS Server with subscription ID via PN GW.

12. The PN GW relays the request to the CPNS Server.

13. The CPNS Server releases the event registration when receiving such request and sends the response with result of un-subscription (e.g., "success" or "failure") and reason of the result if any to the PNE via PN GW.

14. The PN GW relays the request to the PNE.

6.14 Flows for Usage Statistics

6.14.1 Flow for Usage Statistics Collection and Reporting on the PNE side

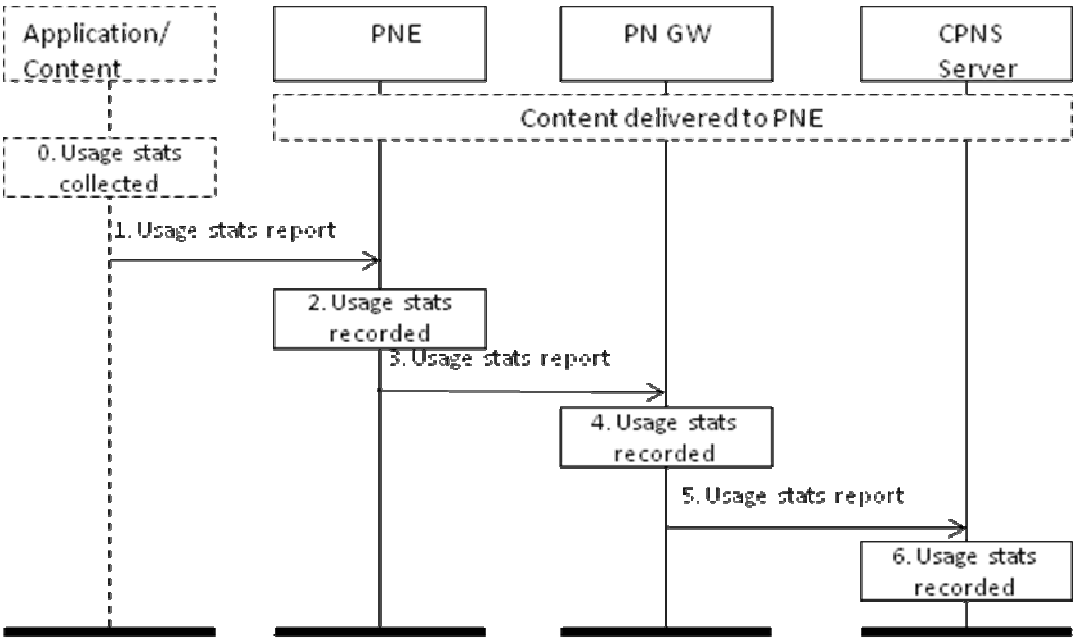


Figure 45 Flow for usage statistics from PNE to CPNS Server

This flow is initiated by the application on the PNE side, which collects the usage statistics information and sends to the PNE.

0. Usage statistics are collected by the application after the content is delivered to the PNE. Any user behaviour following the reception of the content, e.g. opening of the content, rendering it, deleting, do nothing, delete without opening etc. Will be captured by this functionality.

1. Application sends the usage statistics information to the PNE

2. PNE records the usage statistics information received from the application to be reused again if required
3. PNE forwards the usage statistics information to the PN GW
4. PN GW records the usage statistics information received from the PNE to be reused again if required
5. PN GW forwards the usage statistics information to the CPNS Server
6. CPNS Server records the usage statistics information received from the PN GW to be reused again if required or to be aggregated in a report document together with statistics collected from other sources. The information in this report can also be analysed when deciding what content to what device should be sent, which could be decided based on user behaviour and preference.

6.14.2 Flow for Usage Statistics Collection and Reporting on the Server side

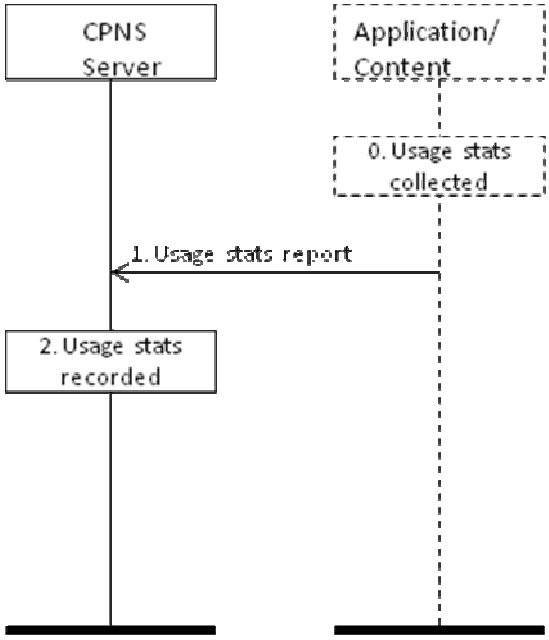


Figure 46 Flow for usage statistics from application to the CPNS Server

This flow is initiated by the application on the CPNS Server side, which collects the usage statistics information and sends to the CPNS Server.

0. Usage statistics are collected by the application from different content providers or different sources
1. Application sends the usage statistics information to the CPNS Server
2. CPNS Server records the usage statistics information received from the application to be reused again if required or to be aggregated in a report document together with statistics collected from other sources.

7. Signalling procedure

7.1 Overview

This section describes the core functionalities of CPNS enabler and the procedures required to support and facilitate these functions.

Before any communication or exchange of messages between the CPNS Entities a physical connection (pairing) using PAN technologies SHOULD be established. Following this, CPNS Entities can discover each other and its supported modes and services.

If a CPNS Device supports both PNE and PN GW functionalities, the Mode of CPNS Device (i.e. PNE, PN GW or BOTH) is set by the User or certain policies configured by operators upon the start up of CPNS Enabler. Subsequent mode changes of CPNS Devices SHALL be able to be done according to User's request or provider's policies.

Other core CPNS functionalities are PN Management, SG Management, Status Management, Service Discovery and Publication, usage statistics collection and reporting, Service and Content Delivery, Device Capability, Security of messages sent between the entities etc.

In the case of security of messages, underlying technologies that can provide secure channels are used when applicable, otherwise additional security is supported.

7.2 CPNS Entity Discovery

This Entity Discovery procedure is only executed among CPNS Devices.

Each CPNS Entity needs to find out the other detected device's Mode and additional information like current PN Information during entity discovery procedure after physical connection. The requesting CPNS Entity and requested CPNS Entity recognize the Mode of CPNS Device they reside in, and the CPNS Device acting as PNE finds out current PN information which CPNS Device stores, in case the requested CPNS Entity is PN GW. If the bearer among CPNS entities can support broadcasting feature for discovery, this message SHOULD be delivered via broadcasting.

7.2.1 Entity Discovery

7.2.1.1 Requesting CPNS Entity

When connecting a network, the CPNS Entity does not know the detected device's mode. If two or more CPNS Entities send the discovery message at a same time, the sub element information of that messages are duplicated. Because of this, the CPNS Device having PN GW Mode SHOULD send EntityDiscoveryRequest message immediately after physical pairing between two CPNS Devices. If the PN GW sends the PNInfo element including member PNEs in PN, there is no need to send additional Entity Discovery message to PNE(s) to know PNE's Mode when the CPNS Device detects other device.For the CPNS Entity Discovery, the CPNS Entity SHALL create the EntityDiscoveryRequest message including

- EntityInfo element SHALL be inserted as the information of requesting CPNS Entity.
    - UserInfo element SHALL be inserted as the information of requesting CPNS Entity
        - UserID attribute SHOULD be inserted from CPNS Application Profile in device.
        - UserName attribute SHALL be inserted.
    - PNEID attribute of active PNE in the requesting device SHALL be inserted.
    - PNGWID attribute of active PN GW in the requesting device SHALL be inserted.
    - PNEName and/or PNGWName attribute SHOULD be inserted if device supports.

- Mode attribute, InactiveMode attribute SHALL be inserted in case the requesting CPNS Device has both of PNE and PN GW functionalities. The CPNS Entity SHALL insert active mode into Mode attribute and inactive mode into InactiveMode attribute. If PNE and PNGW are active, the value of Mode attribute SHALL be "3"(BOTH). If PNE is active but PN GW is inactive, the value of Mode attribute SHALL be "1"(PNE) and InactiveMode attribute SHALL be "2"(PN GW). If PN GW is active but PNE is inactive, the value of Mode attribute SHALL be "2"(PN GW) and InactiveMode attribute SHALL be "2"(PNE).
- PNInfoReq attribute SHALL be inserted as "TRUE", in case the requesting CPNS Entity wants to know the PN information stored by requested CPNS Entity acting as PN GW. In case the requesting CPNS Entity does not want to know the PN Information of requested CPNS Entity acting as PN GW, PNInforReq attribute SHALL be "FALSE" or skipped.
- UICapa attribute SHALL be inserted with "TRUE" by PNE, in case the PN GW stands in for PNE's behalf in specific environment for this PNE. For example, the PN GW needs to decide to accept to PN setup request or service group management request due to lack of User Interface. The CPNS Entity acting PN GW needs to insert text like UserID or password instead of this device at EUKey assignment step after entity discovery procedure.
- Zonebasedservicesupport attribute SHALL be inserted with "TRUE" in case CPNS entity acting PN GW is capable of Zone Based Service.
- Broadcastgroupkeysupport attribute SHALL be inserted when PN GW sends EntityDiscoveryRequest message. If the PN GW supports broadcast Group Key delivery, the value is "TRUE". Otherwise, the value is "FALSE".
- PNInfo element SHALL be inserted, in case the requesting CPNS Entity is acting as PN GW and stores PN Inventory and Disclosure attribute is '2'(Open). If PN GW does not expose its PN Information to unauthenticated PNE, which means Disclosure attribute of PN is '1'(Blocked) or '3'(Selective), PN GW SHALL NOT include PN Information in the EntityDiscoveryRequest message
  - PNID attribute SHALL be inserted.
  - Description attribute SHOULD be inserted.
  - TempPN attribute SHOULD be applied if requesting Entity has PN Inventory with TempPN attribute. Based on preference setting (e.g. User Preference, Operator Policy), this TempPN attribute MAY be skipped. How to configure the User preference is out of scope in CPNS 1.0.
  - Sharing attribute SHOULD be inserted. Based on preference setting (e.g. User Preference, Operator Policy), this Sharing attribute MAY be skipped.
  - PNEInfo element as the member of PN SHALL be inserted. Sub attributes PNEID and Active SHALL be inserted, but PNEName attribute SHOULD be inserted only in case PN Inventory stores name of PNE.

After creating the EntityDiscoveryRequest message, the CPNS Entity SHALL send the EntityDiscoveryRequest message to detected devices. The EntityDiscoveryRequest message SHOULD be sent by broadcast in PAN ,e.g., when the Ethernet or WiFi is used as PANAfter receiving the EntityDiscoveryResponse message, the CPNS Entity SHALL retrieve which CPNS Device have what mode and additionally PN information, if any. If PNE finds out the PNGW with PNEInfo elements and its sub element PNEID, PNE does not need to send additional request to find another PNE in PNEInfo elements of PNGW. Based on this, the CPNS Entity acting PNE can ask to let PNE to join the PN if PN GW has the PN, or to create PN if PN GW has no PN or proper PN. The CPNS Entity acting PN GW can make the PN including detected PNE(s) and invite PNE to be a member of its PN.

7.2.1.2 Requested CPNS Entity

When receiving the EntityDisocveryRequest message, the CPNS Entity recognizes the mode and IDs information of requesting CPNS Entity through EntityInfo element.

When receiving the EntityDiscoveryRequest message, the CPNS Entity SHALL send the EntityDiscoveryResponse message including

- EntityInfo element SHALL be inserted as the information of requested CPNS Entity.
    - UserInfo element SHALL be inserted as the information of requesting CPNS Entity
        - UserID attribute SHOULD be inserted from CPNS Application Profile in device.
        - UserName attribute SHALL be inserted
    - PNEID attribute SHALL be inserted if the requested device has active PNE.
    - PNGWID attribute SHALL be inserted if the requested device has active PN GW.
    - PNEName and/or PNGWName attribute SHOULD be inserted if device supports.
    - Mode attribute, InactiveMode attribute SHALL be inserted in case the requested CPNS Device has both of PNE and PN GW functionalities. The CPNS Entity SHALL insert active mode into Mode attribute and inactive mode into InactiveMode attribute. If PNE and PNGW are active, the value of Mode attribute SHALL be “3”(BOTH). If PNE is active but PN GW is inactive, the value of Mode attribute SHALL be “1”(PNE) and InactiveMode attribute SHALL be “2”(PN GW). If PN GW is active but PNE is inactive, the value of Mode attribute SHALL be “2”(PN GW) and InactiveMode attribute SHALL be “1”(PNE).
    - UICapa attribute SHALL be inserted with “TRUE” by PNE in case the PN GW stands in for PNE’s behalf in specific environment for this PNE. For example, the PN GW needs to decide to accept to PN setup request or service group management request due to lack of User Interface.The CPNS Entity acting PN GW needs to insert text like UserID or password instead of this device at EUKey assignment step after entity discovery procedure.
    - Zonebasedservicesupport attribute SHALL be inserted with “TRUE” in case CPNS entity acting PN GW PN GW is capable of Zone Based Service.
    - Broadcastgroupkeysupport attribute SHALL be inserted when PN GW sends EntityDiscoveryResponse message. If the PN GW supports broadcast Group Key delivery, the value is “TRUE”. Otherwise, the value is “FALSE”.
    - PNInfo element SHALL be inserted, in case the PNInfoReq in the EntityDiscoveryRequest message is “TRUE”, the requested CPNS Entity acting PN GW stores PN Inventory and Disclosure attribute is ‘2’(Open). If PN GW does not expose its PN Information to unauthenticated PNE, which means Disclosure attribute of PN is ‘1’(Blocked) or ‘3’(Selective), PN GW SHALL NOT include PN Information in the EntityDiscoveryResponse message
        - PNID attribute SHALL be inserted.
        - Description attribute SHOULD be inserted, when PN Inventory contains.
        - TempPN attribute SHOULD be inserted if requesting Entity has PN Inventory with TempPN attribute. Based on preference setting (e.g. User Preference, Operator Policy), this TempPN attribute MAY be skipped. How to configure the User preference is out of scope in CPNS 1.0.
        - Sharing attribute SHOULD be inserted. Based on preference setting (e.g. User Preference, Operator Policy), this Sharing attribute MAY be skipped.
        - PNEInfo element as the member of PN SHALL be inserted. Sub attribute PNEID SHALL be inserted, but PNEName attribute SHOULD be inserted only in case PN Inventory stores name of PNE.

After sending the EntityDiscoveryResponse message, the CPNS Entity SHALL retrieve which CPNS Device have what mode and additionally PN information.

7.2.2 PN Discovery

7.2.2.1 PNE

When necessary to discover the current PN from PN GW, PNE SHALL send the EntityDiscoveryRequest message to PN GW including PNInfoReq sub attribute as “TRUE” as described in section 7.2.1.1.

When PNE receives the PNDiscoveryResponse message from PN GW, it can recognize PNInfo element in the PNDiscoveryResponse message.

7.2.2.2 PN GW

When receiving the EntityDiscoveryRequest message from PNE, the PN GW SHALL send the EntityDiscoveryResponse message to PNE. If there is PNInfo available in the PN Inventory, then the sub attributes and elements of that PNInfo element SHALL be included in the message.

7.3 Registration of UserID and password

Before assigning EUKey to PNE/PN GW, CPNS User who owns PNE/PN GW SHALL register his/her own UserID and password with CPNS Server.

Note: How to encrypt the password between PN GW and CPNS Server is out of scope of CPNS Enabler 1.0.

7.3.1 Registration of UserID and password via CPNS Interfaces

CPNS Server and CPNS Device which runs in PN GW mode SHALL authenticate each other using a mechanism external to CPNS Enabler (e.g., using USIM-credential) before starting the registration procedure.

When requested by CPNS User, PN GW SHALL send ID_PWD Registration Request message to CPNS Server.

Before sending the ID_PWD Registration Request message, the PN GW SHALL perform the following procedure:

1. Receive the UserID, Password and User Description from the User.
2. Generate the ID_PWD Registration Request message. The message SHALL contain the UserID, the Password and the User Info.

When receiving ID_PWD Registration Request message, CPNS Server SHALL register UserID and password with itself, and send ID_PWD Registration Response message to PN GW.

Upon receiving the ID_PWD Registration Request message, the CPNS Sever SHALL store the UserID, Password and User Info in the Secure Storage of the CPNS Server. CPNS Server MAY store hash value of Password, instead of storing Password itself.

The CPNS Server SHALL send the ID_PWD Registration Response message to carry the result of the procedure.

7.3.2 Registration of UserID and password not via CPNS Interfaces.

CPNS Server MAY allow CPNS User to register UserID and password not via CPNS interfaces (e.g., provides web interface for CPNS User to register UserID and password).

7.4 EUKey Assignment

7.4.1 EUKey Assignment for PNEs with UI capabilities

7.4.1.1 EUKey Assignment Request

- PNE

EUKey request procedures in PNE differ depending on the capability of CPNS Device in which the PNE is to be deployed.

If PNE runs in the CPNS Device which provides enough UI for CPNS User to insert UserID and password, the PNE SHALL support UserID and password insertion by CPNS User.

Upon requested by CPNS User for EUKey assignment, PNE SHALL:

1. Generate and store a $RAND_{PNE}$. $RAND_{PNE}$ is a random number generated by the PNE.
2. Generate hash value for user authentication data. Hash (AuthData) where AuthData = Hash(Password) | $RAND_{PNE}$ | Time
3. KeyType SHALL be inserted with "1" (UI functionalities supported, with secure PAN),
4. Generate the EUKeyAssignmentRequest message. The message SHALL contain the PNEID, UserID, $RAND_{PNE}$, Time, KeyType and the user authentication data.

After the above procedure, the PNE SHALL send EUKeyAssignmentRequest message to the PN GW.

- PN GW

When receiving EUKeyAssignmentRequest message from PNE, PN GW SHALL forward the EUKeyAssignmentRequest message to CPNS Server.

- CPNS Server

When receiving EUKeyAssignmentRequest message from PN GW, CPNS Server SHALL authenticate the CPNS User who owns PNE.

The authentication of CPNS User by CPNS Server SHALL be performed using UserID and password of CPNS User who owns the PNE. Upon receiving the EUKeyAssignmentRequest message, the CPNS Server SHALL:

1. Generate hash value for user authentication. Hash (AuthData) where AuthData = Hash(Password) | $RAND_{PNE}$ | Time
2. Verify the user authentication data using the CPNS Server generated hash value for user authentication. If the verification is fail, send the EUKeyAssignmentResponse message to the PN GW with fail status code.

7.4.1.2 EUKey Assignment Response

- CPNS Server

If the user authentication succeeds, CPNS Server SHALL:

1. Generate and store a $RAND_{SVR}$. $RAND_{SVR}$ is a random number generated by the CPNS Server.
2. Generate and store a KEK(i.e. Key Encryption Key) where KEK = Hash (Hash(Password) | $RAND_{PNE}$ | $RAND_{SVR}$)
3. Generate and store a EUKey for PNE. The EUKey for PNE is a random number generated by the CPNS Server.
4. Generate the EUKeyAssignmentResponse message. The message SHALL contain the Status, $RAND_{SVR}$, and EUKey for PNE that is encrypted with the KEK.

After the above procedure, the CPNS Sever SHALL send EUKeyAssignmentResponse message to the PN GW.

- PN GW

Upon receiving EUKey by EUKeyAssignmentResponse message sent from CPNS Server, PN GW SHALL forward the EUKey by sending EUKeyAssignmentResponse message to PNE.

- PNE

When receiving EUKey by EUKeyAssignmentResponse message forwarded from PN GW, PNE SHALL securely store EUKey after the decryption.

7.4.2 EUKey Assignment for PNE without UI capabilities

7.4.2.1 EUKey Assignment when PAN is secure

A EUKey for PNE is securely delivered from a CPNS Server to a PNE. It is assumed that PNE and PN GW are owned by the same CPNS User. This procedure is comprised of three parts: ID & Password Registration, ID & Password Installation, and Key Assignment.

Before starting the Key Assignment procedure for PNE without enough UI capabilities for inserting ID and Password, a CPNS Server and a PNGW SHALL perform the mutual authentication & key exchange using the existing mechanism (e.g., 3GPP GBA). Also the PNGW and a PNE SHALL perform the mutual authentication & key exchange using the PAN technologies.

7.4.2.1.1 ID & Password Registration

After the mutual authentication & key exchange between the CPNS Server and the PN GW, the PN GW can start the ID & Password Registration to the CPNS Server. ID & Password Registration procedure is described in the section 7.3.1.

7.4.2.1.2 ID and Password Installation

After the mutual authentication & key exchange between the PN GW and the PNE, the PN GW can start the ID & Password Installation to the PNE.

7.4.2.1.2.1. ID and Password Installation Request

Before sending the ID & Password Installation Request message, the PN GW SHALL perform the following procedure:

1. Receive the ID, Password and subscription information from the User.
2. Generate the ID & Password Installation Request message. The message SHALL contain the ID and the encrypted Password.

After the above procedure, the PN GW SHALL send ID & Password Installation Request message to the CPNS Server.

7.4.2.1.2.2. ID and Password Installation Response

Upon receiving the ID & Password Installation Request message, the PNE SHALL perform the following procedure:

1. Generate the hash value of the Password using SHA-1 hash algorithm.
2. Store the ID and hash value of the Password.

The PNE SHALL send the ID & Password Installation Response message to carry the result of the procedure.

7.4.2.1.3 EUKey Assignment

7.4.2.1.3.1. EUKey Assignment Trigger

Before sending the EUKeyAssignmentTrigger message to the PNE, the PN GW SHALL perform the following procedure:

1. Receive the ID and Password from the User.
2. Generate a $RAND_{PNGW}$. $RAND_{PNGW}$ is a random number generated by the PN GW.
3. Generate hash value for user authentication data and starting the EUKey Assignment procedure. Hash (AuthData) where AuthData = Hash(Password) | $RAND_{PNGW}$ | Time

4. KeyType SHOULD be inserted with “2” (UI functionalities not supported, with secure PAN)

5. Generate the EUKeyAssignmentTrigger message. The message SHALL contain the ID, $RAND_{PNGW}$, Time, KeyType and the user authentication data.

After the above procedure, the PN GW SHALL send EUKeyAssignmentTrigger message to the PNE.

7.4.2.1.3.2. EUKey Assignment Request

Upon receiving the EUKey Assignment Trigger message, the PNE SHALL perform the following procedure:

1. Generate hash value for user authentication data and verify the hash value of the user authentication data. Hash (AuthData) where AuthData = Hash(Password) | $RAND_{PNGW}$ | Time

2. Generate and store a $RAND_{PNE}$. $RAND_{PNE}$ is a random number generated by the PNE.

3. Generate hash value for user authentication data. Hash (AuthData) where AuthData = Hash(Password) | $RAND_{PNE}$ | Time

4. KeyType SHOULD be inserted with “2” (UI functionalities not supported with secure PAN)

5. Generate the EUKey Assignment Request message. The message SHALL contain the ID, $RAND_{PNE}$, Time, KeyType and the user authentication data.

After the above procedure, the PNE SHALL send EUKey Assignment Request message to the PN GW.

Upon receiving the EUKey Assignment Request message, the PN GW SHALL relay the EUKey Assignment Request message to the CPNS Server.

7.4.2.1.3.3. EUKey Assignment Response

Upon receiving the EUKey Assignment Request message, the CPNS Server SHALL perform the following procedure:

1. Generate hash value for user authentication. Hash (AuthData) where AuthData = Hash(Password) | $RAND_{PNE}$ | Time

2. Verify the user authentication data using the CPNS Server generated hash value for user authentication. If the verification is fail, send the EUKeyAssignmentResponse message to the PN GW with fail status code.

3. Generate and store a $RAND_{SVR}$. $RAND_{SVR}$ is a random number generated by the CPNS Server.

4. Generate and store a KEK where KEK = Hash (Hash(Password) | $RAND_{PNE}$ | $RAND_{SVR}$)

5. Generate and store a EUKey. The EUKey is a random number generated by the CPNS Server.

6. Generate the EUKeyAssignmentResponse message. The message SHALL contain the Status, $RAND_{SVR}$, and encrypted PNE Key that is encrypted with the KEK.

After the above procedure, the CPNS Sever SHALL send EUKeyAssignmentResponse message to the PN GW.

Upon receiving the EUKeyAssignmentResponse message, the PN GW SHALL relay the EUKeyAssignmentResponse message to the PNE.

Upon receiving the EUKeyAssignmentResponse message and the Status is Success, the PNE SHALL perform the following procedure:

1. Generate and store a KEK where KEK = Hash (Hash(Password) | $RAND_{PNE}$ | $RAND_{SVR}$)

2. Decrypt the EUKey with the KEK.

7.4.2.2 EUKey Assignment when PAN is not secure

To perform procedure described in this subsection, following conditions need to be satisfied:

- PNE and PN GW are owned by same user
- PNE has secret passphrase, "Temporary Key(TK)", which is preconfigured by manufacturer and stored inside of the PNE
- TK is available to CPNS Server (e.g., stored in CPNS Server, can be retrieved from external database from CPNS Server)

An EUKey for PNE is securely delivered from a CPNS Server to a PNE as illustrated in Figure X of section 6.2.2.1.

Before starting the EUKey Assignment procedure for PNE without enough UI, a CPNS Server and a PNGW SHALL perform the mutual authentication & key exchange using the existing mechanism (e.g., 3GPP GBA). After the step, the PSK1 is shared between the CPNS Server and the PN GW.

7.4.2.2.1 EUKey Assignment

7.4.2.2.1.1. EUKey Assignment Request

Before sending the EUKeyAssignmentRequest message to the CPNS Server, the PN GW SHALL perform the following procedure:

1. Receive the PNE EntityID, CPNS UserID and User Password from the User.
2. Generate and store a $RAND_{PNGW}$. $RAND_{PNGW}$ is a random number generated by the PNGW.
3. Generate hash value for user authentication data. Hash (AuthData) where AuthData = Hash(Password) | $RAND_{PNGW}$ | Time
4. KeyType SHOULD be inserted with "3" (UI functionalities not supported, without secure PAN)
5. Generate the EUKeyAssignmentRequest message. The message SHALL contain the PNE EntityID, CPNS UserID, Time, KeyType and the user authentication data.

After the above procedure, the PN GW SHALL send EUKeyAssignmentRequest message to the CPNS Server

7.4.2.2.1.2. EUKey Assignment Response

Upon receiving the EUKeyAssignmentRequest message, the CPNS Server SHALL perform the following procedure:

1. Generate hash value for user authentication. Hash (AuthData) where AuthData = Hash(Password) | $RAND_{PNGW}$ | Time
2. Verify the received user authentication data using the CPNS Server generated hash value for user authentication (i.e., hash value generated in step1). If the verification fails, send the EUKeyAssignmentResponse message to the PN GW with fail status code.
3. Generate and store a $RAND_{SVR}$.$RAND_{SVR}$ is a random number generated by the CPNS Server
4. Generate Seed value for generating a PNE EUKey or PNE EUKey sets where [$Seed_{PNE}$=Hash($RAND_{SVR}$, $RAND_{PNGW}$)] to avoid receiving frequent EUKeyAssignmentRequest message from PN GW . The update of EUKey is performed during mutual authentication process. A set of EUKeys SHOULD be generated as follows:

   $EUKey_n$=Hash($Seed_{PNE}$)

   $EUKey_{n-1}$=Hash($EUKey_n$)

   $EUKey_{n-2}$=Hash($EUKey_{n-1}$)

   ……

   $EUKey_2$=Hash($EUKey_3$)

   $EUKey_1$=Hash($EUKey_2$)
5. Store it with PNE EntityID and CPNS UserID.
6. Find the Temporary Key, TK_{PNE}, corresponding to the EntityID.

   Note: Temporary Key can be obtained from the PNE Manufacturer. How to acquire the temporary key corresponding to the EntityID is out of scope of CPNS specification
7. Generate the EUKeyAssignmentResponse message. The message SHALL contain the Status, a EUKey or EUKey sets (i.e [$EUKey_{PNE}$]) and Temporary Key.

After the above procedure, the CPNS Server SHALL send EUKeyAssignmentResponse message to the PN GW.

7.4.2.2.1.3. EUKey Assignment Notification

Upon receiving the EUKeyAssignmentResponse message from the CPNS Server, the PN GW SHALL perform the following procedure:

1. The PN GW SHALL store the Temporary Key and a EUKey or set of EUKeys (i.e.[$EUKey_{PNE}$]).
2. If the set of EUKeys are delivered, the PN GW SHALL select the EUKey among EUKey sets, otherwise, the PN GW use the EUKey.
3. Generate the EUKeyAssignment Notification message. The message SHALL contain the EUKey that is encrypted with the Temporary Key.

Upon receiving the EUKeyAssignmentNotification message and the Status is Success, the PNE SHALL perform the following procedure:

1. Decrypt the PNE's EUKey with the Temporary Key and stores PNE's EUKey.

7.4.3 EUKey Assignment for PN GW

If fixed or removable module keeping identity information and credential (i.e. a SIM/USIM/ISIM) is installed and used for secure communication on PN GW, following procedure is not performed.

7.4.3.1 EUKey Request and Creation

- PN GW

  Key request procedures in PN GW differ depending on the capability of CPNS Device in which the PN GW is to be deployed.

  If PN GW runs in the CPNS Device which provides enough UI for CPNS User to insert UserID and password, the PN GW SHALL support UserID and password insertion by CPNS User.

  Upon requested by CPNS User for EUKey assignment, PN GW SHALL send EUKeyAssignmentRequest message to CPNS Server.

- CPNS Server

  When receiving EUKeyAssignmentRequest message from PN GW, CPNS Server SHALL authenticate the PN GW.

  The authentication of PN GW by CPNS Server (i.e., client authentication) SHALL be performed using UserID and password of CPNS User who owns the PN GW.

  If authentication succeeds, CPNS Server SHALL create EUKey and store it with the PN GW's ID (i.e., EntityID) and UserID of CPNS User who owns the PN GW.

7.4.3.2 EUKey Delivery

- CPNS Server

  After creating EUKey, CPNS Server SHALL encrypt the EUKey and send encrypted EUKey to PN GW by EUKeyAssignmentResponse message.

  The EUKey SHOULD be encrypted by a secure material which is calculated from password of CPNS User who owns the PN GW (e.g., hashed password of the CPNS User).

- PN GW

  When receiving Key Delivery message from CPNS Server, PN GW SHALL securely store EUKey included in EUKeyAssignmentResponse message after decryption.

7.5 Mutual Authentication

7.5.1 PNE Authentication

During PN Establishment, PNE Inviting and PNE Joining procedures, the mutual authentication and session key sharing are performed between PNE and CPNS Server and between PNE and PN GW, respectively.. This section explains how the mutual authentication and session key sharing are performed

7.5.1.1 PNE

To start mutual authentication with CPNS Server, PNE SHALL generate a random number, and include its ID and the random number as AuthPNEID and rand_PNE into the AuthIniData sub element of the following messages to be sent to PN GW. Also, if PNE has enough UI, PNE SHALL indicate that it needs LocalEUKey assignment by setting LocalEUKeyAssignment "TRUE" in the AuthIniData sub element of the following messages.

- During PN Establishment procedure
    - PNSetupRequest message from originating PNE
    - PNSetupResponse message from invited PNE
- During PNE Management (PNE Inviting)
    - PNActionResponse (Invite) from invited PNE
- During PNE Management (PNE Joining)
    - PNActionRequest (Join) from joining PNE

Upon receiving AuthenticateRequest message from PN GW, PNE SHALL calculate hash value, "hash_PNE", and session key to be shared with CPNS Server. The calculation SHALL be performed as follows:

- hash_PNE SHALL be calculated from rand_PNE, rand_server (a hash value calculated by CPNS Server and included in the received message), PNE's EUKey and the session key
- the session key SHALL be calculated from rand_PNE, rand_server and PNE's EUKey.

PNE SHALL include its EntityID and hash_PNE as TargetID and HASH into AuthResData sub element of AuthenticateResponse message and send AuthenticateResponse message to PN GW.

In addition, if AuthenticateRequest includes LocalEUKey, PNE SHALL decrypt LocalEUKey included in the received AuthenticateRequest message by its own EUKey and store the LocalEUKey.

Afterwards, if PAN between PNE and PN GW is not a Secure PAN, PNE SHALL perform mutual authentication and session key sharing by using LocalEUKey (when PNE has enough UI) or Temporary Key (when PNE does not have enough UI) in the same way as described in 7.5.2 "PN GW Authentication" (i.e., PNE SHALL perform the same signalling procedure of PN GW described in the section 7.5.2).

Note: mechanism to check if PAN is a Secure PAN is out of scope of CPNS1.0

Upon receiving the following messages from PN GW in each procedure, PNE SHALL authenticate CPNS Server by verifying hash_server (i.e., checks if the same value as hash_server can be calculated from rand_PNE, rand_server, PNE's EUKey, the session key and hash_PNE)

- During PN Establishment procedure
    - PNSetupResponse (received by originating PNE)
    - PNEstablishmentNotify (received by invited PNE)
- During PNE Management (PNE Inviting)

- PNUpdateNotification (received by invited PNE)

- During PNE Management (PNE Joining)
  - PNActionResponse (Join) (received by joining PNE)

7.5.1.2 PN GW

Upon receiving the following messages from PNE,

- During PN Establishment procedure
  - PNSetupRequest message from originating PNE
  - PNSetupResponse message from invited PNE
- During PNE Management (PNE Inviting)
  - PNActionResponse (Invite) from invited PNE
- During PNE Management (PNE Joining)
  - PNActionRequest (Join) from joining PNE

PN GW SHALL include AuthPNEID(s) and rand_PNE(s) included in the received message(s) into the AuthIniData sub element of the following messages and send the message to the CPNS Server. If there are multiple PNEs to be connected to PN during the single procedure (e.g., If one or more invited PNEs are to be connected to PN in addition to originating PNE in the single PN Establishment procedure), PN GW SHALL include all AuthPNEIDs and rand_PNEs sent from the PNEs into the following messages.

- During PN Establishment procedure
  - PNSetupResponse
- During PNE Management (PNE Inviting)
  - PNUpdateRequest
- During PNE Management (PNE Joining)
  - PNUpdateRequest

Upon receiving AuthenticateRequest message from CPNS Server, PN GW SHALL deliver AuthenticateRequest message(s) to PNE(s) to be authenticated. When there are multiple PNEs to be authenticated, PN GW SHALL distribute AuthenticateRequest messages to those PNEs.

Note: Whether or not to use new message header for the message distributed to PNE(s) is out of scope of CPNS 1.0

In addition, for mutual authentication between PN GW and PNE, if AuthenticateRequest message includes LocalEUKey(s), PN GW SHALL decrypt LocalEUKey(s) included in the received AuthenticateRequest message by its own EUKey and store the LocalEUKey(s). PN GW SHALL include copy of LocalEUKey encrypted by PNE's EUKey into AuthenticateRequest message.

Afterwards, if PAN between PNE and PN GW is not a Secure PAN, PN GW SHALL perform mutual authentication and session key sharing by using LocalEUKey (when PNE has enough UI) or Temporary Key (when PNE does not have enough UI) in the same way as described in 7.5.2 "PN GW Authentication" (i.e., PN GW SHALL perform the same signalling procedure of CPNS Server described in section 7.5.2).

Note: mechanism to check if PAN is a Secure PAN is out of scope of CPNS1.0

Upon receiving AuthenticateResponse message(s) from PNE(s) to be authenticated, PN GW SHALL deliver an AuthenticateResponse message to CPNS Server. When there are multiple PNEs to be authenticated, PN GW SHALL deliver an aggregated AuthenticateResponse message with new message header to the CPNS Server.

Upon receiving the following message from CPNS Server,

- During PN Establishment procedure
    - PNSetupResponse
- During PNE Management (PNE Inviting)
    - PNUpdateResponse
- During PNE Management (PNE Joining)
    - PNUpdateResponse

PN GW SHALL include hash_server included in the received message into the AuthFinData sub element of the following messages and send the message to the PNE(s). If there are multiple PNEs to be connected to PN during the single procedure (e.g., If one or more invite PNEs are to be connected to PN in addition to originating PN in the single PN Establishment procedure), PN GW SHALL send the following message to each PNE.

- During PN Establishment procedure
    - PNSetupResponse message to originating PNE
    - PNEstablishmentNotify to the invited PNE(s)
- During PNE Management (PNE Inviting)
    - PNUpdateNotification to invited PNE
- During PNE Management (PNE Joining)
    - PNActionResponse (Join) to joining PNE

7.5.1.3 CPNS Server

Upon receiving rand_PNE(s) from PN GW, CPNS Server SHALL generate a random number, rand_server, and include PNEID and rand_server as TargetID and RAND into the AuthReqData sub element of AuthenticateRequest message. If there are multiple PNEs to be connected to PN during the single procedure (e.g., If one or more invite PNEs are to be connected to PN in addition to originating PN in the single PN Establishment procedure), CPNS Server includes all PNEIDs into the AuthenticateRequest message.

In addition, for mutual authentication between PNE(s) and PN GW, if PNE requests LocalEUKey assignment, CPNS Server SHALL generate LocalEUKey(s) to be shared between PNE(s) and PN GW.

For each LocalEUKey, CPNS Server SHALL create two copies, one for PNE and the other for PN GW, and encrypt each copy by PNE's EUKey and PN GW's EUKey, respectively. CPNS Server SHALL include the copies of LocalEUKey(s) as LocalEUKey_PNE and LocalEUKey_PN GW into the AuthReqData sub element of AuthenticateRequest message to be sent to PNE(s) via PN GW. If there are multiple PNEs to be connected to PN during the single procedure (e.g., If one or more invite PNEs are to be connected to PN in addition to originating PN in the single PN Establishment procedure), CPNS Server creates different LocalEUKeys for each PNE and includes all encrypted LocalEUKey into the AuthenticateRequest message.

Upon receiving AuthenticateResponse message from PN GW, CPNS Server SHALL calculate session key from rand_PNE, rand_server and PNE's EUKey. CPNS Server SHALL authenticate PNE(s) by verifying hash_PNE(s) (i.e., checks if the same hash value can be calculated from rand_server, rand_PNE, PNE's EUKey and the session key).

In addition, CPNS Server SHALL calculate another hash value(s) from rand_PNE, rand_server, PNE's EUKey, the session key and hash_PNE. CPNS Server SHALL include the calculated hash value(s) as HASH into AuthFinData of the following messages and send them to PNE via PN GW

- During PN Establishment procedure
    - PNSetupResponse

- During PNE Management (PNE Inviting)
    - PNUpdateResponse
- During PNE Management (PNE Joining)
    - PNUpdateResponse

7.5.2 PN GW Authentication

If fixed or removable module keeping identity information and credential (i.e., a SIM/USIM/ISIM) is installed and used for secure communication on PN GW, following procedure is not performed.

The session key will be expired after certain amount of time. When there is no session key or session key is expired, PN GW Authentication described below is performed.

Before starting message forwarding between PNE and CPNS Server, PN GW SHALL perform mutual authentication with CPNS Server.

- PN GW

  Before starting message forwarding between PNE and CPNS Server, PN GW SHALL send ConnectRequest message to CPNS Server to trigger mutual authentication. ConnectRequest message SHALL include CPNS Entity ID of the PN GW and random number created by PN GW (in RAND attribute).

  When receiving AuthenticateRequest message, PN GW SHALL create session key from random_PN GW, random_server (random number included in the AuthenticateRequest message) and its own EUKey.

  In addition, PN GW SHALL send AuthenticateResponse message to the CPNS Server. The message SHALL include hash value (in HASH attribute of AuthResData sub element) calculated from ConnectRequest message, AuthenticateRequest message and the PN GW's EUKey.

  When receiving ConnectResponse message, PN GW SHALL verify hash_server (random number included in the ConnectResponse message) included in the message by checking if the same value can be calculated from ConnectRequest message, AuthenticateRequest message, AuthenticateResponse message and the PN GW's EUKey.

- CPNS Server

  When receiving ConnectRequest message from PN GW, CPNS Server SHALL send AuthenticateRequest message to the PN GW. AuthenticateRequest message SHALL include random number created by CPNS Server (in RAND attribute of AuthReqData sub element).

  When receiving AuthenticateResponse message, CPNS Server SHALL create session key from random_PN GW, random_server and EUKey of the PN GW which is sender of the message.

  In addition, CPNS Server SHALL verify HASH included in the message by checking if the same value can be calculated from ConnectRequest message, AuthenticateRequest message and the PN GW's EUKey.

  If verification succeeds, CPNS Server SHALL send ConnectResponse message to the PN GW. The message SHALL include hash value (in HASH attribute) calculated from ConnectRequest message, AuthenticateRequest message, AuthenticateResponse message and the PN GW's EUKey.

7.6 PN Management

7.6.1 PN Establishment

7.6.1.1 PNE

[Procedure in originating PNE]

The PNE SHALL generate a PNSetupRequest message according to format of CPNS Message in section 8. In the PNSetupRequest message, the PNE

1. SHALL include the PNEID as part of OriginEntityID attribute.
2. SHALL choose one of three options and include the type of PN setup in PNSetupType attribute
   A. 1 for '1-1' case which enables the PNE to establish a PN with the PN GW only, or
   B. 2 for 'All' case which enables the PNE to establish a PN with all CPNS devices connected to the PN GW, or
   C. 3 for 'Specific' case which enables the PNE to establish a PN with PNEs to be invited.
3. MAY include PNEIDs to be invited to the PN in InvitedPNEID attribute.
4. SHALL include PNInfo element.

   The PNInfo element contains attributes below.

   A. PNE SHALL choose one of three options and include Disclosure attribute
      i. 1 for preventing PN Information to be delivered, in case Service Discovery is requested after PN setup.
      ii. 2 for allowing PN Information to be delivered, in case Service Discovery is requested after PN setup.
      iii. 3 for asking confirmation to OwnershipEntity whether or not PN Information is delivered, in case Service Discovery is requested after PN setup.
   B. OwnershipEntityID attribute MAY be included. OwnershipEntityID is the ID of authorized CPNS entity which has authorization to allow PN Information open, in case Service Discovery is requested after PN setup.
   C. PNE SHALL choose one of two options and include TempPN.
      i. True, indicating that broken physical connection releases PN after PN setup.
      ii. False, indicating that PN Information remains in CPNS Server, even if physical connection is broken.
   D. PNE SHALL choose one of two options and include Sharing attribute
      i. 1 for sharing the PNE Info and PN GW Info with other PNE member(s) of PN
      ii. 2 for preventing the PNE Info to be shared with other PNE member(s) of PN, but delivering PN GW Info to PNE member(s) of PN
5. SHALL include PNEInfo element.

   The PNEInfo element contains attributes below.

   A. PNEID attribute SHALL be PNEID, which establish the PN.
   B. PNEName attribute MAY include a nickname assigned by CPNS User.
   C. Mode attribute SHALL set the value '1' (PNE) or '3'(BOTH) according to the its local active Mode.
   D. Description attribute MAY include the description of PN (e.g. Home, Office)
6. MAY include DeviceCapa element.

   NOTE: DeviceCapa fragment contains information such as DeviceType, VideoCodec, etc. For CPNS V1.0 format definition is out of scope (e.g. DPE Enabler) and implementation matter.
7. MAY include ServiceProfile element containing Application or Content information as described in section 5.5 CPNS Metadata.
8. SHALL include AuthIniData element as described in section 7.5.1.1.
9. SHALL send PNSetupRequest message towards the PN GW according to the rules and procedures of underlying PAN technology.

Upon receiving the PNSetupResponse message from the PN GW, the PNE

1. SHALL check the answer to PNSetupRequest message in Return attribute.

2. SHALL store, if the value of Return is '1', the derived PN information in sub attributes under PNInfo element in the PN Inventory from the PNSetupResponse message.

[Procedure in invited PNE]

Upon receiving the PNSetupRequest message from the PN GW, the PNE

1. SHALL check the OriginEntityID in order to know who initiate to make the PN.
2. SHALL derive MsgID and PNID from PNSetupRequest message.

The PNE SHALL generate the PNSetup Response according to the format of CPNS Message in section 8. The PNE

1. SHALL include the answer to PNSetupRequest message in Return attribute.
   A. 1 for OK
   B. 2 for Failure, indicating that PNE is not capable of handling the request, e.g., internal error process occurs in the device embedding PNE or CPNS User does not want to participated in
2. SHALL include the received Message ID in MsgID attribute in order to indentify the transaction.

If the value of answer to PNSetupRequest message is '1' (i.e., OK), the following sequences perform. Otherwise, the following sequences are skipped till step 14.

3. SHALL include PNInfo element.

   The PNInfo element contains attributes below.

   A. PNID attribute SHALL set the PNID, which is to be participated in and derived from PNSetupRequest message.
   B. TempPN attribute SHALL be included if PNSetupRequest message includes.
      i. True, indicating that broken physical connection releases PN after PN setup.
      ii. False, indicating that PN Information remains in CPNS Server, even if physical connection is broken.
   C. Sharing attribute SHALL be included if PNSetupRequest message includes.
      i. 1 for sharing the PNE Info and PN GW Info with other PNE member(s) of PN
      ii. 2 for preventing the PNE Info to be shared with other PNE member(s) of PN, but delivering PN GW Info to PNE member(s) of PN
4. SHALL include PNEInfo element.

   The PNEInfo element contains attributes below.

   A. PNEID attribute SHALL set own PNEID to be invited by Originating CPNS Entity.
   B. PNEName attribute MAY include a nickname assigned by CPNS User.
   C. Mode attribute SHALL set the value '1'(PNE) or '3' (BOTH) according to the its local active Mode.
   D. Description attribute MAY include the description of PN (e.g. Home, Office)
5. MAY include DeviceCapa element.

   NOTE: DeviceCapa fragment contains information such as DeviceType, VideoCodec, etc. For CPNS V1.0 format definition is out of scope (e.g. DPE Enabler) and implementation matter.
6. MAY include ServiceProfile element containing Application or Content information as described in section 5.5 CPNS Metadata.
7. SHALL include AuthIniData element as described in section 7.5.1.1
8. SHALL send PNSetupResponse message towards the PN GW according to the rules and procedures of underlying PAN technology.

Upon receiving the PNEstablishmentNotify message from PN GW, the PNE

1. SHALL store the derived PN information in sub attributes under PNInfo element from the PNEstablishmentNotify message.

7.6.1.2 PN GW

[PNE Initiated]

Upon receiving the PNSetupRequest message from the PNE, the PNGW

1. SHALL check the type of PN setup in PNSetupType attribute. If the value of PNSetupType is;
   A. 1 for 1-1' case or empty case which enables the PNE to establish a PN with the PN GW only, the PNGW SHALL send the PNSetupRequest message towards the CPNS Server.
   B. 2 for 'All' case which enables the PNE to establish a PN with all CPNS devices connected to the PN GW, the PNGW SHALL send the PNSetupRequest message towards all the PNEs connected to the PNGW except the requesting PNE.
   C. 3 for 'Specific' case which enables the PNE to establish a PN with PNEs to be invited, the PNGW SHALL send the PNSetupRequest message towards the PNEID(s) to be invited during PN Establishment.
2. SHALL create the PN information for PN Inventory for the corresponding Personal Network.
3. SHALL create and maintains routing table for the routing of inside Personal Network, which is made out of PN Information.

After checking the type of PN setup, if the value of PNSetupType is 2 or 3, the PN GW SHALL generate the PNSetupRequest message according to the format of CPNS Message in section 8. The PN GW

1. SHALL include the PNEID as part of OriginEntityID attribute.
2. MAY include PNEID(s) to be invited to the PN in InvitedPNEID attribute in order to acknowledge which PNE(s) is(are) invited to the PN.
3. SHALL include PNInfo element.

   The PNInfo element contains attributes below.

   A. PNID attribute
   B. Description attribute MAY be created by the originating PNE and include texts which explain the PN.
4. SHALL include PNGWInfo element.

   The PNGWInfo element contains attributes below.

   A. PNGWID attribute SHALL set the PNGWID.
   B. PNGWName attribute MAY include the nickname of PN GW assigned by CPNS User or device type.
5. SHALL include AuthIniData element as described in 7.5.1.2
6. SHALL send PNSetupRequest message towards the PNE(s) to be invited.

Upon receiving the PNSetupResponse message from the PNE, the PN GW SHALL check the answer to PNSetupRequest message in Return attribute in order to confirm participation in PN. If the value of Return attribute is 1, the PN GW SHALL create the information for PN Inventory for the corresponding PN, create and maintain routing table with the derived from PANTech and Address attributes from PNSetupResponse for the routing of inside PN.

When checking if the value of PNSetupType attribute is 1 after receiving the PNSetupRequest message from the originating PNE or if the value of Return attribute is 1 after receiving the PNSetupResponse from the invited PNE, the PNGW SHALL genenrate PNSetupRequest message according to the format of CPNS Message in Section 8.

If the value of PNSetupType attribute is 2 or 3 after receiving the PNSetupRequest message from the originating PNE, the PN GW SHALL wait the response from all the CPNS devices connected to the PN GW if PNSetupType attribute is 2 or

PNEs to be invited if PNSetupType attribute is 3 respectively. After receiving the responses, the PNGW SHALL generate PNSetupRequest message according to the format of CPNS Message in Section 8.

The PN GW

1. SHALL include the PNEID as part of OriginEntityID attribute.
2. SHALL include PNInfo element.

   The PNInfo element contains attributes below.

   A. PNID attribute SHALL set the PNID, which is created in PN GW..
   B. Description attribute SHALL include texts which explain the PN.
   C. Disclosure attribute SHALL be included from PNSetupRequest message from PNE or PN GW SHALL choose one of three options and include.
      i. 1 for preventing PN Information to be delivered, in case Service Discovery is requested after PN setup.
      ii. 2 for allowing PN Information to be delivered, in case Service Discovery is requested after PN setup.
      iii. 3 for asking confirmation to OwnershipEntity whether or not PN Information is delivered, in case Service Discovery is requested after PN setup.
   D. OwnershipEntity attribute MAY be EntityID which has authorization to allow PN Information delivery, in case Service Discovery is requested after PN setup.
   E. TempPN attribute SHALL be included from PNSetupRequest message from PNE or PN GW SHALL choose one of two options and include.
      i. True, indicating that broken physical connection releases PN after PN setup.
      ii. False, indicating that PN Information remains in CPNS Server, even if physical connection is broken. If PN GW decides False, TempPN attribute MAY be skipped.
   F. Sharing attribute MAY be included.
      i. 1 for sharing the PNE Info and PN GW Info with other PNE member(s) of PN. If PN GW decides '1' (Shared), Sharing attribute MAY be skipped
      ii. 2 for preventing the PNE Info to be shared with other PNE member(s) of PN, but delivering PN GW Info to PNE member(s) of PN
3. SHALL include the PNGWInfo element.

   The PNGWInfo element contains attributes below.

   A. PNGWID attribute SHALL set PNGWID.
   B. PNGWName attribute MAY include the nickname of PN GW assigned by CPNS User or device type.
4. SHALL include PNEInfo element which contains all PNE(s) information including DeviceCapa and ServiceProfile from originating PNE and invited PNE(s).
5. SHALL include AuthIniData element as described in 7.5.1.2
6. SHALL send the PNSetupRequest message to the CPNS Server.

Upon receiving the AuthenticateRequest from the CPNS Server, the PN GW SHALL deliver Authenticaterequest to the PNEs as described in 7.5.1.2. Upon receiving the AuthenticateResponse from the requested PNEs, the PN GW SHALL deliver the Authenticateresponse to the CPNS Server described in 7.5.1.2.

Upon receiving the PNSetupResponse message from the CPNS Server, the PN GW

1. SHALL store the PN Information in local PN Inventory under PNInfo element.
2. SHALL include AuthFinData as described in 7.5.1.2 and send the PNSetupResponse message to the originating PNE. If the value in sharing attribute is,

A. 1 – Shared, the PN GW SHALL include PN GW Info and PNE Info, which are derived in PNSetupResponse message from the CPNS Server, in the PNSetupResponse message to the originating PNE.

B. 2 - Protected, the PN GW SHALL include only PN GW Info, which is derived in PNSetupResponse message from the CPNS Server, in the PNSetupResponse message to the originating PNE.

3. SHALL include AuthFinData as described in 7.5.1.2 and send the PNEstablishmentNotify to the invited PNE(s). If the value in sharing attribute is,

A. 1 – Shared, the PN GW SHALL include PN GW Info and PNE Info, which are derived in PNSetupResponse from the CPNS Server, in the PNEestablishmentNotify.

B. 2 - Protected, the PN GW SHALL include only PN GW Info, which is derived in PNSetupResponse from the CPNS Server, in the PNEstablishmentNofity.

[PN GW Initiated]

The PN GW SHALL generate and send PNSetupRequest message to the PNE(s) according to format of CPNS Message in section 8.

Upon receiving the PNSetupResponse message from the PNE, the PN GW SHALL check the answer to PNSetupRequest message in Return attribute in order to confirm participation in PN. If the value of Return attribute is 1, the PN GW SHALL create the information for PN Inventory for the corresponding PN, create and maintain routing table with the derived from PANTech and Address attributes from PNSetupResponse for the routing of inside PN.

After receiving the responses, the PNGW SHALL generate PNSetupRequest message according to the format of CPNS Message in Section 8. The PN GW

1. SHALL include the PNGWID as part of OriginEntityID attribute.
2. SHALL include PNInfo element.

The PNInfo element contains attributes below.

A. PNID attribute SHALL set the PNID, which is created in PN GW..

B. Description attribute SHALL include texts which explain the PN.

C. Disclosure attribute SHALL be included from PNSetupRequest message from PNE or PN GW SHALL choose one of three options and include.

iv. 1 for preventing PN Information to be delivered, in case Service Discovery is requested after PN setup.

v. 2 for allowing PN Information to be delivered, in case Service Discovery is requested after PN setup.

vi. 3 for asking confirmation to OwnershipEntity whether or not PN Information is delivered, in case Service Discovery is requested after PN setup.

D. OwnershipEntity attribute MAY be EntityID which has authorization to allow PN Information delivery, in case Service Discovery is requested after PN setup.

E. TempPN attribute SHALL be included from PNSetupRequest message from PNE or PN GW SHALL choose one of two options and include.

iii. True, indicating that broken physical connection releases PN after PN setup.

iv. False, indicating that PN Information remains in CPNS Server, even if physical connection is broken. If PN GW decides False, TempPN attribute MAY be skipped.

F. Sharing attribute MAY be included.

iii. 1 for sharing the PNE Info and PN GW Info with other PNE member(s) of PN. If PN GW decides ‘1’ (Shared), Sharing attribute MAY be skipped

iv. 2 for preventing the PNE Info to be shared with other PNE member(s) of PN, but delivering PN GW Info to PNE member(s) of PN

3. SHALL include the PNGWInfo element.

The PNGWInfo element contains attributes below.

A. PNGWID attribute SHALL set PNGWID.

B. PNGWName attribute MAY include the nickname of PN GW assigned by CPNS User or device type.

4. SHALL include PNEInfo element which contains all PNE(s) information including DeviceCapa and ServiceProfile from originating PNE and invited PNE(s).
5. SHALL include AuthIniData element as described in 7.5.1.2
6. SHALL send the PNSetupRequest message to the CPNS Server.

Upon receiving the AuthenticateRequest from the CPNS Server, the PN GW SHALL deliver the Authenticaterequest to the PNEs as described in 7.5.1.2Upon receiving the AuthenticateResponse from the requested PNEs, the PN GW SHALL deliver the Authenticateresponse to the CPNS Server as described in 7.5.1.2.

Upon receiving the PNSetupResponse message from the CPNS Server, the PN GW

1. SHALL store the PN Information in local PN Inventory under PNInfo element.
2. SHALL include AuthFinData and send the PNEstablishmentNotify to the invited PNE(s). If the value in sharing attribute is,

A. 1 – Shared, the PN GW SHALL include PN GW Info and PNE Info, which are derived in PNSetupResponse from the CPNS Server, in the PNEestablishmentNotify.

B. 2 - Protected, the PN GW SHALL include only PN GW Info, which is derived in PNSetupResponse from the CPNS Server, in the PNEstablishmentNofity.

7.6.1.3 CPNS Server

Upon receiving the PNSetupRequest message from PN GW, the CPNS Server SAHLL generate the Authenticate Request according to format of CPNS Message in section 8 as described in 7.5.1.3. The CPNS Server

1. SHALL include AuthReqData element as described in 7.5.1.3
2. SHALL send AuthenticateRequest towards the PN GW with PNID.

If the authentication is successful, the CPNS Server SHALL register and store the PN information which is derived from PNSetupRequest message in the PN inventory.

After storing the PN Information in the PN Inventory, the CPNS Server SHALL generate the PNSetupResponse according to the format of CPNS Message in section 8. The CPNS Server

1. SHALL include the answer to PNSetupRequest message in Return attribute.
2. SHALL include the stored PN information in the PN Inventory under PNInfo element.
3. SHALL include AuthFinData element as described in 7.5.1.3
4. SHALL send the PNSetupResponse message to the PN GW.

NOTE : Based on the specific criteria, the CPNS Server can decide whether to allow the PN setup or not. The criteria set by such as operator's decision, capacity of CPNS server, user's configuration, and so forth is out of scope of CPNS v1.0

7.6.2 PNE Management

This section describes managing members of PN, which are PNEs, after PN Establishment procedure. As for PNE inviting and PNE joining, invited PNE and joining PNE SHALL perform mutual authentication with PN GW and CPNS Server before connecting to PN. The procedure for mutual authentication in each entity is described in 7.5.Mutual Authentication

7.6.2.1 PNE Inviting

7.6.2.1.1 PNE

[Procedure in inviting PNE]

After a PN is established, PNE can invite additional PNE to join the PN. To realize this, PNE SHALL create the PNActionRequest message including below sub attributes and elements. PNE SHOULD find out the information of invited PNE in entity discovery procedure.

- Command attribute SHALL be inserted with "2" (Invite) value.
- OriginEntityID attribute SHALL be inserted for invite requesting PNE's PNEID.
- PNEInfo element SHALL be inserted for PNE to be invited.
    - PNEID attribute SHALL be inserted
- PNInfo element SHALL be inserted
    - PNID attribute SHALL be inserted from PN Inventory.
    - Description attribute SHOULD be inserted if PN Inventory contains
    - TempPN attribute SHALL be applied if requesting Entity has PN Inventory with TempPN attribute.
    - Sharing attribute SHALL be inserted from PN Inventory.
    - PNGWInfo element SHALL be inserted from PN Inventory.
        - PNGWID attribute SHALL be inserted.
        - PNGWName attribute SHOULD be inserted if PN Inventory contains.
        - Zonebasedservicesupport attribute SHALL be inserted if PN Inventory contains.
        - Mode attribute SHALL be inserted from PN Inventory.

After creating the PNActionRequest message, PNE SHALL send the PNActionRequest message to PN GW.

When PNE receives the PNActionResponse message with Result attribute "1" (Success) from PN GW, PNE SHOULD store invited PNE's PNEInfo including below attributes in local PN Inventory if the PN GW shares the member information with the member of PN, which means Sharing attribute is "1" .

- PNEID attribute SHALL be inserted.
- PNEName attribute SHOULD be inserted if it is found in entity discovery procedure.
- Active attribute SHALL be inserted with "TRUE" value.

[Procedure in invited PNE]

When the invited PNE receives the PNUpdateNotification message from PNGW, PNE SHALL create PN Inventory and store PNInfo elements in local PN Inventory and then send the PNActionResponse message including Result attribute "1" (Success) to PN GW

PNE's procedure for PNE authentication during PNE inviting is described in 7.5.1.1.

7.6.2.1.2 PN GW

[PN GW initiated invitation request]

After a PN is established, PN GW can invite additional PNE to join the PN after entity discovery procedure. To realize this, PN GW SHALL create the PNActionRequest message for invited PNE including below sub attribute and elements.

- Command attribute SHALL be inserted with "2" (Invite) value.
- PNEInfo element SHALL be inserted for PNE to be invited.
    - PNEID attribute SHALL be inserted
- PNInfo element SHALL be inserted
    - PNID attribute SHALL be inserted from PN Inventory.
    - Description attribute SHOULD be inserted if PN Inventory contains
    - TempPN attribute SHALL be applied if requesting Entity has PN Inventory with TempPN attribute.
    - Sharing attribute SHALL be inserted from PN Inventory.
    - PNGWInfo element SHALL be inserted from PN Inventory.
        - PNGWID attribute SHALL be inserted.
        - Name attribute SHOULD be inserted if PN Inventory contains.
        - Zonebasedservicesupport attribute SHALL be inserted if PN Inventory contains.
        - Mode attribute SHALL be inserted from PN Inventory.
    - PNEInfo element SHOULD be inserted for current member of PN if Sharing attribute is set "1" to share the member information from PN Inventory.
        - PNEID attribute SHALL be inserted.
        - PNEName attribute SHOULD be inserted if PN Inventory contains.
        - Mode attribute SHALL be inserted from PN Inventory.

After creating the PNActionRequest message, PN GW SHALL send the PNActionRequest message to each invited PNE.

[PNE initiated invitation request]

When PN GW receives the PNActionRequest message with Command attribute "2" (Invite) from PNE, PN GW SHALL check that invited PNE is in detected devices by PN GW through entity discovery procedure.

If PNGW does not have information of invited PNE, which means PN GW can't connect with invited PNE physically or can't find invited PNE through entity discovery, PN GW SHALL send the PNActionResponse message with Result attribute "3" (Fail, not connected) to requesting PNE.

If the invited PNE is detected by PN GW, PN GW SHALL forward the PNActionRequest message to PNE to be invited.

[PN GW procedure common to PNE initiated and PN GW initiated invitation cases]

When PN GW receives the PNActionResponse message with Result attribute "1" (Success) from PNE, PN GW SHALL send the PNUpdateRequest message to CPNS Server including below sub attribute and element.

- PNInfo element SHALL be inserted
    - PNID attribute SHALL be inserted
    - PNEInfo element SHALL be inserted for successfully invited PNE.
        - PNEID attribute SHALL be inserted

        - PNEName attribute SHOULD be inserted if it was received in entity discovery procedure.
        - Active attribute SHALL be "TRUE".
        - Update attribute SHALL be inserted with "1" (New) value.
        - Mode attribute SHALL be inserted during entity discovery procedure.
- AuthIniData element SHALL be inserted as described in 7.5.1.2, which describes PN GW's procedure for PNE authentication.

When PN GW receives the PNUpdateResponse message from CPNS Server, PN GW SHALL update PNEInfo in local PN Inventory from the PNUpdateRequest message

After storing PNEInfo in local PN Inventory, if the PN GW shares the member information with the member of PN (Sharing attribute is "1"), PN GW SHALL send the PNUpdateNotification message to newly invited member PNE. Below are attributes and elements included in the message. Also, PN GW SHOULD send the PNUpdateNotification message to existed member PNE(s) including below sub attribute and element.

- PNInfo element SHALL be inserted from PN Inventory.
    - PNID attribute SHALL be inserted from PN Inventory.
    - PNEInfo element SHALL be inserted for the newly invited PNE(s).
        - PNEID attribute SHALL be inserted
        - PNEName attribute SHOULD be inserted if it was received in entity discovery procedure.
        - Active attribute SHALL be "TRUE".
        - Update attribute SHALL be inserted with "1" (New) value.
        - Mode attribute SHALL be inserted.
- AuthFinData element SHALL be inserted as described in 7.5.1.2, which describes PN GW's procedure for PNE authentication.

If the original request was initiated by PNE, PN GW SHALL send PNEActionResponse message including Result attribute "1" (Success) to PNE referring OriginEntityID in PNEActionRequest message.

Additional PN GW's procedure for PNE authentication during PNE inviting is described in 7.5.1.2.

7.6.2.1.3 CPNS Server

When CPNS Server receives the PNUpdateRequest message from PN GW, CPNS Server SHALL update PN Inventory with PNEInfo element in PNInfo element, and then CPNS Server SHALL send the PNUpdateResponse message with Result attribute to PN GW.

CPNS Server's procedure for PNE authentication during PNE inviting is described in 7.5.1.3.

7.6.2.2 PNE Joining

7.6.2.2.1 PNE

After a PN is established, PNE can join PN as a member. To realize this, PNE SHALL send the PNActionRequest message to PNGW in a target PN including below attribute and elements.

- Command attribute SHALL be inserted with "1" (Join) value.
- PNEInfo element SHALL be inserted for joining PNE to PNGW in a target PN.
    - PNEID attribute SHALL be inserted

- PNEName attribute SHOULD be inserted

- PNInfo element SHALL be inserted to notify which PN
  - PNID attribute SHALL be inserted regarding PNGW handles several PNs. And this PNID was obtained when PNE went through entity discovery process to find out proper PN GW or its PN.

- AuthIniData element SHALL be inserted as described in 7.5.1.1, which describes PNE's procedure for PNE authentication.

When PNE receives the PNActionResponse message with Result attribute "1" (Success) from PN GW, PNE SHALL create PN Inventory and then store PNInfo element in local PN Inventory PN Inventory).

Additional PNE's procedure for PNE authentication during PNE joining is described in 7.5.1.1.

7.6.2.2.2 PN GW

When PN GW receives the PNActionRequest message with Command attribute "1" (Join) from PNE, PN GW SHALL send the PNUpdateRequest message to CPNS Server including below attribute and element.

- PNInfo element SHALL be inserted
  - PNID attribute SHALL be inserted
  - PNEInfo element SHALL be inserted for joining PNE
    - PNEID attribute SHALL be inserted
    - PNEName attribute SHOULD be inserted if it was received in the PNActionRequest message or entity discovery procedure.
    - Active attribute SHALL be "TRUE".
    - Update attribute SHALL be inserted with "1" (New) value.
    - Mode attribute SHALL be inserted.

- AuthIniData element SHALL be inserted as described in 7.5.1.2, which describes PN GW's procedure for PNE authentication.

When PN GW receives the PNUpdateResponse message from CPNS Server, PN GW SHALL store PNEInfo in local PN Inventory and then PN GW SHALL send the PNActionResponse message to newly joined PNE including below attribute and element.

- Result attribute SHALL be inserted with "1"(Success) value.

- PNInfo element SHALL be inserted
  - PNID attribute SHALL be inserted from PN Inventory.
  - Description attribute SHOULD be inserted if PN Inventory contains
  - TempPN attribute SHALL be applied if requesting Entity has PN Inventory with TempPN attribute.
  - Sharing attribute SHALL be inserted from PN Inventory.
  - PNGWInfo element SHALL be inserted from PN Inventory.
    - PNGWID attribute SHALL be inserted.
    - PNGWName attribute SHOULD be inserted if PN Inventory contains.
    - Zonebasedservicesupport attribute SHALL be inserted if PN Inventory contains.

        - Mode attribute SHALL be inserted.
    - PNEInfo element SHOULD be inserted for current member of PN if Sharing attribute is set "1" to share the member information from PN Inventory.
        - PNEID attribute SHALL be inserted.
        - PNEName attribute SHOULD be inserted if PN Inventory contains.
        - Active attribute SHALL be inserted.
        - Mode attribute SHALL be inserted.
- AuthFinData element SHALL be inserted as described in 7.5.1.2, which describes PN GW's procedure for PNE authentication.

After sending the PNActionResponse message, if the PN GW shares the member information with the member of PN (Sharing attribute is "1"), PN GW SHOULD create the PNUpdateNotification message for existed member PNE(s) include

- PNInfo element SHALL be inserted from PN Inventory.
    - PNID attribute SHALL be inserted from PN Inventory.
    - PNEInfo element for the newly joined PNE.
        - PNEID attribute SHALL be inserted
        - PNEName attribute SHOULD be inserted if it was received in entity discovery procedure.
        - Active attribute SHALL be "TRUE".
        - Update attribute SHALL be inserted with "1" (New) value.
        - Mode attribute SHALL be inserted.

After creating PNUpdateNotification messages, PN GW SHOULD send PNUpdateNotification messages to the member PNEs in the PN.

Additional PN GW's procedure for PNE authentication during PNE joining is described in 7.5.1.2.

7.6.2.2.3 CPNS Server

When CPNS Server receives the PNUpdateRequest message from PN GW, CPNS Server SHALL update PN Inventory with PNEInfo element in PNInfo element, and then CPNS Server SHALL send the PNUpdateResponse message with Result attribute to PN GW.

CPNS Server's procedure for PNE authentication during PNE joining is described in 7.5.1.3.

7.6.2.3 PNE Expulsion

If all of member PNEs in a PN are owned by same CPNS User, any member PNE can request expulsion of the other member PNE.

7.6.2.3.1 PNE

[Procedure in expelling PNE]

When PNE wants to expel the other PNE, PNE SHALL send the PNActionRequest message to PN GW including below attribute and element.

- Command attribute SHALL be inserted with "4"(Expel) value.
- OriginEntityID attribute SHALL be inserted for PNE which wants to expel other PNE.

- PNEInfo element SHALL be inserted for expelled PNE
    - PNEID attribute SHALL be inserted
- PNInfo element SHALL be inserted to notify that PNE should be expelled from which PN.
    - PNID attribute SHALL be inserted.

When PNE receives the PNActionResponse message with Result "1"(Success) from PN GW, PNE SHALL remove the PNEInfo element of PNInfo from PN Inventory.

[Procedure in expelled PNE]

When PNE receives the PNActionNotification message with Command attribute "1" (Expel) from PN GW, expelled PNE SHALL remove PNInfo element in local PN Inventory and SHALL remove available SGInfo element in local SG Inventory for the SG related with this PN.

7.6.2.3.2 PN GW

When PN GW receives the PNActionRequest message with Command "4"(Expel) from PNE or if PN GW wants to expel a certain member PNE of PN, PN GW SHALL check if the requesting PNE can expel the target PNE, if the requesting PNE can do this, then PN GW SHALL check the expelled PNE is connected with PN GW currently. If expelled PNE is not connected with PN GW and the expulsion request was initiated by PNE, PN GW SHALL send the PNActionResponse message with Result attribute "3" (Fail, not connected) to the requester PNE.

After sending the PNActionResponse message, PN GW SHALL check member PNEs in this PN.

If the expelled PNE is the last member PNE in PN, PN GW SHALL initiate PN release procedure (Section 7.6.3.2 PN GW).

If there are member PNEs of this PN, PN GW SHALL send the PNUpdateRequest message to CPNS Server including below attribute and element

- PNInfo element SHALL be inserted to notify which PN
    - PNID attribute SHALL be inserted.
    - PNEInfo element SHALL be inserted for expelled PNE.
        - PNEID attribute SHALL be inserted.
        - Update attribute SHALL be inserted with "3" (Removed) value.

When PN GW receives the PNUpdateResponse message from CPNS Server, PN GW SHALL check Sharing attribute of this PN. If the PN GW shares the member information with the member of PN (Sharing attribute is "1"), PN GW SHOULD send the PNUpdateNotification messages to existed member PNEs including below attribute and element.

- PNInfo element SHALL be inserted from PN Inventory.
    - PNID attribute SHALL be inserted from PN Inventory.
    - PNEInfo element for the expelled PNE.
        - PNEID attribute SHALL be inserted
        - Update attribute SHALL be inserted with "3" (Removed) value.

After checking Sharing attribute for sending PNUpdateNotification messages, PN GW SHALL send the PNActionNotification message to expelled PNE including below attribute and element.

- Command attribute SHALL be inserted with "1"(Expel) value.
- PNEID attribute SHALL be inserted with expelled PNE's ID

- PNID attribute SHALL be inserted to notify that PNE should be expelled from which PN.

After sending the PNActionNotification message, PN GW SHALL remove PNEInfo element of PNInfo element in local PN Inventory. If the expulsion request was initiated by PNE, PN GW SHALL send the PNActionResponse message with Result attribute with "1" (Success) to requester PNE.

7.6.2.3.3 CPNS Server

When CPNS Server receives the PNUpdateRequest message from PN GW, CPNS Server SHALL update PN Inventory removing PNEInfo element in PNInfo element.

After updating PNInfo element in local PN Inventory, CPNS Server SHALL send the PNUpdateResponse message with Status attribute to PN GW.

7.6.2.4 PNE Leaving

7.6.2.4.1 PNE

When PNE wants to leave a PN, PNE SHALL send the PNActionRequest message to PN GW including below attribute and element.

- Command attribute SHALL be inserted with "3" (Leave) value.
- PNEInfo element SHALL be inserted for PNE to leave
    - PNEID attribute SHALL be inserted
- PNInfo element SHALL be inserted to notify that PNE should leave from which PN.
    - PNID attribute SHALL be inserted.

If PNE is physically disconnected with PN GW forming temporary PN, PNE SHALL remove the PNInfo element in local PN Inventory.

7.6.2.4.2 PN GW

When PN GW receives the PNActionRequest message with Command "3"(Leave) from PNE, PN GW SHALL send the PNUpdateRequest message to CPNS Server including below attribute and element

- PNInfo element SHALL be inserted to notify which PN
    - PNID attribute SHALL be inserted.
    - PNEInfo element SHALL be inserted for left PNE.
        - PNEID attribute SHALL be inserted.
        - Update attribute SHALL be inserted with "3" (Removed) value.

When PN GW receives the PNUpdateResponse message from CPNS Server, PN GW SHALL check Sharing attribute of this PN and SHALL send the PNActionResponse message to physically connected PNE to be left including below attribute and element.

- Result attribute SHALL be inserted with "1"(Success)

After sending the PNUpdateResponse message, PN GW SHALL remove PNEInfo element of PNInfo element in local PN Inventory.

If the PN GW shares the member information with the member of PN (Sharing attribute is "1"), PN GW SHOULD send the PNUpdateNotification messages to existed member PNEs including below attribute and element.

- PNInfo element SHALL be inserted from PN Inventory.
    - PNID attribute SHALL be inserted from PN Inventory.
    - PNEInfo element for the expelled PNE.
        - PNEID attribute SHALL be inserted
        - Update attribute SHALL be inserted with "3" (Removed) value.

If the leaving PNE is the last member in PN, PN GW SHALL initiate PN release procedure.

7.6.2.4.3 CPNS Server

When CPNS Server receives the PNUpdateRequest message from PN GW, CPNS Server SHALL update PN Inventory removing PNEInfo element in PNInfo element.

After updating PNInfo element in local PN Inventory, CPNS Server SHALL send the PNUpdateResponse message with Result attribute "1" (Success) to PN GW.

7.6.3 PN Release

When PNE or PN GW wants to release PN which it belongs to, PNE or PN GW can send release request message.

If the type of PN is temporary PN, the PN should be released when all of the physical connection between gateway and devices are broken, which means PN GW should send release message to CPNS Server and PNE and PN GW should remove the PNInfo element in local PN Inventory each other.

7.6.3.1 PNE

When PNE wants to remove a PN which it belongs to, PNE SHALL send the PNReleaseRequest message to the PN GW including below attributes.

- PNID attribute SHALL be inserted
- PNEID attribute SHALL be inserted for requesting PNE

If PNE receives the PNReleaseResponse message from PN GW, PNE SHALL remove the PNInfo element of PN Inventory related with this PNID.

If PNE receives the PNReleaseNotification message from PN GW, PNE SHALL remove the PNInfo element of PN Inventory related with this PNID.

If the PNE in the temporary PN is unintentionally disconnected without PN Release, that PNE SHALL remove the PNInfo element in local PN Inventory.

7.6.3.2 PN GW

When PN GW receives the PNReleaseRequest message from PNE, PN GW wants to remove a PN which PN GW belongs to, or PN GW is disconnected with all of PNEs forming temporary PN, PN GW SHALL send the PNReleaseRequest message to CPNS Server including below attributes.

- PNID attribute SHALL be inserted
- PNEID attribute for requesting PNE SHALL be inserted if this release request was initiated by PNE.

When PN GW receives the PNReleaseResponse message with Result attribute "1" (Success) from CPNS Server, PN GW SHALL check there are connected PNEs forming this released PN. If there are connected member PNEs, PN GW SHALL send the PNReleaseNotification messages including PNID attribute to the PNEs, which are members in PN. If PNE requested release PN originally, PN GW SHALL NOT send the PNReleaseNotifcation message to the requesting PNE. PN GW SHALL remove PNInfo element in local PN Inventory related with this PNID of PN to be released.

When PN GW receives the PNReleaseNotification message from CPNS Server, PN GW SHOULD display Reason attribute to the User if this message contains Reason attribute.

PN GW SHALL check there are connected PNEs forming this released PN. If there are connected member PNEs, PN GW SHALL send the PNReleaseNotification messages including PNID attribute to the PNEs, which are members in PN. After notification to the member PNE, PN GW SHALL send the PNReleaseReponse message including Result attribute with "1" (Success) to CPNS Server. PN GW SHALL remove PNInfo element in local PN Inventory related with this PNID of PN to be released.

If the PN GW is disconnected with member PNE forming PN to be release, PN GW SHALL send the PNReleaseResponse message to the CPNS Server including.

- Result attribute SHALL be "3" (Fail, PNE disconnected)
- PNEInfo element SHALL be included for the disconnected PNE
    - PNEID attribute SHALL be included for PNE ID.

7.6.3.3 CPNS Server

When CPNS Server receives the PNReleaseRequest message from PN GW, CPNS Server SHALL create the PNReleaseResponse message including

- Result attribute SHALL be inserted with "1"(Success) .

After creating the message, CPNS Server SHALL send the PNReleaseResponse message to PN GW and CPNS Server SHALL remove the PNInfo element related with this PNID in local PN Inventory if there is no Service Group for member PNEs.

If PN release is requested by Operator Policy, CPNS Server SHALL send the PNReleaseNotification message including PNID attribute and Reason attribute to the PN GW, CPNS Server SHALL remove PNInfo element in local PN Inventory.

7.7 Service Group Management

7.7.1 Service Group Creation

7.7.1.1 PNE

When PNE is requested to create Service Group from CPNS User and PNE wants to be SG Owner of certain Service Group, PNE SHALL send the SGCreateRequest message to PN GW including below. If there is no SG Inventory in the PNE, PNE SHALL create SG Inventory first.

- OriginEntityID attribute SHALL be inserted for creation requesting PNE.
- SGInfo element SHALL be inserted
    - SGDescription attribute SHOULD be inserted to describe the Service Group.
    - Sharing attribute SHALL be inserted based on the applicable access level to the SG information .
        - If a member PNE wants to share the SG information with other SG members only, the value of the Sharing attribute will be '2' for Selective access level.
        - If a member PNE wants to restrict access to SG information for any PNE, regardless of whether being of SG member or not, the value of the Sharing attribute will be '3' for Closed access level
    - MaxPNE attribute SHALL be inserted if PNE wants to insert its maximum number of members. CPNS Server SHALL check this MaxPNE whenever the additional PNE joins.

- MaxUser attribute SHALL be inserted if PNE wants to insert its maximum number of CPNS User(s). CPNS Server SHALL check this MaxUser whenever the additional PNE joins using CPNS User information of that PNE.
- ServiceID elements SHALL be inserted if this PNE knows ServiceIDs through service discovery procedure or the other procedure, and wants to get that service.

- PNEInfo element SHALL be inserted for invited PNE(s), if creation requesting PNE wants to invite the other PNEs.
  - PNEID attribute SHALL be inserted to specify PNE to be invited.

When PNE receives the SGCreateResponse message from PN GW, PNE SHALL store following information in the SG Inventory.

- SGInfo element SHALL be stored from the SGCreateResponse message.
- MemberInfo element SHALL be stored from PNEInfo element in the SGCreateResponse message, which PNEInfo element has Result attribute with "1" (Success).

7.7.1.2 PN GW

When PN GW receives the SGCreateRequest message from PNE or PN GW creates the SGCreateRequest message including attribute and elements except OriginEntityID attribute at CPNS User request, PN GW SHALL send the SGCreateRequest message to CPNS Server. When PN GW creates the SGCreateRequest message, PN GW SHALL insert SG Owner using member PNE in PN handled by this PN GW.

When PN GW receives the SGCreateResponse message from CPNS Server, PN GW SHALL create new SGInfo element in local SG Inventory based on following information included in the SGCreateResponse message.

- SGInfo element SHALL be stored from the SGCreateResponse message.
- MemberInfo element SHALL be stored from PNEInfo element with only PNEID and PNGWID attributes (without any elements and Name attribute because they are stored in local PN Inventory) in the SGCreateResponse message if Result attribute is "1" (Success), and value of PNGWID is part of its PN for this PNGW, which means this PNE is forming same PN with this PN GW.

And then PN GW SHALL send the SGCreateResponse message to the requesting PNE for Service Group creation if SG creation request was initiated by PNE.

7.7.1.3 CPNS Server

When CPNS Server receives the SGCreateRequest message, CPNS Server SHALL assign SGID.

If invited PNE's PNEID(s) is inserted in the SGCreateRequest message, CPNS Server SHALL create SGInviteRequest messages per PN GW forming same PN with invited PNEs including

- SGInfo element SHALL be inserted.
  - SGID attribute SHALL be inserted which is assigned by CPNS Server.
  - SGDescription attribute SHOULD be inserted if this is available in the SGCreateRequest message from PN GW..
  - ServiceInfo element SHALL be inserted if the SGCreateRequest message has ServiceInfo element.
    - ServiceID attribute SHALL be inserted if the SGCreateRequest message has this.
    - Keyword attribute SHALL be inserted if CPNS Server finds out appropriate Keyword for this ServiceID in the registered service list.

- MemberInfo element SHALL be inserted with only one sub element for the SG Owner if Sharing attribute is “2”(Selective).
  - PNEID attribute SHALL be inserted.
  - Name attribute SHOULD be inserted for the name of SG Owner PNE if the SGCreateRequest message contains.

- PNEInfo element SHALL be inserted for invited PNEs per PN GW forming same PN.
  - PNEID attribute SHALL be inserted for invited PNE
  - PNGWID attribute SHALL be inserted with proper PN for the invited PNE. If the invited PNE joins multiple PNs, CPNS Server should select proper PN based on certain criteria such as the number of PNEs in PN and capabilities of PN GW (e.g. network capabilities, device capabilities, charging, location).

CPNS Server SHALL send SGInviteRequest messages to selected PN GW(s) forming same PN with invited PNE(s) after CPNS Server finds out appropriate PN in local PN Inventory.

When CPNS Server receives the SGInviteResponse messages from all PN GW(s), which are forming the PNwith invited PNE(s), CPNS Server SHALL request the service to the Service Provider based on ServiceID attribute. Upon Receiving the success response from Service Provider, CPNS Server SHALL create new SGInfo element in SG Inventory and store the SGInfo element from the SGCreatRequest message and store MemberInfo element from PNEInfo element having Result attribute “1” (Success) in the SGInviteResponse message.

CPNS Server SHALL send the SGCreateResponse message to the PN GW, which sent the SGCreateRequest message to CPNS Server originally,. If CPNS Server changes the value of sub attribute in SGInfo element, it SHALL be applied in SGCreateResponse message. (e.g. requester wants to set 10 for MaxPNE, but CPNS Server allows only 5)

After sending the SGCreateResponse message, CPNS Server SHALL initiate Service Group Member Update procedure when the Shairing attribute is “1” or “2”.

NOTE: The member update procedure can be done before sending the SGCreateResponse message to PN GW. This update is possible when CPNS Server sends the SGChangeNotification message for the member update procedure before sending the SGCreateResponse message.

7.7.2 Management of SG Controlling Entities

This section describes managing members of Service Group after Service Group Creation procedure.

7.7.2.1 PNE Invite in Service Group

7.7.2.1.1 PNE

[Procedure in inviter PNE]

When CPNS User requests PNE to invite the other PNE(s), PNE SHALL send the SGInviteRequest message to PN GW including below.

- OriginEntityID attribute SHALL be inserted which is EntityID of the requesting PNE
- SGInfo element SHALL be inserted to provide information of the Service Group to invited PNE
  - SGID attribute SHALL be inserted for Service Group ID
  - SGDescription attribute MAY be inserted. This attribute can be skipped because this is stored in SG Inventory of CPNS Server.
- PNEInfo element SHALL be inserted for PNE(s) to be invited.
  - PNEID attribute SHALL be inserted for PNE to be invited.

When PNE receives the SGInviteResponse message from PN GW, PNE SHALL update local SG Inventory using PNEInfo element for the successfully invited PNE, which means the value of Result attributeis “1” (Success) in the SGInviteResponse message.

[Procedure in invited PNE]

When PNE receives the SGInviteRequest message from PN GW in the same PN, PNE SHALL create the SGInviteResponse message including PNEInfo element with below two attributes.

- PNEID attribute SHALL be inserted.
- Result attribute SHALL be inserted with “1” (Success) if CPNS User accepts SG Invite Request or PNE is pre-configured to automatically accept SG Invite Request, or “5” (fail) if CPNS User rejects SG Invite Request.

And PNE includes additionally below attributes and elements for the PNE in case of Result “1”.

- PNGWID attribute SHALL be inserted from the SGInviteRequest message
- Name attribute SHALL be inserted if device supports.
- UserInfo element SHOULD be inserted from CPNS Profile in device
- DeviceCapa and ServiceProfile element MAY be inserted from CPNS Profile in device if the CPNS User wants to share its information with the other members. This can be inserted depending on its local privacy or sharing policy about CPNS Profile in device.

After creating the SGInviteResponse message, PNE SHALL send the SGInviteResponse message to the PN GW.

7.7.2.1.2 PN GW

When PNGW receives the SGInviteRequest message from PNE or create SGInviteRequest message including elements and attributes except OriginEntityID attribute for requester PNE (see section 7.7.2.1.1) at CPNS User request, PN GW SHALL send the SGInviteRequest message to CPNS Server.

When PN GW receives the SGInviteRequest message from CPNS Server,

- PN GW SHALL send the SGInviteResponse message to CPNS Server including Result attribute “4” (fail, this PNE is disconnected) if physical connections to all of invited PNEs are disconnected, or there is only one invited PNE in the SGInviteRequest message and the PNE is disconnected with PN GW physically.
- PN GW SHALL send SGInviteRequest messages with only one PNEInfo element to each invited PNE
- When PN GW receives all of SGInviteResponse messages from PNEs to which the PN GW sent SGInviteRequest messages, PN GW SHALL send the SGInviteResponse message to CPNS Server including all of PNEInfo element in the SGInviteResponse messages which were sent from PNEs. The Result attribute value is
    - “1”(Success) for the successfully invited PNE
    - “4” (Fail) for the disconnected PNE with PN GW
    - “5” (Fail) for the rejecting PNE from CPNS User.

When PN GW receives the SGInviteResponse message from CPNS Server, PN GW SHALL send the SGInviteResponse message to the requester PNE if the SGInviteRequest message is issued by PNE. PN GW SHALL update the successfully invited PNEInfo (Result attribute is “1” (Success)) with only PNEID and PNGWID attributes (without any elements and Name attribute because they are stored in local PN Inventory) in local SG Inventory if invited PNEs are the member of PN handed by this PN GW.

7.7.2.1.3 CPNS Server

When CPNS Server receives the SGInviteRequest message from PN GW, CPNS Server checks that PNEID attribute is in the SGInviteRequest message.

- If there is OriginEntityID, the CPNS Server SHALL check whether it is the ID of member PNE. . If there is no OriginEntityID attribute, the CPNS Server SHALL check whether the sender of this message (PN GW) is a SG Owner. CPNS Server can allow the invite request of other PNEs following the Operator Policy. If conditions above are not satisfied, CPNS Server SHALL send the SGInviteResponse message to the PN GW including Result attribute as fail "2".
- The CPNS Server SHALL check that invited PNEs can join the Service Group. If sum of the number of invited PNEs and the number of current member PNEs exceeds the maximum number of SG member PNEs, CPNS Server SHALL send the SGInviteResponse message to the PN GW including Result attribute as fail "3".

If above two examinations are successful, CPNS Server SHALL create the SGInviteRequest message including

- SGInfo element SHALL be inserted
    - SGID attribute SHALL be inserted for Service Group ID
    - SGDescription attribute SHALL be inserted if it is kept in the SG Inventory.
    - Sharing attribute SHALL be inserted from SG Inventory.
- ServiceInfo element SHALL be inserted if SG Inventory contains.
    - ServiceID attribute SHALL be inserted if it is kept in the SG Inventory.
    - Keyword attribute SHALL be inserted after finding out Keyword in the registered service list if SG Inventory contains ServiceID.
- MemberInfo element SHALL be inserted if Sharing attribute is "2"(Selective).
    - PNEID attribute SHALL be inserted.
    - Name attribute SHOULD be inserted if it is kept in the SG Inventory.
- PNEInfo element SHALL be inserted per the related PN GWs forming same PN with invited PNEs.
    - PNEID attribute SHALL be inserted for invited PNE.
    - PNGWID attribute SHOULD be inserted with proper PN for the invited PNE. If the invited PNE joins multiple PNs, CPNS Server should select proper PN based on certain criteria such as the number of PNEs in PN and capabilities of PN GW (e.g. network capabilities, device capabilities, charging, location).

And CPNS Server SHALL send SGInviteRequest messages to the related PN GWs with invited PNEs to relay this messages after CPNS Server finds out appropriate PN GWs in local PN Inventory.

When CPNS Server receives the SGInviteResponse message from the PN GW which is forming the PN with invited PNEs, CPNS Server SHALL update SG Inventory with PNEInfo element having Result attribute "1" (Success).

After getting all of SGInviteResponse messages from PN GWs to which CPNS Server had sent SGInviteRequest messages, CPNS Server SHALL send the SGInviteResponse message to the requesting PN GW, which had sent the SGInviteRequest message to CPNS Server at the first step, . This SGInviteResponse SHALL include PNEInfo element from received SGInviteResponse messages.

Finally, the Service Group Member Update procedure SHALL be performed. (see Section 0)

7.7.2.2 PNE Expulsion in Service Group

7.7.2.2.1 PNE

[Procedure in PNE when PNE expels other PNE(s)]

When a certain PNE requests to expel other PNE(s) in the SG,the PNE SHALL send the SGActionRequest message to PN GW including below.

- OriginEntityID attribute SHALL be inserted.
- SGInfo element SHALL be inserted with only SGID attribute to inform the Service Group
- PNEInfo element SHALL be inserted for expelled PNE(s) including
    - PNEID of target PNE and Action attribute with "1" (Expel)

When PNE receives the SGActionResponse message from PN GW, PNE SHALL remove PNE information in MemberInfo element of local SG Inventory using the successfully expelled PNE, which means the value of Result in PNEInfo is "1" (Success) and Action attribute is "1"(Expel).

[Procedure in PNE when PNE is expelled from Service Group]

When PNE receives the SGActionNotification message with Action attribute "1"(Expel), PNE SHALL remove SGInfo element in SG Inventory according to the Service Group which is designated by the SGActionNotification message.

7.7.2.2.2 PN GW

When PN GW receives the SGActionRequest message from PNE or create the SGActionRequest message including elements (see section 7.7.2.2.1) without OriginEntityID attribute at CPNS User request, PN GW SHALL send the SGActionRequest message to CPNS Server.

When PN GW receives the SGActionRequest message from CPNS Server, PN GW SHALL send the SGActionResponse message to CPNS Server including Result attribute "5" (fail, this PNE is disconnected) if all of target PNEs are disconnected, or there is only one PNE in the SGActionRequest message and PNE is disconnected with the PN GW.

After checking connection between PN GW and expelled PNEs, PN GW SHALL create SGActionNotification messages with SGID and PNEInfo (PNEID attribute and Action attribute "1"(Expel)) and then send SGActionNotification messages to each target PNEs if one or more of target PNEs are connected with this PN GW pertaining to the same PN.
And then, PN GW SHALL send the SGActionResponse message to CPNS Server including Result attribute. This Result attribute value is

- "1"(Success) for the successfully expelled PNE
- "4" (Fail) for the disconnected PNE with PN GW.

When PN GW gets the SGActionResponse message from CPNS Server, PN GW SHALL remove successfully expelled PNEInfo with Action attribute "1" (Expel) and Result"1" (Success) from local SG Inventory. And then PN GW SHALL send the SGActionResponse message to the requesting PNE if the SGActionRequest message is issued by PNE.

7.7.2.2.3 CPNS Server

When CPNS Server receives the SGActionRequest message from PN GW, CPNS Server checks Action attribute in sub element of PNEInfo element.

- If the value is "1" (Expel), the CPNS Server SHALL check that OriginEntityID is SG Owner in the Service Group.
- If the value is "1" (Expel), the CPNS Server SHALL check that this target PNE is the member of Service Group.

If either or both of above examinations are fail for all of sub elements of PNEInfo, CPNS Server SHALL send the SGActionResponse message to the PN GW including Result attribute as "2" (Fail, requesting PNE is not authorized for member expulsion) or "3" (Fail, expelled PNE is not the SG member).

If above two examinations are successful for one or more sub elements of PNEInfo, CPNS Server SHALL send SGActionRequest messages to the PN GW(s), which the expelled PNE(s) pertains to, using the PNGWID found in the SG Inventory.

When CPNS Server receives all of SGActionResponse messages from PN GWs, to which CPNS Server sent SGActionRequest message, CPNS Server SHALL update SG Inventory using PNEInfo element having Action attribute "1" (Expel) in SGActionRequest messages and send the SGActionResponse message to the PN GW in the same PN as with requesting PNE including PNEInfo with PNEID and Result attribute

- "1" if the expel is success
- "3"if requesting PNE does not match with SG Owner in CPNS Server examination
- "4" if the Result value is "4" in the SGActionResponse message from the related PN GW

After sending the SGActionResponse message, CPNS Server SHALL initiate Service Group Member Update procedure. (see Section 0)

7.7.2.3 PNE Joining, Leaving Service Group

7.7.2.3.1 PNE

When CPNS User wants PNE to join a Service Group or to leave a Service Group, PNE SHALL create the SGActionRequest message including

- OriginEntityID attribute SHALL be inserted for requesting PNE.
- SGInfo element SHALL be inserted with only SGID attribute to inform the Service Group
- PNEInfo element SHALL be inserted including
    - PNEID attribute SHALL be inserted for requesting PNE
    - PNGWID attribute SHOULD be inserted in case of joining after selecting appropriate PN GW from PN Inventory. If there are several PN GWs in PN Inventory, PNE can select proper PN based on certain criteria such as the considering bigger number of member PNE or early established PN.
    - Action attribute SHALL be inserted with "2" (Join) for joining or "3" (Leave) for leaving

And PNE SHALL send the SGActionRequest message to the selected PN GW.

When PNE receives the SGActionResponse message from PN GW, PNE SHALL

- store SGInfo element to local SG Inventory in case of joining (Action attribute is "2"(Join) and Result attribute is "1" (Success) in PNEInfo element) .
- remove local SG Inventory in case of leaving (Action attribute is "3"(Leave) in PNEInfo element)

7.7.2.3.2 PN GW

When PN GW receives the SGActionRequest message from PNE or PN GW wants connected member PNE to join or leave, PN GW SHALL send the SGActionRequest message to CPNS Server (see section 7.7.2.3.1).

When PN GW receives the SGActionResponse message from CPNS Server, PN GW SHALL,

- in case of joining, add following information of successful joining of PNE (Result attribute "1") in SG Inventory.

If PN GW stores SGInfo related with SGID contained in the SGActionResponse message in local SG Inventory,

- PNEID attribute and PNGWID attribute in PNEInfo element SHALL be added in local SG Inventory.

If PN GW does not store SGInfo related with SGID contained in the SGActionResponse message in local SG Inventory, PNE GW SHALL create one SGInfo element in local SG Inventory and

- SGID attribute, SGDescription attribute SHALL be added into SGInfo element
- ServiceID attribute of ServiceInfo element SHALL be added.
- PNEID attribute and PNGWID attribute of MemberInfo element SHALL be added from PNEInfo element and MemberInfo element in the SGActionResponse message.

- in case of leaving, remove MemberInfo element for left PNE from SG Inventory. If the left PNE is last SG member PNE of a Service Group in PN GW, PN GW SHALL remove SGInfo element from SG Inventory for the Service Group.

And then PN GW SHALL send the SGActionResponse message to the requesting PNE in case the SGActionRequest message was initiated by PNE.

7.7.2.3.3 CPNS Server

When CPNS Server receives the SGActionRequest message from PN GW, CPNS Server checks Action attribute in sub element of PNEInfo element.

- If the value is "2" (Join), the CPNS Server SHALL check maximum number of PNEs (i.e, MaxPNE) or maximum number of CPNS Users (i.e, MaxUser) for the SG
- If the value is "3" (Leave), the CPNS Server SHALL check that this target PNE is the member of Service Group.

If above examination is fail, CPNS Server SHALL send the SGActionResponse message to the PN GW including Result attribute "5" in case of join and "3" as fail in case of leave.

If above two examinations are successful, CPNS Server SHALL update MemberInfo element of SG Inventory using PNEInfo element in the SGActionRequest message and SHALL create the SGActionResponse message including below.

- PNEInfo element SHALL be inserted from the SGActionRequest message
  - PNEID attribute SHALL be inserted
  - Action attribute SHALL be inserted
  - Result attribute SHALL be inserted with "1" (Success)
- SGInfo element SHALL be inserted from local SG Inventory in case of join.

And then CPNS Server SHALL send the SGActionResponse message to the PN GW in the same PN with requesting PNE after finding PNGWID in local SG Inventory.

After sending the SGActionResponse message, CPNS Server SHALL initiate Service Group Member Update procedure. (see Section 7.7.2.4)

7.7.2.4 Service Group Member Update

After SG Creation, SG Update, PNE Invitation, PNE Expulsion, PNE Joining and PNE Leaving procedure, all of the members of Service Group should get the member update notification.

7.7.2.4.1 PNE

When PNE get the SGChangeNotification message from PN GW, PNE SHALL store or update in local SG Inventory.

7.7.2.4.2 PN GW

When the PN GW receives the SGChangeNotification message from CPNS Server, the following attributes SHALL be stored or updated in the local SG Inventory of PN GW.

- SGInfo element
    - SGID attribute is to find out SG in local SG Inventory
- MemberInfo element
    - If PNEID attribute in MemberInfo element is the member PNE managed by this PN GW in PN, PNEID and PNGWID attribute SHALL be updated in local SG Inventory of PN GW.

After updating, PN GW SHALL forward SGChangeNotification messages to its PNEs pertaining to the same PN and its PNEs are members of this Service Group.

7.7.2.4.3 CPNS Server

CPNS Server SHALL send SGChangeNotification messages per related PN GWs forming same PN with member PNEs including below element. CPNS Server SHALL set SGID in Destination ID in common header since the SGChangeNotification message is delivered to all SG member PNEs.

- SGInfo element SHALL be inserted
    - SGID attribute SHALL be inserted
    - MemberInfo element SHALL be inserted if Sharing is “2” (Selective) and CPNS Server gets the SGActionRequest message including PNEInfo element.
        - the information of modified member SHALL be inserted with a proper Result attribute for all of existed members if there is modified member PNE (e.g. join, invite, expel, leave)
        - all of the sub elements of PNEInfo with Result “0” (Current) attribute SHALL be inserted for only the newly joined or invited members after Joining procedure.

NOTE: In Join, Leave, Expel procedure, the joined, left and expelled PNE that received the message including SG Inventory from CPNS Server does not need to get additional SGChangeNotification message. The only Invite procedure, the invited PNE needs to receive the SGChangeNotification message.

7.7.3 Service Group Update

7.7.3.1 PNE

When PNE acting as SG Owner wants to update SGInfo, PNE SHALL send the SGActionRequest message to PN GW including below

- OriginEntityID attribute SHALL be filled with EntityID of requesting PNE.
- SGInfo element SHALL be inserted.
    - SGID attribute SHALL be inserted.
    - SGDescription SHALL be inserted if PNE wants to change.
    - ServiceInfo element SHALL be inserted if PNE wants to change.
        - ServiceID attribute SHALL be inserted if PNE wants to change.
        - ServiceStatusattribute SHALL be inserted with “1” if PNE wants to insert, “2” if PNE wants to remove.

When PNE receives the SGActionResponse message, PNE SHALL update SG Inventory.

7.7.3.2 PN GW

When PN GW receives the SGActionRequest message from PNE, PN GW SHALL forward the SGActionRequest message to CPNS Server.

When PN GW wants to update SGInfo in case PN GW belongs to the same User of the SG Owner as a member of PN, PN GW SHALL send the SGActionRequest message at User request to CPNS Server including below.

- SGInfo element SHALL be inserted.
    - SGID attribute SHALL be inserted.
    - SGDescription SHALL be inserted if PN GW wants to change.
    - ServiceInfo element SHALL be inserted if PN GW wants to change.
        - ServiceID attribute SHALL be inserted if PN GW wants to change.
        - ServiceResult attribute SHALL be inserted with "1" if PN GW wants to insert, "2" if PN GW wants to remove.

When PN GW receives the SGActionResponse message, PN GW SHALL update SG Inventory. If the SGActionRequest message was initiated by PNE, PN GW SHALL forward the SGActionResponse message to PNE.

7.7.3.3 CPNS Server

When PN GW receives the SGActionRequest message from PN GW, CPNS Server SHALL check whether the OriginEntityID is equal to EntityID of SG Owner by referring local SG Inventory. If there is no OriginEntityID in the SGActionRequest message, CPNS Server SHALL check the related PN GW belongs to the same User of SG Owner in local PN Inventory.

If there is a request for the Service Group update from External entities or from the operator's decision, the CPNS Server SHALL be able to execute the process as same as the process initiated by SG member. In this process, the CPNS Server SHALL update in local SG Inventory according to the SGActionRequest message. CPNS Server SHALL send the SGActionResponse message to PN GW.

After sending the SGActionResponse message, CPNS Server SHALL initiate Service Group Member Update procedure.

7.7.4 Service Group Discovery

7.7.4.1 PNE

When CPNS User wants to find out the existed Service Group list, PNE SHALL create the SGDiscoveryRequest message with SGInfo including ServiceID and/or Keyword attributes according to User's request. If the CPNS User wants to receive the member information of found Service Group(s), PNE SHALL set MemberReq with "TRUE".

After creating the SGDiscoveryRequest message, PNE SHALL send the SGDiscoveryRequest message to PN GW.

When PNE receives the SGDiscoveryResponse message from PN GW, PNE can join a certain Service Group in the message (see section 7.7.2.3), or PNE can create new Service Group if there is no matched Service Group (see section 7.7.1.1).

7.7.4.2 PN GW

When PN GW receives the SGDiscoveryRequest message from PNE or create the SGDiscoveryRequest message with SGInfo including ServiceID and/or Keyword attributes at CPNS User request, PN GW SHALL send the SGDiscoveryRequest message to CPNS Server.

When PN GW receives the SGDiscoveryResponse message from CPNS Server and its original request was initiated by PNE, PN GW SHALL send the SGDiscoveryResponse message to the PNE. If the discovery request was originated by PN GW,

PN GW can join a certain Service Group in the message (see section 0), or PN GW can create new Service Group if there is no matched Service Group (see section 7.7.1.1).

7.7.4.3 CPNS Server

When CPNS Server receives the SGDiscoveryRequest message from PN GW, CPNS Server SHALL find the proper Service Group, which has Sharing "1"(Public), based on ServiceID and/or Keyword attributes in SG Inventory. When Keyword is set in SGDiscoveryRequest message,, CPNS Server tries to find out Service Group with proper Service, SGDescription, member identifier related with Keyword.

After finding the proper Service Group, CPNS Server SHALL create the SGDiscoveryResponse message with SGInfo element from local SG Inventory. If the MemberReq is "TRUE", CPNS Server SHALL insert the MemberInfo element in the SGDiscoveryResponse message. After creating the SGDiscoveryResponse message, CPNS Server SHALL send the SGDiscoveryResponse message to PN GW.

7.7.5 Service Group Release

7.7.5.1 PNE

When PNE acting as SG Owner wants to release the Service Group, PNE SHALL create the SGReleaseRequest message including below. PNE SHALL check whether the PNE is SG Owner by referring local SGInventory.

- SGID attribute SHALL be inserted.
- OriginEntityID attribute SHALL be inserted.

After creating the SGReleaseRequest Message, the PNE SHALL send the SGReleaseRequest message to PN GW.

When PNE receives the SGReleaseResponse message, PNE SHALL remove SGInfo element in SG Inventory related with this SGID.

When the PNE receives the SGReleaseNotification message, PNE SHALL remove SGInfo element in SG Inventory related with this SGID.

7.7.5.2 PN GW

When PN GW receives the SGReleaseRequest message from PNE or create SGReleaseRequest message with SGID attribute, PN GW SHALL send the SGReleaseRequest message to CPNS Server. If PN GW belongs to same User with SG Owner as member PNE in PN, PN GW can request SG Release.

When PN GW receives the SGReleaseResponse message from CPNS Server, the PN GW SHALL forwards the SGReleaseResponse message to the PNE. After that, PN GW SHALL remove SGInfo element in local SG Inventory related with this SGID. If the release request is initiated by the PNE which belongs to same PN. the PN GW forwards the SGReleaseResponse message to the PNE.

When PN GW receives the SGReleaseNotification message from CPNS Server, PN GW SHALL send SGReleaseNotification messages to member PNEs of Service Group except PNE which requests SG release. After that, PN GW SHALL remove SGInfo element in local SG Inventory related with this SGID.

7.7.5.3 CPNS Server

When CPNS Server receives the SGReleaseRequest message from PN GW, CPNS Server SHALL check that

- OriginEntityID is equal to EntityID of SG Owner in the Service Group if there is OriginEntityID, OR, PN GW belongs to same user with SG Owner as member PNE in PN Inventory.
- SGID is registered in SG Inventory

If at least one of above examinations fail, CPNS Server SHALL send the SGReleaseResponse message to the PN GW including Result attribute as "2" in case that OriginEntityID is not equal to EntityID of SG Owner or PN GW does not have SG Owner as a member of PN, or "3" in case that SGID is not registered in SG Inventory.

If above all of examinations are successful, CPNS Server SHALL send SGReleaseNotification messages with SGID attribute to the related PN GWs forming same PN with PNEs after finding PNGWID in local SG Inventory. CPNS Server SHALL set SGID in Destination ID in common header since the SGReleaseNotification message is delivered to all SG member PNEs.

And then, CPNS Server SHALL remove SGInfo element in SG Inventory related with this SGID and CPNS Server SHALL send the SGReleaseResponse message to the PN GW which sent the SGReleaseRequest message to CPNS Server.

If the Service Group is released due to the Operator Policy, CPNS Server SHALL send the SGReleaseNotification message including SGID attribute to the related PN GWs forming same PN with PNEs after finding PNGWID in local SG Inventory. Then, CPNS Server SHALL remove SGInfo element in local SG Inventory.

7.7.6 Service Group Owner Transfer

7.7.6.1 PNE

When SG Owner wants to transfer its ownership to other candidate PNE inside the service group, the SG Owner SHALL create SGOwnerTransferRequest message including the SGID of the original SG owner, and SHOULD include the PNEID of the candidate of next SG Owner recommended by the original SG Owner and the reason to transfer if possible.

After creating the SGOwnerTransferRequest message, PNE SHALL send the SGOwnerTransferRequest message to PN GW.

If the new PNE accepts the group ownership , this PNE shall create the SGOwnerTransferResponse message with Accept equal to TRUE indicating the owner transfer is successful and should also include with PNEID of the new SG Owner and SGID of the new SG Owner.

When the original PNE receives the SGOwnerTransferResponse message from PN GW with positive confirmation indicating the ownership transfer is successful, PNE SHALL update its SG Inventory.

When PNE receives SGOwnerChangeNotification message from PN GW , PNE SHALL update its SG Inventory.

7.7.6.2 PN GW

When PN GW receives the SGOwnerTransferRequest message including the SGID of the former SG Owner from PNE, PN GW SHALL send the SGOwnerTransferRequest message to CPNS Server.

When PN GW receives the SGOwnerTransferResponse message from CPNS Server, PN GW SHALL send the SGOwnerTransferResponse message to the PNE.

When PN GW receives the SGOwnerTransferResponse message with positive confirmation indicating the ownership transfer is successful, PN GW SHALL update its SG Inventory.

When PN GW receives SGOwnerChangeNotification message from CPNS server, it delivers SG Owner Change Notification to member PNEs in the SG, PN GW SHALL update its SG Inventory.

7.7.6.3 CPNS Server

When CPNS Server receives the SGOwnerTransferRequest message from PN GW, CPNS Server SHALL forward the SGOwnerTransferRequest message to the candidate SG Owner based on device capabilities, service description, Operator Policy of CPNS Server or the recommendation from the original SG Owner. .

When CPNS Server receives the SGOwnerTransferResponse message with positive confirmation, CPNS Server SHALL update its SG Inventory and forward the SGOwnerTransferResponse message to the original SG Owner.

CPNS Server SHALL deliver the SG Owner change notification to member PNEs in the SG.

When CPNS Server receives the SGOwnerTransferResponse message with negative confirmation, CPNS Server SHALL forward the SGOwnerTransferRequest message to another candidate SG Owner or forward the SGOwnerTransferResponse message to the original SG Owner.

7.8 Group Key Management

7.8.1 Group Key creation

- CPNS Server

When CPNS Server receives a SGCreateRequest message, CPNS Server SHALL create a Group Key and store the Group Key.

After CPNS Server creates Group Key, CPNS Server SHALL deliver a Group Key to all member PNEs in Service Group according to procedures in Section 7.8.5.

7.8.2 Group Key update

- CPNS Server

When CPNS Server receives a SGActionRequest message with Action = “3” (i.e, SG leave request) from a member PNE or SGActionRequest message with Action =”1” (i.e., SG expel request) from SG Owner, CPNS Server SHALL update a Group Key and store the Group Key.

CPNS Server SHOULD update a Group Key periodically and store the Group Key.

After CPNS Server updates Group Key, CPNS Server SHALL deliver a Group Key to all member PNEs in Service Group according to procedures in Section 7.8.5.

7.8.3 Group Key deletion

- CPNS Server

When CPNS Server receives a SGReleaseRequest message from SG Owner, CPNS Server SHALL delete a Group Key.

- PNE

When PNE receives a response message of SGActionRequest message with Action = “3” (i.e, SG leave request), SGActionRequest message with Action =”1” (i.e., SG expel request), or a SGReleaseNotification message, the PNE SHALL delete a Group Key.

7.8.4 GKDK/GKEK management

If PNE or PN GW supports broadcast based Group Key delivery, GKDK/GKEK management procedure described in this sub section SHALL be supported in PNE or PN GW, respectively.

- PNE

When PNE wants to create or join Service Group or is invited to Service Group, PNE SHALL send a GKDKRequest message to PN GW in the same PN except in the following cases.

  - GKDK has been already assigned from the PN GW or
  - PNE detects that the PN GW supports broadcast group key delivery

When PNE receives a GKDKResponse message from PN GW, the PNE SHALL store GKDK.

- PN GW

When PN GW receives a GKDKRequest message from PNE, the PN GW SHALL create GKDK for the PNE and store EntityID of that PNE.

After the GKDK creation, PN GW SHALL send a GKDKResponse message with created GKDK to PNE which sends the GKDK request.

When SG member PNEs in PN change, PN GW SHALL update GKEK.

7.8.5 Group Key delivery

- CPNS Server

To deliver Group Key to SG member PNE(s) in Service Group, CPNS Server SHALL send a GroupKeyDeliveryRequest message to PN GW with Group Key.

- PN GW

When PN GW receives a GroupKeyDeliveryRequest message from CPNS Server, PN GW SHALL send a GroupKeyDeliveryResponse message to CPNS Server.

After sending a GroupKeyDeliveryResponse message to CPNS Server, PN GW SHALL choose a transmission method to deliver Group Key to SG member PNE(s) in PN (i.e., Unicast, Broadcast or hybrid delivery). If PN GW supports broadcast based Group Key delivery, PN GW SHALL choose either of Unicast, Broadcast or hybrid delivery. How to select either of Unicast, Broadcast or hybrid delivery is out of scope.

In the hybrid delivery, Group Key is delivered to some SG member PNE(s) by Unicast and is delivered to other SG member PNE(s) by Broadcast.

If PN GW chooses Unicast or hybrid delivery, PN GW SHALL sends a GroupKeyDeliveryRequest message with Group Key to each SG member PNE by Unicast. If PAN between PN GW and PNE is not Secure PAN, GroupKeyDeliveryRequest message is sent via secure session between PN GW and PNE. Otherwise, the GroupKeyDeliveryRequest message is sent via Secure PAN.

If PN GW chooses Broadcast or hybrid delivery, PN GW SHALL encrypt Group Key using the GKEK. After the Group Key encryption, PN GW SHALL broadcast a GroupKeyDeliveryRequest message in PN with the encrypted Group Key.

- PNE

When PNE receives a GroupKeyDeliveryRequest message from PN GW, the PNE SHALL store Group Key and send a GroupKeyDeliveryResponse message to the PN GW.

If PNE receives GroupKeyDeliveryRequest message via broadcast, PNE SHALL decrypt Group Key using pre-assigned GKDK before storing Group Key.

7.9 Service / Content Publication & Discovery

7.9.1 General

7.9.1.1 Service Discovery

ServiceDiscoveryRequest is activated whenever needed:

- immediately after the PN Registration; or
- when the Service Discovery is initiated explicitly e.g., CPNS user activation and periodical activation

ServiceDiscoveryRequest/Response provides a mechanism to discover service and information of Remote PNE.

To execute service, CPNS Entity SHALL be able to retrieve Service Description (i.e., ServiceProfile). For this purpose, the Service Discovery provides a mechanism to discover services with or without employing searching condition. The searching

condition could be at least one of these attributes, TargetID (i.e., PNEID or CPID), UserID, UserName and/or any arbitrary text keyword to find out service. Additionally, the Service Discovery provides a mechanism to discover service based on Operator Policy combined or not combined with the searching condition

To create Service Group including Remote PNE or to invite Remote PNE to be member of Service Group, the CPNS Entity SHALL be able to retrieve the information of remote Entity from CPNS Server using Service Discovery procedure. The remote Entity is the PNE which isn't physically connected with requesting PNE and is the member of remote PN. For this purpose, the Service Discovery provides a mechanism to discover Remote PNE related information with employing searching condition. The searching condition could be at least one of these attributes, TargetID (i.e., PNEID or CPID), UserID, UserName, PNID and/or any arbitrary text keyword. In this case, CPNS Entity Discovery procedure can be omitted, as the Service Discovery can cover CPNS Entity Discovery procedure.

7.9.1.2 ServiceDescriptionAdvertise

ServiceDescriptionAdvertise provides a mechanism for the CPNS Server advertises the Service Description to the PNE via PN GW. ServiceDescriptionAdvertise message is unicast message. To prevent spam of Service Description, CPNS Server advertises the Service Description to appropriate PNEs according to the criteria (e.g. status and usage statistics).

7.9.1.3 ServiceDescriptionRegistration

ServiceDescriptionRegistration provides a mechanism for the PNE as content provider and external content provider to publish its Service Description to the CPNS Server with ServiceDescriptionRegistrationRequest/Response message.

7.9.2 Service Discovery

7.9.2.1 PNE

To find out service, the PNE SHALL send a ServiceDiscoveryRequest message with following parameter set to CPNS Server via PN GW.

- As searching condition(s), DiscoveryDestination element SHALL be included with at least one of following parameters.
    - TargetID attribute (i.e., PNEID or CPID)
    - UserInfo element with UserID attribute or UserName attribute or both
    - Keyword element
- ContentInfoRequest attribute SHOULD be included to indicate if content related information is requested or not.

  Note: The definition of content related information depends on content/service provider and out of scope of CPNS Enabler.
    - Set the value equals to TRUE to indicate that content related information is requested
    - Set the value equals to FALSE to indicate that PNE does not want to receive any content related information

To find Remote PNE related information, PNE SHALL send the ServiceDiscoveryRequest message to CPNS Server via PN GW including below.

- As searching condition(s), DiscoveryDestination element SHALL be included with at least one of followings parameters.
    - UserInfo element with UserID attribute or UserName attribute or both
    - PNID attribute
    - Keyword element

Upon receiving the ServiceDiscoveryConfirmationRequest from PN GW, the PNE SHALL send the ServiceDiscoveryConfirmationResponse with Result (either allowing or denying to access to PN Information) to the CPNS Server via PN GW.

When PNE receives the ServiceDiscoveryResponse message from PN GW, the PNE can invoke service as defined in Service/Content delivery signaling procedure or can start to create Service Group including Remote PNE, invite the Remote PNE to Service Group considering proper PN or join PN from public PN GW.

7.9.2.2 PN GW

Upon receiving the ServiceDiscoveryRequest message from PNE, the PN GW SHALL forward the message to CPNS Server.

To find Remote PNE related information, PN GW SHALL send the ServiceDiscoveryRequest message to CPNS Server including below.

- As searching condition(s), DiscoveryDestination element SHALL be included with at least one of followings parameters.
    - UserInfo element with UserID attribute or UserName attribute or both
    - PNID attribute
    - Keyword element

Upon receiving the ServiceDiscoveryConfirmationRequest from CPNS Server ,

- If the final destination of the message is the PN GW, the PN GW SHALL send back the ServiceDiscoveryConfirmationResponse message with Result (either allowing or denying to access to PN Information).
- If the final destination of the message is PNE, the PN GW SHALL forward ServiceDiscoveryConfirmationRequest message to the PNE.

Upon receiving the ServiceDiscoveryResponse message from CPNS Server, the PN GW SHALL forward the message to PNE in case PNE initiates ServiceDiscoveryRequest.

7.9.2.3 CPNS Server

7.9.2.3.1 Overall procedure

Upon receiving the ServiceDiscoveryRequest with PNEID or PNID or UserID in DiscoveryDestination element, the CPNS Server SHALL perform PN Inventory access control based on Disclosure and OwnershipEntity attribute.

If the value of Disclosure attribute is

- 1: the CPNS Server SHALL send back the ServiceDiscoveryResponse with Result set to FALSE and Reason (e.g., Access Denied) to the PNE via PN GW.
- 2: the CPNS Server SHALL send back the ServiceDiscoveryResponse with matched information (See section 7.9.2.3.2) in PN Inventory to the PNE via PN GW.
- 3: the CPNS Server SHALL forwards ServiceDiscoveryConfirmationRequest message with UserID or PNID or PNEID to the CPNS Entity which is indicated by OwnershipEntityID attribute.

Upon receiving ServiceDiscoveryConfirmationResponse message from the PN GW,

- If Result in the message is FALSE, the CPNS Server SHALL send back the ServiceDiscoveryResponse with Result set to FALSE and Reason (e.g., Access Denied) to the PNE via PN GW.
- If Result in the message is TRUE, the CPNS Server SHALL send back the ServiceDiscoveryResponse with matched information (See section 7.9.2.3.2) in PN Inventory to the PNE via PN GW.

7.9.2.3.2 Searching relevant information and assembling response message

To find service or Remote PNE related information, CPNS Server SHALL perform following.

In case the ServiceDiscoveryRequest message contains no searching condition,

- And there are Operator's policies, the CPNS Server SHALL find the Service Description based on policy (e.g., Operator Policy).
- And there are no Operator's policies, the CPNS Server SHALL send the ServiceDiscoveryResponse with all the available Service Descriptions to the PNE via PN GW.

Note: The definition and procedure of managing (e.g., registering, updating, and so on) the Operator Policy is out of scope of CPNS Enabler.

In case the ServiceDiscoveryRequest message contains searching condition,

- And there are Operator's policies, the CPNS Server SHALL perform searching based on the searching condition and on the policies and composes search result and send back the ServiceDiscoveryResponse with the Service Description to the PNE via PN GW.
- And there are no Operator's policies, the CPNS Server SHALL perform searching based on the searching condition and composes search result and send back the ServiceDiscoveryResponse with the Service Description to the PNE via PN GW.

When the searching condition is an arbitrary text, the CPNS Server SHALL finds the Service Description with the text for partial match. Partial match refers to matching of keyword value with values in Service Description to find the match that begins with, contains or ends with the keyword value.

In case the ServiceDiscoveryRequest message contains ContentInfoRequest with value of TRUE, then CPNS Server SHALL respond with content related information from the Service Description to the PNE via PN GW.

Note: The definition of content related information depends on content/service provider and out of scope of CPNS Enabler. In result, the mechanism for the CPNS Server to filter only content related information from Service Description is also out of scope of CPNS Enabler.

The ServiceDiscoveryResponse SHALL contain following parameter sets.

- Result attribute SHALL be set as "TRUE".
- TargetInfo element(s) SHALL be included with followings if CPNS Server finds out matched Target supporting services
    - TargetID SHALL be included. If the Target is PNE, TargetID is PNEID. If the target is external content provider, TargetID is CPID.
    - TargetName attribute SHOULD be included. Name attribute indicate Name of PNE or external content Provider hosting the service with the matched Service Description.
    - Active attribute SHALL be included if the TargetID is PNEID.
    - UserInfo element SHOULD be included if Disclosure attribute is '2'(Open) or with the confirmation (i.e., ServiceDiscoveryConfirmationResponse) from CPNS Entity designated by OwnershipEntityID.
    - PNID element SHOULD be included if Disclosure attribute is '2'(Open) or with the confirmation (i.e., ServiceDiscoveryConfirmationResponse) from CPNS Entity with OwnershipEntityID.
    - ServiceProfile element SHALL be included if Target ID is PNE ID and Disclosure attribute is '2'(Open) or with the confirmation (i.e., ServiceDiscoveryConfirmationResponse) from CPNS Entity designated by OwnershipEntityID. If the TargetID is CPID then ServiceProfile SHALL be included, composed from CPNS Profile stored in CPNS Server.

- PNInfo element(s) SHALL be included if CPNS Server finds out Remote PNE information and if Disclosure attribute is '2'(Open) or with the confirmation (i.e., ServiceDiscoveryConfirmationResponse) from CPNS Entity designated by OwnershipEntityID.

When no match with searching condition is found, then the CPNS Server SHALL send the ServiceDiscoveryResponse with no TargetInfo element and Result attribute "FALSE" to the PNE via PN GW.

The detail searching process is out of scope of CPNS Enabler, but to only describe the CPNS Enabler specific searching framework.

- In Remote PNE case where PNE is the content provider, the Service Description as ServiceProfile is included in PN inventory stored in CPNS Server.
- In external content provider case where the External Entity is interfaced with CPNS Server, the Service Description of the provider is stored in the form of CPNS Profile in CPNS Server.

To search for matched text, CPNS Server SHOULD process both Service Description forms (i.e., ServiceProfile in PN Inventory and CPNS Profile).

To assemble the ServiceDiscoveryResponse with Service Description, following MAY need to be taken into consideration.

- In Remote PNE case where PNE is the content provider, the ServiceProfile is included in PN Inventory. The consideration is for such case where single PNE (i.e., content provider) registered in multiple PNs, the CPNS Server SHOULD make sure of no duplicated ServiceProfile hosted by the same PNE be returned.

7.9.3 Service Discovery Advertise

7.9.3.1 CPNS Server

When CPNS Server receives Service Description from external content provider through ServiceDescriptionReigstration, the CPNS Server MAY send ServiceDescriptionAdvertise message including relevant Service Description to PNE via PN GW.

The ServiceDescriptionAdvertise message SHALL contain following parameter sets.

- ZoneBasedServiceSupport attribute MAY be included as "TRUE" if the purpose of this service is for zone based service.
- CPInfo element SHALL be included.
    - CPID attribute SHALL be included. CPID attribute indicates ID of external content provider hosting the service.
    - CPName attribute MAY be included for name of external content provider.
- ServiceProfile element SHALL be included.

For Zone Based Service, the CPNS Server SHALL send the ServiceDescriptionAdvertiseService message to the PN GW which supports Zone Based Service with following parameter retrieved from PN Inventory. PN GW SHALL advertise the Service Description to the PNE. If the ServiceDescriptionAdvertisemessage from CPNS Server indicates to store the Service Description, the PN GW SHALL store the Service Description.

- ZoneBasedServiceSupport attribute MAY be included as "TRUE" to indicate if PN GW need to store the received Service Description.

7.9.3.2 PN GW

When PN GW receives the ServiceDescriptionAdvertise message, the PN GW SHALL forward the message to the PNE.

For Zone Based Service, PN GW SHALL advertise the Service Description to the relevant PNE. If the ServiceDescriptionAdvertisemessage from CPNS Server indicates to store the Service Description, the PN GW SHALL store the Service Description. In case the ServiceDescriptionAdvertise message includes an indication, ZoneBasedServiceSupport and the value is "TRUE" then the PN GW SHALL store the received Service Description.

7.9.3.3 PNE

By receiving the ServiceDescriptionAdvertise, the PNE can invoke service as defined in Service/Content delivery signaling procedure.

7.9.4 Service Description Registration

The Service Description Registration provides a mechanism where PNE acting as content provider or external content provider hosting the service publishes the Service Description to the CPNS Server.

PN Management procedure is responsible for registration of Service Description in case of PNE acting as content provider publishes the Service Description. The detail description can be found in section 8.6.

In addition, after initial registration, to publish Service Description (i.e., ServiceProfile), PNE acting as content provider MAY publish the Service Description using ServiceDescriptionRegistrationRequest message. For the case of external content provider publishing the Service Description (i.e., ServiceProfile information set for the CPNS Server to create CPNS Profile), the ServiceDescriptionRegistrationRequest can be utilized.

7.9.4.1 PNE

The case where PNE acting as content provider publishes Service Description after PN establishment

To publish Service Description (i.e., ServiceProfile) to the CPNS Server, PNE SHALL send the ServiceDescriptionRegistrationRequest message with following parameter sets.

- PNID attribute to designate the target PN Inventory SHALL be included.
- PNEID attribute to designate the target PNEInfo SHALL be included.
- ServiceProfile element SHALL be included.
- Disclosure attribute SHALL be included.
- OwnershipEntityID SHALL be included if the value of Disclosure is “3” (i.e. selective)

By receiving the ServiceDescriptionRegistrationResponse message from PN GW, the PNE acknowledge the result of service description registration.

7.9.4.2 PN GW

The case where PNE acting as content provider registers Service Description

When PN GW receives the ServiceDescriptionRegistrationRequest message from PNE, the PN GW SHALL forward the message to the CPNS Server.

When PN GW receives the ServiceDescriptionRegistrationResponse message from CPNS Server, the PN GW SHALL forward the message to the PNE.

7.9.4.3 CPNS Server

The case where PNE acting as content provider publishes Service Description

Upon receiving the ServiceDescriptionRegistrationRequest message from PN GW, the CPNS Server replaces the ServiceProfile of target PNE Info in relevant PN Inventory.

After updating the PN Inventory, the CPNS Server sends the ServiceDescriptionRegistrationResponse message to the PNE via PN GW.

The case where external content provider publishes Service Description

Upon receiving the ServiceDescriptionRegistrationRequest message from external content provider, the CPNS Server creates and stores the CPNS Profile. The ServiceDescriptionRegistrationRequest message SHALL have CPID attribute and ServiceProfile element and MAY have CPName attribute.

If the CPNS Profile of the requesting external content provider is already stored, identified by CPID, the CPNS Server update or replaces the existing CPNS Profile with received Service Description.

- CPNS Server SHALL send the ServiceDescriptionRegistrationResponse message to the external content provider including Result attribute.

7.10 Service / Content Delivery

The Service/Content Delivery procedure facilitates the delivery of service/content.

Service/Content Delivery is activated when the Service/Content Delivery is initiated explicitly e.g., with user interaction.

Based on specific policies pre-configured in the CPNS server by Operators, content providers or users, the delivery which violates any of these specific policies SHOULD not be delivered. These specific policies SHOULD be shared between CPNS Entities. How to set and share this policy is out of scope.

By performing the Service Discovery procedure, the PNE receives the Service Description, which contains ServiceProfile, CPNS EntityID or CPID hosting application, and so on.

7.10.1 PNE

To execute a specific operation, the PNE SHALL send the InvokeRequest message to the CPNS Server via PN GW with following parameter sets.

- SGID attribute MAY be included to identify the group of services for specific service. This attribute is used only if the specific service is part of a service group.
- ServiceID element SHALL be included to identify service.
    - Operation attribute SHALL be included. Operation attribute is for the operation name specific to each service.
- InputParameterList element SHALL be included. InputParameterList contains the argument for the service invocation.
    - Parameter element(s) MAY be included, which carry the argument value.
        - Name attribute SHALL be included to indicate the name of argument for the service invocation.
        - DataType SHALL be included to indicate the data type of argument value.

In case of Remote PNE connection where PNE is acting as a content provider, upon receiving the InvokeRequest from PN GW, the PNE sends back the InvokeResponse to the PN GW with following parameter sets.

- Result element SHALL be included to indicate result of InvokeRequest. The value TRUE indicate successful service invocation and the value FALSE indicate for some reason the service invocation is failed.
- Reason element MAY be included. The element is included when the Result is FALSE.
- OutputParameterList element MAY be included. The element contains the return value for the service invocation if available.
    - Parameter element(s) SHALL be included, which carry the returned value.
        - Name attribute SHALL be included to indicate the name of returned value for the service invocation.

By receiving the InvokeResponse, the requesting PNE (the PNE request the service invocation) acknowledge the result of InvokeRequest. The requesting PNE can perform another service invocation utilizing the operation set (which is the AppInfo,

carried in ServiceDiscoveryResponse) and application specific value (which is the OutputParameterList, carried in InvokeResponse).

7.10.2 PN GW

Upon receiving the InvokeRequest from PNE, the PN GW forwards the message to the CPNS Server.

Upon receiving the InvokeRequest from CPNS Server, the PN GW forwards the message to the PNE acting as content provider.

Upon receiving the InvokeResponse from PNE acting as content provider, the PN GW forwards the message to the CPNS Server.

Upon receiving the InvokeResponse from CPNS Server, the PN GW forwards the message to the requesting PNE (the PNE requesting the service invocation).

7.10.3 CPNS Server

Upon receiving the InvokeRequest, the CPNS Server SHALL forwards the message to the external content provider based on the received CPID (i.e., ID of external content provider).

In case of Remote PNE case where PNE is acting as content provider, upon receiving the InvokeRequest, the CPNS Server SHALL forwards the message to the PN GW based on the received CPNS EntityID (i.e., PNEID of content provider).

Upon receiving the InvokeResponse, the CPNS Server SHALL forwards the message to the relevant PN GW.

7.11 Zone Based Service

7.11.1 General

The Zone Based Service facilitates the content push service with CPNS enabler.

When the PNE comes to the Zone, by performing the CPNS Entity Discovery & PN Registration function, the PNE is discovered by the PN GW and registered in the PN inventory of the CPNS server without the initial request from PNE or input from the user.

7.11.2 PNE

Only by setting to reply on the PN GW's periodic search, a PNE can be pushed the contents or the service description information.

When the PNE comes to the Zone, the PNE will be found by PN GW by using periodic search described in Appendix C.

After receiving the EntityDiscoveryRequest message from the PN GW, the PNE SHALL send EntityDiscoveryResponse message to the PN GW as described in section 7.2.

After receiving the PNSetupeRequest from the PN GW, the PNE SHALL send PNSetupeResponse message to the PN GW as described in section 7.6.

- The Return attribute SHALL be set
    - 1 for OK.
    - 2 for Failure, indicating that PNE is not capable of handling the request.

7.11.3 PN GW

If the PN GW acts as Zone PN GW, the PN GW SHALL perform periodic search described in Appendix C.

After finding a PNE by periodic search, the PN GW SHALL send EntityDiscoveryRequest message to the PNE as described in section 7.2.

After receiving the EntityDiscoveryResponse message from the PNE, the PN GW SHALL send PNSetupRequest message to the PNE as described in section 7.6.

After receiving the PNSetupeRsponse from the PNE and the value of Return attribute is “1”, the PN GW SHALL send PNSetupRequest message to the CPNS Server as described in section 7.6, and the Zonebasedservicesupport attribute SHALL be set as “1”.

After receiving the ServiceDescriptionAdvertise message from CPNS Server, PN GW SHALL store that Service Description if the ZoneBasedServiceSupport attribute is “1”. After that, PN GW SHALL check if the target PNE is available for the service based on PN Inventory. If the PNE is available for the service, the PN GW SHALL send that Service Description to the PNE by using ServiceDescriptionAdvertise message as described in section 8.8.

In the case that the PN GW already has a stored Service Description, which had been delivered from the CPNS Server beforehand, the PN GW SHALL send the Service Description Advertise to the PNE without receiving the Service Description Advertise from the CPNS Server again.

7.11.4 CPNS Server

Upon receiving the PNSetupRequest message from PN GW, the CPNS Server SHALL send PNSetupResponse message to PN GW as described in section 7.6.

The CPNS Server SHALL generate the ServiceDescriptionAdvertise message according to format of CPNS Message in section 8 when the CPNS Server wants to advertise service to a Zone. The CPNS Server

1. SHALL include CPNS EntityID or CPID (see the Profile) hosting the discovered service in Name attributes.
2. SHALL set ZoneBasedServiceSupport attribute as "1” if the PN GW need to store the Service Description which is received from this message, otherwise the ZoneBasedServiceSupport attribute SHALL be set as “0”.
3. SHALL include the target CPNS metadata (See section 5.10) in element ServiceProfile.

7.12 Device Capability

7.12.1 Device capabilities Query

A CPNS Server SHOULD send Device capabilities Query Request to PNE and PN GW to retrieve information of device capabilities of PNE, and PN GW, respectively. Device capabilities Query Response is accordingly responded and sent from PNE and PN GW back to CPNS Server.

The procedure SHALL be applied when the devices capabilities information is required.

Subsequent Device Capabilities Change Notification SHOULD be triggered by a device capability change, pre-scheduled or requested from CPNS Servers from PNE and PN GWs every time when there is a device capability change of PNE and PN GWs.

7.12.2 DPE

CPNS enabler MAY support interaction with OMA DPE to notify device capabilities of PNE and PN GW. If this interaction is supported, the PNE and PN GW SHALL support the mechanism for device capability notification as specified in OMA DPE. PNE and PN GW initially SHALL notify their capabilities during the PN setup phase. Subsequent device capability notification will be triggered by a device capability change, pre-scheduled or requested from the server.

PNE and PN GWs can act as DPE clients to notify the DPE Server on device capabilities of PNEs and PN GWs. DPE server would notify the CPNS Server every time there would be a device capability change.

7.13 Status Management

7.13.1 General

The Status Management provides a mechanism to publish, collect, subscribe and notify the status of PNE and PN GW.

Each message in Status Management SHALL be formatted as CPNS Messages. The format of each message can be found in section 8.11.

7.13.2 Service Status Publication

The status information is published by target CPNS entity (i.e., PNE or PN GW) or PN or device which holds the status information for collection and notification triggered by the status changes.

The status information is published to CPNS Server and stored in the CPNS Server.

7.13.3 Status Subscription and Notification

To be notified of status changes, the watcher of status SHALL subscribe to the CPNS entity status information notification.

The PNE sends a StatusSubscribeRequest message with TargetID (i.e., PNEID, PNGWID, PNID) for event registration into the CPNS Server. Receiving the message the CPNS Server registers the event and sends back the StatusSubscribeResponse message to the PNE via PN GW.

When the registered event occurs, the CPNS Server SHALL send a StatusNotify message with TargetID and status information, which is StatusVariable (See CPNS metadata format in section 5.10) associated with TargetID to the PNE the watcher via PN GW.

Subscription duration is set in the StatusSubscribeRequest message. The subscription should be released automatically when the duration expires. The subscription can be released explicitly by sending the StatusSubscribeRequest message with zero subscription duration time.

The PNE the watcher of status SHOULD send the StatusSubscribeRequest message with TargetID to the CPNS Server to keep subscription.

7.13.4 PN / PNE Inactive Status Management

If there is a disconnection between PN GW and PNE that are part of the same PN, which is not a temporary PN but a sustained PN, PN GW SHALL notify the CPNS Server about this disconnection and also MAY notify the connected PNEs belonging to the same PN if the Sharing attribute is set as “1”(Shared).

7.13.4.1 PNE

When PNE is disconnected with PN GW forming PN, PNE SHALL set Active attribute “FALSE” of PNInfo element in local PN Inventory.

When PNE receives the StatusNotify message from PN GW in case Sharing attribute is “1”(Shared) in PN Inventory, PNE retrieves the TargetID attribute for disconnected PNE in the message and set Active value as “FALSE” for disconnected PNE’s PNEInfo element in local PN Inventory of that receiving PNE..

7.13.4.2 PN GW

When PN GW is disconnected from PNE forming PN and if there are still other connected PNEs forming the PN, PN GW SHALL create the StatusPublicationRequest message including below sub attributes. In case of Sharing attribute “1” (Shared) in PN Inventory, PN GW SHOULD create the StatusNotify message including below sub attributes as well.

- TargetID attribute SHALL be inserted with PNEID for disconnected PNE.
- Active attribute SHALL be inserted with “FALSE”

After creating message, PN GW SHALL send the StatusPublicationRequest message to CPNS Server and PN GW SHOULD send StatusNotify messages to PNEs forming the same PN.

When PN GW receives the StatusPublicationResponse message from CPNS Server, PN GW SHALL update the PNEInfo element with Active attribute as “FALSE” in local PN Inventory. If there are no other PNEs in the same PN where the disconnected PNE belonged to , PN GW SHALL update PNInfo element with Active attribute as “FALSE” in local PN Inventory.

7.13.4.3 CPNS Server

When CPNS Server receives the StatusPublicationRequest message from PN GW, CPNS Server SHALL update PNEInfo element related with this TargetID with Active attribute in local PN Inventory. If all of PNEs in PN are inactive, CPNS Server SHALL update Active attribute as “FALSE” in PNInfo element of local PN Inventory. CPNS Server SHALL send the StatusPublicationResponse message to PN GW.

7.13.5 PN / PNE Active Status Management

After repairing physical connection, PN GW can restart the PN service using notification message with reconnected PNE.

7.13.5.1 PNE

When PNE is reconnected with PN GW forming PN, PNE SHALL set Active attribute as “TRUE” of PNInfo element in local PN Inventory

When a PNE is reconnected to a PN part of which that PNE was before, other PNEs within the same PN will receive the StatusNotify message from PN GW in case of Sharing attribute is set as “1”(Shared). These PNEs will retrieve the TargetID attribute for the reconnected PNE from StatusNotify message and SHALL set Active value as “TRUE” for reconnected PNE’s PNInfo element in local PN Inventory.

7.13.5.2 PN GW

When PN GW detects that PNE is reconnected to PN and if there were other connected PNEs forming this PN and Sharing attribute set as “1” (Shared) in PNInfo Inventory, PN GW SHOULD send the StatusNotify message to connected PNEs in that PN including below attributes:

- TargetID attribute SHALL be inserted with PNEID for reconnected PNE.
- Active attribute SHALL be inserted with “TRUE”

After sending the StatusNotify message, PN GW SHALL create the StatusPublicationRequest message and SHALL send it to CPNS Server including below attributes.

- TargetID attribute SHALL be inserted with PNEID for reconnected PNE.
- Active attribute SHALL be inserted with “TRUE”

When PN GW receives the StatusPublicationResponse message with Status attribute “TRUE” from CPNS Server, PN GW SHALL update the PNInfo and sub PNEInfo element of reconnected PNE with Active attribute as “TRUE” in PN Inventory. If there is at least one connected PNE forming this PN, PN GW SHALL update PNInfo element with Active attribute as “TRUE” in local PN Inventory.

NOTE: PN GW can send the StatusPublicationRequest message to CPNS Server before sending the StatusNotify message to PNEs. After receiving the StatusPublicationResponse from CPNS Server, PN GW can send the StatusNotify message to PNEs and then PN GW can update PN Inventory in local.

7.13.5.3 CPNS Server

When CPNS Server receives the StatusPublicationRequest message from PN GW, CPNS Server SHALL update PNInfo element and sub PNEInfo element related with this TargetID with Active attribute as “TRUE” in local PN Inventory, and then CPNS Server SHALL send the StatusPublicationResponse message with Status attribute “TRUE” to PN GW.

7.14 Usage Statistics

7.14.1 Usage statistics collection

After content delivery to a PNE the application entity on the PNE side can collect the information of usage statistics of this content. This information can be aggregated in a report which could be sent to the PNE and forwarded to the PN GW and CPNS Server.

Usage statistics collection applies to the PNEs on the receiving sideonly.

The message name for reporting usage statistics on the server side is AppServerUsageStatsReport which contains the following parameters: AppServerID, StatsReportMessageID and UsageStatsData.

The massage name for reporting usage statistics on the PNE side is AppPNEUsageStatsReport which contains the following parameters: AppPNEID, StatsReportMessageID, PNEID, PNGWID and UsageStatsData

Application entity on the server side can also collect the usage statistics information and aggregate in a report which will be sent to the CPNS Server.

7.14.2 Usage statistics reporting

The reporting of usage statistics information to CPNS Server can be done by the application entity on the server side as well as by the application entity on the PNE side. The reporting of this information on the server side can be done via CPNS-4 interface, while on the PNE side can be done via CPNS-5 interface.

PNE SHALL be able to combine a number of received usage statistics reports and forward to the PN GW as part of one message.

The frequency of usage statistics information reporting depends on service provider policies and pre-set schedules

8. CPNS message

8.1 General Consideration

This section describes message containing sub elements and sub attributes.

In message element table, “E” means element and “A” means attribute. If the Type of element is empty, it means that the element has not value but sub attributes.

The basic message formats are

- “~Request” and “~Response” pair for a two way transaction
- “~Notification” for one way transaction.

The request, response and notification messages SHALL have MsgID attribute to specify messages to support several messages sending in a device. The response message SHALL have RequestID attribute to specify this response message is related with which request message.

8.1.1 Common parameter set

For CPNS V1.0 transport protocol binding specification is out of scope but specify the list of message parameter necessary for each message.

This section describes the parameter set which is common to all CPNS messages.

Followings are the principle of common parameter set for CPNS message.

- For the purpose of specifying the adjacent CPNS Entity through which the CPNS message will go, CPNS common parameter set SHALL contain TargetID.
- For the purpose of specifying the end to end routing path, CPNS common parameter set SHALL contain SourceID and DestID which indicate the source and final destination of the CPNS message.
    - CPNS common parameter set MAY contain Route parameter(s) under DestinationRoute if the intermediate route entities are known to the CPNS message originator (Source parameter).
- CPNS common parameter set MAY contain TraceRoute when designated by the CPNS message originator (Source parameter). Each CPNS Entity SHALL append its own ID (as value of Route parameter).
- CPNS common parameter set SHALL contain MsgID parameter to distinguish a CPNS message dialog with others.
- CPNS common parameter MAY contain MsgType parameter to designate specific transport protocol related behavior (e.g., HTTP Client and Server. See Appendix G).

Following table shows the parameter set common to all CPNS messages.

Parameter name	Cardinality	T	Data type	Description
TargetID	0..1	E	String	ID of adjacent CPNS Entity, through which the CPNS message will go traverse to the destination, PNID, or SGID Only if TargetID and DestID are the same, this element will be omitted.
SourceID	1	E	String	ID of CPNS Entity which is the originator of the CPNS message

Destination	1	E	String	Destination element for end to end CPNS message routing path Its sub-element is • DestinationRoute • DestID
DestinationRoute	0..3	E	-	In case the intermediate CPNS Entities to the destination CPNS Entity (Dest) are known to the originating CPNS Entity (Source) and to specify the routing path to the destination, the CPNS Entity assembles the CPNS message with not only Dest element but also DestinationRoute element(s). Its attribute is • DestinationRouteEntity
DestinationRoute Entity	1	A	String	ID of intermediate CPNS Entity for end to end routing path to destination CPNS Entity (Dest)
DestID	1..n	E	String	ID of CPNS Entity, PNID or SGID which is the final destination of the CPNS message In case the Route element(s) is not known to the originating CPNS Entity (Source), the CPNS Entity assembles the Destination element with Dest element only.
TraceRoute	0..1	E	String	To trace the routing path to the destination CPNS Entity (Dest), PNID or SGID, the originating CPNS Entity (Source) SHOULD include the TraceRoute element. Its sub-element is • Route
Route	1..4	E	-	With TraceRoute element, each CPNS Entity SHALL append its EntityID into the Route element. In case of no TraceRoute element is designated by the originating CPNS Entity (Source), the Route element SHALL not be included. Its attribute is • EntityID
EntityID	1	A	String	ID of intermediate CPNS Entity for the purpose of tracing intermediate CNPS Entity on the end to end routing path to destination(Dest)
MsgID	1	E	String	Unique ID to distinguish the message from other messages.

				ID schema is based on service provider and out of scope of CPNS V1.0.
MsgType	0..1	E	String	Indicating the type of message; "Advertise" or "Request" or "Response
Encrypted	0..1	E	Boolean	Indicates if the payload of the CPNS message (i.e., all the elements and attributes except for common parameters) is encrypted. If the payload is encrypted, CPNS Entity can skip to include this element in the message.

Table 6 Common CPNS message parameters

8.2 UserID and Password Registration

Message	Implementation	Direction
ID_PWD Registration Request Message	Conditional	PN GW → CPNS Server
ID_PWD Registration Response Message	Conditional	CPNS Server → PN GW

If PN GW is running on device which does not support mutual authentication using USIM (or GBA), PN GW does not need to proceed with ID_PWD Registration Request/Response Message.

If CPNS Server does not support mutual authentication using USIM (or GBA), CPNS Server does not need to support ID_PWD Registration Request/Response Message.

8.2.1 ID_PWDRegistrationRequest Message

Element	Cardinality	T	Data Type	Description
ID_PWD_Registration_Request	1	E		Its sub elements are: • UserID • Password • UserDescription
UserID	1	E	String	UserID that CPNS User wants to use. This element is empty (i.e., <UserID/>), if CPNS User requests CPNS Server to create UserID.
Password	1	E	String	Password that CPNS User wants to use. This element is empty (i.e., <Password/>), if CPNS User requests CPNS Server to create password.
UserDescription	0…1	E	String	User information such as name and subscription number. This element may be filled according to the Operator Policy.

Table 7 Information elements in ID_PWD Registration Request Message

8.2.2 ID_PWDRegistrationResponse Message

Element	Cardinality	T	Data Type	Description
ID_PWD_Registration	1	E		Its attribute is: • Status

Response				Its sub elements are: • UserID • Password
Status	1	A	Integer	The status of success or fail. 1 – Success 2 – Fail, UserID CPNS User requests to use is already used 3 – Fail, UserID CPNS User requests to use is against the policy for UserID (e.g., UserID is too long) 4 – Fail, Password CPNS User requests to use is against the policy for password (e.g., password is too short) 5 – Fail, failed due to unknown reason.
UserID	0…1	E	String	UserID that is registered with CPNS Server. In case of registration failure, this element is empty .
Password	0…1	E	String	Password that is registered with CPNS Server. In case of registration failure, this element is empty.

Table 8 Information elements in ID_PWD Registration Response Message

8.3 ID & Password Installation

Message	Implementation	Direction
ID_PWD Installation Request Message	Conditional	PN GW → PNE
ID_PWD Installation Response Message	Conditional	PNE → PN GW

8.3.1 ID_PWD Installation Request Message

Element	Cardinality	T	Data Type	Description
ID_PWD_Request	1	E		Its sub elements are: • UserID • Password
UserID	1	E	String	UserID that was already registered in the CPNS Server through the Id & Password Registration. This element contains same User ID and to be installed to PNE.
Password	1	E	String	Password that was already registered in the CPNS Server through the ID & Password Registration. This element contains same Password and to be installed to PNE.

Table 9 Information elements in ID_PWD_Installation Request Message

8.3.2 ID_PWD Installation Response Message

Element	Cardinality	T	Data Type	Description
Subscription_Registration_Response	1	E		Its attributes are: • Status
Status	1	A	Integer	The status of success or fail. 1 – Success 2 – Fail, ID & Password Installation is failed.

Table 10 Information elements in ID_PWD_Installation Response Message

8.4 EUKey Assignment

This subsection provides format of the messages necessary for EUKey assignment for PNE and PN GW.

Message	Implementation	Direction
EUKey Assignment Trigger Message	Conditional	PN GW → PNE
EUKey Assignment Request Message	Mandatory	PNE → PN GW PN GW → CPNS Server
EUKey Assignment Response Message	Mandatory	CPNS Server → PN GW PN GW → PNE
EUKeyAssignmentNotification Message	Conditional	PN GW → PNE

NOTE: EUKeyAssignmentTrigger Message is mandatory if PNE does not have enough UI capabilities for inserting UserID and Password.

8.4.1 EUKeyAssignmentTrigger Message

Element	Cardinality	T	Data Type	Description
EUKeyAssignmentTrigger	1	E		Its attributes are: • UserID Its sub-elements are: • TrgInfo
UserID	1	A	String	UserID of CPNS User who owns both PN GW and PNE
TrgInfo	1	E		EUKey Assignment Trigger information Its sub attributes are • $RAND_{PNGW}$ • Time • AuthInfo
$RAND_{PNGW}$	1	A	Integer	$RAND_{PNGW}$ is a random number generated by the PN GW
Time	1	A	String	Time is the current time as measured by the PN GW
AuthInfo	1	A	String	AuthInfo is a Hash (AuthData) where AuthData = Hash(Password) | Nonce | Time

Table 11 Information elements in EUKeyAssignmentTrigger Message

8.4.2 EUKeyAssignmentRequest Message

Element	Cardinality	T	Data Type	Description
EUKeyAssignmentRequest	1	E		Its attributes are: • UserID • EntityID

				Its sub-element is: • ReqInfo
UserID	1	A	String	UserID of CPNS User who owns an assignee PNE/PN GW
EntityID	1	A	String	EntityID of an assignee PNE/PN GW
ReqInfo	1	E		EUKeyAssignmentRequest information Its sub attributes are • $RAND_{Assignee}$ • Time • AuthInfo
RANDAssignee	1	A	Integer	$RAND_{Assignee}$ is a random number generated by the assignee CPNS Entity (i.e., PNE or PN GW)
Time	1	A	String	Time is the current time measured by the assignee CPNS Entity (i.e., PNE or PN GW)
AuthInfo	1	A	String	AuthInfo is a Hash (AuthData) where AuthData = Hash(Password) | $RAND_{Assginee}$ | Time

Table 12 Information elements in EUKeyAssignmentRequest Message

8.4.3 EUKeyAssignmentResponse Message

Element	Cardinality	T	Data Type	Description
EUKeyAssignmentResponse	1	E		Its attributes are: • Result • UserID • EntityID
Result	1	A	Integer	The Result of success or fail. 1 – Success 2 – Fail, User authentication fails 3 – Fail, Other reasons
UserID	1	A	String	UserID of CPNS User who owns an assignee PNE/PN GW
EntityID	1	A	String	EntityID of an assignee PNE/PN GW
ResInfo	1	E		EUKeyAssignmentResponse information Its sub attributes are • $RAND_{SVR}$ • EUKey • Temporary Key
$RAND_{SVR}$	1	A	Integer	$RAND_{SVR}$ is a random number generated by the CPNS Server
EUKey	1..n	A	String	Encrypted EUKey that is encrypted by the KEK
TemporaryKey	0..1	A	String	Key used for ensuring the security between PNE and PN GW in the case of underlying network does not support sufficient security

				mechanism.

Table 13 Information elements in EUKeyAssignmentResponse Message

8.4.4 EUKeyAssignmentNotification Message

Element	Cardinality	T	Data Type	Description
EUKeyAssignmentNotification	1	E		Its attributes are: • UserID • EntityID • EUKey
UserID	1	A	String	UserID of CPNS User who owns an assignee PNE/PN GW
EntityID	1	A	String	EntityID of an assignee PNE/PN GW
EUKey	1	A	String	Encrypted EUKey that is encrypted by the Temporary Key

Table 14 Information elements in EUKeyAssignmentNotifiation Message

8.5 CPNS Entity Discovery

A device which has the initial Mode following the definition of Entity Mode in section 5.2 can start the entity discovery to recognize the Mode of the other device in PAN.

CPNS Entity Discovery transaction can be done between PNE and PN GW, PNE and PNE, or PN GW and PN GW because the requested CPNS Entity does not know the Mode of other device before the Entity Discovery transaction after physical connection.

Note: The interface between PNE and PNE will not be used for peer to peer but for CPNS entity discovery only in CPNS 1.0.

Message	Implementation	Direction
EntityDiscoveryRequest	Mandatory	PNE → PNE, PNE → PN GW, PN GW → PNE, PN GW → PN GW
EntityDiscoveryResponse	Mandatory	PNE → PNE, PN GW → PNE, PNE → PN GW, PN GW → PN GW

8.5.1 CPNS Entity Discovery Request message

Element	Cardinality	T	Data Type	Description
EntityDiscoveryRequest	1	E		Its sub elements are • UserInfo • EntityInfo • PNInfo
UserInfo	1	E	-	Its attributes are • UserID

				• UserName
UserID	0..1	A	String	CPNS UserID
UserName	1	A	String	CPNS User Name
EntityInfo	1	E		Entity information Its sub attributes are • PNEID • PNGWID • Name • Mode • PNInfoReq • UICapa • Zonebasedservicesupport • Broadcastgroupkeydeliverysupport
PNEID	0..1	A	String	PNE Identification (see section **Error! Reference source not found.**).
PNGWID	0..1	A	String	PN GW Identification (see section **Error! Reference source not found.**).
Name	0..1	A	String	PNE or PN GW Name (e.g. MP3 player, assigned nickname)
Mode	1	A	Integer	The mode of requester. If the mode of requestor is PNE, the value should be "1" (PNE). If the mode of requestor is PN GW, the value should be "2" (PN GW). If the mode of requestor is both of PNE and PN GW, the value should be "3" (BOTH) (e.g. mobile phone) 1 – PNE, If the mode of device is PNE, the value should be "PNE". 2 – PNGW, If the mode of device is PN GW, the value should be "PN GW". 3 – BOTH, If the mode of device is both of PNE and PN GW, the value should be "BOTH" (e.g. mobile phone)
PNInfoReq	0..1	A	Boolean	The value is "TRUE" in case the PNE requests PN information.
UICapa	0..1	A	Boolean	If this device doesn't support UI functionalities below, this value SHALL be set. TRUE: PN GW needs to support confirmation and/or Key assignment functionalities instead of PNE.
Zonebasedservicesupport	0..1	A	Boolean	If this CPNS entity is a capable PN GW of Zone Based Service, this value should be "TRUE".
Broadcastgroupkeydeliverysupport	0..1	A	Boolean	When PN GW sends EntityDiscoveryRequest message, this attribute SHALL be inserted. TRUE: PN GW supports broadcast Group Key delivery FALSE: PN GW does not support broadcast Group Key delivery.
PNInfo	0..n	E		PN information when the requester is PN GW and it handles PN(s). This is helpful information to join request from PNE. Its sub attributes are

				• PNID • Description • TempPN • Sharing Its sub element is • PNEInfo
PNID	1	A	String	PN identification.
Description	0..1	A	String	PN Description. (e.g. home, office)
TempPN	0..1	A	Boolean	If this PN is temporary PN, this is "TRUE". If the physical connection between PNGW and all of PNEs is broken, this PN should be released automatically. If this PN is sustained PN, this TempPN attribute is empty or "FALSE".
Sharing	0..1	A	Integer	The level of PN Inventory in PNE side 1 – Shared, PN GW Info and PNE Info are shared in PNE 2 – Protected, PN GW Info only in PNE
PNEInfo	1..n	E		The member PNEs of PN. Its sub attributes are • PNEID • PNEName Its sub element is • DeviceInfo
PNEID	1	A	String	PNE Identification
PNEName	0..1	A	String	PNE Name (e.g. mp3 player, assigned nickname)
DeviceInfo	0..1	E		Device information Its sub attribute is • Mode • InactiveMode
Mode	0..1	A	Integer	The mode of device 1 – PNE, If the mode of device is PNE, the value should be "PNE". 3 – BOTH, If the mode of device is both of PNE and PN GW, the value should be "BOTH" (e.g. mobile phone)
InactiveMode	0..1	A	Integer	If current mode is PNE and there are functionalities of PN GW in a device, the other function is inactive. (e.g. If the value of Mode is "1"(PNE) and its functionalities are PNE and PN GW in a mobile phone, inactive is set "2" (PN GW) and this means inactive mode is "PN GW".) 1 – PNE 2 – PNGW

Table 15 Information elements in EntityDiscoveryRequest message

8.5.2 CPNS Entity Discovery Response message

Element	Cardinality	T	Data Type	Description
EntityDiscoveryResponse	1	E		Its sub elements are • UserInfo • EntityInfo • PNInfo
UserInfo	1	E	-	Its attributes are • UserID • UserName
UserID	0..1	A	String	CPNS UserID
UserName	1	A	String	CPNS User Name
EntityInfo	1	E		Entity Information Its sub attributes are • PNEID • PNGWID • Name • Mode • UICapa • Zonebasedservicesupport • Broadcastgroupkeydeliverysupport
PNEID	0..1	A	String	PNE Identification (see section **Error! Reference source not found.**).
PNGWID	0..1	A	String	PN GW Identification (see section **Error! Reference source not found.**).
Name	0..1	A	String	PNE or PN GW Name (e.g. player, assigned nickname)
Mode	1	A	Integer	The mode of respondent. If the mode of respondent is PNE, the value should be "1" (PNE). If the mode of respondent is PN GW, the value should be "2" (PN GW). If the mode of respondent is both of PNE and PN GW, the value should be "3" (BOTH) (e.g. mobile phone) 1 – PNE, If the mode of device is PNE, the value should be "PNE". 2 – PNGW, If the mode of device is PN GW, the value should be "PN GW". 3 – BOTH, If the mode of device is both of PNE and PN GW, the value should be "BOTH" (e.g. mobile phone)
UICapa	0..1	A	Boolean	If this device doesn't support UI functionalities below, this value SHALL be set with "TRUE".

				TRUE: PN GW needs to support confirmation and/or Key assignment functionalities instead of PNE.
Zonebasedservicesupport	0..1	A	Boolean	If this CPNS entity is a capable PN GW of Zone Based Service, this value should be "TRUE".
Broadcastgroupkeydeliverysupport	0..1	A	Boolean	When PN GW sends EntityDiscoveryResponse message, this attribute SHALL be inserted. TRUE: PN GW supports broadcast Group Key delivery FALSE: PN GW does not support broadcast Group Key delivery.
PNInfo	0..n	E		PN information when the value of Mode attribute is PN GW. This is helpful information to join request from PNE. Its sub attributes are • PNID • Description • TempPN • Sharing Its sub element is • PNEInfo
PNID	1	A	String	PN identification.
Description	0..1	A	String	PN Description. (e.g. home, office)
TempPN	0..1	A	Boolean	If this PN is temporary PN, this is "TRUE". If the physical connection between PNGW and all of PNEs is broken, this PN should be released automatically. If this PN is sustained PN, this TempPN attribute is empty or "FALSE".
Sharing	0..1	A	Integer	The level of PN Inventory in PNE side 1 – Shared, PN GW Info and PNE Info are shared in PNE 2 – Protected, PN GW Info only in PNE
PNEInfo	0..n	E		The member PNEs of PN. Its sub attributes are • PNEID • PNEName Its sub element is • DeviceInfo
PNEID	1	A	String	PNE Identification
PNEName	0..1	A	String	PNE Name (e.g. mp3 player, assigned nickname)
DeviceInfo	0..1	E		Device information Its sub attribute is

				• Mode • InactiveMode
Mode	0..1	A	Integer	The mode of device 1 – PNE, If the mode of device is PNE, the value should be "PNE". 3 – BOTH, If the mode of device is both of PNE and PN GW, the value should be "BOTH" (e.g. mobile phone)
InactiveMode	0..1	A	Integer	If current mode is PNE and there are functionalities of PN GW in a device, the other function is inactive. (e.g. If the value of Mode is "1"(PNE) and its functionalities are PNE and PN GW in a mobile phone, inactive is set "2" (PN GW) and this means inactive mode is "PN GW".) 1 – PNE 2 – PNGW

Table 16 Information elements in EntityDiscoveryResponse message

8.6 PNE and PN GW Authentication

This subsection provides format of the messages necessary for PNE and PN GW authentication described in section 7.5. These messages are also utilized for secure session establishment between PNE and PN GW.

Message	Implementation	Direction
ConnectRequest Message	Conditional	PNE→PN GW PN GW → CPNS Server
ConnectResponse Message	Conditional	PN GW→PNE CPNS Server → PN GW
AuthenticateRequest Message	Mandatory	CPNS Server → PN GW PN GW → PNE
AuthenticateResponse Message	Mandatory	PNE→ PN GW PN GW → CPNS Server

8.6.1 ConnectRequest Message

Element	Cardinality	T	Data Type	Description
ConnectRequest	1	E		Its sub attributes are: • RAND
RAND	1	A	String	Random value generated by PN GW or PNE (e.g., random_PN GW in section 7.7.)

Table 17 Information elements in ConnectRequest Message

Note: Entity ID of sender PN GW/PNE, which is not shown in the table, is included in source ID of this message.

8.6.2 ConnectResponse Message

Element	Cardinality	T	Data Type	Description
ConnectResponse	1	E		Its sub attributes are: • HASH
HASH	1	A	String	Hash value calculated by CPNS Server (e.g., hash_server in section 7.7.)

Table 18 Information elements in ConnectResponse Message

8.6.3 AuthenticateRequest Message

Element	Cardinality	T	Data Type	Description
AuthenticateRequest	1	E		Its sub element is: • AuthReqData
AuthReqData	1..n	E		Set of information to be delivered to target PNE(s)/PNGW to be authenticated. This sub element is inserted into the message for each CPNS Entity to be authenticated. (i.e., When there are more than one PNEs to be authenticated, more than one elements are inserted.) Its sub attributes are: • EntityID • RAND • LocalEUKey_PNE • LocalEUKey_PNGW
EntityID	1	A	String	Entity ID of target PNE(s) or PN GW to be authenticated by CPNS Server or PN GW
RAND	1	A	String	Ramdom value generated by CPNS Server or PN GW (e.g., random_server in section 7.6.1)
LocalEUKey_PNE	0..1	A	String	LocalEUKey encrypted by target PNE's EUKey. Note: This attribute is included when target entity to be authenticated is PNE which requests LocalEUKey assignment.
LocalEUKey_PNGW	0..1	A	String	LocalEUKey encrypted by PN GW's EUKey Note: This attribute is included when target entity to be authenticated is PNE which requests LocalEUKey assignment and when message is sent from CPNS Server to PN GW.

Table 19 Information elements in AuthenticateRequest Message

8.6.4 AuthenticateResponse Message

Element	Cardinality	T	Data Type	Description
AuthenticateResponse	1	E		Its sub element is: • AuthResData
AuthResData	1..n	E		Set of information to be delivered to target PNE(s)/PNGW to be authenticated. This sub element is inserted into the message for each CPNS Entity to be authenticated. (i.e., When there are more than one PNEs to be authenticated, more than one elements are inserted.) Its sub attributes are: • EntityID • HASH

EntityID	1	A	String	Entity ID of target PNE or PN GW to be authenticated by CPNS Server or PN GW
HASH	1	A	String	Hash value calculated by target PNE or PN GW (i.e., hash_PNE in 7.6.1 or hash_PN GW in section 7.7)

Table 20 Information elements in AuthenticateResponse Message

8.7 PN Management

8.7.1 PN Establishment

Message	Implementation	Direction
PNSetupRequest	Mandatory	PNE → PN GW PN GW → PNE PN GW → CPNS Server
PNSetupResponse	Mandatory	CPNS Server → PN GW PN GW → PNE PNE → PN GW
PNEstablishmentNotify	Mandatory	PN GW → PNE

8.7.1.1 PNSetup Request message

NAME	Cardinality	T	Data Type	Description
PNSetupRequest	1	E		Command when PNE requests to establish a PN to PN GW. Its sub attribute is • OriginEntityID • PNSetupType Its sub element is • InvitedPNEID • PNInfo • AuthIniData
OriginEntityID	1	A	String	The originating CPNS EntityID to establish PN
PNSetupType	1	A	Integer	Type of PN Setup to indicate how the PN is established 1 – '1-1' case which enables the PNE to establish a PN with the PN GW only 2 – 'All' case which enables the PNE to establish a PN with all CPNS devices connected to the PN GW 3 – 'Specific' case which enables the PNE to establish a PN with PNEs to be invited
InvitedPNEID	0..n	E	String	PNEID(s) to be invited during PN Establishment
PNInfo	1	E		PN Information. This is the information to be registered and stored in CPNS Server. Its sub attributes are

				• PNID • Description • Disclosure • OwnershipEntity • TempPN • Sharing Its sub elements are • PNGWInfo • PNEInfo
PNID	0..1	A	String	PN Identification
Description	0..1	A	String	PN Description (e.g., Home, Office)
Disclosure	1	A	Integer	The willingness of openness of PN Information, in case Service Discovery is requested after PN Setup 1 - Blocked; PN should not be unveiled. 2 - Open; PN will be unveiled, when other CPNS Entities asks service discovery. 3 - Confirm Mode: PN can be unveiled, only when the authorized CPNS entity allows
OwnershipEntity	0..1	A	String	The ID of authorized CPNS Entity which has authorization to allow PN Information open, in case Service Discovery is requested
TempPN	1	A	Boolean	If this PN is temporary PN, this is "TRUE". True, indicating that PN Information will not be kept in CPNS Server after broken physical connection . False, indicating that PN Information remains in CPNS Server, even if physical connection is broken. If PN GW decides False, TempPN attribute MAY be skipped.
Sharing	1	A	Integer	The level of PN Inventory in PNE side 1 – Shared, PN GW Info and PNE Info are shared to PNE 2 - Protected, PN GW Info only to PNE
PNGWInfo	0..1	E		PN GW Information. Its sub attributes are • PNGWID • PNGWName
PNGWID	1	A	String	PN GW Identification
PNGWName	0..1	A	String	PN GW Name (e.g. nickname assigned by user or device type)
PNEInfo	0..n	E		PNE Information.

				Its sub attributes are • PNEID • PNEName • Mode • Description Its sub elements are • DeviceCapa • ServiceProfile
PNEID	1	A	String	PNE Identification
PNEName	0..1	A	String	PNE Name (e.g., nickname assigned by user)
Mode	0..1	A	Integer	The mode of device. The member can be "1" or "3". 1 – PNE, If the mode of respondent is PNE, the value should be "PNE". 2 – PNGW, If the mode of respondent is PN GW, the value should be "PN GW". 3 – BOTH, If the mode of respondent is both of PNE and PN GW, the value should be "BOTH" (e.g. mobile phone)
Description	0..1	A	String	PN Description (e.g., Home, Office)
DeviceCapa	0..1	E		Capability information of device embedding PNE DeviceCapa fragment contains information such as DeviceType, VideoCodec, etc. For CPNS V1.0 format definition is out of scope (e.g. DPE Enabler) and implementation matter.
ServiceProfile	0..1	E	-	CPNS enabled application information or content to support certain service and status. NOTE: Section 5.5 CPNS Metadata is referred.
AuthIniData	0..n	E		Set of information used to initiate PNE authentication procedure. The included information is generated by target PNE(s) to be authenticated. Its sub attributes are: • AuthPNEID • rand_PNE • LocalEUKeyAssignment The number of this sub element included in the message differs depending on the message direction; • PNE (inviting PNE)→PN GW: one • PN GW→PNE (invited PNE): none

				• PN GW→CPNS Server: one or more than one, depending on the number of invited PNE
AuthPNEID	1	A	String	Entity ID of target PNE to be authenticated by CPNS Server
rand_PNE	1	A	String	Random value generated by PNE
LocalEUKeyAssignment	1	A	Boolean	Flag to indicate the necessity of LocalEUKey assignment. TRUE: necessary, FALSE: unnecessary

Table 21 Information elements in SETUP Request message

8.7.1.2 PNSetup Response message

Element	Cardinality	T	Data Type	Description
PNSetupResponse	1	E		The response to PNSetup Request message Its sub attributes are • Return Its sub elements are • PNInfo • AuthIniData • AuthFinData
Return	1	A	Integer	The answer to SETUP Reqeust 1 – OK 2 – Failure: CPNS Enabler can't handle the request, e.g., internal error process occurs in the device embedding PNE 3 – Not Accepted: CPNS User does not allow the request NOTE: the answer may be added later according to Operator Policy.
PNInfo	0..1	E		PN Information. This is the information to be registered and stored in CPNS Server. Its sub attributes are • PNID • Description • TempPN • Sharing Its sub elements are • PNGWInfo

				• PNEInfo
PNID	1	A	String	PN Identification
Description	0..1	A	String	PN Description (e.g., Home, Office)
TempPN	0..1	A	Boolean	If this PN is temporary PN, this is "TRUE". If the physical connection between PNGW and PNEs is broken, this PN should be released automatically.
Sharing	0..1	A	Integer	The level of PN Inventory in PNE side 1 – Shared, PN GW Info and PNE Info are shared to PNE 2 - Protected, PN GW Info only is shared to PNE
PNGWInfo	0..1	E		PN GW Information. Its sub attributes are • PNGWID • PNGWName
PNGWID	1	A	String	PN GW Identification
PNGWName	0..1	A	String	PN GW Name (e.g. nickname assigned by user or device type)
PNEInfo	1..n	E		PNE Information. Its sub attributes are • PNEID • PNEName • Mode • Description Its sub elements are • DeviceCapa • ServiceProfile
PNEID	1	A	String	PNE Identification
PNEName	0..1	A	String	PNE Name (e.g., nickname assigned by user)
Mode	1	A	Integer	The mode of device. The member can be "1" or "3". 1 – PNE, If the mode of respondent is PNE, the value should be "PNE". 3 – BOTH, If the mode of respondent is both of PNE and PN GW, the value should be "BOTH" (e.g. mobile phone)
Description	0..1	A	String	PN Description (e.g., Home, Office)
DeviceCapa	0..1	E	-	Capability information of device embedding PNE DeviceCapa fragment contains information such as DeviceType, VideoCodec, etc. For CPNS V1.0 format definition is out of scope (e.g. DPE Enabler) and implementation matter.

ServiceProfile	0..1	E	-	CPNS enabled application information to support certain service and status. NOTE:*See Section 5.105 CPNS Metadata is referred.
AuthIniData	0..1	E	-	Set of information used to initiate PNE authentication procedure. The included information is generated by target PNE(s) to be authenticated. Its sub attributes are: • AuthPNEID • rand_PNE • LocalEUKeyAssignment The number of this sub element included in the message differs depending on the message direction; • PNE (invited PNE)→PN GW: one • CPNS Server→PN GW: none • PN GW→PNE (inviting PNE): none
AuthPNEID	1	A	String	Entity ID of target PNE to be authenticated by CPNS Server
rand_PNE	1	A	String	Random value generated by PNE (i.e., rand_PNE in section 7.6.)
LocalEUKeyAssignment	1	A	Boolean	Flag to indicate the necessity of LocalEUKey assignment. TRUE: necessary, FALSE: unnecessary
AuthFinData	0..n	E	-	Set of information used to authenticate CPNS Server by PNE. Its sub attribute is: • HASH The number of this sub element included in the message defers depending on the message direction; • PNE (invited PNE)→PN GW: none • CPNS Server→PN GW: one or more than one, depending on the number of invited PNEs • PN GW→PNE (inviting PNE): one
HASH	1	A	String	Hash value calculated by target PNE or PN GW (i.e., hash_server in 7.6.)

Table 22 Information elements in SETUP Response message

8.7.1.3 PNEstablishmentNotify message

Element	Cardinality	T	Data Type	Description
PNEstablishmentNotify	1	E		The command to notify PN Inventory from PN GW to PNE Its sub elements are

				• PNInfo • AuthFinData
PNInfo	0..1	E		PN Information. This is the information to be registered and stored in CPNS Server. Its sub attributes are • PNID • Description • TempPN • Sharing Its sub elements are • PNGWInfo • PNEInfo
PNID	1	A	String	PN Identification
Description	0..1	A	String	PN Description (e.g., Home, Office)
TempPN	0..1	A	Boolean	If this PN is temporary PN, this is "TRUE". If the physical connection between PNGW and PNEs is broken, this PN should be released automatically.
PNGWInfo	1	E		PN GW Information. Its sub attributes are • PNGWID • PNGWName
PNGWID	1	A	String	PN GW Identification
PNGWName	0..1	A	String	PN GW Name (e.g. nickname assigned by user or device type)
PNEInfo	1..n	E		PNE Information. Its sub attributes are • PNEID • PNEName Its sub elements are • DeviceCapa • ServiceProfile
PNEID	1	A	String	PNE Identification
PNEName	0..1	A	String	PNE Name (e.g., nickname assigned by user)
DeviceCapa	0..1	E		Capability information of device embedding PNE DeviceCapa fragment contains information such as DeviceType, VideoCodec, etc. For CPNS V1.0 format definition is out of scope

				(e.g. DPE Enabler) and implementation matter.
ServiceProfile	0..1	E	-	CPNS enabled application information to support certain service and status. NOTE: Section 5.5 CPNS Metadata is referred.
AuthFinData	1	E	-	Set of information used to authenticate CPNS Server by PNE. Its sub attribute is: • HASH
HASH	1	A	String	Hash value calculated by target PNE or PN GW (i.e., hash_server in 7.6.)

Table 23 Information elements in PNEstablishmentNotify message

8.7.2 PN Update

Message	Implementation	Direction
PNUpdateRequest	Mandatory	PN GW → CPNS Server
PNUpdateResponse	Mandatory	CPNS Server → PN GW
PNUpdateNotification	Mandatory	PN GW → PNE

8.7.2.1 PN Update Request message

Element	Cardinality	T	Data Type	Description
PNUpdateRequest	1	E		Its sub element is • PNInfo • AuthIniData
PNInfo	1	E		PN Information. This is information of PN to be uploaded. Its sub attributes are • PNID Its sub element is • PNEInfo
PNID	1	A	String	PN Identification.
PNEInfo	0..n	E		PNE Information. If there is modification of PNE, this should be inserted. (e.g. new PNE joined, PNE left) Its sub attributes are • PNEID • PNEName • Mode • Active

				• Update
PNEID	1	A	String	PNE Identification.
PNEName	0..1	A	String	PNE Name (e.g. mp3 player)
Mode	0..1	A	Integer	The mode of device. This member can "1" or "3". 1 – PNE, If the mode of respondent is PNE, the value should be "PNE". 3 – BOTH, If the mode of respondent is both of PNE and PN GW, the value should be "BOTH" (e.g. mobile phone)
Active	1	A	Boolean	The active status of PNE. TRUE – This PNE is active FALSE – This PNE is not active because PNE is temporary disconnected.
Update	1	A	Integer	The update information of this PNE. 1 – New, the PNE is newly joined in this PN 2 – Update, the PNE is updated 3 – Removed, the PNE is removed in this PN
AuthIniData	0..n	E		Set of information used to initiate PNE authentication procedure. The included information is generated by target PNE(s) to be authenticated. Its sub attributes are: • AuthPNEID • rand_PNE • LocalEUKeyAssignment
AuthPNEID	1	A	String	Entity ID of target PNE to be authenticated by CPNS Server
rand_PNE	1	A	String	Random value generated by PNE (i.e., rand_PNE in section 7.6.)
LocalEUKeyAssignment	1	A	Boolean	Flag to indicate the necessity of LocalEUKey assignment. TRUE: necessary, FALSE: unnecessary

Table 24 Information elements in PNUpdateRequest message

8.7.2.2 PN Update Response message

Element	Cardinality	T	Data Type	Description
PNUpdateResponse	1	E		Its sub attributes are • Result Its sub element is: • AuthFinData
Result	1	A	Integer	The status of success or fail. 1 – Success 2 – Fail, this PN is not registered before.

				3– Fail, this PNE is not the member of this PN (for expulsion). 4 – Fail, this PNE was the member of this PN before (for joining).
AuthFinData	0..n	E		Set of information used to authenticate CPNS Server by PNE. Its sub attribute is: • HASH
HASH	1	A	String	Hash value calculated by target PNE or PN GW (i.e., hash_server in 7.6.)

Table 25 Information elements in PNUpdateResponse message

8.7.2.3 PNUpdateNotification message

Element	Cardinality	T	Data Type	Description
PNUpdateNotification	1	E		Its sub element is • PNInfo
PNInfo	1	E		PN Information. Its sub attributes are • PNID Its sub element is • PNEInfo
PNID	1	A	String	PN Identification.
PNEInfo	0..n	E		PNE Information Its sub attributes are • PNEID • PNEName • Mode • Active • Update
PNEID	1	A	String	PNE Identification.
PNEName	0..1	A	String	PNE Name (e.g. mp3 player, assigned nickname)
Mode	1	A	Integer	The mode of device 1 – PNE, If the mode of device is PNE, the value should be “PNE”. 3 – BOTH, If the mode of device is both of PNE and PN GW, the value should be “BOTH” (e.g. mobile phone)
Active	1	A	Boolean	The active status of PNE. TRUE – This PNE is active FALSE – This PNE is not active because PNE is temporary disconnected.
Update	1	A	Integer	The update information of this PNE. 0 – Current, the PNE is member in this PN

				1 – New, the PNE is newly joined in this PN 2 – Update, the PNE is updated 3 – Removed, the PNE is removed in this PN
AuthFinData	0..1	E		Set of information used to authenticate CPNS Server by PNE. Its sub attribute is: HASH
HASH	1	A	String	Hash value calculated by target PNE or PN GW (i.e., hash_server in 7.6.)

Table 26 Information elements in PNUpdateNotification message

8.7.3 PNE Joining, Inviting, Leaving, Expulsion

Message	Implementation	Direction
PNActionRequest	Mandatory	PNE → PN GW PN GW → PNE
PNActionResponse	Mandatory	PN GW → PNE PNE → PN GW
PNActionNotification	Mandatory	PN GW → PNE

8.7.3.1 PNActionRequest message

Element	Cardinality	T	Data Type	Description
PNActionRequest	1	E		Its sub attributes are • Command • OriginEntityID Its sub elements are • PNEInfo • PNInfo • AuthIniData
Command	1	A	Integer	It is a command that a CPNS entity uses it based on the actions to be performed by PN GW or CPNS Server, e.g. join, leave, invite, expel etc. 1 – Join, the PNE wants to join 2 – Invite, the PNE or PN GW wants to invite other PNE(s) 3 – Leave, the PNE wants to leave 4 – Expel, PNE or PNGW wants to expel other PNE.
OriginEntityID	0..1	A	String	PNE Identification that originally requests action related with the other PNE. (e.g. request action of invitation, expulsion)
PNEInfo	1	E		Target PNE Information to join, leave, be invited or be expelled.

				Its sub attribute are • PNEID • PNEName
PNEID	1	A	String	PNE Identification.
PNEName	0..1	A	String	PNE Name (e.g. mp3 player, assigned nickname)
PNInfo	1	E		PN Information Its sub attributes are • PNID • Description • TempPN • Sharing Its sub element is • PNGWInfo
PNID	1	A	String	PN Identification.
Description	0..1	A	String	PN Description. (e.g. Home, Office)
TempPN	0..1	A	Boolean	If this PN is temporary PN, this is "TRUE". If the physical connection between PNGW and all of PNEs is broken, this PN should be released automatically. If this PN is sustained PN, this TempPN attribute is empty or "FALSE".
Sharing	0..1	A	Integer	The level of PN Inventory in PNE side 1 – Shared, PN GW Info and PNE Info are shared in PNE 2 – Protected, PN GW Info only in PNE
PNGWInfo	0..1	E		PN GW Information. Its sub attributes are • PNGWID • PNGWName • Zonebasedservicesupport • Mode • Broadcastgroupkeydeliverysupport
PNGWID	1	A	String	PN GW Identification.
PNGWName	0..1	A	String	PN GW Name (e.g. mobile phone, assigned nickname)
Zonebasedservicesupport	0..1	A	Boolean	If this CPNS entity is a capable PN GW of Zone Based Service, this value should be "TRUE".
Mode	1	A	Integer	The mode of current device 2 – PNGW, If the mode of device is PN GW, the value should be

				"PN GW". 3 – BOTH, If the mode of device is both of PNE and PN GW, the value should be "BOTH" (e.g. mobile phone)
Broadcastgroupkeydeliverysupport	0..1	A	Boolean	TRUE: PN GW supports broadcast Group Key delivery FALSE: PN GW does not support broadcast Group Key delivery.
AuthIniData	0..1	E		Set of information used to initiate PNE authentication procedure. The included information is generated by target PNE(s) to be authenticated. Its sub attributes are: • AuthPNEID • rand_PNE • LocalEUKeyAssignment This element is included in the message if the command attribute is Join and the message direction is from PNE to PN GW.
AuthPNEID	1	A	String	Entity ID of target PNE to be authenticated by CPNS Server
rand_PNE	1	A	String	Random value generated by PNE (i.e., rand_PNE in section 7.6.)
LocalEUKeyAssignment	1	A	Boolean	Flag to indicate the necessity of LocalEUKey assignment. TRUE: necessary, FALSE: unnecessary

Table 27 Information elements in PNActionRequest message

8.7.3.2 PNActionResponse message

Element	Cardinality	T	Data Type	Description
PNActionResponse	1	E		Its sub attributes are • Result Its sub elements are • PNInfo • AuthIniData • AuthFinData
Result	1	A	Integer	The status of success or fail. 1 – Success 2 – Fail, this PN is not registered before. 3 – Fail, this PNE is not connected. 4 – Notification, this PNE has active SG related with this PN.
PNInfo	0..1	E		PN Information. Its sub attributes are • PNID • Description • TempPN

				• Sharing Its sub elements are • PNGWInfo • PNEInfo
PNID	1	A	String	PN Identification.
Description	0..1	A	String	PN Description. (e.g. Home, Office)
TempPN	0..1	A	Boolean	If this PN is temporary PN, this is "TRUE". If the physical connection between PNGW and all of PNEs is broken, this PN should be released automatically. If this PN is sustained PN, this TempPN attribute is empty or "FALSE".
Sharing	1	A	Integer	The level of PN Inventory sharing in PNE side 1 – Shared, PN GW Info and PNE Info are shared in PNE 2 – Protected, PN GW Info only in PNE
PNGWInfo	1	E		PN GW Information Its sub attributes are • PNGWID • PNGWName • Zonebasedservicesupport • Mode • Broadcastgroupkeydeliverysupport
PNGWID	1	A	String	PN GW Identification.
PNGWName	0..1	A	String	PN GW Name (e.g. mobile phone, assigned nickname)
Zonebasedservicesupport	0..1	A	Boolean	If this CPNS entity is a capable PN GW of Zone Based Service, this value should be "TRUE".
Mode	1	A	Integer	The mode of device 2 – PNGW, If the mode of device is PN GW, the value should be "PN GW". 3 – BOTH, If the mode of device is both of PNE and PN GW, the value should be "BOTH" (e.g. mobile phone)
Broadcastgroupkeydeliverysupport	0..1	A	Boolean	TRUE: PN GW supports broadcast Group Key delivery FALSE: PN GW does not support broadcast Group Key delivery.
PNEInfo	1..n	E		PNE Information. If there is modification of PNE, this should be inserted. (e.g. new PNE joined or invited, PNE left) Its sub attributes are • PNEID • PNEName • Active

				• Mode
PNEID	1	A	String	PNE Identification.
PNEName	0..1	A	String	PNE Name (e.g. mp3 player, assigned nickname)
Active	0..1	A	Boolean	The active status of PNE. TRUE – This PNE is active FALSE – This PNE is not active because PNE is temporary disconnected.
Mode	0..1	A	Integer	The mode of device 1 – PNE, If the mode of device is PNE, the value should be "PNE". 3 – BOTH, If the mode of device is both of PNE and PN GW, the value should be "BOTH" (e.g. mobile phone)
AuthIniData	0..1	E		Set of information used to initiate PNE authentication procedure. The included information is generated by target PNE(s) to be authenticated. Its sub attributes are: • AuthPNEID • rand_PNE • LocalEUKeyAssignment This element is included in the message if the command attribute is Invite and the message direction is from invited PNE to PN GW.
AuthPNEID	1	A	String	Entity ID of target PNE to be authenticated by CPNS Server
rand_PNE	1	A	String	Random value generated by PNE (i.e., rand_PNE in section 7.6.)
LocalEUKeyAssignment	1	A	Boolean	Flag to indicate the necessity of LocalEUKey assignment. TRUE: necessary, FALSE: unnecessary
AuthFinData	0..1	E		Set of information used to authenticate CPNS Server by PNE. Its sub attribute is: • HASH This element is included in the message if the command attribute is Join and the message direction is from PN GW to PNE.
HASH	1	A	String	Hash value calculated by target PNE or PN GW (i.e., hash_server in 7.6.)

Table 28 Information elements in PNActionResponse message

8.7.3.3 PNActionNotification message

Element	Cardinality	T	Data Type	Description
PNActionNotification	1	E		Its sub attributes are • Command • PNEID • PNID
Command	1	A	Integer	The command for target PNE.

				If a PNE or PN GW wants to expel other PNE, command from PN GW is "Expel". 1 – Expel, PN GW sends expel notification to PNE.
PNEID	1	A	String	PNE Identification for target PNE. (e.g. expelled PNE, reconnected PNE)
PNID	1	A	String	PN Identification.

Table 29 Information elements in PNActionNotification message

8.7.4 PN Release

Message	Implementation	Direction
PNReleaseRequest	Mandatory	PNE → PN GW PN GW → CPNS Server
PNReleaseResponse	Mandatory	PN GW → PNE CPNS Server → PN GW
PNReleaseNotification	Mandatory	PN GW → PNE CPNS Server → PN GW

8.7.4.1 PN Release Request message

Element	Cardinality	T	Data Type	Description
PNReleaseRequest	1	E		Its sub attributes are • PNID • PNEID • Reason
PNID	1	A	String	PN Identification.
PNEID	0..1	A	String	PNE Identification. The release requesting PNE's PNEID. If PN GW makes the PN release, this attribute is not here.
Reason	0..1	A	String	The reason to release. (e.g. there is no action for a long time)

Table 30 Information elements in PNReleaseRequest message

8.7.4.2 PN Release Response message

Element	Cardinality	T	Data Type	Description
PNReleaseResponse	1	E		Its sub attributes are • Result
Result	1	A	Integer	The status of success or fail. 1 – Success 2 – Fail, this PN is not registered before. 3 – Fail, this PNEs are disconnected.

Table 31 Information elements in PNReleaseResponse message

8.7.4.3 PN Release Notification message

Element	Cardinality	T	Data Type	Description
PNReleaseNotification	1	E		Its sub attributes are • PNID
PNID	1	A	String	PN Identification

Table 32 Information elements in PNReleaseNotification message

8.8 Service Group Management

8.8.1 SG Create

Message	Implementation	Direction
SGCreateRequest	Mandatory	PNE → PN GW PN GW → CPNS Server
SGCreateResponse	Mandatory	CPNS Server → PN GW PN GW → PNE

8.8.1.1 SG Create Request message

Element	Cardinality	T	Data Type	Description
SGCreateRequest	1	E		Its sub attribute is • OriginEntityID Its sub elements are • SGInfo • PNEInfo
OriginEntityID	1	A	String	Entity ID for requesting SG creation
SGInfo	1	E		Service Group Information. Its sub attributes are • SGDescription • Sharing • MaxPNE • MaxUser • ServiceID
SGDescription	0..1	A	String	Service Group description. This is human readable description and helpful to understand or search Service Group.
Sharing	1	A	Integer	The level of SG Inventory sharing

				1- Open, every PNE can have access to SG Inventory 2- Selective, open to SG member PNEs only 3- Closed, no PNE will have access to SG Inventory
MaxPNE	0..1	A	Integer	The maximum number of member PNEs in Service Group.
MaxUser	0..1	A	Integer	The maximum number of CPNS User in Service Group.
ServiceID	0..n	A	String	Service Identification. If the SG creation requester knows ServiceID through service discovery procedure and wants to get that service, this should be inserted as part of the service group creation request.
PNEInfo	0..n	E		PNE Information. This contains the information of invited PNE(s) if the SG creation requester wants to insert. Its sub attribute is • PNEID
PNEID	1	A	String	PNE Identification.

Table 33 Information elements in SGCreateRequest message

8.8.1.2 SG Create Response message

Element	Cardinality	T	Data Type	Description
SGCreateResponse	1	E		Its sub elements are • SGInfo • PNEInfo
SGInfo	1	E		Service Group Information. Its sub attributes are • SGDescription • Sharing • MaxPNE • MaxUser • ServiceID • SGID
SGDescription	0..1	A	String	Service Group description. This is human readable description and helpful to understand or search Service Group.
Sharing	1	A	Integer	The level of SG Inventory sharing 1. Open, every PNE can have access to SG Inventory 2. Selective, open to SG member PNEs only 3. Closed, no PNE will have access to SG Inventory
MaxPNE	0..1	A	Integer	The maximum number of member PNEs in Service Group.
MaxUser	0..1	A	Integer	The maximum number of CPNS User in Service Group.
ServiceID	0..n	A	String	Service Identification. If the SG creation requester knows ServiceID through service discovery procedure and wants to get

				that service, this should be inserted as part of the service group creation request.
SGID	1	A	String	Service Group Identifier
PNEInfo	0..n	E		Service Group member PNE Information. This contains the information of PNE which is invited in Service Group during SG creation procedure. If there is no PNE to be invited, this is empty. Its sub attributes are • PNEID • Result • PNGWID • Name Its sub elements are • UserInfo • ServiceProfile
PNEID	1	A	String	PNE Identification.
Result	1	A	Integer	The status of success or fail. 1 – Success 2 – Fail, this PNE is disconnected.
PNGWID	1	A	String	PNGW Identification of PN having this PNE as a member.
Name	0..1	A	String	PNE Name (e.g. player, assigned nick name)
UserInfo	0..1	E	-	User Information. Its attributes are • UserID • Name
UserID	0..1	A	String	User Identification
Name	0..1	A	String	User Name
ServiceProfile	0..1	E		CPNS enabled application information to support certain service and status.Its sub-elements are • StatusVariable (See section 5.5.2) • ServiceList (See section 5.5.3)

Table 34 Information elements in SGCreateResponse message

8.8.2 SG Invite

Message	Implementation	Direction
SGInviteRequest	Mandatory	PNE → PN GW PN GW → CPNS Server CPNS Server → PN GW PN GW → PNE

SGInviteResponse	Mandatory	PNE → PN GW PN GW → CPNS Server CPNS Server → PN GW PN GW → PNE

8.8.2.1 SG Invite Request message

Element	Cardinality	T	Data Type	Description
SGInviteRequest	1	E		Its sub attribute is • OriginEntityID Its sub elements are • SGInfo • PNEInfo
OriginEntityID	1	A	String	Entity ID for requesting PNE Invite.
SGInfo	1	E		Service Group Information. Its sub attributes are • SGID • SGDescription • SharingSGOwner Its sub elements are • ServiceInfo • MemberInfo
SGID	1	A	String	Service Group Identifier.
SGDescription	0..1	A	String	Service Group description. This is human readable description and helpful to understand or search Service Group.
Sharing	0..1	A	Integer	The level of SG Inventory sharing 1- Open, every PNE can have access to SG Inventory 2- Selective, open to SG member PNEs only 3- Closed, no PNE will have access to SG Inventory
SGOwner	0..1	A	String	Entity Identification of SGOwner.
ServiceInfo	0..n	E		Service Information for this Service Group. Its sub attributes are • ServiceID • Keyword
ServiceID	1	A	String	Service Identification. If the SG creation requester knows ServiceID though service discovery procedure and wants to get that

				service, this should be inserted.
Keyword	0..1	A	String	Service Keyword or tag. This is human readable text. If there is one or more keyword or tag for the Service, they are separated by comma.
MemberInfo	0..n	E	String	The Service Group member PNE information. Its sub attributes are • PNEID • Name
PNEID	1	A	String	PNE Identification.
Name	0..1	A	String	PNE Name (e.g. player, assigned nick name)
PNEInfo	1..n	E		PNE Information to be invited. Its sub attributes are • PNEID • PNGWID
PNEID	1	A	String	PNE Identification.
PNGWID	1	A	String	Identification of PN GW.

Table 35 Information elements in SGInviteRequest message

8.8.2.2 SG Invite Response message

Element	Cardinality	T	Data Type	Description
SGInviteResponse	1	E		Its sub element is • PNEInfo
PNEInfo	0..n	E		PNE Information Its sub attributes are • PNEID • Result • PNGWID • Name Its sub elements are • UserInfo • DeviceCapa • ServiceProfile
PNEID	1	A	String	PNE Identification.
Result	1	A	Integer	The status of success or fail. 1 – Success 2 – Fail, the PNE to ask invitation is not enough to invite, e.g this is

				not SG Owner. 3 – Fail, the capabilities of PNE is not enough to join this SG. 4 – Fail, this PNE is disconnected. 5 – Fail, this PNE doesn't want to join this Service Group.
PNGWID	0..1	A	String	PN GW Identification of PN having this PNE as a member.
Name	0..1	A	String	PNE Name (e.g. player, assigned nick name)
UserInfo	0..1	E	-	User Information. Its attributes are • UserID • Name
UserID	0..1	A	String	UserIDentification
Name	0..1	A	String	User Name
DeviceCapa	0..1	E		Capability information of device embedding PNE Its sub attribute is • UICapa Its sub element is • ExternalCapa
UICapa	0..1	A	Boolean	If this device doesn't support UI functionalities below, this value SHALL be set with "TRUE". TRUE: PN GW needs to support confirmation and/or Key assignment functionalities instead of PNE.
ExternalCapa	0..1	E	-	XML fragment contains information such as DeviceType, VideoCodec, etc. CPNS V1.0 can make use of the format of device capabilities from DPE Enabler specification.
ServiceProfile	0..1	E		CPNS enabled application information to support certain service and status.Its sub-elements are • StatusVariable (See section 5.5.2) • ServiceList (See section 5.5.3)

Table 36 Information elements in SGInviteResponse message

8.8.3 Service Group Action for PNE Expulsion, Joining, Leaving

Message	Implementation	Direction
SGActionRequest	Mandatory	PNE → PN GW PN GW → CPNS Server CPNS Server → PN GW PN GW → PNE
SGActionResponse	Mandatory	PNE → PN GW PN GW → CPNS Server CPNS Server → PN GW PN GW → PNE

SGActionNotification	Mandatory	CPNS Server → PN GW PN GW → PNE

8.8.3.1 Service Group Action Request message

Element	Cardinality	T	Data Type	Description
SGActionRequest	1	E		Its sub attribute is • OriginEntityID Its sub elements are • SGInfo • PNEInfo
OriginEntityID	0..1	A	String	Identity of CPNS Entity requesting a service Group action'
SGInfo	1	E		Service Group Information. Its sub attributes are • SGID • SGDescription Its sub element is • ServiceInfo
SGID	1	A	String	Service Group Identifier.
SGDescription	0..1	A	String	Service Group description. This is human readable description and helpful to understand or search Service Group.
ServiceInfo	0..n	E		Service Information for this Service Group. Its sub attributes are • ServiceID • ServiceStatus
ServiceID	1	A	String	Service Identification.
ServiceStatus	1	A	Integer	The status of the Service. 0 – Current, this Service is available for this Service Group 1 – New, this Service is added. 2 – Deleted, this Service is deleted.
PNEInfo	1..n	E	-	PNE Information Its sub attributes are • PNEID • PNGWID • Action

PNEID	1	A	String	PNE Identification.
PNGWID	0..1	A	String	PN GW Identification in case of joining.
Action	1	A	Integer	The action of the PNE. If a PNE requests to expel the other PNE, its action is “Expel” and CPNS Server can check that this PNE is SG Owner or not. If a PNE gets the expel request, its action is “Expelled” If a PNE request to leave a service group, its action is “Leave” 1 – Expel, this PNE get the expel request. 2 – Join, this PNE wants to join 3 – Leave, this PNE wants to leave the SG

Table 37 Information elements in SGActionRequest message

8.8.3.2 Service Group Action Response message

Element	Cardinality	T	Data Type	Description
SGActionResponse	1	E		Its sub attributes are • SGStatus Its sub elements are • PNEInfo • SGInfo
SGStatus	0..1	A	Boolean	The status of update SG. “TRUE” is success “FALSE” is failure.
PNEInfo	1..n	E		PNE Information Its sub attributes are • PNEID • PNGWID • Action • Result
PNEID	1	A	String	PNE Identification.
PNGWID	0..1	A	String	PN GW Identification.
Action	1	A	Integer	The action of the PNE in Action Request. 1 – Expel, this PNE get the expel request. 2 – Join, this PNE wants to join 3 – Leave, this PNE wants to leave the SG
Result	1	A	Integer	The status of success or fail. 1 – Success 2 – Fail, the PNE is not authorized to request this action, e.g this is not SG Owner. 3 – Fail, this PNE is not the member of this Service Group.

				4 – Fail, this PNE is disconnected. 5 – Fail, this SG is full.
SGInfo	0..1	E		Service Group Information. This is for Action is "2" (Join) in SGActionRequest message. Its sub attributes are • SGID • SGDescription • SGOwner Its sub elements are • ServiceInfo • MemberInfo
SGID	1	A	String	Service Group Identifier.
SGDescription	0..1	A	String	Service Group description. This is human readable description and helpful to understand or search Service Group.
SGOwner	0..1	A	String	Entity Identification of SGOwner
ServiceInfo	0..n	E		Service Information for this Service Group. Its sub attribute is • ServiceID
ServiceID	1	A	String	Service Identification.
MemberInfo	0..n	E	String	The Service Group member information. Its sub attributes are • PNEID • PNGWID • Name Its sub elements are • UserInfo • ServiceProfile
PNEID	1	A	String	PNE Identification.
PNGWID	1	A	String	PN GW Identification.
Name	0..1	A	String	PNE Name (e.g. My player, assigned nickname)
UserInfo	0..1	E	-	User Information. Its attributes are • UserID • Name
UserID	0..1	A	String	User Identification
Name	0..1	A	String	User Name

ServiceProfile	0..1	E		CPNS enabled application information to support certain service and status.Its sub-elements are • StatusVariable (See section 5.5.2) • ServiceList (See section 5.5.3)

Table 38 Information elements in SGActionResponse message

8.8.3.3 Service Group Action Notification message

Element	Cardinality	T	Data Type	Description
SGActionNotification	1	E		Its sub attribute is • SGID Its sub elements are • PNEInfo • SGInfo
SGID	1	A	String	Service Group Identifier.
PNEInfo	1..n	E		PNE Information Its sub attributes are • PNEID • Action
PNEID	1	A	String	PNE Identification.
Action	1	A	String	The action of the PNE. If a PNE gets the expel request, its action is “Expelled” 1 – Expel, this PNE get the expel request.

Table 39 Information elements in SGActionNotification message

8.8.4 SG Change Notification

Message	Implementation	Direction
SGChangeNotification	Mandatory	CPNS Server → PN GW PN GW → PNE

8.8.4.1 SG Change Notification

Element	Cardinality	T	Data Type	Description
SGChangeNotification	1	E		Its sub element is • SGInfo

SGInfo	1	E		Service Group Information. Its sub attributes are • SGID • SGDescription • Its sub elements areServiceInfo • MemberInfo • SGOwner
SGID	1	A	String	Service Group Identifier.
SGDescription	0..1	A	String	Service Group description. This is human readable description and helpful to understand or search Service Group.
ServiceInfo	0..n	E		Service Information for this Service Group. Its sub attributes are • ServiceID • ServiceStatus
ServiceID	1	A	String	Service Identification.
ServiceStatus	0..1	A	Integer	The status of the Service. 0 – Current, this Service is available for this Service Group 1 – New, this Service is added. 2 – Deleted, this Service is deleted.
MemberInfo	0..n	E	String	The Service Group member information. Its sub attributes are • PNEID • PNGWID • Name • Status Its sub elements are • UserInfo • DeviceCapa • ServiceProfile
SGOwner	0..1	A	String	Entity Identification of SGOwner
PNEID	1	A	String	PNE Identification.
PNGWID	0..1	A	String	PN GW Identification
Name	0..1	A	String	PNE Name (e.g. MP3 player, assigned nickname)
Status	1	A	Integer	The status of the PNE.

				0 – Current, this PNE is member of SG 1 – Invited, this PNE was invited. 2 – Expelled, this PNE was expelled. 3 – Joined, this PNE has joined. 4 – Left, this PNE has left.
UserInfo	0..1	E	-	User Information. Its attributes are • UserID • Name
UserID	0..1	A	String	UserIDentification
Name	0..1	A	String	User Name
DeviceCapa	0..1	E		Capability information of device embedding PNE Its sub attribute is • UICapa Its sub element is • ExternalCapa
UICapa	0..1	A	Boolean	If this device doesn't support UI functionalities below, this value SHALL be set with "TRUE". TRUE: PN GW needs to support confirmation and/or Key assignment functionalities instead of PNE.
ExternalCapa	0..1	E	-	XML fragment contains information such as DeviceType, VideoCodec, etc. CPNS V1.0 can make use of the format of device capabilities from DPE Enabler specification.
ServiceProfile	0..1	E		CPNS enabled application information to support certain service and status.Its sub-elements are • StatusVariable (See section 5.5.2) • ServiceList (See section 5.5.3)

Table 40 Information elements in SGChangeNotification message

8.8.5 Service Group Discovery

Message	Implementation	Direction
SGDiscoveryRequest	Mandatory	PNE → PN GW PN GW → CPNS Server CPNS Server → PN GW PN GW → PNE
SGDiscoveryResponse	Mandatory	CPNS Server → PN GW PN GW → PNE PNE → PN GW PN GW → CPNS Server

8.8.5.1 Service Group Discovery Request message

Element	Cardinality	T	Data Type	Description
SGDiscoveryRequest	1	E		Its sub elements are • SGInfo • OriginEntityID
OriginEntityID	1	A	String	Identity of CPNS Entity requesting a service group action
SGInfo	1	E		Service Group Information. Its sub attributes are • ServiceID • Keyword • MemberReq
ServiceID	0..1	A	String	Service Identification. If there is one or more ServiceIDs, they are separated by comma.
Keyword	0..1	A	String	Service Keyword, Service Group Keyword or member identifier. This is human readable text. If there is one or more keyword for the Service Description related with Service Group, Service Group Description attribute or member identifier, they are separated by comma.
MemberReq	0..1	A	Boolean	This value is "TRUE" in case the PNE wants to show the SG member information. If this is TRUE, the SGDiscoveryResponse message will contain MemberInfo element

Table 41 Information elements in SGDiscoveryRequest message

8.8.5.2 Service Group Discovery Response message

Element	Cardinality	T	Data Type	Description
SGDiscoveryResponse	1	E		Its sub element is • SGInfo
SGInfo	0..n	E		Service Group Information. Its sub attributes are • SGID • SGDescription • SGOwner Its sub elements are

				• ServiceInfo • MemberInfo
SGID	1	A	String	Service Group Identifier.
SGDescription	1	A	String	Service Group description. This is human readable description and helpful to understand Service Group.
SGOwner	0..1	A	String	Entity Identification of SGOwner
ServiceInfo	0..n	E		Service Information for this Service Group. Its sub attributes are • ServiceID • Keyword
ServiceID	1	A	String	Service Identification.
ServiceName	0..1	A	String	Service Keyword or tag. This is human readable text which was registered in CPNS Server.
MemberInfo	0..n	E	String	The Service Group member information. Its sub attributes are • PNEID • Name
PNEID	1	A	String	PNE Identification.
Name	0..1	A	String	PNE Name (e.g. mp3 player)

Table 42 Information elements in SGDiscoveryResponse message

8.8.6 Service Group Release

Message	Implementation	Direction
SGReleaseRequest	Mandatory	PNE → PN GW PN GW → CPNS Server
SGReleaseResponse	Mandatory	CPNS Server → PN GW PN GW → PNE
SGReleaseNotification	Mandatory	CPNS Server → PN GW PN GW → PNE

8.8.6.1 Service Group Release Request message

Element	Cardinality	T	Data Type	Description
SGReleaseRequest	1	E		Its sub attributes are • SGID • OriginEntityID

SGID	1	A	String	Service Group Identification.
OriginEntityID	1	A	String	PNE or PN GW Identification of the requesting PNE

Table 43 Information elements in SGReleaseRequest message

8.8.6.2 Service Group Release Response message

Element	Cardinality	T	Data Type	Description
SGReleaseResponse	1	E		Its sub attribute is • Result
Result	1	A	Integer	The status of success or fail. 1 – Success 2 – Fail, the requesting PNE is not authorized to request Service Group release (e.g this is not SG Owner). 3 – Fail, this Service Group was not registered before.

Table 44 Information elements in SGReleaseResponse message

8.8.6.3 Service Group Release Notification message

Element	Cardinality	T	Data Type	Description
SGReleaseNotification	1	E		Its sub attribute is • SGID
SGID	1	A	String	Service Group Identification.

Table 45 Information elements in SGReleaseNotification message

8.8.7 SG Owner Transfer

Message	Implementation	Direction
SGOwnerTransferRequest	Mandatory	PNE → PN GW PN GW → CPNS Server CPNS Server → PN GW PN GW → PNE
SGOwnerTransferResponse	Mandatory	PNE → PN GW PN GW → CPNS Server CPNS Server → PN GW PN GW → PNE

8.8.7.1 SG Owner Transfer Request Message

Element	Cardinality	T	Data Type	Description
SGOwnerTransferRequset	1	E		Its sub attributes are • SGID • CandidatePNEID • TransferReason
SGID	1	A	String	Service Group ID of the original SG owner
CandidatePNEID	0..1	A	String	PNEID of the candidate of SG Owner recommended by the original SG owner.

TransferReason	0..1	A	String	The reason to initiate the owner transfer; such as, low power, leave SG, low capabilities.

Table 46 Information elements in SG Owner Transfer Request Message

8.8.7.2 SG Owner Transfer Response Message

Element	Cardinality	T	Data Type	Description
SGOwner TransferResponse	1	E		Its sub attributes are • Accept • PNEID • SGID
Accept	1	A	Boolean	If the SG owner transfer procedure is successful and the SG owner candidate PNE accepts the SG owner transfer, this value shall be "TRUE"; otherwise " FALSE".
PNEID	0..1	A	String	PNE Identification of the new SG owner
SGID	0..1	A	String	Service Group ID of the new SG owner

Table 47 Information elements in SG Owner Transfer Response Message

8.8.8 SG Owner Change Notification

Message	Implementation	Direction
SGOwnerChangeNotification	Mandatory	CPNS Server → PN GW PN GW → PNE

Table 48 SG Owner Change Notification

Element	Cardinality	T	Data Type	Description
SGOwner Change Notification	1	E		Its sub attributes are • SGOwner • SGID
SGOwner	1	A	String	Entity Identification of SG Owner.
SGID	1	A	String	Service Group Identifier.

Table 49 SG Owner Change Notification Message

8.9 Group Key Management

8.9.1 GKDK request

Message	Implementation	Direction
GKDKRequest	Conditional	PNE → PN GW
GKDKResponse	Conditional	PN GW → PNE

The above message should be implemented when PNE/PNGW supports underlying broadcast mechanism

8.9.1.1 GKDKRequest message

Element	Cardinality	T	Data Type	Description
GKDKRequest	1	E		Its sub element is: • PNEID
PNEID	1	E	String	EntityID of PNE which requests GKDK request

Table 50 Information elements in GKDKRequest Message

8.9.1.2 GKDKResponse message

Element	Cardinality	T	Data Type	Description
GKDKResponse	1	E		Its sub elements are: • Result • GKDK
Result	1	E	Boolean	Result of GKDKRequest True: Success False: Fail
GKDK	1	E	Binary	Assigned GKDK

Table 51 Information elements in GKDKResponse Message

8.9.2 Group Key delivery

Message	Implementation	Direction
GroupKeyDeliveryRequest	Mandatory	CPNS Server → PN GW PN GW → PNE
GroupKeyDeliveryResponse	Mandatory	PN GW → CPNS Server PNE → PN GW

8.9.2.1 GroupKeyDeliveryRequest message

Element	Cardinality	T	Data Type	Description
GroupKeyDeliveryRequest	1	E		Its sub elements are: • SGID • EncryptedGroupKey
SGID	1	E	String	SG ID of Service Group in which Group Key is delivered
EncryptedGroupKey	1.. n	E	Binary	Delivered encrypted Group Key

				Note: If Group Key is sent from CPNS Server to PN GW, cardinality is 1. If Group Key is sent from PN GW to PNE and unicast Group Key delivery is applied, cardinality is 1. If Group Key is sent from PN GW to PNE and broadcast Group Key delivery is applied, cardinality is 1..n.

Table 52 Information elements in GroupKeyDeliveryRequest Message

8.9.2.2 GroupKeyDeliveryResponse message

Element	Cardinality	T	Data Type	Description
GroupKeyDeliveryResponse	1	E		Its sub element is: • Result
Result	1	E	Boolean	Result of GroupKeyDeliveryRequest True: Success False: Fail

Table 53 Information elements in GroupKeyDeliveryResponse Message

8.8 Service / Content Publication & Discovery

8.8.1 Overview

Service Publication and Discovery consists of following CPNS messages.

- ServiceDiscoveryRequest
- ServiceDiscoveryResponse
- ServiceDescriptionAdvertise
- ServiceDescriptionRegistrationRequest
- ServiceDescriptionRegistrationResponse
- ServiceDiscoveryConfirmationRequest
- ServiceDiscoveryConfirmationResponse

8.8.2 ServiceDiscoveryRequest and ServiceDiscoveryResponse

This section describes the direction of ServiceDiscoveryRequest and ServiceDiscoveryResponse.

Message	Requirement	Direction
ServiceDiscoveryRequest	Mandatory	PNE→ PN GW PN GW→ CPNS Server
ServiceDiscoveryResponse	Mandatory	CPNS Server → PN GW PN GW → PNE

8.8.2.1 ServiceDiscoveryRequest message

This message is used by PNE to request CPNS Server to find Service Description.

Element	Cardinality	T	Data type	Description
ServcieDiscovery Request	1	E	-	Its sub-elements are • DiscoveryDestination
DiscoveryDestination	1	E	-	Attribute and sub-element variation of searching condition. In combination or single searching condition, Service Discovery provides mechanism to find service or Remote PNE related information. Its sub attributes • TargetID • PNID • ContentInfoRequest Its sub-elements are • Keyword
TargetID	0..1	A	String	Identifier of content provider (PNEID or CPID) as searching condition
PNID	0..1	A	String	Identifier of PN as searching condition
ContentInfoRequest	0..1	A	Boolean	The attribute SHOULD be included to indicate if content related information is requested or not. Note: The definition of content related information depends on content/service provider and out of scope of CPNS Enabler. TRUE: Content related information is requested FALSE: PNE does not want to receive any content related information
UserInfo	0..1	E	-	User Information as searching condition Its attributes are • UserID • UserName
UserID	0..1	A	String	User Identifier
UserName	0..1	A	String	User Name
Keyword	0..1	E	String	Arbitrary text as searching condition

Table 54 Information element in ServiceDiscoveryRequest

8.8.2.2 ServiceDiscoveryResponse message

This message is used by CPNS Server to deliver the result of ServiceDiscoveryRequest message to the PNE.

Element	Cardinality	T	Data type	Description
ServiceDiscovery Response	1	E	-	Its sub-elements are

				• Result • Reason • TargetInfo • PNInfo
Result	1	E	Boolean	Result of ServiceDiscoveryRequest TRUE-success FALSE-failure
Reason	0..1	E	String	Cause of failure e.g., when the Disclosure attribute is "1" then the Reason element contains the cause of rejection such as "Access Denied" or if there is no matched service description found then the Reason element contains the cause of failure such as "No match found" (See Section 7.9 for the detail)
TargetInfo	0..n	E	-	The element containing relevant information of content provider which host the matched/returned service description Its attribute is • TargetID • TargetName • Active Its sub elements are • UserInfo • PNID • ServiceProfile
TargetID	1	A	String	Identifier of content provider (PNEID or CPID) (see the CPNS Profile in section 5.10.2) If the Target is PNE, TargetID is PNEID. If the target is external content provider, TargetID is CPID.
TargetName	0..1	A	String	Name of content provider (PNEName or CPName) (See the CPNS Profile in section 5.10.2) If the Target is PNE, TargetName is PNEName. If the Target is external content provider, TargetName is CPName.
Active	0..1	A	Boolean	In case the Target Entity is PNE, this attribute is included to indicate the active status of PNE. TRUE – This PNE is active because PNE is physically connected. FALSE – This PNE is not active because PNE is physically disconnected.
UserInfo	0..1	E	-	User information

				Based on Disclosure attribute UserInfo can be unveiled. Access control based on Disclosure attribute can be found in section 5.8(PN Inventory) and 7.9(Service Discovery). Its attributes are • UserID • UserName
UserID	1	A	String	CPNS User ID
UseName	0..1	A	String	CPNS User Name
PNID	1..n	E	String	List of PN ID(s) the searched PNE resides in Based on Disclosure attribute PNID can be unveiled. Access control based on Disclosure attribute can be found in section 5.8(PN Inventory) and 7.9(Service Discovery).
ServiceProfile	1	E	-	The Service Description i.e., ServiceProfile (See the CPNS Profile in section 5) Based on Disclosure attribute ServiceProfile can be unveiled. Access control based on Disclosure attribute can be found in section 5.8(PN Inventory) and 7.9(Service Discovery).
PNInfo	0..n	E		Information about the PN which searched PNE resides in The information is the Remote PNE related information and is used for Service Group Management (See section 7.9) Based on Disclosure attribute PNInfo can be unveiled Access control based on Disclosure attribute can be found in section 5.8(PN Inventory) and 7.9(Service Discovery). Its sub attributes are • PNID • Description Its sub element is • PNGWInfo • PNEInfo
PNID	1	A	String	Identifier of PN
Description	0..1	A	String	PN Description. (e.g. home, office)
PNGWInfo	1	E		PNGW Information of PN GW in the PN Its sub attributes are

				• PNGWID • PNGWName
PNGWID	1	A	String	Identifier of PN GW
PNGWName	0..1	A	String	Name of PN GW, assigned nickname (e.g. my mobile phone)
PNEInfo	0..n	E		PNE Information of PNE which are the member of the PN Its sub attributes are • PNEID • PNEName
PNEID	1	A	String	Identifier of PNE.
PNEName	0..1	A	String	Name of PNE, assigned nickname (e.g. mp3 player)

Table 55 Information element in ServiceDiscoveryResponse

8.8.3 ServiceDescriptionAdvertise

This section describes the direction of ServiceDescriptionAdvertise.

Message	Requirement	Direction
ServiceDescriptionAdvertise	Mandatory	CP → CPNS Server CPNS Server →PN GW PN GW→PNE

8.8.3.1 ServiceDescriptionAdvertise message

This message is used by CPNS Server and PN GW for Zone Based Service to advertise Service Description to the PNE.

Element	Cardinality	T	Data type	Description
ServiceDescriptionAdvertise	1	E	-	Its attribute is • ZoneBasedServiceSupport Its sub-elements are • DeviceInfo • CPInfo • ServiceProfile
ZoneBasedServiceSupport	0..1	A	Boolean	Boolean value indicates that the message is for Zone based or not. TRUE: For zone based service and Service Description will be stored in PN GW FALSE: Not for zone based service, default.
DeviceInfo	0..1	E		Device information of PNE, which is the content provider Its attributes are • PNEID • PNEName

				• PNID
PNEID	1	A	String	Identifier of PNE
PNEName	0..1	A	String	Assigned nickname for PNE.
PNID	1	A	String	Identifier of PN which has this member PNE.
CPInfo	0..1	E		External Content Provider information Its sub attributes are • CPID • CPName
CPID	1	A	String	Identifier of external content provider.
CPName	0..1	A	String	Name of external content provider.
ServiceProfile	1	E	-	The target CPNS metadata (See section 5.10)

Table 56 Message Directions for ServiceDescriptionAdvertise

8.8.4 Service Description Registration

This section describes the direction of the message for Service Description publication

Message	Requirement	Direction
ServiceDescriptionRegistrationRequest	Mandatory	PNE→ PN GW PN GW→ CPNS Server CP → CPNS Server
ServiceDescriptionRegistrationResponse	Mandatory	CPNS Server→ PN GW PN GW→ PNE CPNS Server → CP

8.8.4.1 ServiceDescriptionRegistrationRequest message

This message is used by PNE interfaced application to publish the Service Description.

Element	Cardinality	T	Data type	Description
ServcieDescriptinRegistrationRequest	1	E	-	Its attributes are • PNID • PNEID • CPID • CPName • Disclosure • OwnershipEntity Its sub-element is • ServiceProfile
PNID	0..1	A	String	Identifier of PN
PNEID	0..1	A	String	Identifier of PNE, content provider
CPID	0..1	A	String	Identifier of external content provider.
CPName	0..1	A	String	Name of external content provider.
Disclosure	1	A	Integer	The willingness of openness of PN Information, in case

				Service Discovery is requested after PN Setup 1 - Blocked; PN information should not be unveiled. 2 - Open; PN information will be unveiled, when other CPNS Entities asks service discovery. 3 - Selective: PN can be unveiled, only when the authorized CPNS entity allows in case service discovery request contains PNID or UserID
OwnershipEntity	0..1	A	String	The ID of authorized CPNS Entity which has authorization to allow PN Information open, in case Service Discovery is requested If the value of Disclosure attribute is 3 then, OwnerShipEntity SHALL be inserted.
ServiceProfile	1	E	-	The Service Description Sub-elements are the Service Description (e.g., XML fragment), based on structure of Service Description (metadata) described in section 5.10.2.

Table 57 Information element in ServiceDescriptionRegistratiojnRequest

8.8.4.2 ServiceDescriptionRegistrationResponse message

This message is used by CPNS Server to deliver the result of Service Description publication.

Element	Cardinality	T	Data type	Description
ServcieDescriptinRegistrationRequesponse	1	E	-	Its sub-elements are • Result • Reason
Result	1	E	Boolean	Result of ServiceDescriptionRegistrationRequest message TRUE - success FALSE - failure
Reason	0..1	E	String	Cause of failure

Table 58 Information element in ServiceDescriptionRegistrationResponse

8.8.5 ServiceDiscoveryConfirmationRequest message

This section describes the direction of the message for ServiceDiscoveryConfirmation.

Message	Requirement	Direction
ServiceDiscoveryConfirmationRequest	Conditional	CPNS Server→ PN GW PN GW→ PNE
ServiceDiscoveryConfirmationResponse	Conditional	PNE→ PN GW PN GW→ CPNS Server

8.8.5.1 ServiceDiscoveryConfirmationRequest message

This message is used by CPNS Server to ask confirmation regarding providing the PN information.

Element	Cardinality	T	Data type	Description
ServiceDiscoveryConfirmationReq	1	E	-	Its attribute is

uest				• ID
ID	1	E	String	UserID or PNID, PNEID which sends ServiceDiscoveryRequest message

Table 59 Information element in ServiceDiscoveryConfirmationRequest

8.8.5.1 ServiceDiscoveryConfirmationResponse message

This message is used by PNE or PN GW to respond with confirmation regarding providing the PN information.

Element	Cardinality	T	Data type	Description
ServiceDiscoveryConfirmationResponse	1	E	-	Its attribute is • Result
Result	1	E	Boolean	Result of ServiceDescriptionConfirmationRequest message TRUE – Allowing access to PN Information. FALSE – Denying access to PN Information.

Table 60 Information element in ServiceDiscoveryConfirmationResponse

8.9 Service / Content Delivery

8.9.1 Overview

Service / Content delivery consists of following CPNS messages.

- InvokeRequest
- InvokeResponse

8.9.2 InvokeRequest and InvokeResponse

This section describes the direction of InvokeRequest and InvokeResponse.

Message	Requirement	Direction
InvokeRequest	Mandatory	PNE→PN GW PN GW→CPNS Server CPNS Server→External Entity
InvokeResponse	Mandatory	PN GW→ PNE CPNS Server→ PN GW External Entity→CPNS Server

8.9.2.1 InvokeRequest message

This message is used by PNE to deliver the operation command to the entity hosting application.

Element	Cardinality	T	Data Type	Description
InvokeRequest	1	E	-	Its attributes are • SGID Its sub-elements are

				• ServiceID • InputParameterList
SGID	0..1	A	String	Unique identifier to identify the group of services part of which is the specific service. This attribute is used only if the specific service is part of a service group.
ServiceID	1	E	String	Identifier of the service (e.g., operation set) Its attributes are • Operation
Operation	1	A	String	Operation name The Operation is the method to invoke specific application function e.g., ChannelStop (the PNE to request from CPNS Server to stop one or multiple delivery service), ChannelResume (the PNE to request from CPNS Server to resume one or multiple delivery service)
InputParameterList	1	E	-	The arguments for the service invocation Its sub-elements are • Parameter
Parameter	0..n	E	String	Its sub-elements is • Value Its attributes are • Name
Name	1	A	String	Name of service invocation parameter
Value	1	E	String	Value of parameter

Table 61 Information element in InvokeRequest

8.9.2.2 InvokeResponse message

This message is used by CPNS Server to deliver the result of InvokeRequest message to the PNE.

Element	Cardinality	T	Data type	Description
InvokeResponse	1	E	-	Its sub-elements are • Result • Reason • OutputParameterList
Result	1	E	Boolean	Result of InvokeRequest TRUE-success FALSE-failure
Reason	0..1	E	String	Depends on Invoke result (i.e., in case of Result is FALSE)
OutputParameter List	0..1	E	-	The return value depends on Invoke result (i.e., in case of Result is TRUE)

				The list of information element to be returned against InvokeRequest e.g., the list of XML fragment (output XML parameter) Its sub-elements are • Parameter
Parameter	0..n	E	String	Its sub-elements is • Value Its attributes are • Name
Name	1	A	String	The name of information element to be returned e.g., name of output XML parameter found in Service Description (metadata)
Value	1	E	String	Value of parameter

Table 62 Information element in InvokeResponse

8.10 Device Capability

8.10.1 Device Capabilities Query Message

Message	Implementation	Direction
DeviceCapabilitiesQueryRequest	Mandatory	CPNS Server → PN GW, PN GW → PNE
DeviceCapabilitiesQueryResponse	Mandatory	PNE → PN GW, PN GW → CPNS Server

8.10.1.1 Device Capabilities Query Request Message

Element	Cardinality	T	Data Type	Description
DeviceCapabilities QueryRequest	1	E		Its sub elements are • Target ID • PNID
Target ID	1	A	String	If this message is sent to a PNE, the value shall be the PNE Identification of the target device. If this message is sent to a PN GW, the value shall be the PN GW Identification of the target device.
PNID	0..1	A	String	PN Identification of target device resides in .

Table 63 Information elements in Device Capabilities Query Request Message

8.10.1.2 Device Capabilities Query Response Message

Element	Cardinality	T	Data Type	Description
DeviceCapabilitiesQuery Response	1	E		Its sub elements are • Target ID

				• DeviceCapa
Target ID	1	A	String	If this message is sent to a PNE, the value shall be the PNE Identification of the target device. If this message is sent to a PN GW, the value shall be the PN GW Identification of the target device.
DeviceCapa	1	E		Capability information of device embedding PNE Its sub attribute is • UICapa Its sub element is • ExternalCapa
UICapa	0..1	A	Boolean	If this device doesn't support UI functionalities, this value SHALL be set with "TRUE". TRUE: PN GW needs to support confirmation and/or Key assignment functionalities instead of PNE.
ExternalCapa	0..1	E	-	XML fragment contains information such as DeviceType, VideoCodec, etc. CPNS V1.0 can make use of the format of device capabilities from DPE Enabler specification.

Table 64 Device Capabilities Query Response Message

8.10.2 Device Capabilities Change Notification Message

Message	Implementation	Direction
DeviceCapabilitiesChangeNotification	Conditional	PNE → PN GW, PN GW → CPNS Server
DeviceCapabilitiesChangeNotificationConfirm	Conditional	CPNS Server → PN GW, PN GW → PNE

8.10.2.1 Device Capabilities Change Notification Message

Element	Cardinality	T	Data Type	Description
DeviceCapabilities ChangeNotification	1	E		Its sub elements are • Device ID • DeviceCapa
Device ID	1	A	String	PNE Identification of the device if the device is a PNE; PN GW Identification of the device if the device is a PN GW.
DeviceCapa	1	E		Capability information of device embedding PNE Its sub attribute is • UICapa Its sub element is

				• ExternalCapa
UICapa	0..1	A	Boolean	If this device doesn't support UI functionalities, this value SHALL be set with "TRUE". TRUE: PN GW needs to support confirmation and/or Key assignment functionalities instead of PNE.
ExternalCapa	0..1	E	-	XML fragment contains information such as DeviceType, VideoCodec, etc. CPNS V1.0 can make use of the format of device capabilities from DPE Enabler specification.

Table 65 Information elements in Device Capabilities Change Notification Message

8.10.2.2 Device Capabilities Change Notification Confirm Message

Element	Cardinality	T	Data Type	Description
DeviceCapabilities ChangeNotification Confirm	1	E		Its sub elements are • Target ID
Target ID	1	A	String	CPNS Server return the confirm message to the original sender. If Device Capabilities Change Notification message is from a PNE, then this value shall be a PNE Identification. If Device Capabilities Change Notification message is from a PN GW, then this value shall be a PN GW Identification.

Table 66 Information elements in Device Capabilities Change Notification Confirm Message

8.11 Status Management

8.11.1 Overview

Status Management consists of following CPNS messages.

- StatusSubscribeRequest
- StatusSubscribeResponse
- StatusNotify
- StatusPublicationRequest
- StatusPublicationResponse

8.11.2 StatusSubscribeRequest and StatusSubscribeResponse

This section describes the direction of StatusSubscribeRequest and StatusSubscribeResponse.

Message	Requirement	Direction
StatusSubscribeRequest	Mandatory	PNE→ PN GW PN GW→ CPNS Server
StatusSubscribeResponse	Mandatory	CPNS Server→ PN GW PN GW → PNE

8.11.2.1 StatusSubscribeRequest message

This message is used by PNE to subscribe the CPNS entity (i.e., PNE and PN GW) status information.

Element	Cardinality	T	Data type	Description
StatusSubscribeRequest	1	E	-	Its sub-attributes are • TargetID • SubscriptionDuration
TargetID	1	A	String	PNEID, PNGWID, or PNID
SubscriptionDuration	1	A	Integer	"0" Unsubscribe command "n" duration time (sec)

Table 67 Information element in StatusSubscribeRequest

8.11.2.2 StatusSubscribeResponse message

This message is used by CPNS Server to deliver the result of Subscribe message to the PNE.

Element	Cardinality	T	Data type	Description
StatusSubscribeResponse	1	E	-	Its sub-attributes are • Result • Reason
Result	1	E	Boolean	The result of subscription request. TRUE – success. FALSE – Failure.
Reason	0..1	E	String	Depends on the subscription result (i.e., in case of Result is "FALSE"(Failure))

Table 68 Information element in StatusSubscribeResponse

8.11.3 StatusNotify

This section describes the direction of Notify.

Message	Requirement	Direction
StatusNotify	Mandatory	CPNS Server→ PN GW PN GW→ PNE

8.11.3.1 StatusNotify message

This message is used by PN GW or CPNS Server to deliver the status information to the PNE.

Element	Cardinality	T	Data type	Description
StatusNotify	1	E	-	Its sub attribute is • TargetID • Active Its sub-elements are • StatusVariable
TargetID	1	A	String	PNEID, PNGWID or PNID
Active	0..1	A	Boolean	The active status of PNE, PNGW or PN.

				True – This PNE or PNGW is active because it is physically connected. Or this PN is active because at least one more member PNEs are physically connected. False – This PNE is not active because PNE is physically disconnected. Or this PN is not active because all of member PNEs are disconnected.
StatusVariable	0..n	E	String	If TargetID is PNEID and PNE supports enabled application with Service Description, this is the status variable from ServiceProfile element of CPNS Profile (see section 5.10) Its sub-element is • Value Its sub attribute is • StatusName
StatusName	1	A	String	Name of status variable found in CPNS Profile metadata (see section 5.10)
Value	1	E	String	Value of StatusVariable

Table 69 Information element in StatusNotify

8.11.4 Status Publication

This section describes the direction of the message for status publication

Message	Requirement	Direction
StatusPublicationRequest	Mandatory	PNE→ PN GW PN GW→ CPNS Server
StatusPublicationResponse	Mandatory	CPNS Server→ PN GW PN GW→ PNE

8.11.5 StatusPublicationRequest message

This message is used by PNE or PN GW to publish status to CPNS Server.

Element	Cardinality	T	Data type	Description
StatusPublication Request	1	E	-	Its sub attributes are • TargetID • Active Its sub-elements are • StatusVariable
TargetID	1	A	String	Identifier associated with the status variables PNEID, PNGWID or PNID
Active	0..1	A	Boolean	The active status of PNE, PNGW or PN. TRUE – This PNE or PNGW is active because it is physically

				connected. Or this PN is active because at least one more member PNEs are physically connected. FALSE – This PNE is not active because PNE is physically disconnected. Or this PN is not active because all of member PNEs are disconnected.
StatusVariable	0..n	E	String	If TargetID is PNEID and PNE supports enabled application with Service Description, this is the status variable from ServiceProfile element of CPNS Profile (see section 5.10) Its sub-element is • Value Its attribute is • StatusName
StatusName	1	A	String	Name of status variable found in CPNS Profile metadata (see section 5.10)
Value	1	E	String	Value of StatusVariable

Table 70 Information element in StatusPublicationRequest

8.11.6 StatusPublicationResponse message

This message is used by CPNS Server to deliver the result of Status publication.

Element	Cardinality	T	Data type	Description
StatusPublication Requesponse	1	E	-	Its sub-attributes are • Result • Reason
Result	1	A	Boolean	The result of Status publication request. TRUE – Success. FALSE – Failure.
Reason	0..1	A	String	Depends on the Result (i.e., in case of Result is "FALSE"(Failure))

Table 71 Information element in StatusPublicationResponse

8.12 Usage Statistics Report message format

8.12.1 Usage Stat Report from the App to the CPNS Server

Message	Implementation	Direction
AppServerUsageStatReport	Mandatory	App → CPNS Server (This is through interface CPNS-4)

8.12.1.1 AppServerUsageStatsReport message

This message is used by the App on the server side to report usage statistics to the CPNS Server.

The CPNS Server SHALL be able to receive the parameters as shown in the table below.

Element	Cardinality	T	Data Type	Description

AppServerUsageStatsReport	1	E		Indicates the name of the message
AppServerID	1	A	String	Indicates the unique identifier of the application on the CPNS Server side This identifier can also be used for other functions or messages to identify the application on the Server side
StatsReportMessageID	1	A	String	Unique identifier to identify the stats report when requested This parameter can be used by other functions and requests
UsageStatsData	1..n	E	String	Gives the list of structures that contain usage stats information. One structure for example can contain usage stats information about video content or music etc. UsageStatsData can contain information about one service or channel, but there can be multiple reports containing information about many services or channels that can be reported at the same time as part of the same message

Table 72 Information element in AppServerUsageStatsReport

8.12.2 Usage Stat Report from App to the PNE

Message	Implementation	Direction
AppPNEUsageStatsReport	Mandatory	App → PNE (This is through interface CPNS-5) PNE → PN GW PN GW → CPNS Server

8.12.2.1 AppPNEUsageStatsReport message

This message is used by the App on the PNE side to report usage statistics to the CPNS Server via PNE and PN GW.

The PNE SHALL be able to receive the parameters from the application as shown in the table below.

Element	Cardinality	T	Data Type	Description
AppPNEUsageStatsReport	1	E		Indicates the name of the message
AppPNEID	1	A	String	Indicates the unique identifier of the application on the PNE side This identifier can also be used for other functions or messages to identify the application on the PNE side
StatsReportMessageID	1	A	String	Unique identifier to identify the stats report when requested This parameter can be used by other functions and requests
PNEID	1	A	String	Indicates the unique identifier of the PNE. This can be physical address of the PNE This identifier can also be used for

				other functions or messages to identify the PNE
PNID	1	A	String	Indicates the unique identifier of the PN. This identifier can also be used for other functions or messages to identify the PN
UsageStatsData	1..n	E	String	Gives the list of structures that contain usage stats information. One structure for example can contain usage stats information about video content or music etc. UsageStatsData can contain information about one service or channel, but there can be multiple reports containing information about many services or channels that can be reported at the same time as part of the same message

Table 73 Information element in AppPNEUsageStatsReport

9. CPNS Transport Protocol (Informative)

The CPNS Enabler supports following protocols as optional.

- XML based overlay network protocol (See Appendix X)
- SMS based CPNS protocol (See Appendix Y)
- HTTP (See Appendix Z)

Appendix A. Change History (Informative)

A.1 Approved Version History

Reference	Date	Description
n/a	n/a	No prior version

A.2 Draft/Candidate Version 1.0 History

Document Identifier	Date	Sections	Description
Draft Versions OMA-TS-CPNS_Core-V1_0	10 Jun 2010	all	initial version
	18 Jun 2010	all	Merging SD to TS
	03 Aug 2010	1	Updated according to the minutes 2010-0217 and contribution 2010-0211R02
	19 Aug 2010	6	Updated according to the contribution 2010-0228R01
	20 Aug 2010	6.1	Updated according to the contribution 2010-0215R01
	31 Aug 2010	6.2	Updated according to the contribution 2010-0221R03
	10 Sept 2010	5, 7, 8	Updated according to the contribution 2010-0185R01, 2010-0234R01, 2010-0238R01, 2010-0239R01, 2010-0242R01
	28 Sept 2010	4	Updated according to the contribution 2010-0266R01
	25 Oct 2010	3	Updated according to the contribution 2010-0293
	25 Oct 2010	5	Updated according to the contribution 2010-0235R02, 0271, 0267R03, 0290, 0292
	25 Oct 2010	6	Updated according to the contribution 2010-0245R03, 0247R05
	25 Oct 2010	8	Updated according to the contribution 2010-0308R02
	25 Oct 2010	Appendix	Updated according to the contribution 2010-0246R02, 0279
	8 Nov 2010	5, 6, 7, 8	Updated according to the contribution 2010-0317, 170R07, 172R07, 295R01, 304R04, 300R01, 282R03, 298R03, 299R03, 184R05, 303R02
	9 Nov 2010	7	Updated according to the contribution 2010-0284R01
	26 Nov 2010	5, 6, 7, 8	Updated according to the contribution 2010-0177R03, 270R02, 322R02, 328, 334R01, 335R01, 346R01, 351R01, 366, 276R02, 367R01
	10 Dec 2010	5, 6, 7, 8	Updated according to the contribution 2010-0288R01, 0318R01, 0339R01, 0342R01, 310R06, 348R01
	15 Dec 2010	6	Updated according to the contribution 2010-0175R03, 0176R04
	27 Dec 2010	8, Appendix	Updated according to the contribution 2010-0319R03, 0378
	17 Jan 2011	4, 5, 6, 7, 8	Updated according to the contribution 2010-0398R01, 0400R01, 0390, 0391, 329R02, 330R02, 331R02, 332R03, 333R02, 336R05, 338R03, 373R05, 374R04, 376R03, 381R04, 387R01, 388R01, 392R01, 393R01, 394R02, 399R01, 402R02, 403R01, 404R01, 405R01, 406R01, 408R01, 171R09, 277R05, 278R04, 365R02, 287R05, 280R04, 2011-0002R01, 0007R02, 0010R02 Updated according to the LATE(Yokosuka) contribution 2010-0355R01, 2011-0003, 0004, 0005, 0006, 0011, 0014, 0015, 0016, 0017, 0018, 0019
	18 Jan 2011	8	Updated according to the contribution 2010-0337R03, 382, 2011-0013R01
	18 Feb 2011	3, 4, 5, 7, 8	CONR Updated according to the contribution Changes done online captured in CONRR, 2011-0036R01,0039R02,0040R01, 0046, 0047R01,0053R01, 0059R01, 0060, 0069R02,0072R01, 0073R02,0074R01, 0075R01,
	18 Feb 2011	All	Clean up
	25 Feb 2011	All	Changes done online captured in CONRR
	15 Mar 2011	All	Updated according to the contribution 2011-0080R01,0055R01, 0082, 0085R01,0089R01, 0091R01,0026R02
	16 Mar 2011	7	Updated according to the contribution 2011-0095, 0097, 0086R01

Document Identifier	Date	Sections	Description
	31 Mar 2011	7, 8	Updated according to the contribution 2011-0049R01,0062R02,0103R01,0106R01, 0113R01,0117R02,0120R01,0121
	1 April 2011	7	Updated according to the contribution 2011-0118R01 and Clean up
	7 April 2011	7	Updated according to the contribution 2011-0031R02,0112R03,0119R03
	15 April 2011	3,5,6,7, 8,Appendix	Updated according to the contribution 2010-0372R01,2011- 0045R01,0057R01,0061R02,0063R03,0065R02,0090R01,0094R01,099R03,0102R04,0116R05,0130R01,0132R01,0134R02,0135R01,0136R02,0137R01,0138R01,0139R01,0140R02,0141R01,0142R01,0143R01,0145R01,0146R01,0147R01,0148R01,0149R01,0150,0151R02,0152R02,0153R01,0154R01,0155R01,0159R01,0160,0161R02,0163R02,0164R02,0166R01,0167R01,0168,0169R01,0170R02,0171R01,0176R01,0177R01,0179R01,0180,0181R02,0183,0184R01,185R01,186 and Clean up
	20 April 2011	5,6,7,8	Updated according to the contribution 2011-0162R02, 0189R01, 190R01
Candidate Version OMA-TS-CPNS_Core-V1_0	03 May 2011	All	Status changed to Candidate Status by TP ref # OMA-TP-2011-0150-INP_CPNS_V1_0_ERP_for_Candidate_Approval

Appendix B. Static Conformance Requirements (Normative)

The notation used in this appendix is specified in [SCRRULES].

B.1 General high level external dependency (GEN)

Item	Function	Reference	Requirement
CPNS-GEN-C-001-O	Device capability notification; PNE	Section 7.12.2	
CPNS-GEN-C-002-O	Device capability notification; PN GW	Section 7.12.2	
CPNS-GEN-S-001-O	Device capability notification; CPNS Server	Section 7.12.2	

B.2 SCR for CPNS Devices

Item	Function	Reference	Requirement
CPNS-CMETA-C-001-M	Support of CPNS Profile	Section 5.10.2	
CPNS-ED-C-001-M	Entity Discovery; Requesting CPNS Entities	Section 7.2.1.1	CPNS-CMETA-C-001-M
CPNS-ED-C-002-M	Entity Discovery; Requested CPNS Entities	Section 7.2.1.2	CPNS-CMETA-C-001-M
CPNS-ED-C-003-M	Entity Discovery; Zonebasedservice;PNE	Section 7.11.2	CPNS-ED-C-001-M
CPNS-ED-C-004-M	Entity Discovery; Zonebasedservice;PNG W	Section 7.11.3	CPNS-ED-C-002-M

B.3 SCR for PNE

Item	Function	Reference	Requirement
CPNS-PMETA-C-001-M	Support of PN Inventory	Section 5.8	
CPNS-SMETA-C-001-M	Support of SG Inventory	Section 5.9	
CPNS-ED-C-003-M	PN Discovery	Section 7.2.2.1	
CPNS-EKA-C-001-O	Requesting EUKey assignment for PNEs with UI capabilities	Section 7.4.1	
CPNS-EKA-C-002-O	Requesting EUKey assignment for PNEs without UI capabilities when PAN is secure	Section 7.4.2.1	
CPNS-EKA-C-003-O	Requesting EUKey assignment for PNEs without UI capabilities when PAN is not secure	Section 7.4.2.2	
CPNS-MA-C-001-M	Performing mutual authentication with CPNS Server and	Section 7.5.1	

Item	Function	Reference	Requirement
	optionally with PN GW		
CPNS-PNM-C-001-M	PN Establishment; Procedure in originating PNE	Section 7.6.1.1	CPNS-CMETA-C-001-M
CPNS-PNM-C-002-M	PN Establishment; Procedure in invited PNE	Section 7.6.1.1	CPNS-CMETA-C-001-M
CPNS-PNM-C-003-M	PN Establishment; Zonebasedservice	Section 7.11.2	CPNS-PNM-C-002-M
CPNS-PNM-C-004-M	PNE Management; PNE Inviting; Procedure in inviting PNE	Section 7.6.2.1.1	CPNS-PMETA-C-001-M
CPNS-PNM-C-005-M	PNE Management; PNE Inviting; Procedure in invited PNE	Section 7.6.2.1.1	CPNS-PMETA-C-001-M
CPNS-PNM-C-006-M	PNE Management; PNE Joining	Section 7.6.2.2.1	CPNS-PMETA-C-001-M
CPNS-PNM-C-007-M	PNE Management; PNE Expulsion; Procedure in expelling PNE	Section 7.6.2.3.1	CPNS-PMETA-C-001-M
CPNS-PNM-C-008-M	PNE Management; PNE Expulsion; Procedure in expelled PNE	Section 7.6.2.3.1	CPNS-PMETA-C-001-M AND CPNS-SMETA-C-001-M
CPNS-PNM-C-009-M	PNE Management; PNE Leaving	Section 7.6.2.4.1	CPNS-PMETA-C-001-M
CPNS-PNM-C-010-M	PNE Management; PN Release	Section 7.6.3.1	CPNS-PMETA-C-001-M
CPNS-SGM-C-001-M	Service Group Management; Service Group Creation	Section 7.7.1.1	CPNS-SMETA-C-001-M
CPNS-SGM-C-002-M	Service Group Management; Management of SG Controlling Entities; PNE Invite in Service Group;Procedure in inviter PNE	Section 7.7.2.1.1	CPNS-SMETA-C-001-M
CPNS-SGM-C-003-M	Service Group Management; Management of SG Controlling Entities; PNE Invite in Service Group;Procedure in invited PNE	Section 7.7.2.1.1	CPNS-CMETA-C-001-M
CPNS-SGM-C-004-M	Service Group Management; Management of SG Controlling Entities; PNE Expulsion in Service Group; Procedure in PNE when PNE expels other PNE(s)	Section 7.7.2.2.1	CPNS-SMETA-C-001-M

Item	Function	Reference	Requirement
CPNS-SGM-C-005-M	Service Group Management; Management of SG Controlling Entities; PNE Expulsion in Service Group; Procedure in PNE when PNE is expelled from Service Group	Section 7.7.2.2.1	CPNS-SMETA-C-001-M
CPNS-SGM-C-006-M	Service Group Management; Management of SG Controlling Entities; PNE Joining, Leaving Service Group	Section 7.7.2.3.1	CPNS-PMETA-C-001-M AND CPNS-SMETA-C-001-M
CPNS-SGM-C-007-M	Service Group Management; Management of SG Controlling Entities; Service Group Member Update	Section 7.7.2.4.1	CPNS-SMETA-C-001-M
CPNS-SGM-C-008-M	Service Group Management; Service Group Update	Section 7.7.3.1	CPNS-SMETA-C-001-M
CPNS-SGM-C-009-M	Service Group Management; Service Group Discovery	Section 7.7.4.1	
CPNS-SGM-C-010-M	Service Group Management; Service Group Release	Section 7.7.5.1	CPNS-SMETA-C-001-M
CPNS-SGM-C-011-M	Service Group Management; Service Group Owner Transfer	Section 7.7.6.1	CPNS-SMETA-C-001-M
CPNS-GKM-C-001-M	Group Key deletion	Section 7.8.3	
CPNS-GKM-C-002-O	GKDK request to PNGW and GKDK storage	Section 7.8.4	
CPNS-GKM-C-003-M	Unicast based Group Key reception	Section 7.8.5	
CPNS-GKM-C-004-M	Group Key storage	Section 7.8.5	
CPNS-GKM-C-005-O	Broadcast based Group Key reception	Section 7.8.5	
CPNS-GKM-C-006-O	Decryption of Group Key by using GKDK	Section 7.8.5	
CPNS-SPD-C-001-M	Service Discovery	Section 7.9.2.1	
CPNS-SPD-C-002-M	Service Discovery Advertise	Section 7.9.3.3	
CPNS-SPD-C-003-M	Service Discovery Advertise;Zonebasedservice	Section 7.11.2	CPNS-SPD-C-002-M
CPNS-SPD-C-004-M	Service Discovery Registration	Section 7.9.4.1	CPNS-PNM-C-001-M

Item	Function	Reference	Requirement
CPNS-SCD-C-001-M	Service / Content Delivery	Section 7.10.1	CPNS-PMETA-C-001-M
CPNS-DC-C-001-M	Devcie capability Query	Section 7.12.1	
CPNS-SM-C-001-M	Service Status Publication	Section 7.13.2	CPNS-CMETA-C-001-M
CPNS-SM-C-002-M	Service Subscription and Notification	Section 7.13.3	
CPNS-SM-C-003-M	PN / PNE Inactive Status Management	Section 7.13.4.1	CPNS-PMETA-C-001-M
CPNS-SM-C-004-M	PN / PNE Active Status Management	Section 7.13.5.1	CPNS-PMETA-C-001-M
CPNS-US-C-001-M	Usage statistics collection/reporting	Section 7.14.1, 7.14.2	

B.4 SCR for PN GW

Item	Function	Reference	Requirement
CPNS-PMETA-C-002-M	Support of PN Inventory	Section 5.8	
CPNS-SMETA-C-002-M	Support of SG Inventory	Section 5.9	
CPNS-ED-C-004-M	PN Discovery	Section 7.2.2.2	CPNS-PMETA-C-001-M
CPNS-IPR-C-001-O	Requesting registration of UserID and Password via CPNS Interfaces	Section 7.3.1	
CPNS-EKA-C-004-O	Facilitating EUKey assignment for PNEs with UI capabilities	Section 7.4.1	
CPNS-EKA-C-005-O	Facilitating EUKey assignment for PNEs without UI capabilities when PAN is secure	Section 7.4.2.1	
CPNS-EKA-C-006-O	Facilitating EUKey assignment for PNEs without UI capabilities when PAN is not secure	Section 7.4.2.2	
CPNS-EKA-C-007-O	Requesting EUKey assignment for PN GW	Section 7.4.3	
CPNS-MA-C-002-M	Facilitating mutual authentication between PNE and CPNS Server and optional mutual authentication with PNE	Section 7.5.1	
CPNS-MA-C-003-O	Performing mutual authentication with CPNS Server	Section 7.5.2	
CPNS-PNM-C-011-M	PN Establishment; PNE Initiated	Section 7.6.1.2	CPNS-PMETA-C-002-M
CPNS-PNM-C-012-M	PN Establishment; PN GW Initiated	Section 7.6.1.2	CPNS-PMETA-C-002-M
CPNS-PNM-C-013-M	PN Establishment; Zonebasedservice	Section 7.11.3	CPNS-PNM-C-012-M

Item	Function	Reference	Requirement
CPNS-PNM-C-014-M	PNE Management; PN GW; PN GW initiated invitation request	Section 7.6.2.1.2	CPNS-PMETA-C-002-M
CPNS-PNM-C-015-M	PNE Management; PNE initiated invitation request	Section 7.6.2.1.2	
CPNS-PNM-C-016-M	PNE Management; PN GW procedure common to PNE initiated and PN GW initiated invitation cases	Section 7.6.2.1.2	CPNS-PMETA-C-002-M
CPNS-PNM-C-017-M	PNE Management; PNE Joining	Section 7.6.2.2.2	CPNS-PMETA-C-002-M
CPNS-PNM-C-018-M	PNE Management; PNE Expulsion	Section 7.6.2.3.2	CPNS-PMETA-C-001-M AND CPNS-PMETA-C-002-M
CPNS-PNM-C-019-M	PNE Management; PNE Leaving	Section 7.6.2.4.2	CPNS-PMETA-C-002-M
CPNS-PNM-C-020-M	PNE Management; PN Release	Section 7.6.3.2	CPNS-PMETA-C-002-M
CPNS-SGM-C-012-M	Service Group Management; Service Group Creation	Section 7.7.1.2	CPNS-SMETA-C-002-M
CPNS-SGM-C-013-M	Service Group Management; Management of SG Controlling Entities; PNE Invite in Service Group	Section 7.7.2.1.2	CPNS-SMETA-C-002-M
CPNS-SGM-C-014-M	Service Group Management; Management of SG Controlling Entities; PNE Expulsion in Service Group	Section 7.7.2.2.2	CPNS-SMETA-C-002-M
CPNS-SGM-C-015-M	Service Group Management; Management of SG Controlling Entities; PNE Joining, Leaving Service Group	Section 7.7.2.3.2	CPNS-SMETA-C-002-M
CPNS-SGM-C-016-M	Service Group Management; Management of SG Controlling Entities; Service Group Member Update	Section 7.7.2.4.2	CPNS-SMETA-C-002-M
CPNS-SGM-C-017-M	Service Group Management; Service Group Update	Section 7.7.3.2	CPNS-SMETA-C-002-M
CPNS-SGM-C-018-M	Service Group Management; Service Group Discovery	Section 7.7.4.2	
CPNS-SGM-C-019-M	Service Group	Section 7.7.5.2	CPNS-SMETA-C-002-M

Item	Function	Reference	Requirement
	Management; Service Group Release		
CPNS-SGM-C-020-M	Service Group Management; Service Group Owner Transfer	Section 7.7.6.2	CPNS-SMETA-C-002-M
CPNS-GKM-C-007-O	GKDK assignment to PNE and storage of PNE ID	Section 7.8.4	
CPNS-GKM-C-008-O	GKEK creation and update	Section 7.8.4	
CPNS-GKM-C-009-M	Unicast based Group Key delivery to PNE	Section 7.8.5	
CPNS-GKM-C-010-O	Encryption of Group Key by using GKEK	Section 7.8.5	
CPNS-GKM-C-011-O	Broadcast based Group Key delivery to PNE	Section 7.8.5	
CPNS-GKM-C-012-O	Hybrid based Group Key delivery to PNE	Section 7.8.5	
CPNS-SPD-C-005-M	Service Discovery	Section 7.9.2.2	
CPNS-SPD-C-006-M	Service Discovery Advertise	Section 7.9.3.2	
CPNS-SPD-C-007-M	Service Discovery Advertise;Zonebasedservice	Section 7.11.3	CPNS-SPD-C-006-M AND CPNS-PMETA-C-002-M
CPNS-SPD-C-008-M	Service Discovery Registration	Section 7.9.4.2	CPNS-PNM-C-011-M
CPNS-SCD-C-002-M	Service / Content Delivery	Section 7.10.2	
CPNS-DC-C-002-M	Devcie capability Query	Section 7.12.1	
CPNS-SM-C-005-M	Service Status Publication	Section 7.13.2	
CPNS-SM-C-006-M	Service Subscription and Notification	Section 7.13.3	
CPNS-SM-C-007-M	PN / PNE Inactive Status Management	Section 7.13.4.2	CPNS-PMETA-C-002-M
CPNS-SM-C-008-M	PN / PNE Active Status Management	Section 7.13.5.2	CPNS-PMETA-C-002-M
CPNS-US-C-002-M	Usage statistics collection/reporting	Section 7.14.1, 7.14.2	

B.5 SCR for CPNS Server

Item	Function	Reference	Requirement
CPNS-CMETA-S-001-M	Support of CPNS profile	Section 5.10.2	
CPNS-PMETA-S-001-M	Support of PN Inventory	Section 5.8	
CPNS-SMETA-S-001-M	Support of SG Inventory	Section 5.9	
CPNS-IPR-S-001-O	Registering UserID and Password via CPNS	Section 7.3.1	

Item	Function	Reference	Requirement
	Interfaces		
CPNS-EKA-S-001-O	Assigning EUKey for PNEs with UI capabilities	Section 7.4.1	
CPNS-EKA-S-002-O	Assigning EUKey for PNEs without UI capabilities when PAN is secure	Section 7.4.2.1	
CPNS-EKA-S-003-O	Assigning EUKey for PNEs without UI capabilities when PAN is not secure	Section 7.4.2.2	
CPNS-EKA-S-004-O	Assigning EUKey for PN GW	Section 7.4.3	
CPNS-MA-S-001-M	Performing mutual authentication with PNE	Section 7.5.1	
CPNS-MA-S-002-O	Performing mutual authentication with PN GW	Section 7.5.2	
CPNS-PNM-S-001-M	PN Establishment	Section 7.6.1.3	CPNS-PMETA-S-001-M
CPNS-PNM-S-002-M	PNE Management; PNE Inviting	Section 7.6.2.1.3	CPNS-PMETA-S-001-M
CPNS-PNM-S-003-M	PNE Management; PNE Joining	Section 7.6.2.2.3	CPNS-PMETA-S-001-M
CPNS-PNM-S-004-M	PNE Management; PNE Expulsion	Section 7.6.2.3.3	CPNS-PMETA-S-001-M
CPNS-PNM-S-005-M	PNE Management; PNE Leaving	Section 7.6.2.4.3	CPNS-PMETA-C-002-M
CPNS-PNM-S-006-M	PNE Management; PNE Release	Section 7.6.3.3	CPNS-PMETA-S-001-M
CPNS-SGM-S-001-M	Service Group Management; Service Group Creation	Section 7.7.1.3	CPNS-PMETA-S-001-M AND CPNS-SMETA-S-001-M
CPNS-SGM-S-002-M	Service Group Management; Management of SG Controlling Entities; PNE Invite in Service Group	Section 7.7.2.1.3	CPNS-PMETA-S-001-M AND CPNS-SMETA-S-001-M
CPNS-SGM-S-003-M	Service Group Management; Management of SG Controlling Entities; PNE Expulsion in Service Group	Section 7.7.2.2.3	CPNS-SMETA-S-001-M
CPNS-SGM-S-004-M	Service Group Management; Management of SG Controlling Entities; PNE Joining, Leaving Service Group	Section 7.7.2.3.3	CPNS-SMETA-S-001-M
CPNS-SGM-S-005-M	Service Group	Section	CPNS-SMETA-S-001-M

Item	Function	Reference	Requirement
	Management; Management of SG Controlling Entities; Service Group Member Update	7.7.2.4.3	
CPNS-SGM-S-006-M	Service Group Management; Service Group Update	Section 7.7.3.3	CPNS-SMETA-S-001-M
CPNS-SGM-S-007-M	Service Group Management; Service Group Discovery	Section 7.7.4.3	CPNS-SMETA-S-001-M
CPNS-SGM-S-008-M	Service Group Management; Service Group Release	Section 7.7.5.3	CPNS-PMETA-S-001-M AND CPNS-SMETA-S-001-M
CPNS-SGM-S-009-M	Service Group Management; Service Group Owner Transfer	Section 7.7.6.3	CPNS-SMETA-S-001-M
CPNS-GKM-S-001-M	Group Key creation and storage	Section 7.8.1	
CPNS-GKM-S-002-M	Group Key update according to member leave and expulsion	Section 7.8.2	
CPNS-GKM-S-003-O	Periodical Group Key update	Section 7.8.2	
CPNS-GKM-S-004-M	Group Key deletion	Section 7.8.3	
CPNS-GKM-S-005-M	Group Key delivery to PNGW	Section 7.8.5	
CPNS-SPD-S-001-M	Service Discovery	Section 7.9.2.3	CPNS-PMETA-S-001-M AND CPNS-CMETA-S-001-M
CPNS-SPD-S-002-M	Service Discovery Advertise	Section 7.9.3.1	CPNS-CMETA-S-001-M
CPNS-SPD-S-003-M	Service Discovery Advertise;Zoneasedservice	Section 7.11.4	CPNS-SPD-S-002-M AND CPNS-PMETA-S-001-M
CPNS-SPD-S-004-M	Service Discovery Registration; The case where PNE acting as content provider publishes Service Description	Section 7.9.4.3	CPNS-PNM-S-001-M AND CPNS-PMETA-S-001-M
CPNS-SPD-S-005-M	Service Discovery Registration; The case where external content provider publishes Service Description	Section 7.9.4.3	CPNS-CMETA-S-001-M
CPNS-SCD-S-001-M	Service / Content Delivery	Section 7.10.3	CPNS-CMETA-S-001-M AND CPNS-PMETA-C-001-M
CPNS-DC-S-001-M	Devcie capability Query	Section 7.12.1	
CPNS-SM-S-001-M	Service Status Publication	Section 7.13.2	
CPNS-SM-S-002-M	Service Subscription and Notification	Section 7.13.3	

Item	Function	Reference	Requirement
CPNS-SM-S-003-M	PN / PNE Inactive Status Management	Section 7.13.4.3	CPNS-PMETA-S-001-M
CPNS-SM-S-004-M	PN / PNE Active Status Management	Section 7.13.5.3	CPNS-PMETA-S-001-M
CPNS-US-S-001-M	Usage statistics collection/reporting	Section 7.14.1, 7.14.2	

Appendix C. PN GW Zoned –Based Service (Informative)

PN-GW performs periodical search considering “if there is a newly-found PNE“.

Let T=Timer of Periodical-Search of Zone PN GW,

- T will gradually decrease, meaning more aggressive/frequent search for possible PNE(s) once the condition of the newly found PNE is met. A pre-defined minimal T is configured depending on the capabilities of PN GW.

In Contrast,

- T will gradually increase, meaning less aggressive/frequent search for possible PNE(s) once there is no newly found PNE in the Zone. A pre-defined maximal T is configured depending on the capabilities of PN GW.

Appendix D. Example of specific procedure for secure group key delivery (Informative)

This appendix explains outline of group key delivery procedure using LKH (Logical Key Hierarchy), which is one of candidate mechanisms to realize broadcast group key delivery. The LKH is specified in RFC 2627 and actualizes efficient and secure broadcast group key delivery.

D.1 GKDK/GKEK management

D.1.1 GKDK

When PN GW receives GKDK assignment request from a PNE in the same PN, PN GW creates GKDK for the PNE.

GKDK is created using key hierarchy which is composed of key materials and stored in PN GW. The key hierarchy is constructed when PN GW receives GKDK assignment request from PNE and does not store the key hierarchy. .

- Key hierarchy construction

Figure 47 shows the example of key hierarchy. To construct the key hierarchy, PN GW creates logical tree structure and key materials at first, and then allocates each key material to root, intermediate or leaf node in the logical tree. Once a key hierarchy is created, the key hierarchy is stored in PN GW.

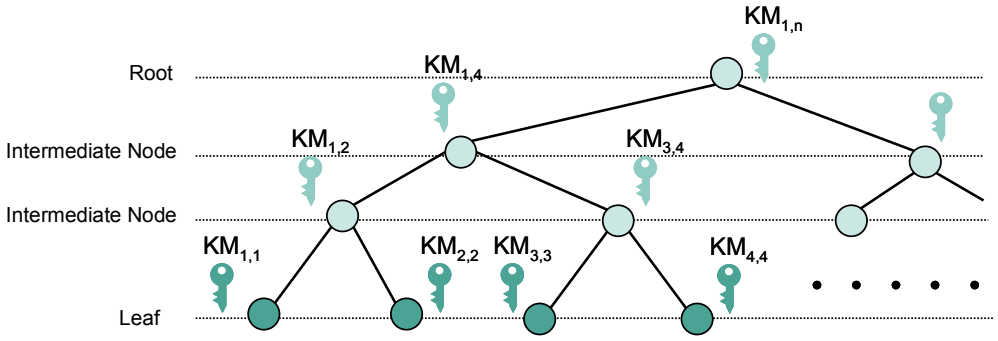


Figure 47 Example of key hierarchy

- GKDK creation

Figure 48 shows the example of GKDK creation. GKDK creation is performed by the following procedure.

1. PN GW allocates leaf node of key hierarchy to PNE.
2. PN GW gathers key materials in the path from corresponding leaf node to root, and packs all gathered materials into one GKDK. The arrow in Figure 48 shows how key materials are gathered when creating PNE A-1's GKDK, which consists of $KM_{1,1}$, $KM_{1,2}$, $KM_{1,4}$, $KM_{1,n}$. GKDKs for other PNEs are as follows:.
   - PNE A-2: $KM_{2,2}$, $KM_{1,2}$, $KM_{1,4}$, $KM_{1,n}$
   - PNE A-3: $KM_{3,3}$, $KM_{3,4}$, $KM_{1,4}$, $KM_{1,n}$
   - PNE A-4: $KM_{4,4}$, $KM_{3,4}$, $KM_{1,4}$, $KM_{1,n}$

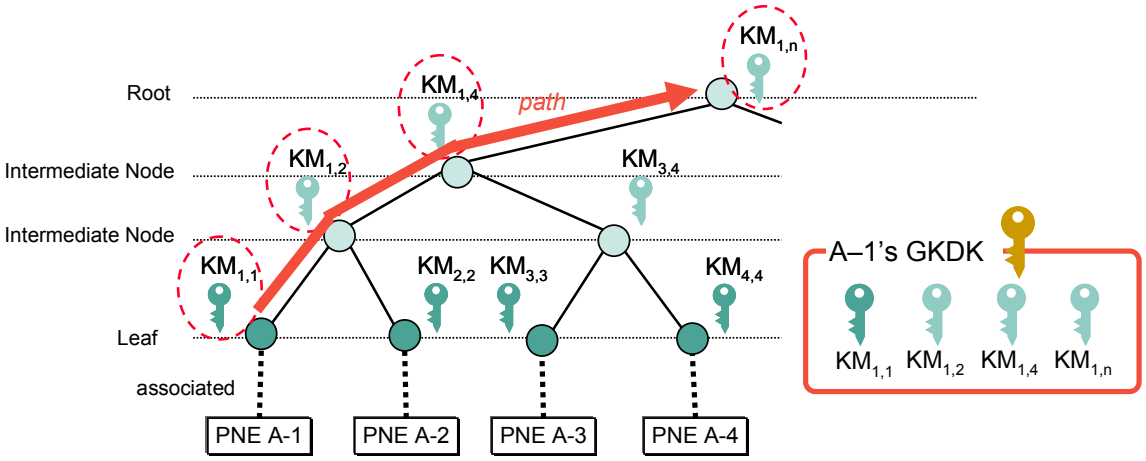


Figure 48 Example of GKDK creation

After the GKDK is created, PN GW sends a GKDK assignment response to a requester PNE with the created GKDK.

D.1.2 GKEK

Figure 49 shows the example of GKEK creation when PNE A-1, 2 and 3 are SG member PNEs. The GKEK creation is performed by the following procedure.

1. PN GW chooses subset trees in the key hierarchy so that SG member PNEs in PN are covered. In the figure, PN GW chooses the subset tree rooted by $KM_{1,2}$, which covers PNE A-1 and 2, and the subset tree rooted by $KM_{3,3}$, which covers PNE A-3.
2. PN GW selects key materials which are the root nodes of the subset trees ($KM_{1,2}$ and $KM_{3,3}$).
3. PN GW creates GKEK by assembling the selected key materials.
4. PN GW stores the created GKEK.

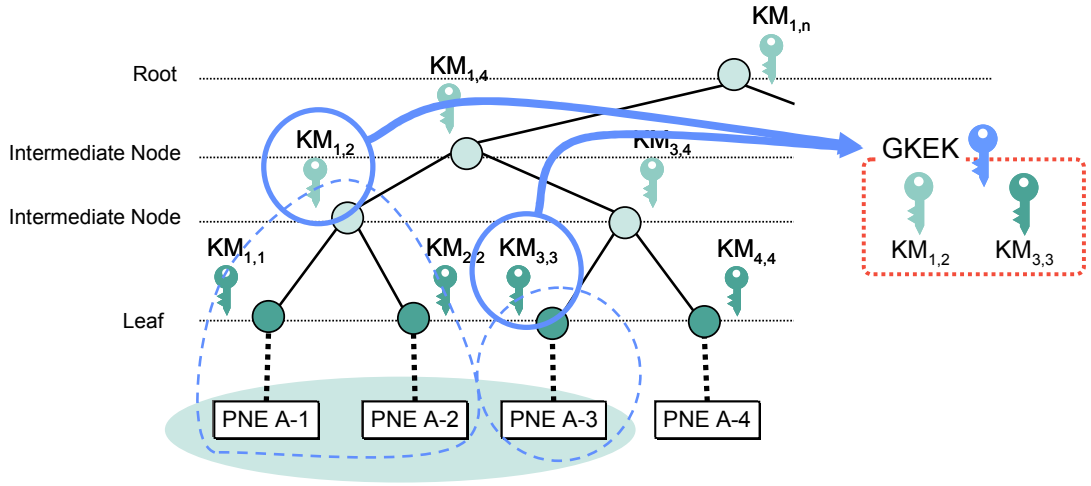


Figure 49 Example of GKEK creation

D.2 Secure group key delivery

Figure 50 shows an example of secure group key delivery. The example in this subsection is based on the same scenario shown in the previous subsection (see Figure 49).

- Group Key encryption and delivery

The procedures are as follows.

1. When receiving Group Key from CPNS Server, PN GW makes two copies of the Group Key.
2. PN GW encrypts one copy using $KM_{1,2}$ and encrypts another copy using $KM_{3,3}$.
3. PN GW packs the two encrypted Group Keys in a single message (i.e. Group Key delivery request) and broadcasts the message in PN.

- Group Key decryption

The procedures are as follows.

1. SG member PNEs (i.e., PNE A-1, A-2 or A-3) unpacks the message and picks up the two encrypted Group Key.
2. PNE decrypts Group Key using key materials in GKDK.
   - PNE A-1 and A-2 decrypt Group Key using $KM_{1,2}$ (i.e., from Group Key encrypted by $KM_{1,2}$).
   - PNE A-3 decrypts Group Key using $KM_{3,3}$ (i.e., from Group Key encrypted by $KM_{3,3}$).

Note that, though PNE A-4, which is in the same PN but not an SG member, receives encrypted Group Key, PNE A-4 can not decrypt Group Key, since the PNE A-4 does not have corresponding key materials (i.e., $KM_{1,2}$ and $KM_{3,3}$)

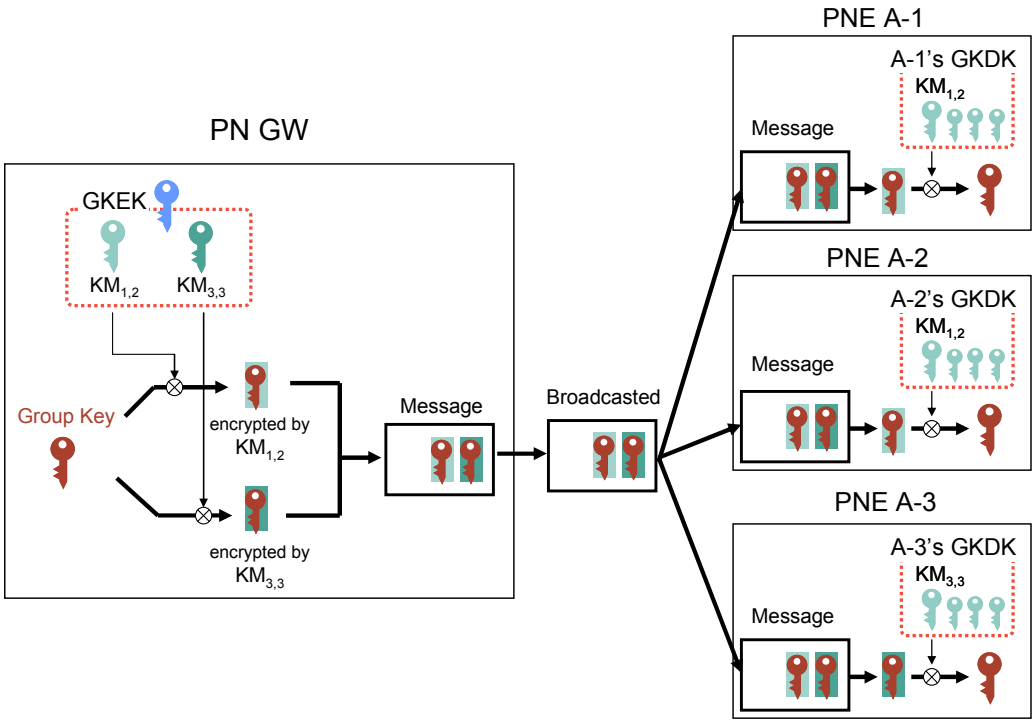


Figure 50 Example of secure group key delivery

Appendix E. Service Invocation example (Informative)

This section shows the example of Remote PNE connection service invocation of lighting service. For documentation purpose, XML based protocol is used.

The procedure scenario uses following CPNS functions.

- Service Discovery
- Service/Content Delivery

In addition, the procedure refers to PUCC technical specifications for implementation practice of service discovery and service invocation [PUCC-DDSI] and corresponding metadata [PUCC-META].

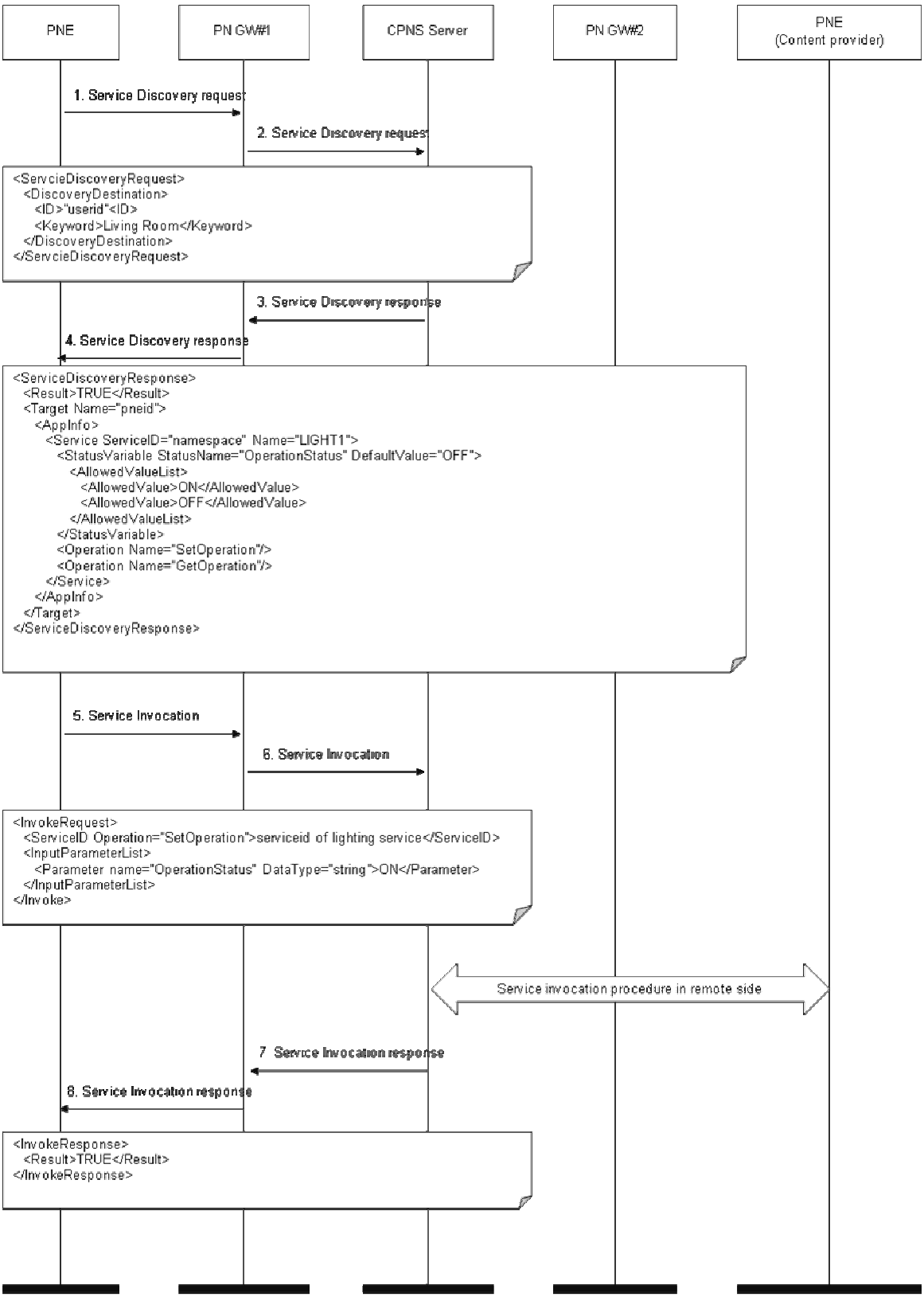


Figure 51 Service Invocation example flow

1. The consumer PNE send Service Discovery request with Keyword, “Living Room”, to find metadata for lighting service.

2. The PN GW#1 relays the request to the CPNS Server.
3. The CPNS Server responds the matched metadata.
4. The PN GW#1 relays the response back to the PNE.
5. The consumer PNE sends the Service Invocation to invoke lighting service with operation, SetOperation and argument, ON.
6. The PN GW#1 relays the request to the CPNS Server
7. Upon receiving the invocation response from remote side, the CPNS Server relays back the invocation response to PN GW#1.
8. The PN GW#1 relays back the response to the consumer PNE.

Appendix F. XML based overlay network protocol (Informative)

In convergence of PAN and WAN, CPNS Enabler will be most effective for the service such as health care and consumer electronic convergence in which various digital equipments are connected together using various communication protocol. In that sense, the key success for CPNS Enabler is the applicability to various underlying networks.

The section focuses on XML based overlay network protocol and refers to PUCC technical specifications i.e., [PUCC-ARCH] and [PUCC-BASIC] for the implementation practice description.

For the purpose of XML based overlay network protocol description, the section is consisted of following subsections.

- CPNS message routing mechanism
- CPNS message common entry
- Transport protocol binding

The basis of XML based overlay protocol is agnostic to underlying protocol such as HTTP, TCP, UDP, SIP, etc; therefore in the following subsections applicability of specific CPNS interface to transport protocol is not specified.

Followings are the principles of XML based overlay protocol.

- Communication protocol which uses XML for description of message format and rules.
- The transport protocol to transport CPNS message, packaged in XML document format
- The message receiver extracts the method and its parameter from XML document and executes function accordingly.
- Then the receiver may return another XML document to the message sender.

Following shows CPNS XML based overlay protocol layer.

The key for easy XML based overlay protocol implementation is well defined XML structure and flexible enough for future extension. Putting all information element but with different purpose together on the same level of XML tree leads to confusing protocol specification and difficult to implement/extend for future use.

Upon the underlying network protocol, the CPNS common is the logical layer for those common elements found in CPNS messages. And upon CPNS common various CPNS messages provide the functions of CPNS Enabler.

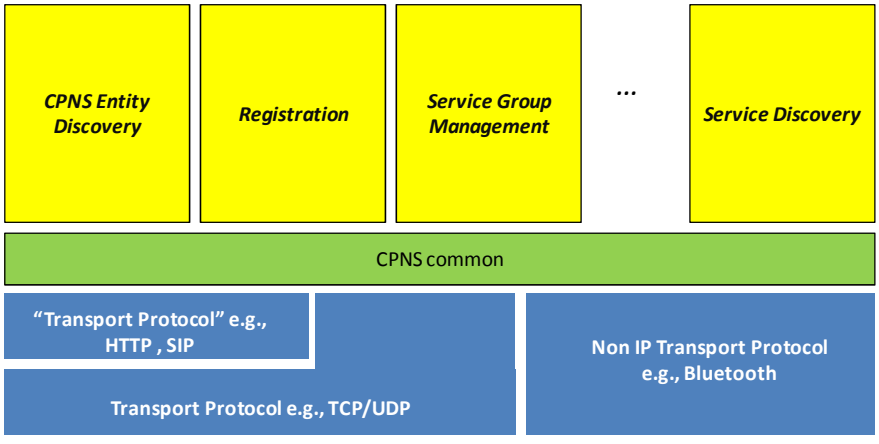


Figure 52 CPNS XML based protocol layer

F.1 CPNS message routing mechanism

This section describes overview of CPNS message routing mechanism. Following model is used for documentation purpose in further description.

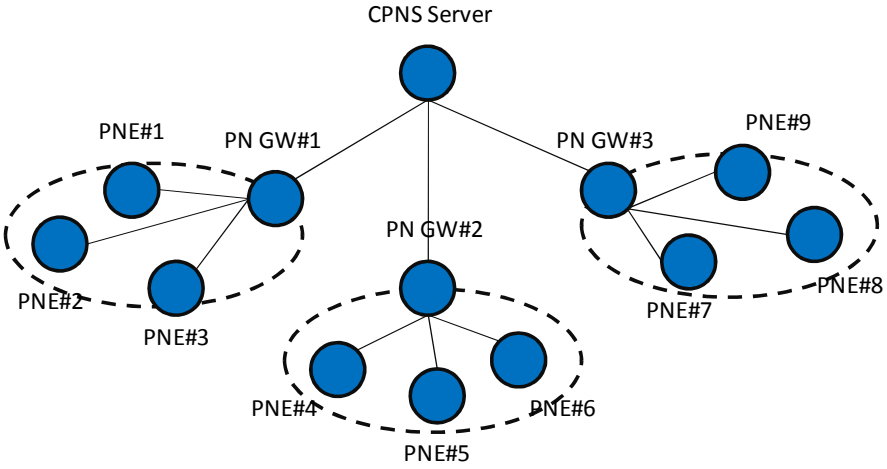


Figure 53 CPNS topology model

Followings are the basic principles of CPNS message routing mechanism

- The CPNS Server and PN GW store two types of topology information in the form of PN Inventory and SG Inventory. The format of each inventory can be found in Section 5.
    - PN GW and CPNS Server collect inventory information via PN Management procedure and SG Management procedure.
- Each CPNS Entity stores transport binding table that the format and resolution mechanism is implementation matter. Following shows the implementation practice.
    - CPNS device (i.e., PNE and PN GW) exchanges its transport resource information (e.g., transport layer address, transport layer protocol such as TCP, HTTP and SMS and address type such as IPv4, IPv6, and Bluetooth) via CPNS Entity Discovery to build transport binding table (See Table 74).
- CPNS messages are routed by utilizing inventory information (i.e., PN Inventory and SG Inventory) and transport binding table.

For the purpose of CPNS message routing mechanism description, the section is consisted of following subsections.

- CPNS Entity Discovery
- CPNS PN Establishment & Registration
- Service Publication & Discovery
- Service Discovery
- Service/Content Delivery
- Usage Statistics Collection & Reporting
- Service Group Management

F.1.1 CPNS Entity Discovery

CPNS device exchanges own transport layer resource through CPNS Entity Discovery on physical pairing path. For instance, PNE1 and PN GW#1 exchange such information through CPNS Entity Discovery.

NOTE: At the step of CPNS Entity Discovery each entity does not have resource knowledge of each such as who is PNE and who is PN GW, but for the documentation purpose the CPNS Entity name is used.

NOTE: For simplicity all other information description defined in normative section is not described here.

Following shows the example of resource information from PNE1.

<OwnEntityID>PNE1</OwnEntityID>
<ConnectionCapability>10</ConnectionCapability> # the max number of connections. An entity can specify number of connection using this element.
<TransportAddress protocol="TCP" type="IPv4">192.168.64.1</TransportAddress>

Following shows the example of resource information in response from PN GW#1.

<OwnEntityID>PN GW#1</OwnEntityID>
<ConnectionCapability>10</ConnectionCapability> # the max number of connections. An entity can specify number of connection using this element.
<TransportAddress protocol="TCP" type="IPv4">192.168.64.128</TransportAddress>

Through the procedure (e.g., CPNS Entity Discovery), PNE1 and PN GW#1 build the transport binding table.

Following shows the PNE1 transport binding table as an example.

EntityID	Protocol Type	Address Type	Address
PN GW#1	TCP	IPv4	192.168.64.128

Table 74 Transport binding table in PNE1

- EntityID is the CPNS EntityID
- Protocol Type is the type of underlying network protocol e.g., TCP, UDP, HTTP, SIP, Bluetooth, etc
- Address Type is the type of address e.g., IPv4, URL (for HTTP), Bluetooth, and so on
- Address is the transport layer address and can be IP or non IP (e.g., Bluetooth address)

F.1.2 CPNS PN Establishment & Registration

CPNS PN Establishment & Registration consist of several CPNS messages. For simplicity PNE initiated procedure is used.

Through CPNS Entity Discovery, each entity share transport layer resources and already build transport binding table for CPNS message routing.

In accordance of the transport binding table, PNE1 sends PN setup to PN GW#1. In case PN GW has other physical pairing with e.g.,PNE2. PN GW#1 sends PN setup notify message to PNE2 and receive the response accordingly defined in normative section.

Upon receiving the PN setup notify response, PN GW#1 sends PN registration request with PN Inventory to the CPNS Server under the assumption that the transport address of CPNS Server is pre-configured to PN GW#1 or known to PN GW#1 by using other mean of address resolution.

The CPNS Server sends back the PN registration response to PN GW#1. Querying CPNS EntityID in PN Inventory and transport binding table, the PN GW#1 sends the response back to appropriate PNE(s).

F.1.3 Service Publication & Discovery

Service Publication & Discovery consists of two sub functions i.e., Service Publication and Service Discovery.

F.1.3.1 Service Publication

For Service Publication routing description, the section consider PNE#7 as application hosting device. The PN management for the PNE where PNE#7 resides in is already performed, which means all transport resource information are exchanged and PN GW has both PN Inventory and transport binding table for all PNE(s) reside in the PN.

The PNE#7 in accordance of transport binding table publishes service description to the CPNS Server via PN GW#3. In case the TraceRoute common message element is set, the PN GW#3 records own CPNS EntityID in the message in the publication request message. Upon receiving the service description and successfully registering the service description, the CPNS Server sends back the response message through the route path (i.e., Route entry of TraceRoute) in reverse order. Upon receiving the response message, the PN GW#3 queries the transport binding table to resolve the transport address and send back the response message to PNE#7.

F.1.3.2 Service Discovery

Service Discovery consists of two CPNS messages i.e., Service Discovery and Service description advertise. For simplicity, this section only describes Service Discovery.

Let's say PNE2 is the consumer PNE and looking for lighting service which is to turn on and off the remotely located light.

The PNE2 sends Service Discovery request to PN GW#1 in accordance of transport binding table. The PN GW#1 sends the message to the CPNS Server. In case the TraceRoute common message element is set, the PN GW#1 records own CPNS EntityID in the message in the Service Discovery request message. Upon receiving the message and successfully found the matched CPNS metadata, the CPNS Server sends back the response message through the route path (i.e., Route entry of TraceRoute) in reverse order. Upon receiving the response message, the PN GW#1 queries the transport binding to resolve the transport address and send back the response message to PNE2.

F.1.4 Service/Content Delivery

Service/Content Delivery facilitate data delivery, which means the function controls the control message for the data delivery.

This section describes service invocation message routing.

PNE2 knows the CPNS EntityID hosting the lighting service by Service Discovery. The PNE2 assembles the service invocation message and set destination ID as PNE#7 and sends the message to PN GW#1 in accordance of transport binding table.

Upon receiving the message, PN GW relays the message to the CPNS Server based on preconfigured address of CPNS.

Upon receiving the message, the CPNS Server resolve the responsible PN GW for the PNE#7 and sends the message to appropriate PN GW i.e., PN GW#3 and the PN GW#3 sends the message to PNE#7. In case the TraceRoute common message element is set, intermediate CPNS Entity records own CPNS EntityID to the message. The PNE#7 sends back the response message through the route path (i.e., Route entry of TraceRoute) in reverse order. At each CPNS entity send the message in accordance of transport binding table.

F.1.5 Usage Statistics Collection & Reporting

The PNE1 sends stat report to the PN GW#2 in accordance of transport binding table and PN GW#2 relays the report to the CPNS message. In case the TraceRoute common message element is set, the PN GW#1 records own CPNS EntityID in the message in the message. The CPNS Server sends back the response message through the route path (i.e., Route entry of TraceRoute) in reverse order.

F.1.6 Service Group Management

The Service Group Management consists of several messages for management of Service Group. The same scheme is applied to the Service Group Management messages routing.

As for management of service itself, when the Service Group ID is designated in Service Invocation message, then the content is distributed among PNEs in the Service Group and the data routing schema is out of scope of CPNS Enabler.

F.2 CPNS message common entry

The description can be found in Section 8.1.1.

F.3 Transport protocol binding

For CPNSv1.0 transport protocol binding specification is informative. This section covers following transport protocol binding description as deployment practice.

NOTE: Binding scheme for other protocol binding example such as UDP and other can be found in [PUCC-BASIC].

- Bluetooth binding
- HTTP binding

F.3.1 Bluetooth binding

This section describes Bluetooth binding specification.

The Logical Link Control and Adaptation Layer Protocol (L2CAP) is used for CPNS message delivery.

Following shows the L2CAP packet structure encapsulating CPNS messages. In the Data part of the packet CPNS messages related information are contained. In Sub-Options, the Header part contains necessary info-set (i.e, Frame Type and Connection Type) for the frame and messages part contain CPNS messages with necessary info-set (i.e., Value type and Value length).

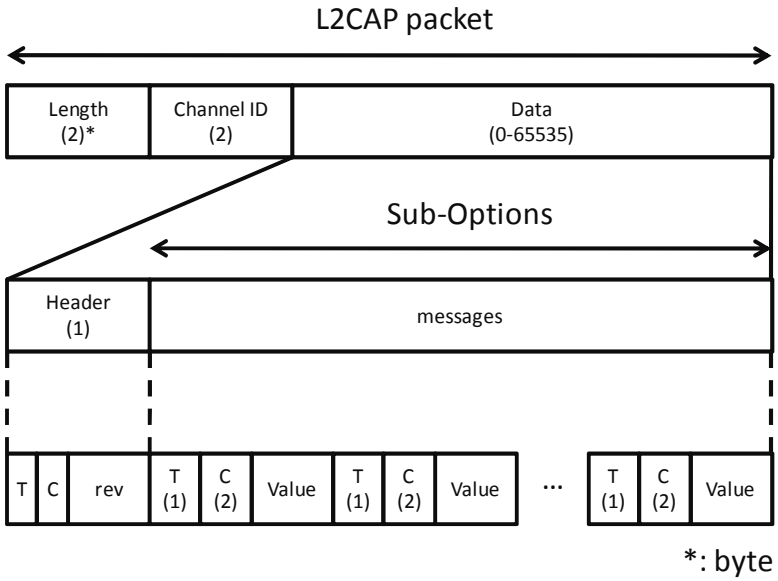


Figure 54 Bluetooth binding

F.3.1.1 Bluetooth binding format

Following shows the basic encapsulation format of CPNS XML based overlay protocol. All CPNS messages are encapsulated in following frame.

Part	Format
Header	• T as in Frame Type : 1 bit (tbd) o Set to 1 • C as in Connection Type : 1 bit o Connection type indicates connection type and when the value is set to 0 the transport connection should not be terminated after the frame. When the value is set to 1 the transport connection should be terminated after the frame. • Rev as in Reserved : 6 bit
Sub-Options	• Sub-Options part consisted of Type, Length, and Value. o Type define value type: 1 byte ▪ 0x01 : Indicate the value is CPNS message ▪ 0x02: Indicate the value is Source EntityID ▪ 0x03: Indicate the value is Destination EntityID o Length define value length: 2 bytes o Value is the CPNS message

Table 75 Frame format for Bluetooth binding

F.3.2 HTTP binding

This section describes HTTP binding specification.

For HTTP binding, since HTTP is the client-server model based protocol, a CPNS entity needs to act as HTTP client and another as HTTP server in dialog. Given that, two deployment scenarios can be considered. One is when a CPNS entity supports both HTTP client and HTTP server role and another case is when a CPNS Entity only supports either HTTP client or HTTP server.

The URL format is used for the transport layer address of the HTTP binding. The URL of the HTTP server role is somehow known to the CPNS Entity (i.e., PN GW) acting as HTTP client role in advance.

F.3.2.1 Case1: A CPNS Entity has both HTTP server and client capability

Since a CPNS Entity is equipped with both HTTP server and client role, CPNS message is exchanged asynchronously over independent HTTP session per CPNS message delivery direction.

Following figure shows the example of CPNS Entity#1 sends a CPNS request message (indicated by message type) to CPNS Entity#2.

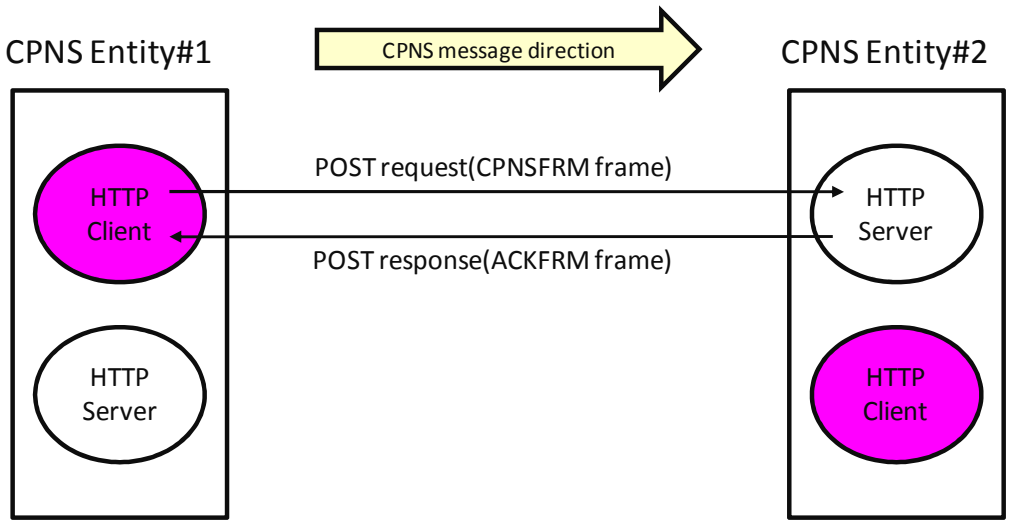


Figure 55 CPNS Entity#1 sending CPNS message to CPNS Entity#2

Following figure shows the example of CPNS Entity#2 sends a CPNS response message (indicated by message type) to CPNS Entity#1. It may be the CPNS response message to the CPNS request message in Figure 55.

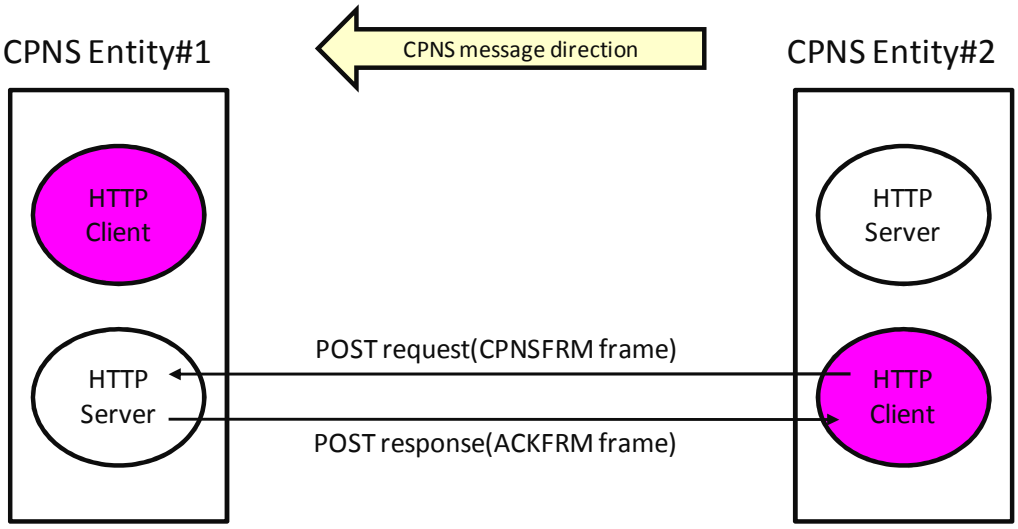


Figure 56 CPNS Entity#2 sending CPNS message to CPNS Entity#1

When message type indicates the message is “advertise”, then HTTP client of responsible CPNS Entity sends the adverse type CPNS message over HTTP POST request and receive HTTP POST response with ACKFRM but no CPNS response message.

For all message type “request”, “response”, and “advertise”, the HTTP POST request is used for CPNS message transmission as shown in Figure 55 and Figure 56. As alternative, the CPNS message (e.g., CPNS response message) can be conveyed over HTTP POST response but not shown here but can be found in detail in PUCC technical specification [PUCC-BASIC].

Following table shows the binding of HTTP Method (See RFC2616) and CPNS message request/response.

MsgType of CPNS message	Direction of CPNS message	HTTP message
Request	Send	POST request
	Receive	POST request

Response	Send	POST request or POST response
	Receive	POST response or POST response
Advertise	Send	POST request
	Receive	POST request

Table 76 CPNS message type and HTTP method association in case 1

F.3.2.2 Case2: A CPNS Entity has either HTTP server or client capability

The consideration with this case is that because HTTP based message can't be pushed from the HTTP server role to the HTTP client role, when CPNS Entity (e.g., CPNS Server) with HTTP server role needs to send a message with MsgType "Request" or "Advertise", polling is performed periodically from the CPNS Entity (e.g., PN GW) to the CPNS Entity with HTTP server role.

Following figure shows the example of CPNS Entity#1 and CPNS Entity#2 exchange CPNS request & response message over on HTTP dialog. The HTTP POST request is used for CPNS request message delivery and HTTP OST response for delivery of CPNS response message.

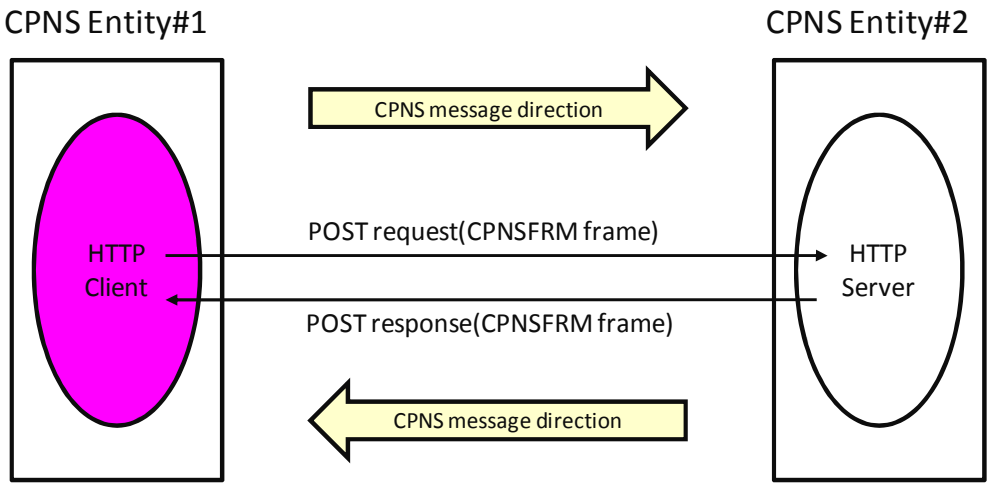


Figure 57 CPNS Entity#1 and CPNS Entity#2 exchange CPNS request & response message

Following figure shows the example of CPNS Entity#2 with HTTP Server role advertises CPNS message to CPNS Entity#1. For CPNS Entity with HTTP server role to advertise message, the CPNS Entity with HTTP client role needs to indicate the poling is set in the body of HTTP POST request beforehand. With the polling and when CPNS Entity with HTTP server role sends the message, the HTTP POST response is used for the CPNS message delivery. Polling specific description (e.g., cycle/polling duration value) is out of scope.

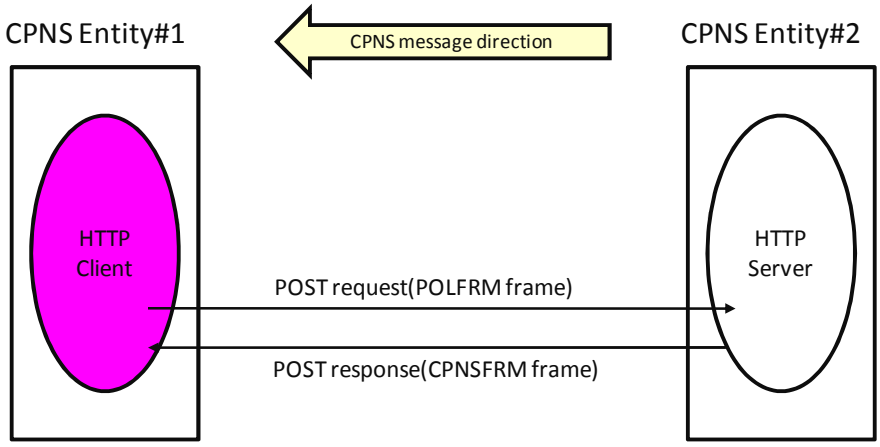


Figure 58 CPNS Entity#2 advertises CPNS message to CPNS Entity#1

Following table shows the HTTP Method (See RFC2616) associated with CPNS message request and response.

MsgType of CPNS message	Direction of CPNS message	HTTP message
Request	Send	POST request
	Receive	POST response NOTE: With polling
Response	Send	POST request
	Receive	POST response NOTE: With polling or not
Advertise	Send	POST request
	Receive	POST response NOTE: With polling

Table 77 CPNS message type and HTTP method association in case 2

NOTE: The HTTP POST response in above specification only corresponds to the status code of 200 OK and the behaviour of case with other status code is not specified.

F.3.2.3 HTTP binding format

Following shows the basic encapsulation format of CPNS XML based overlay protocol with regard to above example. All CPNS messages are encapsulated in following frame. More information about encapsulation scheme can be found in PUCC technical specification [PUCC-BASIC].

Part	Format
Header	• CPNSFRM <Connection type> <Frame number> <Size> <Destination CPNS EntityID> <Source CPNS EntityID> o The header for CPNS message delivery ▪ Connection type indicates connection type and when the value is set to 0 the transport connection should not be terminated after the frame. When the value is set to 1 the transport connection should be terminated after the frame and for HTTP the value is 1. ▪ Frame number is sequential number used to distinguish frames. ▪ Size is to designate size of payload in the octet number. ▪ Destination CPNS EntityID is the identifier which identifies the

	destination Entity. ▪ Source CPNS EntityID is identifier which identifies the source Entity. • ACKFRM o The header for HTTP POST response with no CPNS message in payload • POLFRM o The header for polling as in HTTP POST request • NOMSGFRM o The header for polling response indicating no message
Payload	• For the case of header is CPNSFRM contains CPNS messages. • For the case of header is ACKFRM contains no content and should not be used. • For the case of header is POLFRM contains no content and should not be used. • For the case of header is NOMSGFRM contains no content and should not be used.
Trailer	FRMEND

Table 78 Frame format for HTTP binding

Following shows the example syntax of frame. The header is CPNSFRM which indicate that the frame contains CPNS messages. The Connection Type indicates the transport protocol connection should be terminated after the frame. The Frame number indicates the 1st frame. As indicated by Destination CPNS EntityID and Source CPNS EntityID the message the direction of the message is from CPNS Entity#1 to CPNS Entity#2.

```
CPNSFRM 1 1  n CPNS Entity#1 CPNS Entity #2
<CPNS messages/>
FRMEND
```

Appendix G. SMS Based CPNS protocol (Informative)

G.1 General

The CPNS Protocol should be applicable to all kinds of transport networks for convergence perspective. In addition, the CPNS protocol should take backward compatibility into consideration for expanding cellular network service. Thus, Easy implementation is another important aspect to the CPNS Protocol. For easy implementation, the CPNS Protocol requires well formed structure. With this regard, SMS based, precisely User Data in SMS is regarded as one of CPNS Protocol options.

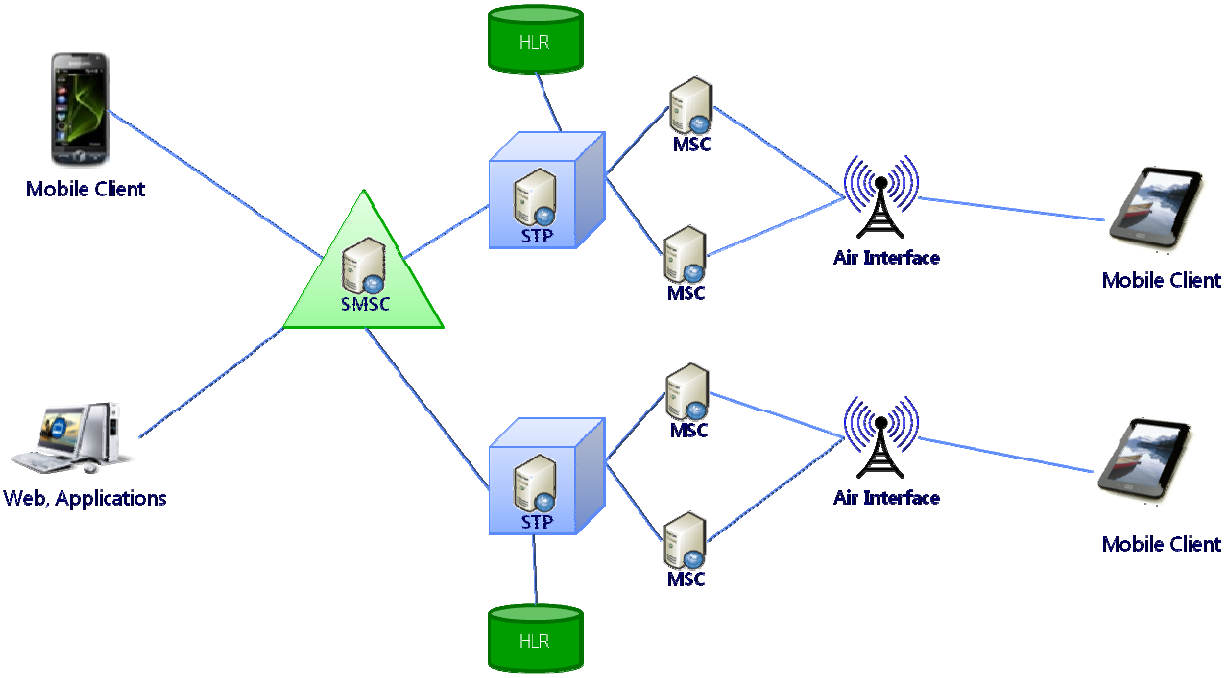


Figure 59 Mobile Networks for SMS Delivery

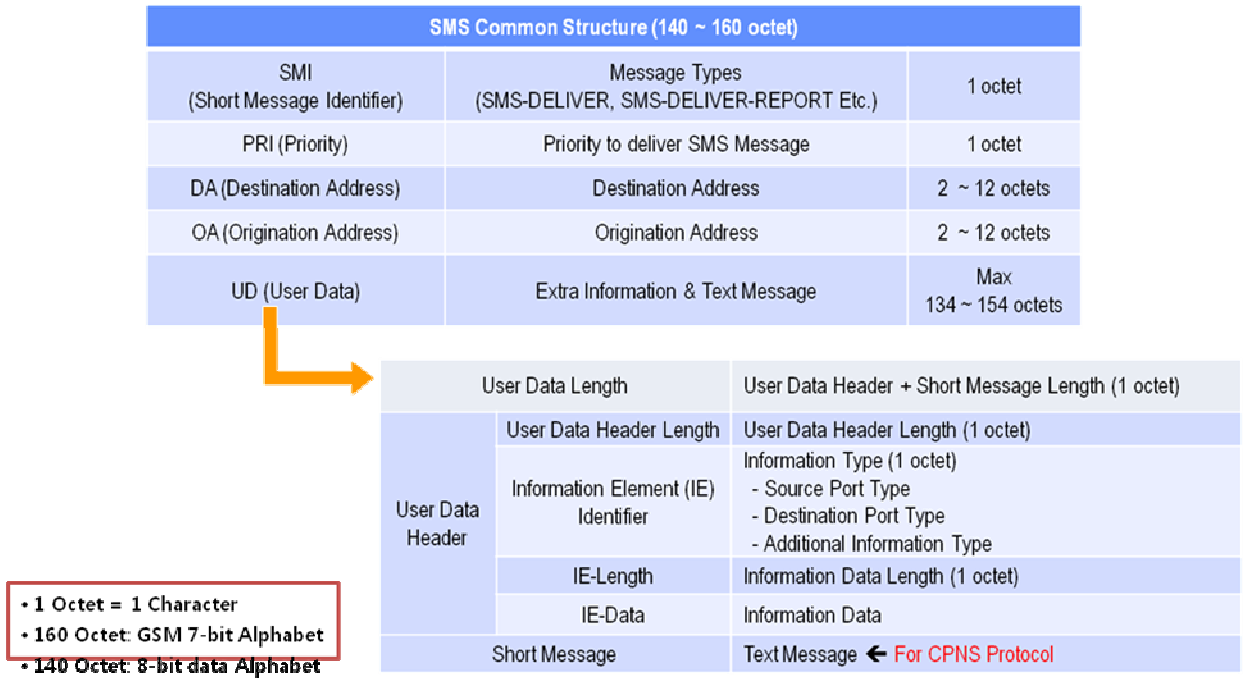


Figure 60 SMS Message Format

Short Message Service (SMS) is the text communication service component of phone, web or mobile communication systems, using standardized communications protocols that allow the exchange of short text messages between fixed line or mobile phone devices. SMS text messaging is the most widely used data application in the world.

The format of SMS consists of SMI (Short Message Identifier), Prioirty, Destination Address, Origination Address and User Data. SMS itself can be one of option to be used for delivery of CPNS commands in WAN for the CPNS. For the CPNS Protocol, User Data Extension part will be used to make CPNS command with well formed structure.

With any underlying network, the CPNS common is the logical layer for those common elements found in CPNS messages. And upon CPNS common various CPNS messages provide the functions of CPNS Enabler.

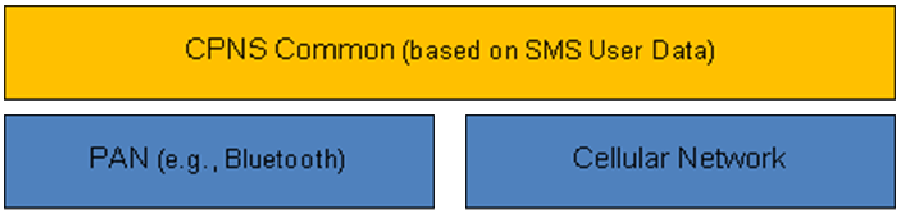


Figure 61 SMS Based CPNS Protocol Layer

G.2 Format

G.2.1 Common CPNS Command

The following is the common part for all CPNS Commands.

The value of Command group can be flexible to define the CPNS Methods. The command will be grouped based on the similar format according to the header style. For example, the Command has grouped based on the format style whether URL as a string is contained or not.

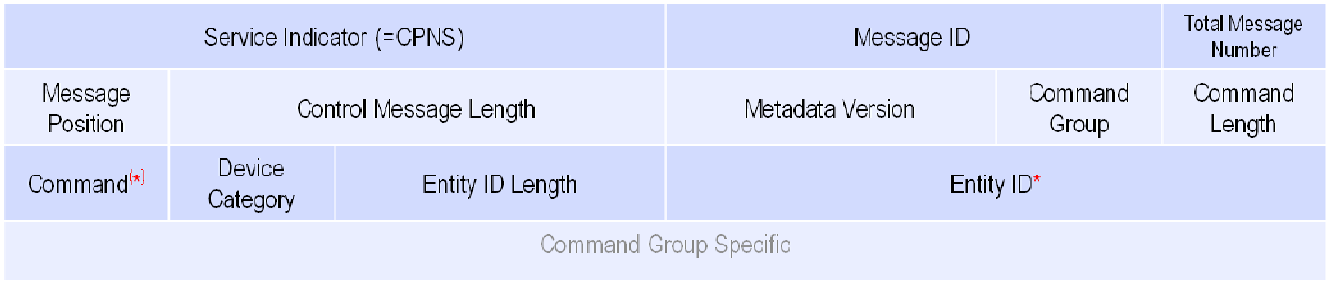


Figure 62 SMS Based CPNS message – common part

This Common part consists of various headers like below. (First element: Length, Second element: Value) (Unit: Octet)

- Service Indicator (4, CPNS) – pointing out CPNS service
- Message ID (3, 0~FFF) – ID which distinguish Message, When ID value reaches 'FFF', the value returns '000'
- Total Message Number (1,1~F) – the number of message which one CPNS method is comprised of
- Message position (1,1~F) – the sequence number of CPNS method. '1' in value means starting point.
- Message Length (3,0~FFF) – the message length after message length field. If the message length exceeds limitation of SMS message length, then the message will be separated into based on the message length.
- Device Metadata Version (2,0~FF) – Metadata version which PNE, PN GW and CPNS Server refer. Version should be valid among PNE, PN GW and CPNS Server for consistency of CPNS Methods.
- Command Group (1, X) - based on the Value, Command Group has different meaning.
  i. 0 – Device Wakeup: Asking to enable the device ready to use CPNS Service
  ii. 1 – CPNS Methods Group (except Service Request)
  iii. 2 – CPNS Methods Group (Service Request)
  iv. 3 ~ E – Reserved
  v. F – Response: delivery of result of requesting CPNS Methods
- Command Length (1,0~F) – the length of command, default value is 1
- Command (1, X) – based on the Value, Command is different.
  i. 0 – PN Setup Request
  ii. 1 – Service Advertisement
  iii. 2 ~ F – Additional commands
  iv. String – directly putting the command in the field
- Device Category (2, 0~FF) – Category of device which performs CPNS command
- EntityID Length (2, 0~FF) – Length of EntityID
- EntityID (*, string) – Unique ID of Entity to consume the service

G.2.2 Service Request CPNS Command

In addition to common CPNS command, Service Request CPNS command is defined with appropriate URL.

Service Indicator (= CPNS)		Message ID		Total Message Number
Message Position	Control Message Length	Metadata Version	Command Group	Command
Device Category	Entity ID Length	(PN GW) Entity ID *		
URL Length	URL *			
Additional Information				

The Service Request consists of common parts and URL related parts. (First element: Length, Second element: Value) (Unit: Octet)

- Common parts – applying headers to all CPNS commands to refer the section X.2.1
- URL Length (3, 0 ~ FFF) – Length of URL which PNE invokes services
- URL (*, string) – URL to invoke service by PNE

G.2.3 CPNS Method except Service Request

The different CPNS command with Service Request such as PN Setup command or Service Publication can be defined with Argument related headers. Each Argument has different CPNS command respectively. The length may vary. URL can be shortened by specific mechanism.

Service Indicator (= CPNS)		Message ID		Total Message Number
Message Position	Control Message Length	Metadata Version	Command Group	Command
Device Category	Entity ID Length	Entity ID *		
Argument Count	Argument Length	Argument Value *		
Device Category	Entity ID Length	Entity ID*		
Argument Count	Argument Length	Argument Value*		
Additional Information				
…				

The different CPNS command with Service Request consists of common parts and Argument parts. (First element: Length, Second element: Value) (Unit: Octet)

- Argument Count (1, 0~F) – Required Argument number for performing CPNS method
- Argument Length (2, 0~FF) – Length of Argument
- Argument Value (*,string) – Value of Argument

G.2.4 Response CPNS Command

The Response CPNS Command is sent according to the received CPNS command.

Service Indicator (= CPNS)		Message ID		Total Message Number
Message Position	Control Message Length	Metadata Version	Command Group	Result
Device Category	Entity ID Length	Entity ID *		
Description Length	Description *			
Additional Information if any				

The Response CPNS command consists of result header and description. (First element: Length, Second element: Value) (Unit: Octet)

- Result (1, X) – acknowledging the result to the request. Based on the Value, Response is different.
  i. 0 – OK
  ii. 1 ~ E – Reserved
  iii. F – Failure
- Description Length (2, 0~FF) – Length of Description
- Description (*, string) – Description of failure, if any.

Appendix H. HTTP binding (Informative)

H.3 General

CPNS Server and PN GW support HTTP 1.1 [RFC2616] for CPNS-2 and CPNS-7

PN GW and PNE support HTTP 1.1 [RFC2616] for CPNS-1 and CPNS-6

Note: If HTTP is implemented on the PN side, PN GW and PNE support HTTP 1.1 [RFC2616] for CPNS-1 and CPNS-6

CPNS-1: HTTP protocol is an optional protocol for CPNS, but if implemented, this specification defines HTTP 1.1 [RFC2616] for CPNS-1 and as such both PNE and PN GW support this protocol. This specification also can define other protocols and delivery mechanisms such as WiFi, Bluetooth etc., in addition to HTTP.

CPNS-2: This specification defines HTTP 1.1 [RFC2616] for CPNS-2 and as such both PN GW and CPNS Server support this protocol. This specification also can define other protocols and delivery mechanisms such as WAP Push, DCD, SMS etc., in addition to HTTP 1.1.

CPNS-3: Protocols through an interface between two PN GW is FFS or for the next release.

CPNS-4: This specification defines HTTP 1.1 [RFC2616] for CPNS-4 and as such CPNS Server supports this protocol.

CPNS-5: This can be an implementation specific and therefore the CPNS spec does not define it.

CPNS-6: HTTP protocol is an optional protocol for CPNS, but if implemented, this specification defines HTTP 1.1 [RFC2616] for CPNS-6 and as such both PN GW and PNE support this. This specification also can define other protocols and delivery mechanisms such as WiFi, Bluetooth etc., in addition to HTTP.

CPNS-7: This specification defines HTTP 1.1 [RFC2616] for CPNS-7 and as such both CPNS Server and PN GW support this protocol. This specification also defines other protocols and delivery mechanisms such as WAP Push, DCD, SMS etc., in addition to HTTP 1.1..

H.4 Content type of formatted messages

CPNS Server and PN GW support formatted messages as entity-bodies with application media type (application/vnd.oma.cpns) that go through interfaces CPNS-2 and CPNS-7. The application media type is used when there is a single message in the HTTP request/response.

CPNS Server and PN GW support formatted messages as entity-bodies with multipart/mixed subtypes that go through interfaces CPNS-2 and CPNS-7. These messages as entity-bodies with multipart/mixed types can support different content-type headers as part of the same HTTP message.

CPNS Server and PN GW support formatted messages as entity-bodies with multipart/related subtypes that go through interfaces CPNS-2 and CPNS-7. These messages as entity-bodies with multipart/related types can support different message parts as parts of an aggregated message.

PN GW and PNE support formatted messages as entity-bodies with application media type (application/vnd.oma.cpns) that go through interfaces CPNS-1 and CPNS-6. The application media type is used when there is a single message in the HTTP request/response.

PN GW and PNE support formatted messages as entity-bodies with multipart/mixed subtypes that go through interfaces CPNS-1 and CPNS-6. These messages as entity-bodies with multipart/mixed types can support different content-type headers as part of the same HTTP message.

PN GW and PNE support formatted messages as entity-bodies with multipart/related subtypes that go through interfaces CPNS-1 and CPNS-6. These messages as entity-bodies with multipart/related types can support different content-type headers as part of the same HTTP message

Note: If HTTP is implemented on the PN side, PN GW and PNE support the above mentioned media types.

H.5 HTTP Methods

All the messages from PN GW to CPNS Server through interface CPNS-2 are sent as HTTP POST method requests.

All the responses from CPNS Server to PN GW through interface CPNS-7 are sent as appropriate HTTP status codes or responses.

All the messages from PNE to PN GW through interface CPNS-1are sent as HTTP POST method requests.

All the responses from PN GW to PNE through interface CPNS-6 are sent as appropriate HTTP status codes or responses.

Note: If HTTP is implemented on the PN side, PN GW and PNE support the above mentioned HTTP methods

H.5.1 HTTP Message requests from PNE to CPNS Server via PN GW

Message	Implementation	Direction	HTTP Methods
HTTP POST	Mandatory	PN GW → CPNS Server	POST
Response to HTTP POST	Mandatory	PN GW ← CPNS Server	HTTP Response, 200 OK
HTTP POST	Conditional	PNE → PN GW	POST
Response to HTTP POST	Conditional	PNE ← PN GW	HTTP Response, 200 OK

Element	Cardinality	T	Data Type	Description
HTTP POST	1			HTTP method
Request-URI	1	A	String	URI of a new resource to be identified. URI of PN GW when initiated by PNE or URI of CPNS Server when initiated/forwarded by PN GW
Host request-header	1	A	String	Specifies the hostname of the resource being requested
PNE request-header	0..1	A	String	Contains information about the entity originating the request
Content-Length entity-header	1	A	Integer	Defines the length of the entity-body
Content-Type entity-header	0..1	A	String	MIME media type of the entity-body, one of “application/vnd.oma.cpns”, “multipart/related”, or “multipart/mixed”, as applicable
Message-body	0..1	A	String	Messages through CPNS-1 and CPNS-2

Table 79 HTTP Message requests from PNE to CPNS Server via PN GW

H.5.2 HTTP Message responses to HTTP Post requests

Element	Cardinality	T	Data Type	Description
HTTP Response to POST	1			HTTP response, 200 OK
Request-URI	1	A	String	Responses to requests from identified URIs
Host request-header	1	A	String	Specifies the hostname of the resource being requested
PNE request-header	0..1	A	String	Contains information about the entity originating the request
Content-Length entity-header	1	A	Integer	Defines the length of the entity-body
Content-Type entity-header	0..1	A	String	MIME media type of the entity-body, one of "application/vnd.oma.cpns", "multipart/related", or "multipart/mixed", as applicable
Message-body	0..1	A	String	Response messages through CPNS-6 and CPNS-7

Table 80 HTTP Message responses to HTTP Post requests

Appendix I. Common Parameter usage (Informative)

This section shows the example usage of common parameter (See 8.1.1).

Following shows a routing path model for common parameter, in case where Entity (D)'s Entity ID is known to Entity (A) but list of intermediate CPNS Entity to the Entity (D) is not known.

Note: The intention of the figure is not syntax definition but to show the image of common parameter set for particular routing model.

In request message, Entity (A) sends a CPNS message to Entity (D).

- Target parameter contains the Entity ID of adjacent CPNS Entity, which the CPNS message is sent to.
- Source parameter contains the ID of Entity (A) showing the originator of the message.
- Since the routing path to Entity (D) is not known to Entity (A), the Destination parameter contains only the ID of Entity (D).
- In this model, since the TraceRoute parameter is included each intermediate CPNS Entity appends its Entity ID as the list of Route parameters under TraceRoute parameter.

In response message, Entity (D) sends back a CPNS message to Entity (A).

- Target parameter contains the Entity ID of adjacent CPNS Entity, which the CPNS message is send to.
- Source parameter contains the ID of Entity (D) showing the originator of the message.
- Since the routing path to Entity (A) is known to Entity (D) from received TraceRoute parameter, the Destination parameter contains not only destination Entity ID but also Entity IDs of intermediate CPNS Entities on the end to end routing path.

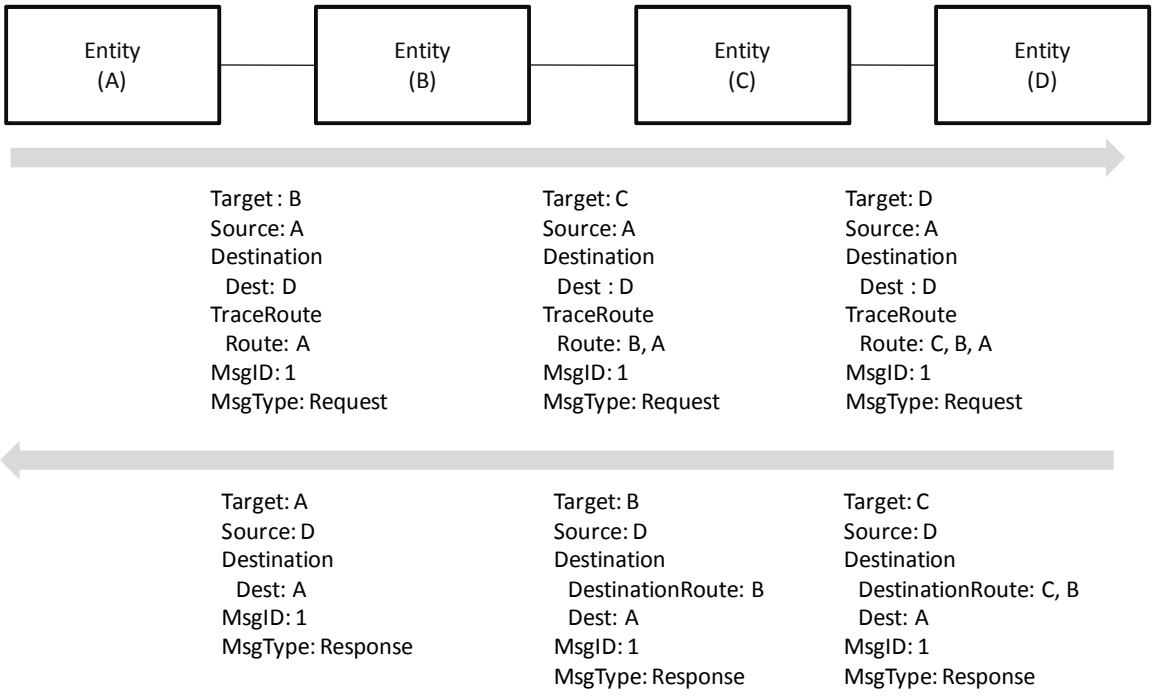


Table 81 routing path model for common parameter description