Converged Personal Network Service Architecture

Approved Version 1.0 – 23 Oct 2012

Open Mobile Alliance

OMA-AD-CPNS-V1_0-20121023-A

Contents

1. SCOPE (INFORMATIVE) 5
2. REFERENCES 6
2.1 NORMATIVE REFERENCES 6
2.2 INFORMATIVE REFERENCES 6
3. TERMINOLOGY AND CONVENTIONS 8
3.1 CONVENTIONS 8
3.2 DEFINITIONS 8
3.3 ABBREVIATIONS 8
4. INTRODUCTION (INFORMATIVE) 9
4.1 VERSION 1.0 9
5. ARCHITECTURAL MODEL 10
5.1 DEPENDENCIES 10
5.1.1 Interaction with Device Management Enabler 10
5.1.2 Dependency on DPE 10
5.1.3 Dependency on DRM 10
5.2 ARCHITECTURAL DIAGRAM 10
5.2.1 Architecture principle 11
5.3 FUNCTIONAL COMPONENTS AND INTERFACES DEFINITION 11
5.3.1 Functional Components 11
5.3.2 Functional Interfaces 12
5.4 SECURITY CONSIDERATIONS 15
5.5 FUNCTIONAL MODULES 15
5.5.1 Device Capabilities 15
5.5.2 Device Management 16
5.5.3 Status management 16
5.5.4 Usage Statistics Collection & Reporting 16
5.5.5 Service Publication & Discovery 17
5.5.6 CPNS Entity Discovery & PN Registration 17
5.5.7 Security 18
5.5.8 Service/Content Delivery 18
5.5.9 Service Group Management 19
5.5.10 PN Management 19
APPENDIX A. CHANGE HISTORY (INFORMATIVE) 21
A.1 APPROVED VERSION HISTORY 21
APPENDIX B. CPNS LOGICAL ENTITIES AND PHYSICAL ENTITIES (INFORMATIVE) 22
B.1 TERMINOLOGY 22
B.2 CLIENT-SERVER DEPLOYMENT EXAMPLES 22
B.2.1 Basic Client-Server Deployment 22
B.2.2 Client-Server Deployment with Combined PNE & PN GW 23
B.3 PEER-TO-PEER DEPLOYMENT EXAMPLE 24
B.3.1 Peer-to-Peer Deployment with Dedicated Authentication/Authorisation Server 24
APPENDIX C. FUNCTIONAL DIAGRAM (INFORMATIVE) 26
APPENDIX D. FEASIBILITY STUDY OF SECURITY OF CPNS INTERFACES WHEN UTILIZING UNDERLYING NETWORK SECURITY MECHANISMS (INFORMATIVE) 27
D.1 SYSTEM ASSUMPTION 27
D.2 SECURITY OF CPNS INTERFACES 28
D.2.1 CPNS-1,6 28
D.2.2 CPNS-2, 3 and 7 28
D.2.2.1 Using IMS signaling channel 28
D.2.2.2 Using IMS media channel 29

D.2.3 CPNS-4 29
APPENDIX E. SERVICE PUBLICATION & DISCOVERY OVERVIEW (INFORMATIVE) 30
E.1 INTRODUCTION 30
E.2 DESCRIPTION 30
E.3 DHT AND OVERLAY ROUTING 30
APPENDIX F. ZONE BASED SERVICE (INFORMATIVE) 31
F.1 ZONE 31
F.2 PUSH SERVICE USING THE ZONE PN GW 31

Figures

Figure 1: CPNS Architecture Diagram 11
Figure 2: CPNS Logical Entities and Physical Entities 22
Figure 3: Basic Client-Server Deployment 23
Figure 4: Client-Server Deployment with Combined PNE & PN GW 24
Figure 5: Peer-to-Peer Deployment with Dedicated Authentication/Authorisation Server 25
Figure 6: Functional diagram 26
Figure 7: System assumption 28
Figure 8: High level architecture of Service Publication and Discovery functionality and operations 30
Figure 9: Example 8-node DHT and related overlay routing for Service Publication or Discovery 30

1. Scope (Informative)

The scope of the CPNS (Converged Personal Network Service) architecture document is to define the architecture for the CPNS v1.0 Enabler. This document provides the functional capabilities needed to support the Enabler as described in CPNS requirements document [CPNS-RD].

2. References

2.1 Normative References

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

[DM-AD] "Device Management Architecture", Open Mobile Alliance™, OMA-AD-DM-V1_3, URL:http://www.openmobilealliance.org/

[PRS-IMPS-AD] "Presence IMPS Architecture v1.3", Open Mobile Alliance™, OMA-AD-IMPS-V1_3, URL:http://www.openmobilealliance.org/

[PRS-SIMPLE-AD] "Presence SIMPLE Specification", Open Mobile Alliance™, OMA-AD-Presence_SIMPLE-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

[SEC_CF AD] "Security Common Functions Architecture", Open Mobile AllianceTM, OMA-AD-SEC_CF-V1_1,

URL: http://www.openmobilealliance.org/

2.2 Informative References

[3GPP TS 33.203] "3G security; Access security for IP-based services"

E.g. 3GPP TS 33.203 (Release 9)

http://www.3gpp.org/ftp/Specs/html-info/33203.htm

[3GPP TS 22.127] "Service requirement for the Open Services Access (OSA); Stage 1"

E.g. 3GPP TS 22.127 (Release 8)

http://www.3gpp.org/ftp/Specs/html-info/22127.htm

[3GPP TS23.198] "Open Service Access (OSA); Stage 2"

E.g. 3GPP TS 23.198 (Release 8)

http://www.3gpp.org/ftp/Specs/html-info/23198.htm

[3GPP TR 33.828] "IMS media plane security"

E.g. 3GPP TR 33.828 (Release 8)

http://www.3gpp.org/ftp/Specs/html-info/33828.htm

[Bluetooth Security White Paper] "Bluetooth Security White Paper"

Bluetooth SIG Security Expert Group,

http://grouper.ieee.org/groups/1451/5/Comparison of PHY/Bluetooth_24Security_Paper.pdf

[DLNA] http://www.dlna.org/home

[IEEE802.11i] "IEEE Standard 802.11i-2004: Wireless Medium Access Control(MAC) and Physical Layer(PHY) Specifications Amendment 6: Medium Access Control(MAC) Security Enhancements"

[OMA-AD-DPE] "Device Profile Evolution Architecture", Open Mobile Alliance™, OMA-AD-DPE-V1_0, URL:http://www.openmobilealliance.org/

[OMADICT] "Dictionary for OMA Specifications", Version 2.8., Open Mobile Alliance™, OMA-ORG-Dictionary-V2.8, URL:http://www.openmobilealliance.org/

[OMA-DRM-AD] "Digital Rights Management (DRM) Architecture v2.1", Open Mobile Alliance™, OMA-AD-DRM-V2_1, URL:http://www.openmobilealliance.org/

[P2PSIP Internet-Draft] "REsource LOcation And Discovery (RELOAD) Base Protocol", C. Jennings, B. Lowecamp, E. Rescorla, S. Baset, H. Schulzrinne, Nov 9, 2009,

URL: http://www.ietf.org/id/draft-ietf-p2psip-base-06.txt

[UPnP Forum] http://www.upnp.org

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 are normative, unless they are explicitly indicated to be informative.

3.2 Definitions

Entity-User Key	A security key assigned to each PNE(s) and PN GW(s) for ensuring security of communication through CPNS interfaces
Group Key	A security key which all member entities in the same Service Group share and is used for secure communication in the Service Group
Group Key Management	The process of managing keys for groups
Keyword	A term that captures the essence of an application or content service accessible in CPNS, and is intended for use in Service Discovery to search for the corresponding service description. Keywords maybe stored in a centralized or distributed fashion in CPNS.
Metadata Directory	In the context of Service Publication and Discovery, a logical repository of service metadata comprising keywords and/or service description documents. Those metadata are published on the Metadata Directory by the Service Offerer, and discovered by the Service Consumer. A Metadata Directory may be stored centrally, or in a distributed manner, on the CPNS Server(s).
Service Consumer	A PNE that consumes service(s) provided by Service Offerer(s), upon performing Service Discovery.
Service Description	A document that contains service metadata, and is specified using a description language.
Service Offerer	A PNE or external Application/Content Server that offers a service for consumption by other PNEs acting as Service Consumers, and which publishes metadata about that service on a Metadata Directory.

3.3 Abbreviations

3GPP	3rd Generation Partnership Project
DLNA	Digital Living Network Alliance
DRM	Digital Rights Management
DPE	Device Profile Evolution
PNE	Personal Network Element
PN GW	Personal Network Gateway
OMA	Open Mobile Alliance
SSL	Secure Socket Layer
TLS	Transport Layer Security
UICC	Universal Integrated Circuit Card
UPnP	Universal Plug and Play

4. Introduction (Informative)

This Architecture Document defines the architecture of CPNS (Converged Personal Network Service) Enabler based on the CPNS requirements defined in [CPNS-RD].

This Architecture Document will define the functional interfaces between the CPNS entities themselves and between CPNS entities and other External entities.

This document will also describe and define the following functions and capabilities:

- Functions of CPNS Server
- Functions of PN GWs
- Functions of PNEs
- Interactivity between services and entities in the Personal Network and WAN/Cellular networks
- Content and Service delivery
- Service Discovery and Publication
- CPNS entity Discovery and PN registration
- Statistics collection and reporting of data and service usage
- Device capabilities of CPNS entities
- Management of PN
- Security related function

4.1 Version 1.0

The Architecture Document of CPNS Enabler 1.0 addresses the requirements targeted for this release that are solved by architecture design.

However, this release of the AD does not address the requirements that were deferred for future releases, such as requirements on peer-to-peer implementation, charging third parties for delivering the information to them and etc.

5. Architectural Model

The architecture model is based on the requirements defined in [CPNS-RD].

5.1 Dependencies

The CPNS Enabler will be dependent on the following:

5.1.1 Interaction with Device Management Enabler

NOTE: This dependency with OMA DM is optional.

CPNS entities can interact with DM Enabler for device management. For those CPNS entities which has DM client can be managed by DM server. The DM management could be initiated by DM client on CPNS entities or DM server.

PN GW may forward DM messages between DM server and PNE or may convert DM messages between DM Server and PNE.

In this case, CPNS entities SHALL conform to the functionality and interfaces as described in [DM-AD].

5.1.2 Dependency on DPE

The CPNS Enabler is dependent on the OMA DPE Enabler. This dependency is optional.

CPNS entities can interact with DPE Enabler to provide/obtain device capabilities.

CPNS entities (e.g. PNE, PN GW) can act as DPE clients to notify the DPE Server on device capabilities of PNEs and PN GWs respectively. Thus, entities, e.g. CPNS Server that would be interested in CPNS device capabilities could subscribe to the DPE Server and would be notified every time there would be a device capability change.

In this case, CPNS entities will comply with functionalities and interfaces as described in [OMA-AD-DPE]

5.1.3 Dependency on DRM

The CPNS Enabler is dependent on the OMA DRM Enabler. This dependency is optional.

CPNS entities can interact with DRM Enabler to protect CPNS content.

When CPNS content is required to be protected, DRM service is invoked through the CPNS server or through external entities, e.g. Content server.

In this case, CPNS entities will comply with functionalities and interfaces as described in **[**OMA-DRM-AD**].**

5.2 Architectural Diagram

Figure 1 shows the architectural diagram of OMA CPNS v1.0.

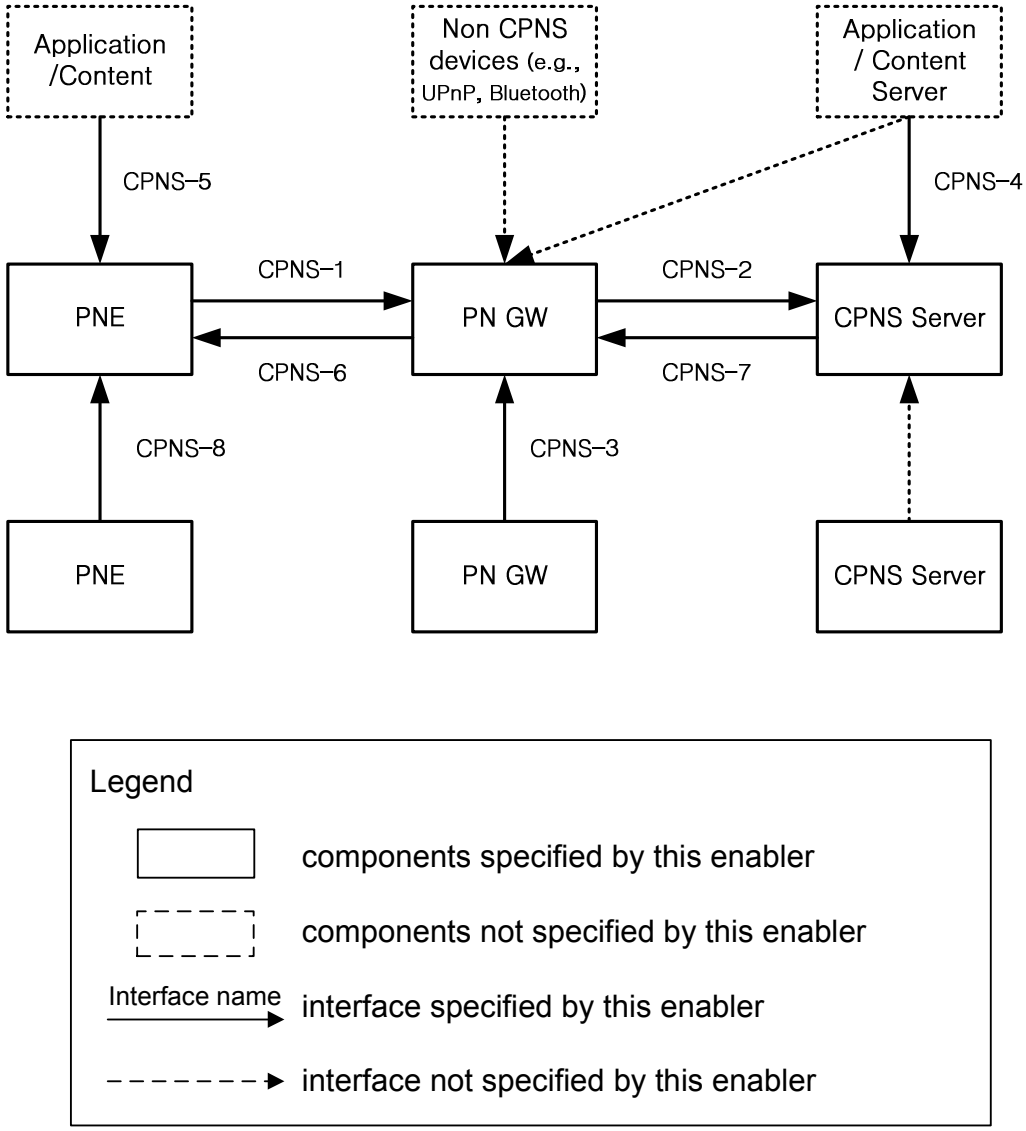

Figure 1: CPNS Architecture Diagram

5.2.1 Architecture principle

CPNS architecture consists of logical entities (i.e., PNE, PN GW, and CPNS Server). From the architectural perspective, the physical deployments are not restricted as far as capability of physical devices allow.

CPNS Enabler is agnostic to underlying network protocols.

5.3 Functional Components and Interfaces definition

5.3.1 Functional Components

This section describes the OMA CPNS v1.0 functional components.

5.3.1.1 CPNS Server

The CPNS Server is a CPNS Enabler component that resides in the core network performs the following functions:

- Device Capabilities
- Usage Statistics Collection & Reporting
- Service Publication & Discovery
- CPNS Entity Discovery & PN Registration
- Service and Content Delivery
- PN Management
- Service Group Management
- Security-related functions
- Status Management

5.3.1.2 PN GW

The PN GW is a CPNS Enabler component that performs the following functions:

- Device Capabilities
- Status Management
- Usage Statistics Collection & Reporting
- CPNS Entity Discovery & PN Registration
- Service and Content Delivery
- PN Management
- Service Group Management
- Security-related functions

5.3.1.3 PNE

The PNE is a CPNS Enabler component that resides on the personal network and performs the following functions:

- Device Capabilities
- Status Management
- Usage Statistics Collection & Reporting
- CPNS Entity Discovery & PN Registration
- Service and Content Delivery
- PN Management
- Service Group Management
- Security-related functions

NOTE: Please refer the section 5.5. for the details of each functions.

5.3.2 Functional Interfaces

This section describes the OMA CPNS v1.0 functional interfaces.

5.3.2.1 CPNS-1

This interface exposed by the PN GW supports the following functions.

- Device Capabilities
- Device Management
- Status Management
- Service Publication and Discovery
- Usage Statistics Collection and Reporting
- CPNS Entity Discovery and PN Registration
- Service / Content Delivery
- PN Management
- Service Group Management
- Security

5.3.2.2 CPNS-2

This interface exposed by CPNS Server supports the following functions.

- Device Capabilities
- Status Management
- Service Publication and Discovery
- Usage Statistics Collection and Reporting
- CPNS Entity Discovery and PN Registration
- Service / Content Delivery
- PN Management
- Service Group Management
- Security

5.3.2.3 CPNS-3

This interface exposed by PN GW supports the following functions.

- Service / Content Delivery
- Service Group Management
- Security

Note: this interface will be standardized in the future release after CPNS1.0

5.3.2.4 CPNS-4

This interface exposed by CPNS Server supports the following functions.

- Device Capabilities
- Usage Statistics Collection and Reporting
- Service Publication and Discovery

- Charging
- Service / Content Delivery

5.3.2.5 CPNS-5

This interface exposed by PNE supports the following functions.

- Service Publication and Discovery
- Service / Content Delivery
- Device Capabilities
- Status Management
- Usage Statistics Collection and Reporting
- PN Management
- Service Group Management

5.3.2.6 CPNS-6

This interface exposed by PNE supports the following functions.

- Device Capabilities
- Device Management
- Status Management
- Service Publication and Discovery
- Usage Statistics Collection and Reporting
- CPNS Entity Discovery and PN Registration
- Service / Content Delivery
- PN Management
- Service Group Management
- Security

5.3.2.7 CPNS-7

This interface exposed by PN GW supports the following functions.

- Device Capabilities
- Status Management
- Service Publication and Discovery
- Usage Statistics Collection and Reporting
- CPNS Entity Discovery and PN Registration
- Service / Content Delivery
- PN Management
- Service Group Management
- Security

5.3.2.8 CPNS-8

This interface exposed by PNE supports the following functions.

- CPNS Entity Discovery and PN Registration

Note: only the Entity Discovery within the same PAN is performed through this interface.

5.4 Security Considerations

The Converged Personal Network Service Enabler 1.0 provides the means to ensure security in CPNS including authentication, authorization, data integrity and data confidentiality.

If security mechanism is provided by the underlying network infrastructure (e.g., a cellular system) and its security level of the underlying network infrastructure is sufficient, the security function can utilize the security mechanism from the infrastructure. Otherwise, the security function utilizes CPNS Enabler's own security mechanism for the CPNS Service.

The CPNS Enabler 1.0 supports:

- Authentication/authorization of CPNS Users/CPNS Entities by Entity User Key
- Protection of data integrity and confidentiality
- Security-key (i.e. Entity User Key and Group Key) management
- Secure content/service sharing inside Service Groups by Group Key

As for the first two bullets, there is a suitable mechanism specified in OMA SEC_CF [SEC_CF AD]. In addition, OMA SEC_CF can be a solution for the third bullet when security-key is assigned to PN GW with pre-configured credential (e.g., UICC).

The security function is described in 5.5.7.2.

5.5 Functional Modules

5.5.1 Device Capabilities

5.5.1.1 Definition/role

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.

5.5.1.2 Description

This function permits the collection and delivery of information about the static or rarely changed parameters of the device as shown below.

- Device type, e.g. 3G handset, MP3 player, Settop Box…
- Hardware characteristics of a device, e.g. the size of the screen, the size of the battery, the type of µprocessor, the size of the memory, the type of chipset (main chipset, accelerator chipset, network chipset…)
- Software characteristics of a device, e.g. Installed applications, the version of the applications, the drivers for the hardware components, the versions of the drivers…

This function also permits the collection and delivery of information about dynamic parameters of the device as shown below.

- Current networks that the device connects to, e.g. UMTS network, CDMA, GSM, WIFI, Bluetooth, NFC…
- Current hardware status, e.g. currently available memory, current estimated remaining battery time, etc.

- Current software status, e.g. currently running applications, currently active drivers, etc.

In addition, this function collects, updates and manages the device capabilities in the way suitable for the CPNS service

OMA DPE Enabler facilitates the delivery of device capabilities, both static and dynamic device information to the CPNS server.

CPNS Enabler when appropriate may use DPE Enabler to make available the static and dynamic device information. If and when implemented OMA DPE Enabler can interact with the CPNS Enabler via the interfaces defined by the OMA DPE Enabler.

5.5.2 Device Management

5.5.2.1 Definition/Role

This function enables device management for PN GW and PNE.

5.5.2.2 Description

This function allows PNE and PN GW to be managed by interaction with device management (DM) server. The device management of PNE is performed through PN GW. PNE MUST deploy DM client for the device management. PN GW interacts with DM server. For the purpose of device management, PN GW may forward DM messages between DM server and PNE or may convert DM messages between DM Server and PNE. The examples of device management are firmware update, software update, device capability configuration and so on.

NOTE 1: How to Interact with Device Management server is out of CPNS scope.

5.5.3 Status management

5.5.3.1 Definition/role

This function provides a means for CPNS entities to publish, collect, subscribe to and notify the status of the CPNS entities.

5.5.3.2 Description

This function allows following status management functions.

- Status information report
    - In response to status information retrieval request, status information can be reported to requester.
    - Under certain circumstances triggered by a specific event (threshold hit, etc.), status information can be reported to target CPNS entity.
        - In occurrence of the event, status information is reported to the CPNS entity who requests the policy based status information report

This function provides information about:

- Status of PNE and PN GW(e.g. Online, Offline, Busy, etc)

5.5.4 Usage Statistics Collection & Reporting

5.5.4.1 Definition/role

This function is used to collect, summarise, and report;

- The use of the services in the CPNS entity
- The device capabilities applied when the services are consumed.

5.5.4.2 Description

This function allows:

- The collection of all the information from the devices about the service usage and the device capabilities and status during the service usage
- Applying user preferences for usage statistics reporting of each service consumption (e.g. IPTV viewing is not allowed to be reported, but game play is)
- Reporting to the CPNS server(s) and external entities according to the user preferences as required.

5.5.5 Service Publication & Discovery

5.5.5.1 Definition/role

The Service Publication and Discovery function provides the means by which service description is published by external entities and PNEs and subsequently can be discovered by PNEs through the CPNS server.

5.5.5.2 Description

This function performs following sub-functions:

- Publish service description
- Discover and retrieve service description
- Deliver and receive the service description to/from the relevant entity
- Advertise service description
- Store service description in the CPNS Server offered by PNEs and/or External entities

The service descriptions of service offered by PNE or external entities (e.g., an application/content server owned by the service provider or a 3rd party provider) mainly contain information such as;

- what services are available to CPNS user
- source of the service (i.e., CPNS entity identification, service identification, service requirement or capability of device hosting the service)

5.5.6 CPNS Entity Discovery & PN Registration

5.5.6.1 Definition/Role

This function enables discovery of the current operational CPNS Mode (PNE or PN GW) in a device and registration of the Personal Network for CPNS Services.

5.5.6.2 Description

This function facilitates discovery of CPNS entities by other CPNS entities and PN to be registered to CPNS Server. With the discovery function, a CPNS entity knows the role of other CPNS entities.

The PN GW when used for Zone Based Service performs the periodic searching for discovering PNE(s)

NOTE: in the case of discovery, CPNS server is not included in the CPNS entities.

This function facilitates registration of information of PNE(s) and PN GW in PN Inventory stored in CPNS Server.

5.5.7 Security

5.5.7.1 Definition/role

The function provides the means to ensure security in CPNS such as authentication, authorization, data integrity and data confidentiality. If security mechanism is provided by underlying network infrastructure (e.g., cellular system) and its security level is sufficient, the function can utilize security mechanism provided by underlying network infrastructure.

5.5.7.2 Description

The function in each CPNS entity performs the following security operations. Depending on security mechanisms provided by underlying network, part of the following operations can be achieved by underlying network.

- Each CPNS entity authenticates and authorizes CPNS entity connecting through CPNS interface.
- Each CPNS entity ensures data authenticity, integrity and confidentiality of the communication through the interface. This can be done by establishing secure session (e.g. SSL/TLS session) between CPNS entities.
- CPNS Server or PN GW provisions an Entity-User Key in CPNS entity. For secure key provisioning, key provision signalling is intermediated by PN GW connected to secure underlying network.
- CPNS Server or PN GW creates, deletes and updates a Group Key when Service Group is created, deleted and its membership is updated, respectively. It also distributes the Group Key to group members by either of push or pull based method in a secure manner.

5.5.8 Service/Content Delivery

5.5.8.1 Definition/role

The Service/Content Delivery function facilitates the delivery of service/content to/from the CPNS and External entities, Between the PNEs and PN GWs:

- Between PN GWs and CPNS server
- Between CPNS Server and External entities
- Between PN GW and External entities

Service/Content Delivery function also facilitates the content forwarding from one serviced PNE to another PNE

5.5.8.2 Description

Service /Content Delivery Function Features the following:

- Invoking Services based on device capability
- Service Control (e.g. start, stop)
- Two Service/Content delivery modes: Push/ Pull
- Supporting single/ multiple services
- Aggregation and distribution for multiple PNEs,
    - Aggregation of common and specific data for multiple PNEs
    - Distribution of common and specific data to the respective PNE(s)
- Non-CPNS Device Proxy

This is a proxy that allows the user to use suitable devices, e.g. devices supporting UPnP [UPnP Forum], DLNA [DLNA] and Bluetooth, to consume provided CPNS services.

The proxy is implemented in the PN Gateway. The purpose of the proxy is to make the devices look like CPNS PNEs when viewed from the CPNS Enabler. In the case of UPnP/DLNA, this is done by mapping the required CPNS functionality to the relevant UPnP/DLNA functions.

5.5.9 Service Group Management

5.5.9.1 Definition/role

This function provides the means to manage a Service Group.

5.5.9.2 Description

This function does the following:

- Handles requests regarding Service Group management
- Manages Service Group membership
- Enables PNE and PN GW to request following:
    - Create and delete a Service Group
    - Invite and expel PNE(s) to/from a Service Group
    - Join and leave a Service Group

5.5.10 PN Management

5.5.10.1 Definition/role

This function provides the means to manage a Personal network, and to update PN Inventory.

5.5.10.2 Description

This function manages PN and PN Inventory.

PN Management functionality in CPNS Server performs following operations:

- Manage and store PN Inventory
- Handle request(s) from PNE for PN Inventory of local PN or remote PN
- Handle request(s) from PNE to join, leave and remove PN
- Handle request(s) from PNE to add and expel other PNEs

PN Management functionality in PN GW performs following operations:

- Manage and store PN Inventory of PN that belongs to itself
- Request to remove a PN
- Request to add /expel PNE(s) to/from the PN

PN Management functionality in PNE performs following operations:

- Request for PN Inventory
- Request to add / expel PNE(s) to/from PN
- Request to join / leave PN
- Request to remove a PN

The PN Inventory may include list of PN(s) and the information of PNE(s) and PN GW(s) belonging to a PN. The information of PNE(s) contains device capability and information of service / content. The PN Inventory in CPNS Server can

contain the information about PNs from multiple PN GWs, while the PN Inventory in a PN GW can contain the information of PN(s) belonging to the PN GW itself.

Appendix A. Change History (Informative)

A.1 Approved Version History

Reference	Date	Description
Approved Version OMA-AD-CPNS-V1_0	23 Oct 2012	Status changed to Approved by TP: TP ref#: OMA-TP-2012-0390-INP_CPNS_1_0_ERP_for_notification.zip

Appendix B. CPNS Logical Entities and Physical Entities(Informative)

B.1 Terminology

In the figures in this appendix, interior boxes represent logical entities, and exterior boxes represent physical entities. The terms ‘Mobile Phone’, ‘PMP’ and ‘Server’ refer to physical entities. The logical CPNS Server entity is referred to as ‘CS’, and “Application/Content Entity” (ACE) refers to the entities (external to CPNS) that use CPNS to consume and offer services.

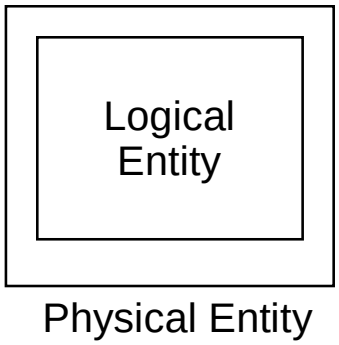

Figure 2: CPNS Logical Entities and Physical Entities

B.2 Client-Server Deployment Examples

B.2.1 Basic Client-Server Deployment

The first deployment example shows a basic client-server deployment with a CPNS logical entity in Mobile Phone A, Mobile Phone B and Server 1.

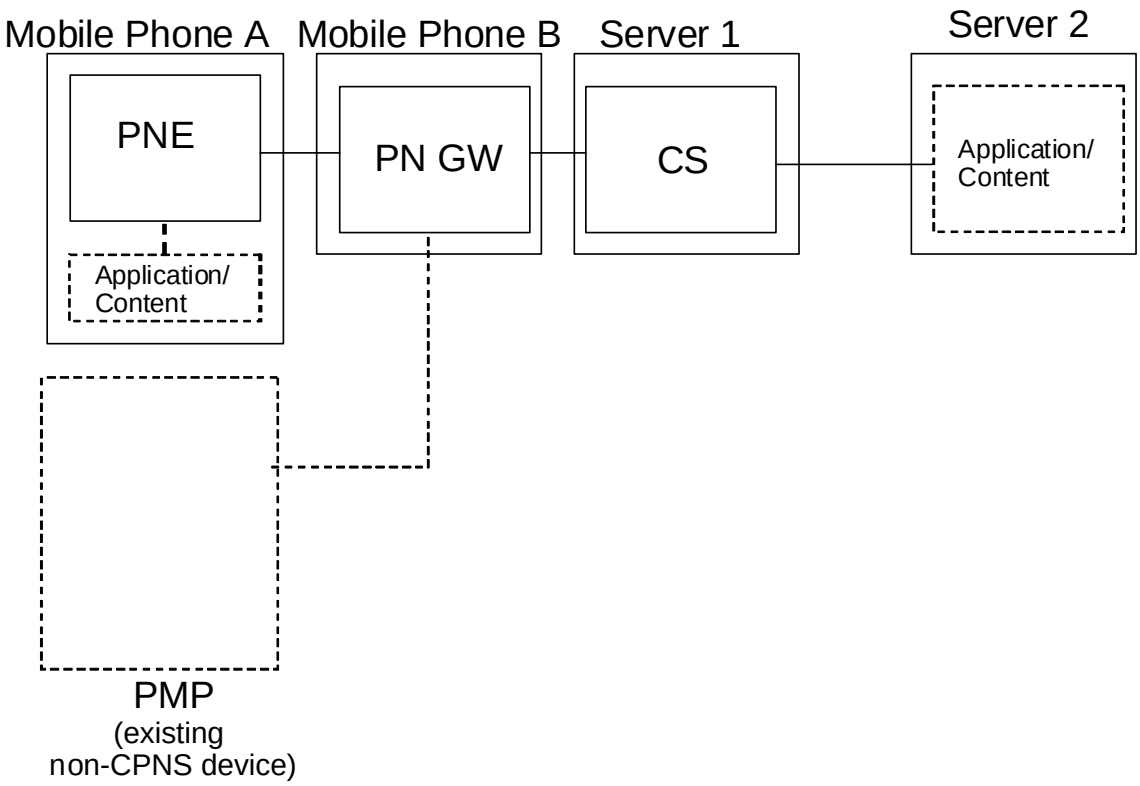

Figure 3: Basic Client-Server Deployment

B.2.2 Client-Server Deployment with Combined PNE & PN GW

The second deployment example shows the same client-server deployment as in the first example, except that Mobile Phone B is a smart phone that can also offer and consume CPNS services in addition to the PN GW role.

To enable this, Mobile Phone B on the next slide assumes the additional role of a PNE so that it can interface with the ACE(s) on Mobile Phone B that offer and consume services

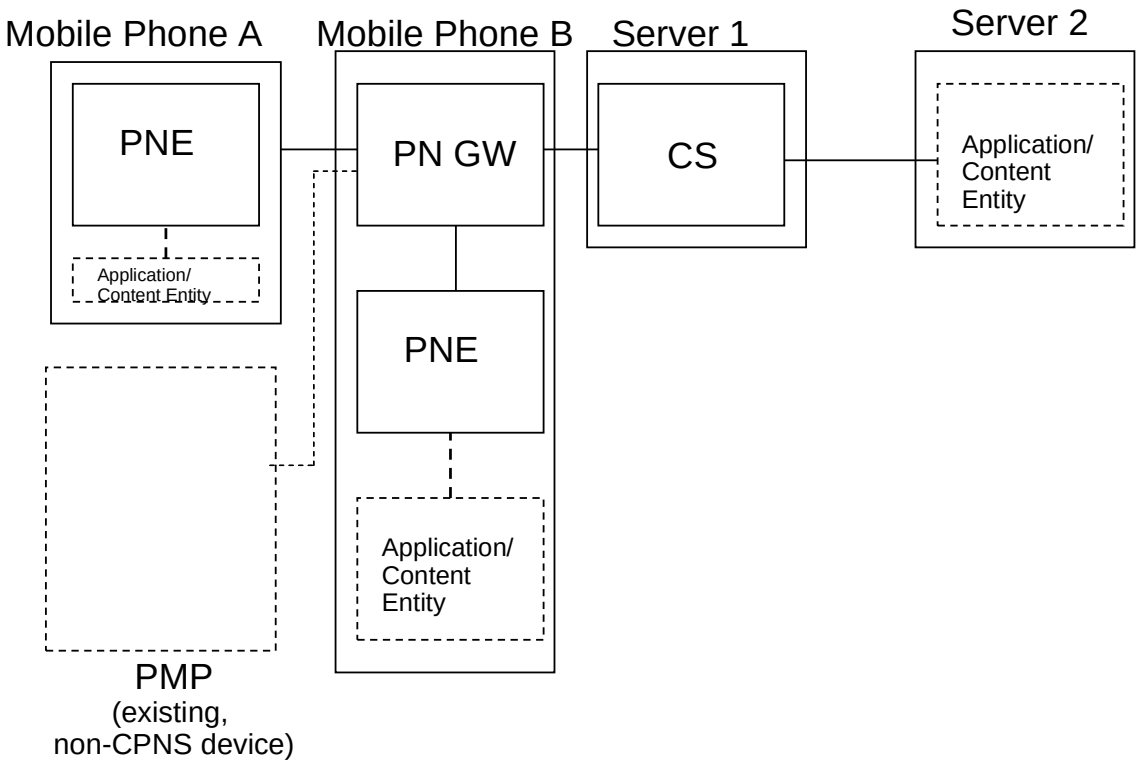

Figure 4: Client-Server Deployment with Combined PNE & PN GW

B.3 Peer-to-Peer Deployment Example

B.3.1 Peer-to-Peer Deployment with Dedicated Authentication/Authorisation Server

A CPNS deployment in which the CS Service Publication and Discovery is implemented on the Devices in a CPNS network, while the CS AUC/AUZ function is performed by a Server

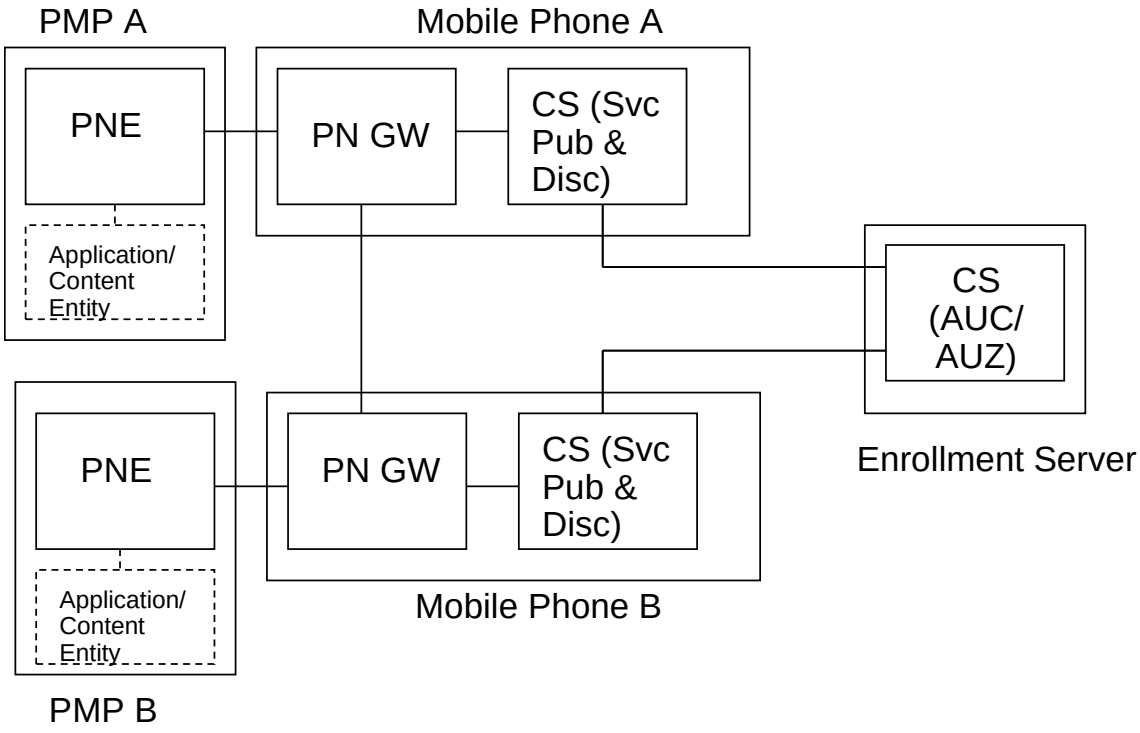

Figure 5: Peer-to-Peer Deployment with Dedicated Authentication/Authorisation Server

Appendix C. Functional Diagram (Informative)

This figure shows the functional diagram of OMA CPNS v1.0

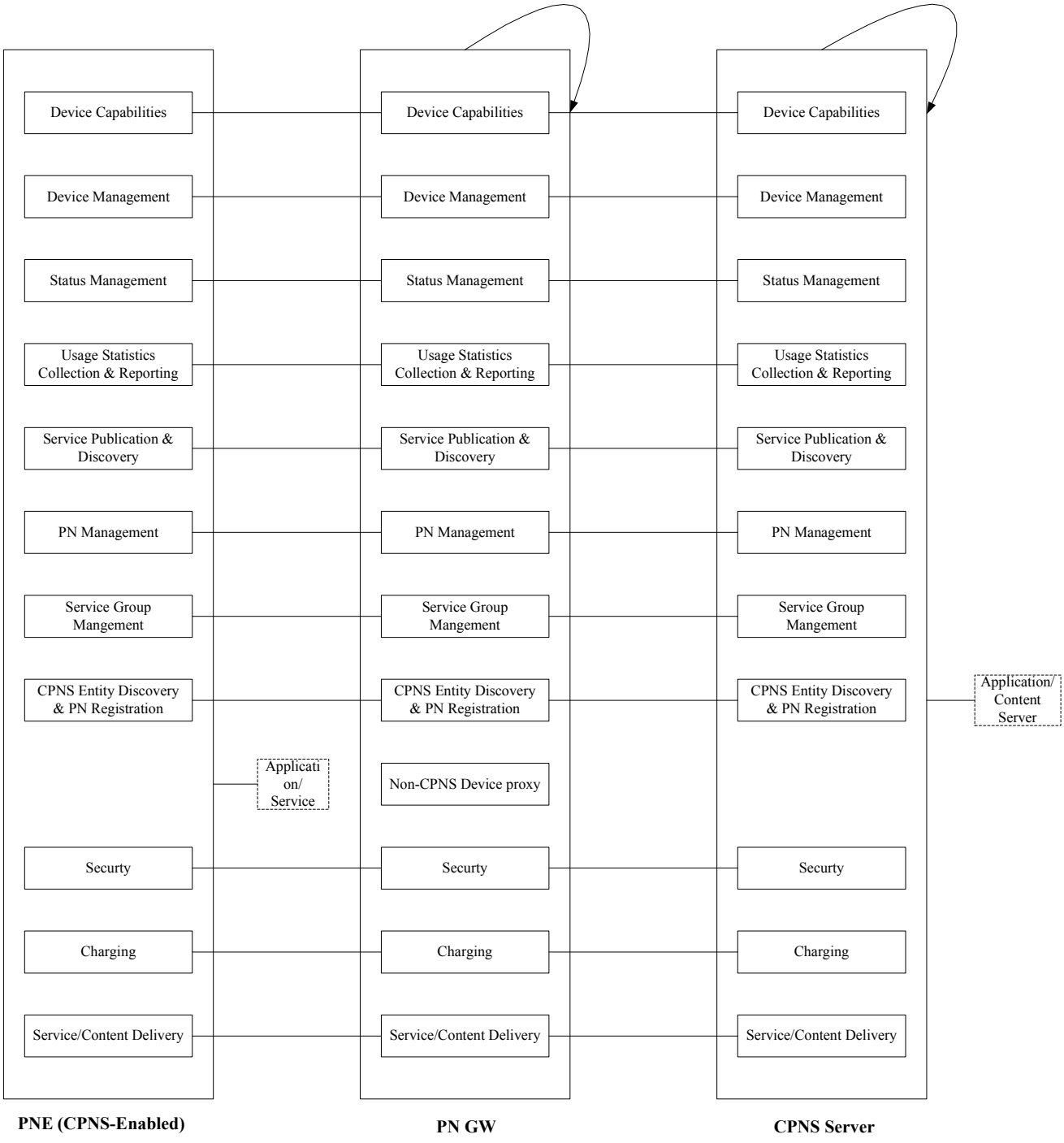

Figure 6: Functional diagram

Appendix D. Feasibility study of security of CPNS interfaces when utilizing underlying network security mechanisms (Informative)

As described in section 5.3.1.9, CPNS Enabler can utilize security mechanisms provided by underlying network infrastructures to ensure communication security in CPNS. This section shows an example scenario where CPNS Enabler ensures security by utilizing security mechanisms of underlying network infrastructures.

D.1 System Assumption

Figure 15 shows an example of the proposed security platform. Underlying network infrastructures assumed in this example are as follows.

- WAN

  As the underlying WAN infrastructure, IMS (IP Multimedia Subsystem) is deployed. Since IMS provides security mechanisms, which will be described later in the next sub section, WAN in this example is a secure WAN.

  CPNS Servers and PN GWs connect to IMS as IMS application servers (ASs) and subscribers, respectively.

- PN

  It is assumed that PN technologies with security mechanisms are used. Examples of such PN technologies include WiFi and Bluetooth [IEEE802.11i, Bluetooth Security White Paper].

  PN GWs and PNEs are connected by using those technologies.

Communication of each CPNS interface is conducted on the following network infrastructures.

- CPNS-1,6: PN technologies with security mechanisms
- CPNS-2, 3 and 7: IMS (secure WAN)
- CPNS-4: The Internet (non-secure WAN)

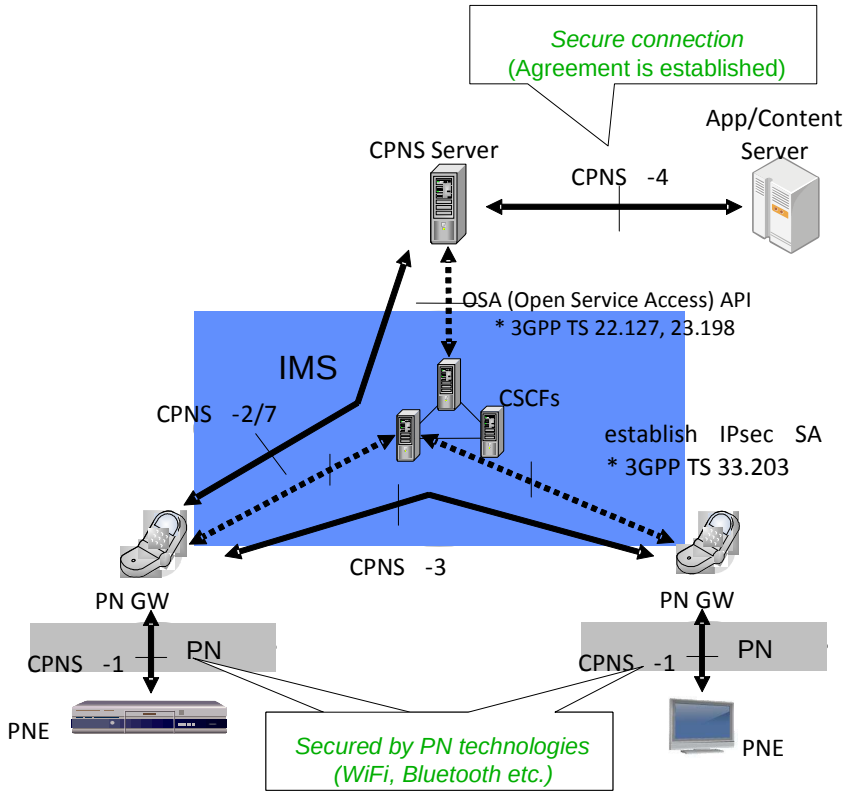

Figure 7: System assumption

D.2 Security of CPNS Interfaces

D.2.1 CPNS-1,6

When using WiFi as the PN technology, one of typical ways to ensure security of CPNS-1,6 is to pre-configure a shared secret key like a WEP key in both PN GW and PNE before starting communication. By doing this, PN GW and PNE can authenticate with each other and data confidentiality and integrity can be also ensured.

When using Bluetooth as the PN technology, PN GW and PNE can establish a secure connection by means of the initial pairing process. During this process, a user enters a PIN code to one or both of them, which is used to generate a secure key, which is then used for authentication and ensuring data confidentiality and integrity.

D.2.2 CPNS-2, 3 and 7

Security of CPNS-2, 3 and 7 can be ensured by IMS security mechanisms. Two different scenarios can be assumed: (1) Messages of the CPNS interfaces are exchanged using IMS signalling channel (i.e. C-plane) and (2) Messages of the CPNS interfaces are exchanged using IMS media channel (i.e. U-plane). The following sub sections explain how security is ensured in those scenarios.

D.2.2.1 Using IMS signaling channel

When PN GWs registers with IMS, PN GWs and IMS authenticate each other and establish secure connections by IPSec [3GPP TS 33.203]. By using the secure connections, PN GWs can securely send or receive SIP messages to/from IMS. When CPNS Servers connect with IMS via OSA (Open Service Access) API [3GPP TS 22.127, 3GPP TS23.198], providers of CPNS Servers need to establish service agreements with IMS providers. The service agreements require that CPNS Servers

and SCS (Service Capability Server) on IMS authenticate each other and establish secure connections by IPSec or SSL. As a result, since SIP messages between PN GWs and CPNS Servers are passed through the IPSec connection between PN GWs and IMS and the secure connection between IMS and CPNS Servers, data confidentiality and integrity of CPNS signalling messages can be ensured.

D.2.2.2 Using IMS media channel

IMS media channel security between UEs has been almost standardized in 3GPP [3GPP TS 33.328]. In the specification, there are two solutions, including solutions based on Key Management Service (KMS) and Session Description Protocol Security Descriptions (SDES). By applying these solutions, communication in the CPNS-3 can be secured.

D.2.3 CPNS-4

In the system assumption described in B.1, CPNS Servers and application/content servers connects with each other through the Internet (non-secure WAN) In order to provide secure content/service delivery services over the non-secure WAN, providers of CPNS Servers and application/content servers conclude security agreements. In such a scenario, secure connection can be based on IPSec or SSL between CPNS Servers and application/content servers. During the establishment of secure connection, CPNS Servers and application/content servers can authenticate with each other. After the establishment, data confidentiality and integrity can be also ensured.

Appendix E. Service Publication & Discovery overview (informative)

E.1 Introduction

This clause provides supplemental description of Service Publication & Discover function.

E.2 Description

There are three functional entities in Service Publication and Discovery: a) a metadata directory which stores service descriptions and/or keywords, b) a publisher, used by the service offerer to publish information about services to the metadata directory, and c) a discoverer, used by the service consumer to discover information about services from the metadata directory.

An example of a metadata directory is one that is maintained on the network- based CPNS Server or an external entity. An illustration of the above functions, and associated interactions, is shown in Figure x as below:

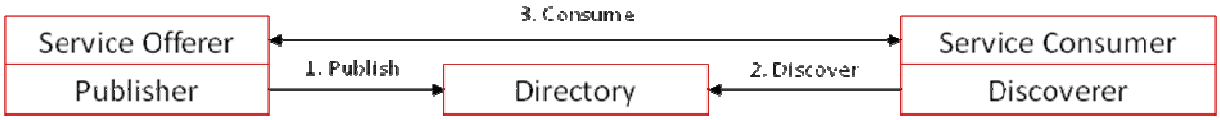

Figure 8: High level architecture of Service Publication and Discovery functionality and operations

E.3 DHT and Overlay Routing

In the deployment of distributed metadata directory, in order for either the service offerer to publish service information to, or the service consumer to discover service information from, the peer node responsible for the affiliated resource, overlay routing is performed. This operates by each responsible node (starting with the service offerer for publication, or service consumer for discovery) on the overlay routing the message to the finger closest to the destination node. An example of an 8-node DHT (Distributed Hash Table – see [P2PSIP Internet-Draft]) is shown in Fig. Y below, whereby node 100 is assumed to be either the service offerer or the service consumer, and node 800 contains the metadata directory. In this example, three hops are required to route the Service Publication or Discovery message from node 100 to node 800. It is assumed that each node in the diagram contains an integrated PN GW function that supports the overlay routing.

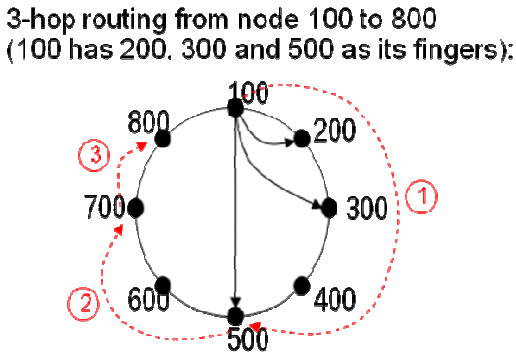

Figure 9: Example 8-node DHT and related overlay routing for Service Publication or Discovery

Appendix F. Zone Based Service (Informative)

F.1 Zone

The Zone in the CPNS service represents the specific geographic area which is determined by users or by the signalling capacities of bearer used. The Zone provides specific service/contents using a certain allocated PN GW.

In case of many CPNS users with their PNE(s) are located in the same Zone, the PNE(s) respectively constructs the Personal Network with the allocated Zone PN GW. The Zone PN GW may belong to the numerous PN(s).

F.2 Push service using the Zone PN GW

The Zone Based Service facilitates the content push service with CPNS enabler.

When the PNE comes to the Zone, with 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 receiving the request from PNE or input from the user.

Only by setting to reply on the PN GW's periodic search, a PNE can be pushed the contents or the service description information.

This service needs several preconditions described below:

- The target PNE(s) should be subscribed and authorized for the service beforehand.
- The target PNE(s) can be discovered, connected and serviced, only when allowed by the user(s).
- The PN GW should check if the PNE is available for pushing content.