



Presence SIMPLE
Architecture Document
Approved Version 1.0 – 25 Jul 2006

Open Mobile Alliance
OMA-AD-Presence_SIMPLE-V1_0-20060725-A

Use of this document is subject to all of the terms and conditions of the Use Agreement located at <http://www.openmobilealliance.org/UseAgreement.html>.

Unless this document is clearly designated as an approved specification, this document is a work in process, is not an approved Open Mobile Alliance™ specification, and is subject to revision or removal without notice.

You may use this document or any part of the document for internal or educational purposes only, provided you do not modify, edit or take out of context the information in this document in any manner. Information contained in this document may be used, at your sole risk, for any purposes. You may not use this document in any other manner without the prior written permission of the Open Mobile Alliance. The Open Mobile Alliance authorizes you to copy this document, provided that you retain all copyright and other proprietary notices contained in the original materials on any copies of the materials and that you comply strictly with these terms. This copyright permission does not constitute an endorsement of the products or services. The Open Mobile Alliance assumes no responsibility for errors or omissions in this document.

Each Open Mobile Alliance member has agreed to use reasonable endeavors to inform the Open Mobile Alliance in a timely manner of Essential IPR as it becomes aware that the Essential IPR is related to the prepared or published specification. However, the members do not have an obligation to conduct IPR searches. The declared Essential IPR is publicly available to members and non-members of the Open Mobile Alliance and may be found on the “OMA IPR Declarations” list at <http://www.openmobilealliance.org/ipr.html>. The Open Mobile Alliance has not conducted an independent IPR review of this document and the information contained herein, and makes no representations or warranties regarding third party IPR, including without limitation patents, copyrights or trade secret rights. This document may contain inventions for which you must obtain licenses from third parties before making, using or selling the inventions. Defined terms above are set forth in the schedule to the Open Mobile Alliance Application Form.

NO REPRESENTATIONS OR WARRANTIES (WHETHER EXPRESS OR IMPLIED) ARE MADE BY THE OPEN MOBILE ALLIANCE OR ANY OPEN MOBILE ALLIANCE MEMBER OR ITS AFFILIATES REGARDING ANY OF THE IPR'S REPRESENTED ON THE “OMA IPR DECLARATIONS” LIST, INCLUDING, BUT NOT LIMITED TO THE ACCURACY, COMPLETENESS, VALIDITY OR RELEVANCE OF THE INFORMATION OR WHETHER OR NOT SUCH RIGHTS ARE ESSENTIAL OR NON-ESSENTIAL.

THE OPEN MOBILE ALLIANCE IS NOT LIABLE FOR AND HEREBY DISCLAIMS ANY DIRECT, INDIRECT, PUNITIVE, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR EXEMPLARY DAMAGES ARISING OUT OF OR IN CONNECTION WITH THE USE OF DOCUMENTS AND THE INFORMATION CONTAINED IN THE DOCUMENTS.

© 2006 Open Mobile Alliance Ltd. All Rights Reserved.

Used with the permission of the Open Mobile Alliance Ltd. under the terms set forth above.

Contents

1. SCOPE (INFORMATIVE)	5
2. REFERENCES	6
2.1 INFORMATIVE REFERENCES	6
3. TERMINOLOGY AND CONVENTIONS	7
3.1 CONVENTIONS	7
3.2 DEFINITIONS	7
3.3 ABBREVIATIONS	7
4. INTRODUCTION (INFORMATIVE).....	9
4.1 TARGET AUDIENCE	9
4.2 REQUIREMENTS.....	9
5. CONTEXT MODEL (INFORMATIVE).....	10
5.1 COLLABORATION WITH SERVICE ENABLERS	10
5.2 COLLABORATION WITH DEVICE MANAGEMENT	10
5.3 COLLABORATION WITH XDM ENABLER	10
6. ARCHITECTURAL MODEL (INFORMATIVE)	11
6.1 SYSTEM AND SUBSYSTEM DESCRIPTIONS	11
6.1.1 Presence Functional Entities	11
6.1.1.1 Presence Server	11
6.1.1.2 Presence Source.....	12
6.1.1.3 Watcher.....	12
6.1.1.4 Resource List Server (RLS).....	12
6.1.1.5 XML Document Management Client (XDMC).....	12
6.1.1.6 Presence XML Document Management Server (Presence XDMS)	12
6.1.1.7 Resource List Server XML Document Management Server (RLS XDMS).....	12
6.1.1.8 Content Server	12
6.1.2 External Entities Providing Services to Presence	13
6.1.2.1 SIP/IP Core network.....	13
6.1.2.2 Shared XML Data Management Server (XDMS)	13
6.1.2.3 Aggregation Proxy.....	13
6.1.2.4 Device Management Server	13
6.1.3 Description of the Reference Points.....	13
6.1.3.1 Reference Point PRS-1: Presence Source – SIP/IP Core.....	14
6.1.3.2 Reference Point PRS-2: Watcher – SIP/IP Core network.....	14
6.1.3.3 Reference Point PRS-3: SIP/IP Core – Presence Server	14
6.1.3.4 Reference Point PRS-4: SIP/IP Core – Resource List Server	14
6.1.3.5 Reference Point PRS-5: Presence Server – Shared XDM Server.....	14
6.1.3.6 Reference Point PRS-6: Presence XDM Server – SIP/IP Core.....	15
6.1.3.7 Reference Point PRS-7: Aggregation Proxy – Presence XDM Server	15
6.1.3.8 Reference Point PRS-8: Presence Server - Presence XDM Server	15
6.1.3.9 Reference Point PRS-9: Resource List Server – Shared XDM Server.....	15
6.1.3.10 Reference Point PRS-10: Resource List Server – RLS XDM Server.....	15
6.1.3.11 Reference Point PRS-11: RLS XDM Server – SIP/IP Core	15
6.1.3.12 Reference Point PRS-12: RLS XDM Server – Aggregation Proxy.....	16
6.1.3.13 Reference Point PRS-13: Presence Source – Content Server.....	16
6.1.3.14 Reference Point PRS-14: Watcher – Content Server	16
6.1.3.15 Reference Point PRS-15: Presence Server – Content Server.....	16
6.1.3.16 Reference Point XDM-1: XDM Client – SIP/IP Core.....	16
6.1.3.17 Reference Point XDM-3: XDM Client- Aggregation Proxy.....	16
6.1.3.18 Reference Point XDM-2: Shared XDMS – SIP/IP Core	16
6.1.3.19 Reference Point XDM-4: Shared- Aggregation Proxy.....	16
6.1.3.20 Reference Point IP-1: SIP/IP Core network – External Presence Network (based on a SIP/IP Core).....	17
6.1.3.21 Reference Point DM-1: DM Client – DM Server.....	17
6.1.4 Presence Information Format.....	17
6.1.5 Privacy	17
6.1.5.1 Subscription Authorisation Rules.....	17

6.1.5.2	<i>Presence Content Rules</i>	17
6.1.6	Security	17
6.1.6.1	<i>SIP Signaling Security</i>	17
6.1.7	Charging.....	18
6.1.7.1	<i>Charging Architecture</i>	18
6.1.8	Registration	18
6.1.9	Presence Service Provisioning.....	18
APPENDIX A.	CHANGE HISTORY (INFORMATIVE)	19
A.1	APPROVED VERSION HISTORY	19

1. Scope

(Informative)

The scope of this document is to provide an architecture for the OMA presence service Enabler, which includes a general network-agnostic model, for mobile presence using the IETF SIMPLE specifications.

2. References

2.1 Informative References

OMA:

- [OMA DM] OMA Device Management, V1.1.2 (based on SyncML DM)
- [OMA XDMAD] “XML Document Management (XDM) Architecture, V 1.0”, Open Mobile Alliance
- [OMA PROAD] OMA – Provisioning Architecture Overview V1.1
- [OMA PROCONT] OMA – Provisioning Content V1.1
- [OMA PRESRD] “Presence Requirements“,OMA-RD_Presence-V1_0, Version 1.0, 21 September 2004, [URL:http://www.openmobilealliance.com/](http://www.openmobilealliance.com/)
- [OMA PROSEC] OMA - Provisioning Bootstrap V1.1
- [OMA PROUA] OMA – Provisioning User Agent Behaviour V1.1

IETF:

- [RFC2119] “Key words for use in RFCs to Indicate Requirement Levels”, S. Bradner. March 1997, (<http://www.ietf.org/rfc/rfc2119.txt>)
- [RFC2778] “A Model for Presence and Instant Messaging”, M. Day et al., Feb. 2000, RFC 2778, (<http://www.ietf.org/rfc/rfc2778.txt>)
- [RFC3265] “Session Initiation Protocol (SIP)-Specific Event Notification”, A.B.Roach, June 2002, RFC 3265, (<http://www.ietf.org/rfc/rfc3265.txt>)
- [RFC3856] “A Presence Event Package for the Session Initiation Protocol (SIP)”, J.Rosenberg, Aug. 2004, RFC3856, (<http://www.ietf.org/rfc/rfc3856.txt>)
- [RFC3863] “Presence Information Data Format (PIDF)”, H.Sugano et al., Aug 2004 (<http://www.ietf.org/rfc/rfc3863.txt>)
- [CONTENTIND] “A mechanism for Content Indirection in Session Initiation Protocol (SIP) Messages”, E. Burger, Oct. 2004. (<http://www.ietf.org/internet-drafts/draft-ietf-sip-content-indirect-mech-05.txt>)
- Note: IETF Draft Work in progress

3GPP / 3GPP2

- [3GPP TS 23.141] “Presence Service; Architecture and functional description”, 3GPP TS 23.141, Release 6, 2005
- [3GPP2 X.S0027-001-0] “Presence Service; Architecture and functional description”, Revision 0, Version 1.0, 3GPP2, 2004.
- [3GPP TS 23.228] “IP Multimedia Subsystem (IMS); Stage 2”, 3GPP TS 23.228, Release 6, 2005
- [3GPP2 X.S0013-002-A] “All-IP Core Network Multimedia Domain: IP Multimedia Subsystem - Stage 2”, Revision A, Version 1.0, 3GPP2, 2005
- [3GPP TS 24.141] “Presence service using the IP Multimedia (IM) Core Network (CN) subsystem; Stage-3“, 3GPP TS 24.141, Release 6, 2005
- [3GPP2 X.P0027-003-0] “Presence Service using IP Multimedia Core Network Subsystem; Stage 3”, Revision 0, Version 1.0, 3GPP2, 2005
- Note: 3GPP2 Work in progress.
- [3GPP TS 33.222] “Generic Authentication Architecture (GAA);
Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS)” 3GPP TS 33.222, Release 6, 2006

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

Context Collaboration Model	An extension of the Context Model. It expands on the Context Model by describing the interactions (collaborations) between the entities of this architecture and external entities (e.g. entities in other architectures).
Contextual Item	A logical entity in an architecture
Context Model	A model that identifies all contextual items relevant to understanding architecture.
Presence Information	Defined in [OMA PRESRD]
Presence Information Element	Defined in [OMA PRESRD]
Presence Reference Architecture	Replaced instances of “Presence Reference Architecture” with “Presence Architecture” and delete the definition.
Presence Source	Defined in [OMA PRESRD]
Presentity	Defined in [OMA PRESRD]
Watcher	Defined in [OMA PRESRD]

3.3 Abbreviations

3GPP	3 rd Generation Partnership Project
3GPP2	3 rd Generation Partnership Project 2
AD	Architecture Document
BAC	Browser and Content (OMA Working Group)
DM	Device Management
GAA	Generic Authentication Architecture
GS	Game Services (OMA Working Group)
IETF	Internet Engineering Task Force
MWG	Messaging Workin Group
MWS	Mobile Web services
OMA	Open Mobile Alliance

PoC	Push-to-talk over Cellular
RD	Requiremnt Document
RLS	Resource List Server
SIMPLE	SIP Instant Message and Presence Leveraging Extensions
SIP	Session Initiaion Protocol
TLS	Transport Layer Security
UE	User Equipment
URI	Uniform Resource Identifier
WG	Workin Group
XCAP	XML Configuration Access Protocol
XDM	XML Document Management
XML	Extensible Markup Language

4. Introduction (Informative)

The OMA Presence Enabler is a service that manages the collection and controlled dissemination of presence information over mobile networks. Multiple standards fora are working on presence. This section describes the OMA Presence Service and how it relates to similar work of other industry/standards fora.

The IETF has defined protocols and formats for presence in its SIMPLE (SIP Instant Messaging and Presence Leveraging Extensions) activity (see [RFC3856]). The work of OMA and other fora leverages these standards.

3GPP and 3GPP2 have defined an aligned Presence Service framework in [3GPP TS 23.141] and [3GPP2 X.S0027-001-0]. This framework has a defined presence reference architecture both in “network layer” and “application layer” meaning that 3GPP and 3GPP2 specifications [3GPP TS 24.141] and [3GPP2 X.P0027-003-0] respectively define end-to-end presence information flows. The term “network layer” refers to the communication that is required between the Presence Service functional elements (e.g. Presence Server) and various network elements as they are defined in the network architectures of 3GPP and 3GPP2 (e.g. MSC, HLR). The term “application layer” refers to the communication that is required between the various Presence Service elements (e.g. Presence Server and Presence Source), which includes the “application layer” functional entities.

Additionally, there are presence services that exist or can be envisaged that do not leverage core network infrastructure as defined by 3GPP and 3GPP2. However, those presence services are still relevant to the mobile domain and thus supported by this architecture.

4.1 Target Audience

The target audience for this document includes but is not limited to the following:

- The Working Group(s) that will create specifications based on this subject matter
- Working Groups that need to understand the architecture of this subject matter
- Architecture Working Group
- Interoperability Working Group (e.g. for early analysis of interoperability requirements)
- Security Working Group
- Mobile Commerce and Charging Working Group

4.2 Requirements

All the requirements as defined in the [OMA PRESRD] are met with this document.

5. Context Model (Informative)

5.1 Collaboration with Service Enablers

The Presence Enabler provides a variety of services that can be invoked from other Enablers. Those Enablers can assume one or both of the following roles:

- Presence Source: publishes presence information to the Presence Enabler.
- Watcher: subscribes to retrieve presence information from the Presence Enabler

5.2 Collaboration with Device Management

The Device Management Enabler can be utilised to configure terminals with relevant data. The Presence Enabler does not define interfaces between Device Management Clients and Presence Sources or Watchers.

5.3 Collaboration with XDM Enabler

The Presence Server also assumes the role of an XDMC in order to interact with an XDM service.

The Presence Server has three reference points to XDM related functional blocks (PRS-5, PRS-8, PRS-3). The presence specific XDMS box has three connections they are named (PRS-6, PRS-7, PRS-8). The XDM reference points are described in section 6.1.3. The PRS-3 reference point description could be found later in this document.

6. Architectural Model (Informative)

The following figure illustrates the OMA Presence architecture

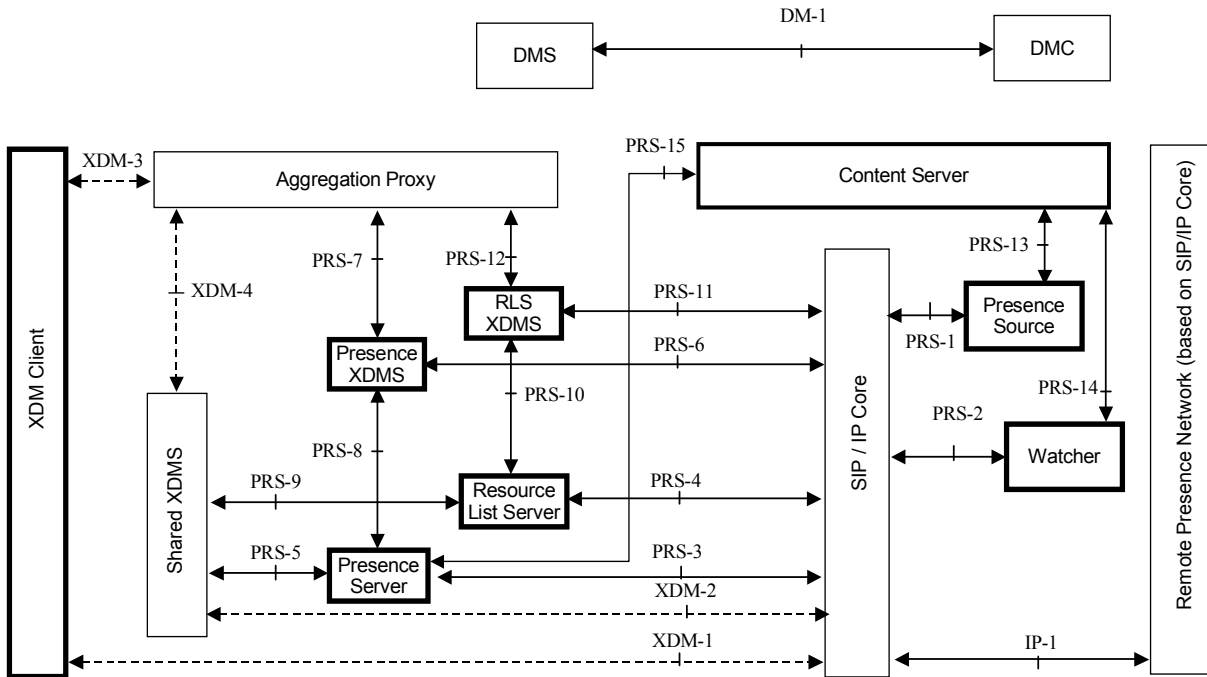


Figure 1-SIMPLE Presence Reference Architecture

Elements shown in bold are defined in this architecture document. The remaining elements are external to this specification.

The reference points shown here are only those that are specified in the Presence Enabler. Other relevant reference points are specified in the XDM Enabler.

The access network used by the Presence architecture may include any radio or other access as well as the other nodes required to support IP connectivity and IP mobility.

6.1 System and Subsystem Descriptions

6.1.1 Presence Functional Entities

This section describes the entities specified as part of the Presence Enabler.

6.1.1.1 Presence Server

The Presence Server (PS) supports the following:

- Accepts and stores Presence Information published to it.
- Distributes Presence Information and Watcher Information.

The PS is able to subscribe to changes to documents stored in the Shared and Presence XDMS. The PS is able to fetch documents from the Shared XDMS and the Presence XDMS.

6.1.1.2 Presence Source

The Presence Source is an entity that provides presence information to a Presence Service [RFC2778]. The Presence Source can be located in a user's terminal or within a network entity.

6.1.1.3 Watcher

A watcher is an entity that requests presence information about a Presentity, or Watcher Information about a watcher, from the Presence Service.

6.1.1.4 Resource List Server (RLS)

The Resource List Server (RLS) is the functional entity that accepts and manages subscriptions to presence lists, which enables a Watcher application to subscribe to the presence information of multiple presentities using a single subscription transaction.

The RLS is able to subscribe to changes to documents stored in the Shared and RLS XDMS. The RLS is able to fetch documents from the Shared XDMS and the RLS XDMS.

6.1.1.5 XML Document Management Client (XDMC)

The XDMC supports the following functions depending on its different instantiations (e.g., PoC XDMC, Presence XDMC, Shared XDMC):

- Manage related XML documents (e.g., Presence authorisation rules)
- Subscribe to SIP event package for changes to XML documents stored in any XDMS

The XDMC includes an XCAP client and a SIP User Agent.

6.1.1.6 Presence XML Document Management Server (Presence XDMS)

The Presence XDMS is an XCAP server and SIP Notifier as defined in [RFC3265] that supports the following functions:

- Manages XML documents (e.g. Presence authorization policies) which are specific to the Presence service Enabler.
- Enables single subscription to changes to multiple documents stored on the Presence XDMS.
- Notifies subscribers of changes to the Presence-specific documents stored in the network.

6.1.1.7 Resource List Server XML Document Management Server (RLS XDMS)

The RLS XDMS is an XCAP server and SIP Notifier as defined in [RFC3265] that supports the following functions:

- Manages XML documents (e.g. Presence lists), which are specific to the use of a RLS.
- Enables single subscription to changes to multiple documents stored on the RLS XDMS.
- Notifies subscribers of changes to such documents stored in the network.

6.1.1.8 Content Server

The Content Server is the functional entity that is capable of managing MIME objects for Presence, allowing the Presence Sources or the Presence Server to store MIME objects within, and support retrieval of those objects by Watchers or the Presence Server as required for content indirection [CONTENTIND].

The Content Server relies on external authentication and authorization done for the Presence Sources and Watchers. When realized with 3GPP IMS or 3GPP2 MMD networks, GAA [3GPP TS 33.222] can be used for that purpose, acting as an Authentication Proxy.

Note: Any usage of the content server for tasks not related to presence content indirection is outside the scope of this document.

6.1.2 External Entities Providing Services to Presence

This section describes the entities specified by other OMA Enablers or external organizations.

6.1.2.1 SIP/IP Core network

The SIP/IP Core is a network of servers, such as proxies and/or registrars, that perform a variety of services in support of the Presence Service, such as routing, authentication, compression, etc. The specific features offered by different types of SIP/IP Core networks will depend on the particulars of those networks.

This release of the Presence Enabler utilises IMS and MMD networks. Future releases may fully specify how the Presence Enabler utilises additional types of SIP/IP Cores. It is possible that certain future deployments may not have a SIP/IP Core at all, which would be an item for further study.

When the Presence Service is realized using IMS or MMD, the OMA Presence Sources, Watchers, and PS will utilize the capabilities of IMS as specified in 3GPP [3GPP TS 23.228] and 3GPP2 [3GPP2 X.S0013-002-A], respectively. In such cases the IMS network performs the following additional functions in support of the Presence Service:

- Routes the SIP signalling between the Presence Sources, Watchers, and the PS
- Provides discovery and address resolution services
- Supports SIP compression
- Performs authentication and authorization of the Presence Sources, Watchers and PS
- Maintains the registration state
- Provides charging information

6.1.2.2 Shared XML Data Management Server (XDMS)

The functionality of the Shared XDMS is described in [OMA XDMAD].

6.1.2.3 Aggregation Proxy

The functionality of the Aggregation Proxy is described in [OMA XDMAD].

6.1.2.4 Device Management Server

Device Management supports the following functions that are needed in support of the Presence Service:

- Initializes and updates all the configuration parameters necessary for the Watcher and Presence Source

6.1.3 Description of the Reference Points

The Reference Points named as PRS are in scope of this Architecture.

6.1.3.1 Reference Point PRS-1: Presence Source – SIP/IP Core

The PRS-1 reference point supports the communication between the Presence Source and the SIP/IP Core network. The protocol for the PRS-1 reference point is SIP and the traffic is routed to the PS via the SIP/IP Core.

PRS-1 Is used to publish presence information.

PRS-1 supports SIP compression/decompression when the Presence Source resides in the terminal.

6.1.3.2 Reference Point PRS-2: Watcher – SIP/IP Core network

The PRS-2 reference point supports the communication between the watcher and SIP/IP Core network. The protocol for the PRS-2 reference point is SIP and the traffic is routed to the PS via the SIP/IP Core.

PRS-2 is used to:

- Subscribe to a Presentity's presence information and receive notifications
- Subscribe to presence information and receive notifications for presence lists
- Subscribe to watcher information and receive notifications

PRS-2 supports SIP compression when the Watcher resides in the terminal.

6.1.3.3 Reference Point PRS-3: SIP/IP Core – Presence Server

The PRS-3 reference point supports the communication between the SIP/IP Core network and the PS. The protocol for the PRS-3 reference point is SIP.

PRS-3 is used to route the SIP messages from the SIP/IP Core to (and from) the appropriate PS in order to:

- Publish presence information
- Subscribe to presence information and receive notifications
- Subscribe to watcher information and receive notifications
- Subscribe to changes to documents stored in the Shared or Presence XDMS

6.1.3.4 Reference Point PRS-4: SIP/IP Core – Resource List Server

The PRS-4 reference point supports the communication between the SIP/IP Core network and the Resource List Server. The protocol for the PRS-4 reference point is SIP.

PRS-4 is used to route the SIP messages from the SIP/IP Core to (and from) the appropriate RLS in order to

- receive a subscription and send notifications for a presence list
- subscribe to presence information and to receive notifications for a Presentity in a presence list .

6.1.3.5 Reference Point PRS-5: Presence Server – Shared XDM Server

The PRS-5 reference point supports the communication between the Shared XDMS and the Presence Server.

The PRS-5 reference point supports the following:

- Transfer of URI Lists to the Presence Server

The protocol for the PRS-5 reference point is XCAP.

6.1.3.6 Reference Point PRS-6: Presence XDM Server – SIP/IP Core

The PRS-6 reference point supports the communication between the Presence XDMS and the SIP/IP Core. The protocol for the PRS-6 reference point is SIP.

The PRS-6 reference point provides the following functions:

- Subscription to the modification of Presence-specific XML documents.
- Notification of the modification of Presence-specific XML documents.

6.1.3.7 Reference Point PRS-7: Aggregation Proxy –Presence XDM Server

The PRS-7 reference point is between the Aggregation Proxy and the Presence XDMS. The protocol for the PRS-7 reference point is XCAP.

The PRS-7 reference point provides the following functions:

- Presence-specific XML document management (e.g. create, modify, retrieve, delete)

6.1.3.8 Reference Point PRS-8: Presence Server - Presence XDM Server

The PRS-8 reference point is between the Presence Server and the Presence XDMS. The protocol for the PRS-8 reference point is XCAP.

The PRS-8 reference point provides the following functions:

- Presence-specific XML document management (e.g. create, modify, retrieve, delete)

6.1.3.9 Reference Point PRS-9: Resource List Server – Shared XDM Server

The PRS-9 reference point supports the communication between the Shared XDMS and the Resource List Server (RLS).

The PRS-9 reference point supports the following:

- Transfer of URI Lists to the RLS

The protocol for the PRS-9 reference point is XCAP.

6.1.3.10 Reference Point PRS-10: Resource List Server – RLS XDM Server

The PRS-10 reference point supports the communication between the Resource List Server XDMS (RLS XDMS) and the Resource List Server (RLS).

The PRS-10 reference point supports the following:

- Transfer of RLS-specific documents (e.g., Presence Lists) from the RLS XDMS to the RLS.

The protocol for the PRS-10 reference point is XCAP.

6.1.3.11 Reference Point PRS-11: RLS XDM Server – SIP/IP Core

The PRS-11 reference point supports the communication between the RLS XDMS and the SIP/IP Core. The protocol for the PRS-11 reference point is SIP.

The PRS-11 reference point provides the following functions:

- Subscription to the modification of RLS-specific XML documents.
- Notification of the modification of RLS-specific XML documents.

6.1.3.12 Reference Point PRS-12: RLS XDM Server – Aggregation Proxy

The PRS-12 reference point is between the Aggregation Proxy and the RLS XDMS. The protocol for the PRS-12 reference point is XCAP.

The PRS-12 reference point provides the following functions:

- RLS-specific document management (e.g. create, modify, retrieve, delete)

6.1.3.13 Reference Point PRS-13: Presence Source – Content Server

The PRS-13 reference point is between the Presence Source and the Content Server. The protocol for the PRS-13 reference point is HTTP.

The PRS-13 reference point provides the following functions:

- Presence Sources store MIME objects related to presence publication in the Content Server

Note: The presence source is responsible to correlate the presence publication with the MIME objects it has stored on the Content Server.

6.1.3.14 Reference Point PRS-14: Watcher – Content Server

The PRS-14 reference point is between the Watcher and the Content Server. The protocol for the PRS-14 reference point is HTTP.

The PRS-14 reference point provides the following functions:

- Watchers retrieve MIME objects relating to presence notification from the Content Server

6.1.3.15 Reference Point PRS-15: Presence Server – Content Server

The PRS-15 reference point is between the Presence Server and the Content Server. The protocol for the PRS-15 reference point is HTTP.

The PRS-15 reference point provides the following functions:

- The Presence Server retrieve MIME objects relating to presence from the Content Server
- The Presence Server store MIME objects related to presence in the Content Server

6.1.3.16 Reference Point XDM-1: XDM Client – SIP/IP Core

The XDM-1 reference point is described in [OMA XDMAD].

6.1.3.17 Reference Point XDM-3: XDM Client- Aggregation Proxy

The XDM-3 reference point is described in [OMA XDMAD].

6.1.3.18 Reference Point XDM-2: Shared XDMS – SIP/IP Core

The XDM-2 reference point is described in [OMA XDMAD].

6.1.3.19 Reference Point XDM-4: Shared- Aggregation Proxy

The XDM-10 reference point is described in [OMA XDMAD].

6.1.3.20 Reference Point IP-1: SIP/IP Core network – External Presence Network (based on a SIP/IP Core)

The IP-1 reference point supports the communication between the SIP/IP Core network and an External Presence Network based on a SIP/IP Core network. The protocol for the IP-1 reference point is SIP.

6.1.3.21 Reference Point DM-1: DM Client – DM Server

The DM-1 reference point is described in [OMA DM]. The presence Enabler will define the presence configuration object(s).

6.1.4 Presence Information Format

The Presence Service uses the Presence Information Data Format (PIDF) [RFC3863] and its extensions as the base format through which presence information is represented.

The OMA Presence Enabler defines the semantics of several presence elements, and allows for those elements to be extended. Those elements are represented in XML using the PIDF format.

6.1.5 Privacy

The following sections describe a variety of policies that presentities can define to control the dissemination of their presence information.

6.1.5.1 Subscription Authorisation Rules

Subscriptions authorization rules determine how incoming subscriptions are handled.

Subscription authorisation rules determine the watchers who can be allowed to subscribe to the presence information of a Presentity and those that cannot. The subscription authorisation rules may include lists that can be stored in the Presence XDMS or the Shared XDMS.

The subscription authorization rules support the following actions:

- Accept
- Reject
- Polite blocking
- Deferred decision

For a particular Presentity, more than one these subscription authorization rules may exist.

6.1.5.2 Presence Content Rules

Presence Content rules determine which presence information will be disseminated to potential Watchers that have been accepted by Subscription Authorization rules. A Presentity can define content rules that apply for one or more Watchers.

The documents containing the Presence Content Rules are stored in the Presence XDMS.

6.1.6 Security

This section describes the mechanisms required for the secure operation of a Presence service.

6.1.6.1 SIP Signaling Security

Mutual authentication between a Presence Server and a Presence Source, can be performed prior to any interaction between said Server and Source. Mutual authentication between a Presence Server and a Watcher, can be performed prior to any interaction between said Server and Watcher. For an IMS realization, the PS relies on the security mechanisms provided by the SIP/IP Core network, for securing the service environments e.g. authentication of the service usage.

6.1.7 Charging

6.1.7.1 Charging Architecture

Both online and offline charging are supported.

6.1.8 Registration

When the SIP/IP Core corresponds with 3GPP/3GPP2 IMS, the Presence Source and the Watcher implemented by a UE will use the 3GPP/3GPP2 IMS registration mechanisms.

In a non-3GPP/3GPP2 network, this document has no requirement regarding the SIP registration procedures.

6.1.9 Presence Service Provisioning

The Presence Service provider can set up the Presence Service configurations remotely in the terminal device by using the device management mechanism specified in [OMA PROAD]. The updates of the Presence Service configurations are remotely performed in the terminal device by using [OMA DM].

A UE running the Presence Watcher and Presence Source functions, compliant with [OMA PROUA] is able to receive the contents sent by service provider. The exact syntax and definition of parameters needed for Presence Enabler are specified in [OMA PROCONT]. The bootstrap mechanism defined in [OMA PROSEC] and [OMA DM] is used to enhance the security of the provisioning.

Appendix A. Change History

(Informative)

A.1 Approved Version History

Reference	Date	Description
OMA-AD-Presence-SIMPLE-V1_0	25 Jul 2006	TP approved: OMA-TP-2006-0223R04-INP_Presence_SIMPLE_V1_0_for_final_approval