Presence SIMPLE Specification

Approved Version 1.1 – 27 June 2008

Open Mobile Alliance

OMA-TS-Presence_SIMPLE-V1_1-20080627-A

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

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.

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms set forth above.

Contents

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

Figures

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

1. Scope

This document provides the specifications for the Presence Service enabler based on the IETF SIMPLE (SIP Instant Messaging and Presence Leveraging Extensions) technology. This enabler is specified such that it is available to be used by other service enablers.

This release of the specification utilizes a SIP/IP Core network based on the 3GPP IMS and 3GPP2 MMD network capabilities.

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

2. References

2.1 Normative References

OMA

[OMA–DM-v1-1-2] OMA Device Management, V1.1.2, Open Mobile Alliance™, (based on SyncML DM), OMA-DM-V1_1_2. URL: http://www.openmobilealliance.org/

[OMA-DM-v1-2] OMA Device Management, V1.2, Open Mobile Alliance™, (based on SyncML DM), OMA-DM-V1_2, URL: http://www.openmobilealliance.org/

[PRESAC] "Presence Application Characteristics file of Presence V1.0", Version 1.0, Open Mobile Alliance™, OMA-SUP-AC_ap0002_presence-V1_0, URL: http://www.openmobilealliance.org/

[PRESAD] "Presence using SIMPLE", Version 1.1, Open Mobile Alliance™, OMA-AD-Presence_ SIMPLE-V1_1, URL: http://www.openmobilealliance.org/

[PRESDDS] "Presence SIMPLE Data Specification", Version 1.0, Open Mobile Alliance™, OMA-DDS-Presence_ SIMPLE-V1_0, URL: http://www.openmobilealliance.org/

[PRESMO] "OMA Management Object for SIMPLE Presence", Version 1.1, Open Mobile Alliance™, OMA-TS-Presence_SIMPLE_MO-V1_1, URL: http://www.openmobilealliance.org/

[PRESREQ] "Presence SIMPLE Requirements", Version 1.1, Open Mobile Alliance™, OMA-RD-Presence_SIMPLE-V1_1, URL: http://www.openmobilealliance.org/

[PRESXDM] "Presence XDM Specification", Version 1.1, Open Mobile Alliance™, OMA-TS-Presence_SIMPLE_XDM-V1_1, URL: http://www.openmobilealliance.org/

[Provisioning Content] OMA – Provisioning Content V1.1, Open Mobile Alliance™, URL: http://www.openmobilealliance.org/

[RLSXDM] "Resource List Server (RLS) XDM Specification", Version 1.1, Open Mobile Alliance™, OMA-TS-Presence_SIMPLE_RLS_XDM- V1_1, URL: http://www.openmobilealliance.org/

[SharedXDM] "Shared XDM Specification", Version 1.1, Open Mobile Alliance™, OMA-TS-XDM_Shared-V1_1, URL: http://www.openmobilealliance.org/

[XDMSPEC] "XML Document Management Specification", Version 1.1, Open Mobile Alliance™, OMA-TS-XDM_Core-V1_1, URL: http://www.openmobilealliance.org/

IETF

[PARFORMAT] "Presence Information Data format (PIDF) Extension for Partial Presence", M. Lonnfors et al., November 19, 2007, (http://www.ietf.org/internet-drafts/draft-ietf-simple-partial-pidf-format-10.txt)

Note: IETF Draft work in progress

[PARNOT] Session Initiation Protocol (SIP) extension for Partial Notification of Presence Information", M.Lonnfors et al., January 21, 2008 (http://www.ietf.org/internet-drafts/draft-ietf-simple-partial-notify-10.txt)

Note: IETF Draft work in progress

[PARPUBLISH] " Publication of Partial Presence Information", M.LonnforsA. Niemi et al., February 19, 2008, (http://www.ietf.org/internet-drafts/draft-ietf-simple-partial-publish-07.txt)

Note: IETF Draft work in progress

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

[RFC2246] "The TLS Protocol Version 1.0", T. Dierks et al., January 1999, RFC 2246, (http://www.ietf.org/rfc/rfc2246.txt)

[RFC2387] "The MIME Multipart/Related Content-type", E. Levinson, Aug. 1998, RFC 2387, (http://www.ietf.org/rfc/rfc2387.txt)

[RFC2392] "Content-ID and Message-ID Uniform Resource Locators", E. Levinson, Aug. 1998, RFC 2392, (http://www.ietf.org/rfc/rfc2392.txt)

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

[RFC2616] "Hypertext Transfer Protocol -- HTTP/1.1", URL: http://www.ietf.org/rfc/rfc2616.txt

[RFC2778] "A Model for Presence and Instant Messaging", M. Day et al., Feb. 2000, RFC 2778, (http://www.ietf.org/rfc/rfc2778.txt)

[RFC2818] "HTTP Over TLS", E. Rescorla, May 2000, RFC 2818, (http://www.ietf.org/rfc/rfc2818.txt)

[RFC3261] "Session Initiaton Protocol (SIP)", Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M. and E. Schooler,June 2002, RFC 3261, (http://www.ietf.org/rfc/rfc3261.txt)

[RFC3265] "Session Initiation Protocol (SIP)-Specific Event Notification", A.B.Roach, June 2002, RFC 3265, (http://www.ietf.org/rfc/rfc3265.txt)

[RFC3320] "Signaling Compression (SigComp)", Price, R., et al., Jan. 2003, RFC 3320, (http://www.ietf.org/rfc/rfc3320.txt)

[RFC3323] "A Privacy Mechanism for the Session Initiation Protocol (SIP)", Peterson, J., Nov. 2002, RFC 3323, (http://www.ietf.org/rfc/rfc3323.txt)

[RFC3325] "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks", Jennings, C., et al, Nov. 2002, RFC 3325, (http://www.ietf.org/rfc/rfc3325.txt)

[RFC3485] "The Session Initiation Protocol (SIP) and Session Description Protocol (SDP) Static Dictionary for Signaling Compression (SigComp)", Garcia-Martin, M., et al.,Feb. 2003, RFC 3485, (http://www.ietf.org/rfc/rfc3485.txt)

[RFC3486] "Compressing the Session Initiation Protocol (SIP)", Camarillo, G., Feb. 2003, RFC 3486, (http://www.ietf.org/rfc/rfc3486.txt)

[RFC3856] "A Presence Event Package for the Session Initiation Protocol (SIP)", J.Rosenberg, Jan. 2003, RFC 3856, (http://www.ietf.org/rfc/rfc3856.txt)

[RFC3857] "A Watcher Information Event Template-Package for the Session Initiation Protocol (SIP)", J.Rosenberg, Aug. 2004, RFC 3857, (http://www.ietf.org/rfc/rfc3857.txt)

[RFC3858] "An Extensible Markup Language (XML) Based Format for Watcher Information", J.Rosenberg, Aug. 2004, RFC 3858, (http://www.ietf.org/rfc/rfc3858.txt)

[RFC3859] "Common Profile for Presence (CPP)", J.Peterson, Aug. 2004, RFC 3859, (http://www.ietf.org/rfc/rfc3859.txt)

[RFC3863] "Presence Information Data Format (PIDF)", H.Sugano et al., Aug 2004 (http://www.ietf.org/rfc/rfc3863.txt)

[RFC3903] "An Event State Publication Extension to the Session Initiation Protocol (SIP) ", A. Niemi, Oct. 2004, (http://www.ietf.org/rfc/rfc3903.txt)

[RFC3966] "The tel URI for Telephone Numbers". H. Schulzrinne, Dec. 2004, , (http://www.ietf.org/rfc/rfc3966.txt)

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

[RFC4483] "A Mechanism for Content Indirection in Session Initiation Protocol (SIP) Messages", E. Burger, Ed, May 2006 ,URL: http://www.ietf.org/rfc/rfc4483.txt

[RFC4660] "Functional Description of Event Notification Filtering", H.Khartabil et al, Sep 2006 (http://www.ietf.org/rfc/rfc4660.txt)

[RFC4661] "An Extensible Markup Language (XML) Based Format for Event Notification Filtering", H.Khartabil et al, Sep 2006, (http://www.ietf.org/rfc/rfc4661.txt)

[RFC4662] "A Session Initiation Protocol (SIP) Event Notification Extension for Resource Lists", A. B. Roach et al., August 2006, (http://www.ietf.org/rfc/rfc4662.txt)

[RFC5025] "Presence Authorization Rules", J. Rosenberg, December 2007, RFC 5025, (http://www.ietf.org/rfc/rfc5025.txt)

3GPP/3GPP2

[3GPP TS 23.228] "IP Multimedia Subsystem (IMS); Stage 2", 3GPP TS 23.228, Release 6, 2005

[3GPP TS 24.109] "Bootstrapping interface (Ub) and network application function interface (Ua); Protocol details ; Stage 3", 3GPP TS 24.109, Release 6

[3GPP TS 24.141] "Presence service using the IP Multimedia (IM) Core Network (CN) subsystem; Stage-3", 3GPP TR 24.141, Release 6, 2005

[3GPP TS 24.229] "Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

Description Protocol (SDP); Stage 3", 3GPP TS 24.229, Release 6, 2005

[3GPP TS 26.141] "IP Multimedia System (IMS) Messaging and Presence; Media formats and codecs (Release 6)", 3GPP, 2005

[3GPP TS 32.240] "Charging management; Charging architecture and principles",3GPP TS 32.240, Release 6, 2005

[3GPP TS 32.260] "Charging Management; IP Multimedia Subsystem (IMS) Charging", 3GPP TS 32.260, Release 6, 2005

[3GPP TS 33.203] "Access Security for IP-based services", 3GPP TS 33.203, Release 6, 2005

[3GPP2 C.P0071-0] "IP Multimedia Domain(MMD) Codecs and Transport Protocols", Revision 0, Version 1.0, 3GPP2, 2005

[3GPP2 S.R0086-A] "IMS Security Framework", Revision A, Version 1.0, 3GPP2, 2004

[3GPP2 X.S0027-003-0] "Presence Service using IP Multimedia Core Network Subsystem; Stage 3", Revision 0, Version 1.0, 3GPP2, 2008

[3GPP2 X.S0013-002-A] "All-IP Core Network Multimedia Domain: IP Multimedia Subsystem - Stage 2", Revision A, Version 1.0, 3GPP2, 2005

[3GPP2 X.S0013-004-A] "All-IP Core Network Multimedia Domain: IP Multimedia Call Control Protocol Based on SIP and SDP Stage 3", Revision A, Version 1.0, 3GPP2, 2005

[3GPP2 X.S0013-008-A] "All-IP Core Network Multimedia Domain: IP Multimedia Subsystem – Offline Accounting, Information Flows and Protocol", Revision A, Version 1.0, 3GPP2, 2005

2.2 Informative References

[3GPP TS 23.141] "Presence Service; Architecture and functional description", 3GPP TS 23.141, Release 6, 2005

[3GPP TS 29.228] "IP Multimedia (IM) Subsystem Cx and Dx Interfaces; Signalling flows and message contents", 3GPP TS 29.228 Release 6 2005

[3GPP2 S.R0062-0] "Presence for Wireless Systems Stage 1 Requirements", Revision 0, Version 1.0, 2002

[3GPP2 X.S0013-003-A] "All-IP Core Network Multimedia Domain: IP Multimedia (IMS) session handling; IP Multimedia (IM) call model; Stage 2", Revision A, Version 1.0, 2005

[3GPP2 X.S0013-006-A] "All-IP Core Network Multimedia Domain: Cx Interface based on the Diameter Protocol; Protocol Details", Revision A, 2005

[3GPP2 X.S0027-001-0] "Presence Service; Architecture and functional description", Revision 0, Version 1.0, 3GPP2, 2004

[RFC4474] "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)", J.Peterson et al., August 2006, (http://www.ietf.org/rfc/rfc4474.txt)

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

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

Composition	The function of the PS to combine the “views” of the various Presence Sources in one single raw presence document for a particular Presentity.
Content Server	The Content Server is the functional entity that is capable of managing MIME objects for Presence, allowing the Presence Sources to store MIME objects within, and support retrieval of those objects by Watchers. Source: [PRESAD]
Event Package	Event Package: An event package is an additional specification, which defines a set of state information to be reported by a notifier to a subscriber. Event packages also define further syntax and semantics based on the framework defined by this document required to convey such state information. Source: [RFC3265]
Event Publication Agent (EPA)	The User Agent Client (UAC) that issues PUBLISH requests to publish event state. Source: [RFC3903]
Event State Compositor (ESC)	The User Agent Server (UAS) that processes PUBLISH requests, and is responsible for compositing event state into a complete, composite event state of a resource. Source: [RFC3903]
Presence Content Rules	Presence Content Rules determine which Presence Information is disseminated to Watchers that have been accepted by Subscription Authorization Rules. A Presentity can define Presence Content Rules that apply to one or more Watchers. Source: [PRESAD]
Presence External Agent (PEA)	Presence source element that is located outside of the provider's network. Source: [3GPP TS 23.141]/ [3GPP2 X.S0027-001-0]
Presence Information	Dynamic set of information pertaining to a Presentity that may include Presence Information Elements such as the status, reachability, willingness, and capabilities of that Presentity. Note: This definition is compatible with the 3GPP/3GPP2 definitions, as well as the IETF definition, though the latter is quite generic. Source: [PRESREQ]
Presence Information Element	A basic unit of Presence Information. Source: [PRESREQ]
Presence List	Pre-defined list of Presentities stored in RLS XDMS (see [RLSXDM]) which enables a Watcher to subscribe to Presence Information of multiple Presentities using a single subscription.
Presence Network Agent (PNA)	Network located element that collects and sends network related Presence Information on behalf of the Presentity to a Presence Server. Source: [3GPP TS 24.141]/ [3GPP2 X.S0027-003-0]
Presence Source	A logical entity that provides *Presence Information* pertaining to exactly one or more *Presentities* to the *Presence Server*. Presence User Agents, Presence Network Agents, and Presence External Agents are examples of *Presence Sources*.

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

	Note: In [RFC3856], Presence Sources are referred to as Presence User Agents. In [RFC2778], they are referred to as Presentities. Source: [PRESREQ]
Presence User Agent (PUA)	A terminal or network located element that collects and sends user related Presence Information to a Presence Server on behalf of a Principal. Source: [3GPP TS 24.141]/ [3GPP2 X.S0027-003-0]
Presentity	A logical entity that has *Presence Information* (see definition below) associated with it. This *Presence Information* may be composed from a multitude of *Presence Sources*. A *Presentity* is most commonly a reference for a person, although it may represent a role such as "help desk" or a resource such as "conference room #27". The Presentity is identified by a SIP URI (as defined in [RFC3261]), and may additionally be identified by a tel URI (as defined in [RFC 3966]) or a pres URI (as defined in [RFC3859]). Note: This definition maps better to the [RFC2778] definition of a Principal, rather than that of [RFC2778] Presentity. This definition is compatible with the[RFC3856]. Source: [PRESREQ]
Resource List Server (RLS)	A 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. Source: [PRESAD]
Subscription Authorisation Rules	Subscription Authorisation Rules determine those Watchers who are allowed to subscribe to the Presence Information of a Presentity and those who are not allowed. The Subscription Authorization Rules may include lists that can be stored in the Presence XDMS or the Shared XDMS. Source: [PRESAD]
Watcher	Any uniquely identifiable entity that requests Presence Information about a Presentity, from the presence service. Special types of Watcher are fetcher, poller, and subscribed-Watcher. (Differs slightly from [RFC2778] and [3GPP2 X.S0027-003-0] definitions). Source: [PRESREQ]
Watcher information	Information about watchers that have received or may receive presence information about a particular presentity within a particular recent span of time. (Differs slightly from [RFC2778], is identical to [3GPP2 X.S0027-003-0] definition). Source: [PRESREQ]
Watcher Information Subscriber	Any uniquely identifiable entity that requests Watcher information about a Watcher, from the presence service.

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

3.3 Abbreviations

3GPP	3rd Generation Partnership Project
3GPP2	3rd Generation Partnership Project 2
AD	Architecture Document
AS	Application Server
CID	Content ID
DM	Device Management
EPA	Event Publication Agent
ESC	Event State Compositor
IETF	Internet Engineering Task Force
IM	Instant Messaging
IMS	IP Multimedia Subsystem
IP	Internet Protocol
MIME	Multipurpose Internet Mail Extensions
MWG	Messaging Working Group
MWS	Mobile Web services
OMA	Open Mobile Alliance
OMNA	Open Mobile Naming Authority
OTAP	Over the Air Provisioning
PEA	Presence External Agent
PIDF	Presence Information Data Format
PNA	Presence Network Agent
PoC	Push-to-talk over Cellular
PS	Presence Server
PUA	Presence User Agent
RD	Requirement Document
RFC	Request For Comments
RLS	Resource List Server
RPID	Rich Presence Information Data
SIMPLE	SIP Instant Message and Presence Leveraging Extensions
SIP	Session Initiation Protocol
TLS	Transport Layer Security
UA	User Agent
UE	User Equipment
UMTS	Universal Mobile Telecommunications System
URI	Uniform Resource Identifier
WG	Working Group
WLAN	Wireless LAN
XCAP	XML Configuration Access Protocol

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

XDMS	XML Document Manipulation Server
XML	Extensible Markup Language
XUI	XCAP User Identifier

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

4. Introduction

This document defines an application level specification for the OMA SIP/SIMPLE-based Presence Service, and makes use of the implementations of the SIP protocol in the 3GPP IMS (IP Multimedia Subsystem) and 3GPP2 MMD (Multimedia Domain) for collecting and disseminating Presence Information between the various Presence Sources and their Watchers as described in ([PRESAD]).

In addition to the SIP methods for subscription, publication, and notification of presence state based on [RFC3265], [RFC3856] and [RFC3903], this specification also addresses:

- The partial publication and notification of (only the changed) Presence Information, based on [PARPUBLISH], [PARNOT] and [PARFORMAT];
- Triggers for the generation of notifications when specific events take place;
- Notification of watcher information state based on [RFC3857] and [RFC3858];
- The handling of large Presence Information content, based on support of [RFC2387] and [RFC4483];
- The control of the content of the notification sent to a Watcher, based on [RFC4660] and [RFC4661];
- Subscriptions to a Presence List, based on [RFC4662];
- Subscription authorization rules for Watchers, based on [PRESXDM];
- Presence content rules for Watchers, based on [PRESXDM]; and
- Compression of SIP requests.

The Presence Services makes use of various data repositories in the network that store information related to Presentities and Watchers, specifically:

- The Presence XDMS (see [PRESXDM]) for storage of documents related to a Presentity, such as subscription authorization rules and presence content rules for Watchers;
- The Shared XDMS (see [SharedXDM]) for URL Lists which may be referenced from other documents;
- The RLS XDMS (see [RLSXDM]) for storing a Watcher's Presence List; and
- The Content Server (see [PRESAD]) for managing MIME objects.

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

5. Presence Functional Entities

5.1 Presence Source

The Presence Source is an entity that provides Presence Information to a Presence Service. The Presence Source MAY be located in the user's terminal or within a network entity.

When the SIP/IP Core network corresponds with 3GPP IMS or 3GPP2 MMD networks, the Presence Source MAY be implemented in a UE or an AS as defined in [3GPP TS 23.228] and [3GPP2 X.S0013-002-A] respectively.

5.1.1 Publication of Presence Information

A Presence Source SHALL implement the Event Publication Agent (EPA) function and support the PUBLISH method according to the procedures described in [RFC3903].

A Presence Source SHALL support the 'application/pidf+xml' content type, according to [RFC3863].

The Presentity SHALL be identified by a SIP URI (as defined in [RFC3261]), and may additionally be identified by a tel URI (as defined in [RFC3966]) or a pres URI (as defined in [RFC3859]). The tel URI SHALL take the international public telecommunication number format with a leading "+" sign. If the Presence Source is aware of the SIP URI of the Presentity, the Presence Source SHOULD insert the SIP URI in the Request-URI of the PUBLISH request rather than a pres URI or a tel URI. The Presence Source SHALL insert the same URI in the "entity" attribute of the <presence> element as in the Request-URI of the PUBLISH request.

When the SIP/IP Core network corresponds to 3GPP IMS or 3GPP2 MMD networks, and the Presence Source is a UE, it SHALL set the entity attribute of the <presence> element of the presence document, defined in [RFC3863], to its registered public user identity, as defined in [3GPP TS 24.229] and [3GPP2 X.S0013-004-A]. If more than one registered public user identity is available:

- the Presence Source SHALL set the value of the "entity" attribute of the <presence> element in the presence document with the value of the P-Preferred-Identity header field used in the SIP PUBLISH request, if present, as defined in [3GPP TS 24.229] and [3GPP2 X.S0013-004-A].
- if there is no P-Preferred-Identity header field included in the SIP PUBLISH request, the Presence Source SHALL include its default public user identity, as defined in [3GPP TS 24.229] and [3GPP2 X.S0013-004-A], in the "entity" attribute of the <presence> element of the presence document,

When the SIP/IP Core network corresponds to 3GPP IMS or 3GPP2 MMD networks and if the Presence Source is an AS, it SHALL set the value of the "entity" attribute of the <presence> element in the presence document with a URI value from the P-Asserted-Identity header field used in the SIP PUBLISH request as defined in [3GPP TS 24.229] and [3GPP2 X.S0013-004-A].

The Presence Source SHALL support the presence data model defined in [PRESDDS]. The Presence Source SHALL use the elements defined in [PRESDDS] when publishing Presence Information with semantics identical to those elements.The Presence Source MAY support other PIDF extensions to publish elements whose semantics do not match with those defined in [PRESDDS], as long as a Watcher that does not understand those extensions can ignore them without changing the meaning of the Presence Information Elements that are understood.

The Presence Source SHALL be free to provide any value of the instance identifier attributes (id) for <tuple>, <person> and <device> (see [PRESDDS]) as this is being used only to syntactically differentiate between the elements and is not linked with any composition actions in the PS or resolution of conflicts in Watcher.

For a given Presentity, the information published by each Presence Source is composed into a single raw presence document as described in section 5.4.3.1.

5.1.1.1 Partial publication

Partial publication is a mechanism such that a given Presence Source can publish only those parts of the Presence Information that have changed since its last publication, rather than the full presence state.

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

A Presence Source MAY support partial publication. A Presence Source performing partial publication SHALL support the following:

- Partial publication procedure, according to [PARPUBLISH]; and
- Partial presence extension to PIDF, according to [PARFORMAT].

5.1.1.2 Handling of large objects

The Presence Source MAY implement the 'multipart/related' content type as described in [RFC2387], in order to aggregate other MIME objects with the 'application/pidf+xml' or 'application/pidf-diff+xml' content types.

If a Presence Information Element has a value of a reference to a MIME object, the Presence Source can either:

- Use the content indirection mechanism as defined in [RFC4483], store the MIME object in the Content Server and send it indirectly by utilising the cid URI as described in [RFC2392] referring to the indirected content part of the 'multipart/related' content-type in the PUBLISH request; or
- Send the MIME object directly together with the presence document by utilising the cid URI as described in [RFC2392] referring to the embedded content part of the 'multipart/related' content-type in the PUBLISH request.

The MIME object format SHALL conform to [3GPP TS 26.141] and [3GPP2 C.P0071-0].

5.1.1.2.1 Performing content indirection

If the Presence Source decides to use the content indirection mechanism for publishing an initial or modified value of a Presence Information element, the Presence Source SHALL follow the following procedures:

1. Store the MIME object.

   NOTE: The procedure for storing MIME objects is not defined by this specification.

   The Presence Source MAY be provisioned with the HTTP or optionally HTTPS URI of the content server where the MIME objects will be stored. This can be done with OTA Provisioning or local configuration. In case it is performed with OTA Provisioning it SHALL use the value of the CONTENT-SERVER-URI defined in Appendix B.1.

2. Construct an HTTP URI or optionally an HTTPS URI referencing the stored MIME object.

3. Use the 'multipart/related' content type as described in [RFC2387] with the content indirection mechanism as specified in [RFC4483] for the publication of Presence Information format as follows:

   a) Set a cid URI as described in [RFC2392] referencing to other MIME multipart body which contains the content indirection information as the value of the XML element whose value is delivered as an indirect content;

   b) Include the presence document of the format 'application/pidf+xml' or 'application/pidf-diff+xml' in the root of the body of the 'multipart/related' content;

   c) Specify the part having information about the MIME object by using the 'message/external-body' content type, defining the HTTP or HTTPS URI, versioning information and other information about the MIME object as described in [RFC4483]. The versioning information is used for determining whether or not the MIME object indirectly referenced by a URI has changed or not.

5.1.1.2.2 Handling of direct content

When the Presence Source decides to publish the MIME object as a direct content inside the presence document, the Presence Source SHALL utilise the 'multipart/related' content type as described in [RFC2387] in the PUBLISH request with the following procedures:

1) Set a cid URI as described in [RFC2392] referencing to other multipart body which contains the MIME object;

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

2) Include the presence document of the format ‘application/pidf+xml’ or ‘application/pidf-diff+xml’ in the root of the body of the ‘multipart/related’ content.

If the Presence Source supports OTA Provisioning, the size limit for MIME data direct content in a PUBLISH request as set via OTA Provisioning SHALL NOT be exceeded.

In case it is performed with OTA Provisioning, it SHALL use the value of CLIENT-OBJ-DATA-LIMIT parameter is defined in Appendix B.1.

If the Presence Source does not support OTA Provisioning, the size limit for MIME data direct content in a PUBLISH request SHOULD be set by other means at the Presence Source and its value SHALL be the same as defined for OTA Provisioning compliant Presence Sources.

5.1.1.3 Limiting the rate of publications

The service provider MAY configure a Presence Source with the shortest allowed time period between two PUBLISH requests. This can be done with OTA Provisioning or local configuration. In case of OTA Provisioning, it SHALL use the value of SOURCE-THROTTLE-PUBLISH (defined in Appendix B.1).

If such configuration is present for the Presence Source, the Presence Source SHALL NOT generate PUBLISH requests more often than instructed by the configured value.

5.1.1.4 Compression of a PUBLISH Request

The Presence Source in a UE SHOULD compress the SIP signaling according to [RFC3320] and [RFC3485] to reduce the transmission delays. If signaling compression is used, the Presence Source SHALL indicate support for SigComp to the SIP/IP Core network and request SigComp from the SIP/IP Core network as described in [RFC3486].

When the SIP/IP Core network corresponds with 3GPP IMS or 3GPP2 MMD networks the signalling compression procedures as defined in [3GPP TS 24.229] / [3GPP2 X.S0013-004-A] SHALL be used.

5.1.2 Example realizations of a Presence Source (Informative)

5.1.2.1 Presence User Agent

The Presence Source MAY be implemented as a Presence User Agent (PUA) as defined by 3GPP/3GPP2 in [3GPP TS 23.141] and [3GPP2 X.S0027-001-0] respectively. The PUA is a Presence Source realization residing in the terminal or network. The PUA collects user related Presence Information from its corresponding Presentity and sends it to the PS.

5.1.2.2 Presence Network Agent

The Presence Source MAY be implemented as a Presence Network Agent (PNA) as defined by 3GPP/3GPP2 in [3GPP TS 23.141] and [3GPP2 X.S0027-001-0] respectively. The PNA collects the network related Presence Information from the various network elements and send it to the PS.

The PNA may also notify the PS when the terminal is disconnected. The interfaces between the PNA and the various elements are defined in 3GPP/3GPP2 (see Figure 1and Figure 2) and are out of scope of the current specification.

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

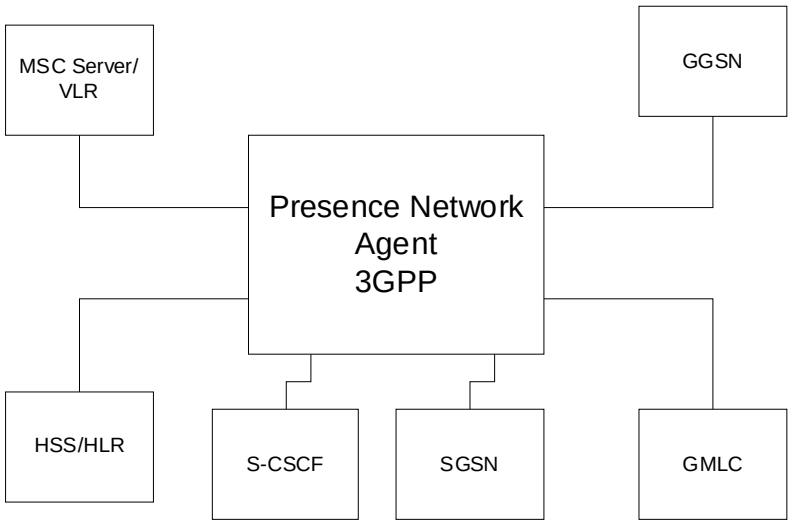

Figure 1-PNA in 3GPP

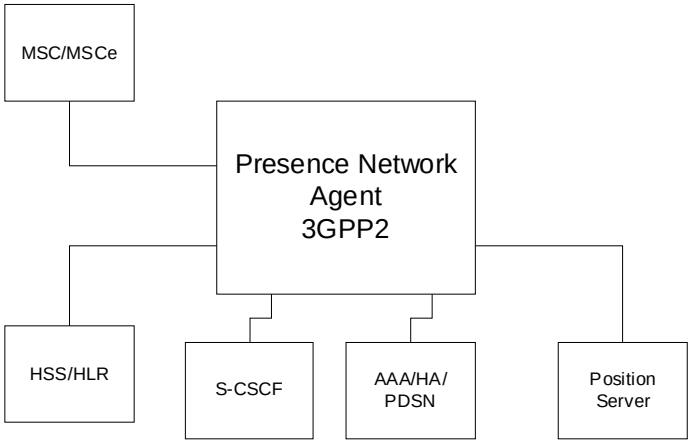

Figure 2-PNA in 3GPP2

The options of using a PNA in a non-3GPP/3GPP2 environment is shown on Figure 3:

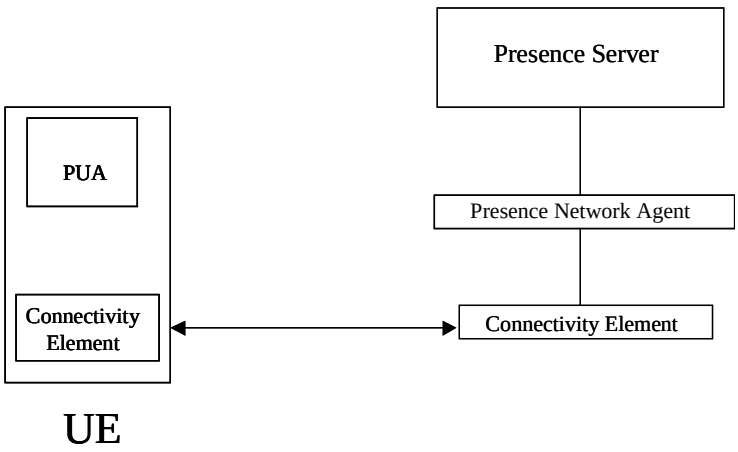

Figure 3-PNA in a non-3GPP/3GPP2 architecture.

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

5.1.2.3 Presence External Agent

The Presence Source MAY be implemented as a Presence External Agent (PEA) as defined by 3GPP/3GPP2 in [3GPP TS 23.141] and [3GPP2 X.S0027-001-0] respectively. The PEA performs the following functions:

- Supply Presence Information from external networks;
- Handle the interworking and security issues involved in interfacing to external networks; and
- Resolve the location of the PS associated with the Presentity.

Examples of Presence Information that the PEA may supply, include:

- Third party services (e.g. calendar applications, corporate systems);
- Internet Presence Services;
- Non SIMPLE-based Presence Services; and
- Services that use Presence (e.g. PoC, IM).

5.2 Watcher

The Watcher is an entity that subscribes to Presence Information about a Presentity or list of Presentities (i.e. Presence List).

When the SIP/IP Core network corresponds with 3GPP IMS or 3GPP2 MMD networks, the Watcher MAY be implemented in a UE or an AS as defined in [3GPP TS 23.228] and [3GPP2 X.S0013-002-A] respectively.

5.2.1 General

A Watcher SHALL support the 'application/pidf+xml' content type, according to [RFC3863].

5.2.2 Subscription to Presence Information

A Watcher SHALL support subscription and notification of Presence Information, according to the subscriber procedures described in [RFC3265] and [RFC3856].

If the Watcher is aware of the SIP URI of the Presentity, the Watcher SHOULD insert the SIP URI in the Request-URI of the SUBSCRIBE request rather than a pres URI or a tel URI.

If the Watcher only knows the tel URI or pres URI of the Presentity, the tel URI or pres URI may get translated to a SIP URI by the SIP/IP Core network. In this case, the Watcher MAY learn the translated URI from the "entity" attribute of the <presence> element included in the NOTIFY request and use it for future subscriptions.

5.2.2.1 Subscription to a Presence List

Presence Lists enable a Watcher to subscribe to multiple Presentities using a single subscription.

A Watcher MAY subscribe to a Presence List. If a Watcher subscribes to a Presence List, it SHALL support the SIP event notification extension for resource lists, according to the subscriber procedures described in [RFC4662].

NOTE: As described in section 5.5.2, the RLS can enforce a limit on the number of back-end subscriptions allowed for a single Presence List subscription, in which case the Watcher will not receive <instance> elements for those <resource> elements corresponding to Presentities that could not be subscribed by the RLS. The Watcher may be configured with the MAX-NUMBER-OF-SUBSCRIPTIONS-IN-PRESENCE-LIST parameter (defined in Appendix B.1) to indicate the limit being enforced by the RLS. How the Watcher makes use of this parameter is out of scope of this specification.

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

5.2.3 Presence information processing

The Watcher SHALL support the presence data model defined in [PRESDDS], and interpret the received Presence Information according to the watcher processing rules defined in [PRESDDS].

5.2.4 Partial Notifications

Partial notification is a mechanism for receiving only those parts of the Presence Information that have changed since the last notification received by the Watcher, rather than the full presence state.

A Watcher subscribing to Presence Information MAY request partial notifications. A Watcher requesting partial notifications SHALL support the following:

- SIP extension for partial notifications, according to the Watcher procedures described in [PARNOT]; and
- Partial presence extension to PIDF, according to [PARFORMAT].

5.2.5 Event Notification Filtering

Event notification filtering is a mechanism for the Watcher to control the content and triggers of notifications.

A Watcher subscribing to Presence Information MAY request event notification filtering. A Watcher requesting event notification filtering SHALL support the following:

- Event notification filtering, according to the subscriber procedures described in [RFC4660]; and
- Content-type 'application/simple-filter+xml', according to [RFC4661].

5.2.6 Handling of large objects

A Watcher MAY implement the 'multipart/related' content type as described in [RFC2387], in order to aggregate other MIME objects with the 'application/pidf+xml' or the 'application/pidf-diff+xml' content type. In this case, the Watcher SHALL indicate the support for the 'multipart/related' content type by using the "Accept" header field in the SUBSCRIBE request.

5.2.6.1 Fetching indirect content

A Watcher MAY support the content indirection mechanism [RFC4483]. If supported, the Watcher SHALL indicate the support for the 'message/external-body' content type by using the "Accept" header field in the SUBSCRIBE request.

If the Watcher receives an indirect content in a NOTIFY request, the Watcher SHALL fetch the content from the Content Server as defined in [RFC4483].

If the URI received as indirect content in the NOTIFY request is an HTTPS URI the Watcher SHALL perform according to [RFC2818].

5.2.7 Compression of Subscription Signaling

5.2.7.1 Compression of SIP signaling

A Watcher in a UE SHOULD compress the SIP signaling according to [RFC3320] and [RFC3485] to reduce the transmission delays. If signaling compression is used, the Watcher SHALL indicate support for SigComp to the SIP/IP Core network and request SigComp from the SIP/IP Core network as described in [RFC3486].

When the SIP/IP Core network corresponds with 3GPP IMS or 3GPP2 MMD networks the signalling compression procedures as defined [3GPP TS 24.229] / [3GPP2 X.S0013-004-A] SHALL be used.

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

5.3 Watcher Information Subscriber

The Watcher Information Subscriber is an entity that subscribes to the dynamically changing set of Watchers defined in section 5.2 and state of their subscriptions.

When the SIP/IP Core network corresponds with 3GPP IMS or 3GPP2 MMD networks, the Watcher Information Subscriber MAY be implemented in a UE or an AS as defined in [3GPP TS 23.228] and [3GPP2 X.S0013-002] respectively.

5.3.1 Subscription to Watcher Information

A Watcher Information Subscriber MAY be co-located with a Presence Source or a Watcher and SHALL support subscription and notification of Watcher information, according to the subscriber procedures described in [RFC3265] and [RFC3857].

A Watcher Information Subscriber SHALL support the 'application/watcherinfo+xml' content type, according to [RFC3858].

A Presentity for which the presence service is activated SHOULD have a corresponding Watcher Information Subscriber, e.g. to support reactive authorization. The mechanism how this is achieved is outside the scope of this document.

If subscription to Watcher information event package is required, the Presentity SHALL subscribe to the Watcher information event package with one of its corresponding Watcher Information Subscribers upon activation of the service. This information can be used, for instance, for reactive authorization.

5.3.1.1 Event notification filtering

Event notification filtering is a mechanism for the Watcher Information Subscriber to control the content of notifications sent to it.

A Watcher Information Subscriber subscribing to Watcher information MAY request event notification filtering. A Watcher Information Subscriber requesting event notification filtering SHALL support the following:

- Event notification filtering, according to the subscriber procedures described in [RFC4660]; and
- Content-type 'application/simple-filter+xml', according to [RFC4661].

5.3.2 Compression of Watcher Information signaling

5.3.2.1 Compression of SIP signaling

A Watcher Information Subscriber in a UE SHOULD compress the SIP signaling according to [RFC3320] and [RFC3485] to reduce the transmission delays. If signaling compression is used, the the Watcher Information Subscriber SHALL indicate support for SigComp to the SIP/IP Core network and request SigComp from the SIP/IP Core network as described in [RFC3486].

When the SIP/IP Core network corresponds with 3GPP IMS or 3GPP2 MMD networks the signalling compression procedures as defined [3GPP TS 24.229] / [3GPP2 X.S0013-004-A] SHALL be used.

5.4 Presence Server

The Presence Server (PS) is an entity that accepts, stores and distributes Presence Information. The PS performs the following functions:

- Handles publications from one or multiple Presence Source(s) of a certain Presentity. This includes refreshing Presence Information, replacing existing Presence Information with newly published information, or removing Presence Information, for a given Presence Source (see section 5.4.1).
- Handles subscriptions from Watchers to Presence Information and generates notifications about the Presence Information state changes (see section 5.4.2).

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

- Processes the Presence Information in various stages and applies Watcher preferences (see section 5.4.3).
- Handles subscriptions from Watcher Information Subscribers to Watcher information and generates notifications about the Watcher information state changes (see section 5.4.4).
- Use certain XDM functions supporting the PS (see section 5.4.5).

When the SIP/IP Core network corresponds with 3GPP IMS or 3GPP2 MMD networks, the PS SHALL be implemented in an AS as defined in [3GPP TS 23.228] and [3GPP2 X.S0013-002-A] respectively.

5.4.1 Presence Information publication acceptance from Presence Sources

A PS SHALL implement the Event State Compositor (ESC) function and support the PUBLISH method according to the procedures described in [RFC3903].

A PS SHALL support the 'application/pidf+xml' content type according to [RFC3863].

5.4.1.1 Applying Presence Publication

As part of the publication process, the PS may need to replace existing Presence Information with new incoming information received by Presence Sources (see Section 4.4 of [RFC3903]).

The PS SHALL handle incoming publications as defined in [RFC3903].

5.4.1.2 Presence publication authorisation

Before accepting a PUBLISH request, the PS SHALL perform identity verification and authorization of the publication attempt of the Presence Source, per local policy.

When the SIP/IP Core corresponds to 3GPP IMS or 3GPP2 MMD then the PS SHALLverify the identity of the Presence Source of the PUBLISH request as described in [3GPP TS 24.229]/ [3GPP2 X.S0013-004-A] sub-clause 5.7.1.4.

The PS publication authorisation policy SHALL authorize the publication for the Presentity, and SHOULD reject the publication for all other users.

The PS SHALL perform authorisation of the publication by verifying that the identity of the source of the PUBLISH request matches against the value of the "entity" attribute of the <presence> element in the Presence Information document as described in [RFC3863].

If the Presentity is identified by a SIP URI and also pres URI or a tel URI, the PS SHALL consider these URIs equivalent for the purposes of publication and publication authorization.

In case of successful authorization, the PS accepts the PUBLISH request and SHALL process the PUBLISH request in accordance with [RFC3903].

5.4.1.3 Handling of partial publications

The PS MAY support partial publication.

If the Presence Source generates a partial publication request as described in chapter 5.1.1.1 using the 'application/pidf-diff+xml' content-type defined in [PARFORMAT] the PS SHALL process the PUBLISH request in accordance with [RFC3903] and [PARPUBLISH].

5.4.1.4 Handling of large objects

The PS MAY support the 'multipart/related' content type in accordance with [RFC2387].

If supported, the PS SHALL process a presence document represented as 'multipart/related' content type as follows:

- If the 'multipart/related' content type contains direct MIME object data, the PS SHALL check the size of the direct MIME object data.

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

- If the size exceeds the upper limit as defined by PS policies, the PS SHALL stop processing and return the SIP response "413 Request Entity Too Large". The upper limit used by the PS SHALL be at least equal to or greater than the respective limit defined for the Presence Source.
- If the size of the direct MIME object data is within the PS's upper limit, the PS SHALL either store the MIME object in case of initial publication or replace an existing content in case of modify operation.

- If the 'multipart/related' content type contains an indirect MIME object included in a 'message/external-body' content type and the content indirection [RFC4483] mechanism is supported by the PS, the PS SHALL associate the value of the relevant presence attribute with the external content.

If the PS does not support the 'multipart/related' content type, then the PS shall send a 415 (Unsupported Media Type) response and indicate the supported content types in the "Accept" header field.

5.4.2 Presence state event package

The PS SHALL support subscriptions for the presence event package, according to the procedures described in [RFC3265] and [RFC3856].

Before accepting a SUBSCRIBE request for the presence event package, the PS SHALL perform authorization of the subscription attempt of the Watcher, per Presentity policy. The policies to authorize the Watcher's subscription request are described in section 5.4.3.2. If the PS accepts the SUBSCRIBE request, the PS SHALL process the SUBCRIBE request in accordance with [RFC3265] and [RFC3856] with the following clarification:

- the PS SHALL NOT terminate a subscription because the Presentity's Presence Information which is being monitored does not exist. This allows a Watcher to remain subscribed to the Presentity and get its Presence Information whenever it is available.

If the Presentity is identified by a SIP URI and also a pres URI or a tel URI, the PS SHALL consider these URIs equivalent for the purposes of presence event package subscriptions.

The PS SHALL support notification of changes to the presence event package, according to the procedures described in [RFC3265] and [RFC3856], to authorized Watchers after applying the steps in section 5.4.3.

5.4.2.1 Handling of large objects

The PS MAY generate notifications using the 'multipart/related' content type in accordance with [RFC2387], if:

- the Presence Information formatted as 'application/pidf+xml' or 'application/pidf-diff+xml includes references to other MIME objects; and
- the Watcher indicates support for the 'multipart/related' content type using the "Accept" header field in the SUBSCRIBE request.

If the Watcher does not indicate support for the 'multipart/related' content type or a MIME object cannot be accessed by the PS, the PS SHOULD exclude the MIME object from the notification.

If the size of the MIME object data in the NOTIFY request exceeds the limit defined for the Watcher the PS SHALL handle the MIME object data as indirect content, i.e. store the MIME object data in the Content Server and include an HTTP or optionally HTTPS URI in the notification pointing to the stored MIME object.

If the reference to the MIME object is an HTTPor optionally HTTPS URI, the PS SHALL either:

- fetch the content using the HTTP GET method defined in [RFC2616] and include as direct content in the notification; or
- include an HTTP or optionally HTTPS URI as indirect content in the notification pointing to the MIME object.

Access to indirect content SHALL be restricted to the Watcher. Any appropriate mechanism may be used, given it does not impose any requirements to the Watcher other than having to issue an HTTP GET to fetch the indirect content from the provided URI.

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

In the case of sending the MIME object as direct content, the PS SHALL modify the value of the relevant Presence Information Element in the presence document to refer to the MIME object included in the 'multipart/related' content type.

5.4.3 Presence Information processing

The PS processes the Presence Information published by the Presence Sources before delivering it to the Watchers by applying the following steps in this order (see Figure 4):

1) Composition Policy (See section 5.4.3.1);
2) Presence Authorization Content Rules (See section 5.4.3.2);
3) Event notification filtering (See section 5.4.3.3);
4) Partial notification processing (See section 5.4.3.4);
5) Event notification throttling (See section 5.4.3.5); and
6) Notification generation (See section 5.4.3.6).

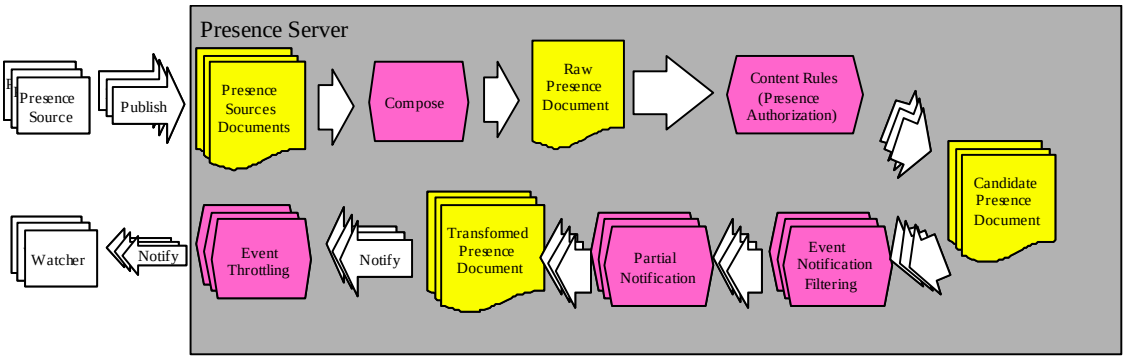

Figure 4 -Presence Information Processing Stages

5.4.3.1 Applying Composition Policy

The function of the PS to combine the "views" of the various Presence Sources in one single raw presence document for a particular Presentity is called composition. The PS SHALL support the presence data model defined in [PRESDDS].

Before applying the Composition Policy the PS SHALL, if a <timestamp> element exists in a <tuple> element, <person> element or <device> element, overwrite its value with the time the PUBLISH request was received. If a <timestamp> element does not exist in a <tuple> element, <person> element or <device> element, the PS SHALL add a <timestamp> element respectively. The PS SHALL NOT update <timestamp> element value on publication refreshes.

The PS SHALL ensure that consecutive publications never are assigned the same timestamp, such that in the case of conflicts Watchers are always able to differentiate between elements by looking at the time of their publication.

The PS SHALL apply the following Composition Policy.

NOTE: Local policy can augment this composition policy in which case implementations have to ensure that the semantics of this enabler are not violated.

5.4.3.1.1 Composition Policy

The PS SHALL compose the information from the different Presence Sources according to the following rules, based on the "service", "device", and "person" components of the presence data model (see [PRESDDS]):

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

- Service component

  If the following conditions all apply:

  - If one <tuple> element includes a <contact> element, other <tuple> elements include an identical <contact> element; and
  - If one <tuple> element includes a <service-description> element, other <tuple> elements include an identical <service-description> element. Two <service-description> elements are identical if they contain identical <service-id> and <version> elements; and
  - If one <tuple> element includes a <class> element, other <tuple> elements include an identical <class> element; and
  - If there are no conflicting elements (i.e. same elements with different values) or attributes under the <tuple> elements. Different <timestamp> values are not considered as a conflict.

  then the PS SHALL:

  1) Aggregate elements within a <tuple> element that are published from different Presence Sources into one <tuple> element. Identical elements with the same value and attributes SHALL not be duplicated; and
  2) Set the "priority" attribute of the <contact> element in the aggregated <tuple> element to the highest one among those in the input <tuple> elements, if any "priority" attribute is present; and
  3) Set the <timestamp> of the aggregated <tuple> to the most recent one among the ones that contribute to the aggregation; and
  4) Keep no more than one <description> element from the <service-description> elements of the aggregated <tuple> element when there are different values of the <description> elements.

  In any other case, the PS SHALL keep <tuple> elements from different Presence Sources separate.

- Device component

  If the <deviceID> of the <device> elements that are published from different Presence Sources match, then the PS SHALL

  1) Aggregate the non-conflicting elements within one <device> element; and
  2) Set the <timestamp> of the aggregated <device> element to the most recent one among the ones that contribute to the aggregation; and
  3) Use the element from the most recent publication for conflicting elements.

- Person component

  If the following conditions all apply:

  - If one <person> element includes a <class> element, other <person> elements include an identical <class> element; and
  - If there are no conflicting elements (same elements with different values or attributes) under the <person> elements. Different <timestamp> values are not considered as a conflict.

  then the PS SHALL:

  1) Aggregate elements within a <person> element that are published from different Presence Sources into one <person> element. Identical elements with the same value SHALL not be duplicated.
  2) Set the <timestamp> of the aggregated <person> element to the most recent one among the ones that contribute to the aggregation.

  In any other case, the PS SHALL keep <person> elements from different Presence Sources separate.

The PS SHALL ignore the values of instance identifier attributes (id) of <tuple>, <person> and <device> instances in presence documents published by Presence Sources.

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

The PS MAY change the values of instance identifier attributes (id) of <tuple>, <person> and <device> instances in presence documents that have been published by Presence Sources.

5.4.3.2 Applying Presence Authorisation Rules

The authorisation decision in the PS SHALL be determined based on authorisation policies defined by the service provider (local policy) and the Presence Authorisation Rules document stored in the Presence XDMS.

Presence Information is considered very sensitive personal information; therefore an authorisation mechanism SHALL be supported.

The PS SHALL apply the Presence Authorisation Rules to all authenticated SUBSCRIBE requests and outgoing notifications for the presence event package.

When the Presentity changes the Presence Authorization Rules, the PS SHALL ensure it applies the Presence Authorization Rules with those most recent changes. The Presence Authorization Rules can be changed either directly, when the Presence Authorization Rules document stored in Presence XDMS is updated, or indirectly, when the URI Lists stored in the Shared XDMS and referenced in the Presence Authorization Rules document are updated. The mechanism to achieve this is out of scope of this specification.

As defined in [PRESXDM] the Presence Authorisation Rules has two parts defined by the Presentity:

- Subscription Authorisation Rules, which determine if a Watcher is allowed to subscribe to the Presentity's Presence Information; and
- Presence Content Rules, which determine the subset of the Presentity's Presence Information the Watcher is allowed to watch.

When a SUBSCRIBE request is received for the presence event package, the PS SHALL fetch the Presentity's Presence Authorisation Rules document stored in the Presence XDMS according to the procedures defined in [XDMSPEC] section 6.1.1. When fetching the document, the PS SHALL construct the HTTP URI as follows:

- Set the XCAP Root URI as described in [XDMSPEC];
- Set the AUID to "org.openmobilealliance.pres-rules" as defined in [PRESXDM]; and
- Set the XUI to the SIP URI or tel URI of the Presentity.

For example, the HTTP URI of the Presence Authorisation Rules document for a Presentity with a SIP URI of sip:user@domain.com would be http://xcap.example.com/services/org.openmobilealliance.pres-rules/users/sip:user@domain.com/presrules, if the XCAP Root URI is http://xcap.example.com/services.

The PS SHALL determine which rules in the Presence Authorisation Rules document are applicable and evaluate the combined permissions according to the procedures described in [XDMSPEC] section 6.6.2.3, with the following clarifications:

- When realized in 3GPP IMS or 3GPP2 MMD networks, the PS SHALL use the received P-Asserted-Identity header (as defined in [3GPP TS 24.229] and [3GPP2 X.S0013-004-A]) in the SUBSCRIBE request to determine the URI value(s) used for matching against a conditions element;
- If a presence subscription is identified as anonymous (see section 7.1), the PS SHALL always evaluate the rule with the <anonymous-request> condition element as defined in [XDMSPEC];

  NOTE 1: Handling of anonymous presence subscription is different from handling described in [RFC5025].

- If an attempt to resolve an <external-list> condition element fails, the PS SHALL check if the evaluated URI value(s) match any other rule with <external-list> condition element and if not, the PS SHALL apply the "block" action defined below; and

  NOTE 2: In this case, default rules defined by <other-identity> element are ignored.

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

- If there is no matching rule then the PS SHALL apply the "block" action defined below.

After evaluating the combined permissions the PS SHALL handle the subscription for this Watcher based on the value of the <sub-handling> action as follows:

- if the value is "block" or there is no value, then the PS SHALL reject the subscription by responding to the SUBSCRIBE request to rules and procedures of [RFC5025] section 3.2;
- if the value is "polite-block", then the PS SHALL politely block the subscription following the procedures defined in section 5.4.3.2.1;
- if the value is "confirm", then the PS SHALL place the subscription in "pending" state according to rules and procedures of [RFC5025] section 3.2. The further treatment of the subscription will depend on the local policy of the PS, a typical example of such a local policy is the request for "reactive authorisation" from the Presentity; or
- if the value is "allow", then the PS SHALL place the subscription in the "active" state according to rules and procedures of [RFC5025] section 3.2 and apply the Presence Content Rules defined under the "transformations" element of the matched rules as specified in [PRESXDM].

While Watcher subscriptions are active, a Presentity may update its Subscription Authorization Rules. The PS SHALL re-evaluate the subscription state for each Watcher based on the new Subscription Authorization Rules. For example, a Presentity may decide to block subscriptions from a Watcher. If the Watcher has active subscriptions to the Presentity, the PS terminates these subscriptions and blocks any future subscription requests from this Watcher.

Furthermore, while Watcher subscriptions are active a Presentity may update its Presence Content Rules. The PS SHALL re-determine the subset of the Presentity's Presence Information the Watcher is allowed to watch. For example, a Presentity may decide to stop disseminating specific Presence Information Elements to its Watchers. In such a case the PS will generate presence notifications that will omit those specific Presence Information Elements.

NOTE 3: The mechanism for the PS to ensure that updates to the Presence Authorization Rules are being applied to active Watcher subscriptions is out of scope of this specification.

5.4.3.2.1 Polite blocking

Polite blocking is a mechanism to deny providing Presence Information updates , while indicating to the Watcher that the subscription is active.

If the result of applying Subscription Authorisation Rules is to perform polite blocking (see section 5.4.3.2), the PS SHALL perform the following:

1) The PS SHALL respond to the SUBSCRIBE request according to rules and procedures of [RFC5025] section 3.2;
2) The PS SHALL then send only one NOTIFY request to the PS, with the following content:
    a) provide only the <tuple> elements of the "raw presence document" of the Presentity indicating that the Presentity is "unwilling" and "unavailable" for communication (see [PRESDDS] for the exact details of how these states are mapped to relevant Presence Information Elements). If further child elements are contained in the "raw presence document" within the <tuple> elements apart from "willingness" and "availability", they SHALL be omitted by the PS.
    b) not provide <device> and <person> information elements, if existent in the Presentity's "raw presence document"
    c) perform all the next stages in the Presence Information processing framework, as they are listed in section 5.4.3 and detailed in relevant sub-sections (e.g. apply filtering, partial notifications, throttling, etc.).

5.4.3.3 Applying event notification filtering

The PS MAY support event notification filtering according to the following procedures:

- Event notification filtering, according to the procedures described in [RFC4660]; and

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

- Content type ‘application/simple-filter+xml’, according to [RFC4661].

If the PS supports event notification filtering; and

- understands the particular filter included in the payload of the SUBSCRIBE request using the content type ‘application/simple-filter+xml’, the PS SHALL apply the requested filter. As a result, the authorized Watchers are notified of the actual Presence Information after first applying the privacy filtering procedures as described in section 5.4.3.2 then the event notification filtering procedures described in this section; or

- does not understand the particular filter included in the payload of the SUBSCRIBE request as requested by the Watcher, the PS SHALL indicate it to the Watcher as specified in [RFC4660].

5.4.3.4 Applying partial notification

The PS SHALL support partial notifications. If the Watcher indicates preference for partial notifications in the SUBSCRIBE request for the presence event package, the PS SHALL generate partial notifications in accordance with [PARNOT] and [PARFORMAT].

5.4.3.5 Applying event notification throttling

The PS MAY have local throttling configuration setting that limit the rate at which notifications are generated (i.e. the shortest time period between two NOTIFY messages for a given Watcher). In this case, the PS SHALL NOT generate NOTIFY messages more often than the throttling configuration dictates, except when generating the notification either upon receipt of a SUBSCRIBE request or upon subscription state changes.

5.4.3.6 Generation of Notifications

At the last stage of the Presence Information processing the PS SHALL generate new NOTIFY requests for each Watcher and transmit each of those to the respective Watcher when the content of the new notification is different from the last one that was transmitted.

The PS SHALL set the “entity” attribute of the <presence> element included in the NOTIFY request to the same URI as the one used in the Request-URI of the received SUBSCRIBE request.

5.4.4 Watcher information event package

Before accepting a SUBSCRIBE request for the Watcher information event package, the PS SHALL perform authorization of the subscription attempt of the Watcher Information Subscriber, per local policy. The default policy SHALL be to authorize the subscription if the Watcher Information Subscriber is the Presentity, and to reject the subscription for all other users. If the PS accepts the SUBSCRIBE request, the PS SHALL process the SUBSCRIBE request in accordance with [RFC3265], [RFC3857], [RFC3858].

5.4.4.1 Applying event notification filtering

The PS MAY support event notification filtering according to the following procedures:

- Event notification filtering, according to the procedures described in [RFC4660]; and

- Content type ‘application/simple-filter+xml’, according to [RFC4661].

If the PS supports event notification filtering; and

- understands the particular filter included in the payload of the SUBSCRIBE request, the PS SHALL apply the requested filter; or

- does not understand the particular filter included in the payload of the SUBSCRIBE request, the PS SHALL indicate it to the subscriber as specified in [RFC4660] and [RFC4661].

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

5.4.5 XDM Functions

Certain PS functionality depends on particular documents stored in the Presence and Shared XDMSs. In order to provide this functionality the PS SHALL support the following :

- Retrieval of XML documents stored in the Presence XDMS and Shared XDMS, according to [XDMSPEC] section *"Procedures at the XDM Client"* (via the PRS-8 and PRS-5 reference points, respectively); and
- XCAP application usages specified in [PRESXDM] and [SharedXDM].

5.5 Resource List Server

The Resource List Server (RLS) performs the following functions:

- Accepts subscriptions to Presence Lists;
- Authorizes the Watcher's usage of the Presence List;
- Creates and manages back-end subscriptions to all Presentities in the Presence List, on behalf of the Watcher;
- Sends notifications to the Watcher, based on information received from the back-end subscriptions;
- Applies aggregation and rate control mechanisms to the notifications, as appropriate.

When the SIP/IP Core network corresponds with 3GPP IMS or 3GPP2 MMD networks, the RLS SHALL be implemented in an AS as defined in [3GPP TS 23.228] and [3GPP2 X.S0013-002-A] respectively.

5.5.1 General

The RLS SHALL support list subscriptions to the presence event package, according to the RLS procedures described in [RFC4662].

Before accepting a list subscription, the RLS SHALL perform authorization of the usage of a Presence List by the Watcher, per local policy.

If the list subscription is authorized, the RLS SHALL resolve the Presence List into individual Presentities according to section 5.5.4.

When sending a list notification, the RLS SHALL set the "uri" attribute of each <resource> element included in the RLMI document to the URI for the Presentity that is stored in the Presence List.

NOTE: If a Presentity is identified by a pres URI or a tel URI in the Presence List, the pres URI or the tel URI is included in the RLMI document correspondingly even if the RLS has knowledge of an equivalent SIP URI.

5.5.2 Back-end Subscriptions

For list subscriptions to the presence event package, the RLS SHALL generate back-end subscriptions to learn the Presence Information of Presentities in the list.

Some or all back-end subscriptions may be virtual subscriptions. For back-end subscriptions using SIP, the RLS SHALL support subscription and notification of Presence Information, according to the procedures described in sections 5.2.1, 5.2.2, 5.2.4, 5.2.5 and 5.2.6.

When the SIP/IP Core network corresponds to 3GPP IMS or 3GPP2 MMD networks, the RLS SHALL follow the procedures described in section 5.7.3 of [3GPP TS 24.229] and [3GPP2 X.P0013-004-A] and insert a URI value from the P-Asserted-Identity header of the incoming SIP SUBSCRIBE request (as defined in [3GPP TS 24.229] and [3GPP2 X.P0013-004-A]) to the SIP SUBSCRIBE request of the back-end subscription, as opposed to acting as an authentication service ([RFC4474]) required by the [RFC4662].

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

If the OTA Provisioning parameter MAX-NUMBER-OF-SUBSCRIPTIONS-IN-PRESENCE-LIST or local policy instructs, the RLS SHALL limit the number of back-end subscriptions. The RLS SHALL:

- initiate no more back-end subscriptions as instructed by the provisioning parameter or local policy; and
- return no <instance> element for those <resource> elements that could not be subscribed from the Presence List document due to this limitation. The <instance> and <resource> elements are part of the Resource List Meta-Information (RLMI) document as defined in [RFC4662].

When the Watcher adds Presentities to the Presence List while the list subscription is active, the RLS SHALL generate back-end subscriptions for the newly added Presentities, and SHALL include the newly added Presentities in the next list notification. This procedure SHALL NOT require the Watcher to re-subscribe to the Presence List.

When the Watcher removes Presentities from the Presence List while the list subscription is active, the RLS SHALL terminate back-end subscriptions to the recently removed Presentities, and SHALL indicate that the back-end subscriptions have been terminated in the next list notification. This procedure SHALL NOT require the Watcher to re-subscribe to the Presence List.

The Presence List can be changed either directly, when the Presence List document stored in RLS XDMS is updated, or indirectly, when the URI List stored in the Shared XDMS and referenced in the Presence List document is updated.

NOTE: The mechanism for the RLS to ensure that updates to the Presence List are being applied to active list subscriptions is out of scope of this specification.

When the Watcher refreshes the subscription, the RLS SHOULD refresh the back-end subscriptions accordingly. The RLS SHOULD try to re-generate the back-end subscriptions for those Presentities whose corresponding <resource> element in the last list notification:

- did not include an <instance> element, if the omission was not caused by a limit to the maximum number of back-end subscriptions; or
- included an <instance> element whose “state” attribute was set to “terminated”.

5.5.3 Event Notification Filtering

The RLS MAY support event notification filtering according to the following procedures:

- Event notification filtering, according to the RLS and notifier procedures described in [RFC4660] with the clarifications described in this section; and
- Content type ‘application/simple-filter+xml’, according to [RFC4661].

If the RLS supports event notification filtering; and

- understands the particular filter included in the payload of the SUBSCRIBE request, the RLS SHALL:
  - if the filter element contains a “uri” attribute and its value matches with the URI of a Presentity in the Presence List, supply the filter document in the back-end subscription to the matching Presentity;
  - if the filter element contains a “domain” attribute and its value matches with the domain of a set of Presentities in the Presence List, supply the filter document in the back-end subscriptions to the Presentities matching the “domain” attribute, but and not matching the “uri” attribute in other filters in the filter-set; and
  - if the filter element does not contain a “uri” or “domain” attribute, supply the filter document in the back-end subscriptions to all Presentities in the Presence List not matching a “uri” or a “domain” attribute in other filters in the filter-set; or
- does not understand the particular filter included in the payload of the SUBSCRIBE request as requested by the Watcher, the RLS SHALL indicate it to the Watcher as specified in [RFC4660].

For every filter propagated in a back-end subscription targeted to a Presentity, the RLS SHALL remove the “uri” or “domain” attribute if included in the RLS filter obtained from the Watcher.

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

5.5.4 XDM Functions

In order to resolve Presence Lists into individual Presentities, the RLS SHALL support the following:

- Retrieval of XML documents stored in the RLS XDMS and Shared XDMS, according to [XDMSPEC] "*Document Management*" (via the PRS-10 and PRS-9 reference points, respectively); and
- XCAP application usages specified in [RLSXDM] and [SharedXDM].

On receiving a SIP SUBSCRIBE request directed at a Presence List identified by a Request-URI, the RLS SHALL access the global "index" document described in [RLSXDM] using the XCAP path
[XCAP Root URI]/rls-services/global/index.

The RLS SHALL retrieve the Presence List from the contents of the <service> element within the index document whose "uri" attribute value matches the Request-URI of the received SUBSCRIBE request. If the RLS is unable to retrieve the Presence List from the RLS XDMS, the RLS SHALL reject the SUBSCRIBE request with a 404 (Not Found) response.

The Presence List can contain references to URI Lists stored in the Shared XDMS. If the RLS is unable to retrieve a URI List from the Shared XDMS, then that URI List SHOULD be ignored; if so, the Watcher is made aware of this when the URIs which could not be de-referenced are omitted from the list notification.

When realized in 3GPP IMS or 3GPP2 MMD networks, the RLS SHALL insert a URI from the received P-Asserted-Identity header (as defined in [3GPP TS 24.229] and [3GPP2 X.P0013-004-A]) from the SIP SUBSCRIBE request in the "X-3GPP-Asserted-Identity" header, as defined in [3GPP TS 24.109] or the "X-XCAP-Asserted-Identity" header as defined in [XDMSPEC], of the HTTP GET request.

5.5.5 Rate control and Aggregation

Subject to rate limitations described below, the RLS SHALL generate notifications when it receives updated information from back-end subscriptions.

The RLS MAY have local throttling configuration settings that limit the rate at which notification are generated (i.e. the shortest time period between two NOTIFY message). In this case, the RLS SHALL NOT generate NOTIFY messages more often than the throttling configuration dictates, except when generating the notification either upon receipt of a SUBSCRIBE request or upon subscription state changes.

If multiple back-end notifications arrive while rate control restrictions apply, the RLS MAY aggregate those notifications (i.e. combine the presence content into a single NOTIFY message) and transmit them when those restrictions expire. The mechanism by which multiple notifications are aggregated is described in [RFC4662].

5.6 XDM Client

The XDM Client SHALL support the XDM Client procedures described in [XDMSPEC] section *"Procedures at the XDM Client"* and the XCAP application usages described in [PRESXDM], [RLSXDM], and [SharedXDM].

5.7 Presence XDMS

The Presence XDMS SHALL support the XDM Server procedures described in [XDMSPEC] section *"Procedures at the XDM Server"* and the XCAP application usages described in [PRESXDM].

5.8 RLS XDMS

The RLS XDMS SHALL support the XDM Server procedures described in [XDMSPEC] section *"Procedures at the XDM Server"* and the XCAP application usages described in [RLSXDM].

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

5.9 Content Server

The Content Server SHALL support HTTP GET and PUT methods [RFC2616], and the procedures defined in [RFC4483].

The Content Server SHALL store a MIME object when receiving it in an HTTP PUT request behind the HTTP URI therein.

The Content Server SHALL return a MIME object in a 200 OK response to an HTTP GET request. The Content Server SHALL fetch the MIME object from the Request URI of the HTTP GET request.

The Content Server can be used by Presence Sources as described in section 5.1.1.2, Watchers as described in section 5.2.6 and the PS as described in sections 5.4.1.4 and 5.4.2.1.

NOTE: The procedure for storing MIME objects is not defined by this specification.

5.10 Shared XDMS

The Shared XDMS is described in [XDMSPEC] section 5.2.

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

6. Void

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

7. Security

The security mechanism provides the protection to the Presence Service environment.

7.1 Privacy

7.1.1 Watcher privacy

If the Watcher desires subscription privacy, it SHALL set the From header field of the SIP SUBSCRIBE request to anonymous value as defined in [RFC3261].

The Watcher MAY indicate further privacy preferences in accordance with [RFC3323].

When the SIP/IP Core network corresponds with 3GPP IMS or 3GPP2 MMD networks, the Watcher SHALL include a Privacy header value set to “id” as described in [RFC3325].

7.1.2 Watcher Information Subscriber Privacy

A subscription to Watcher information SHALL be authorized if the Watcher Information Subscriber is the Presentity and SHALL be rejected for all other users.

Anonymous Watcher information subscription SHALL be rejected.

7.1.3 Presentity Privacy

Privacy of the Presentity, i.e. who receives which of the Presentity’s Presence Information is ensured by the presence authorization mechanism described in section 5.4.3.2.

7.1.4 Handling of anonymous presence subscriptions in Presence Server

The PS SHALL consider a subscription as anonymous if any of the following conditions are true:

- When the SIP/IP Core network corresponds with 3GPP IMS or 3GPP2 MMD networks, and the SIP SUBSCRIBE request contains a Privacy header value set to "id" or "user" as described in [3GPP TS 24.229]/[3GPP2 X.S0013-004-A] section 5.7.1.4; or
- The SIP SUBSCRIBE request contains a From header indicating an anonymous value as described in [RFC3261].

Authorization of anonymous subscriptions SHALL be according to the Presentity’s Subscription Authorization Rules for anonymous subscriptions (see section 5.4.3.2).

7.2 Authentication of SIP requests

The PS or RLS SHALL authenticate all incoming SIP requests. The PS or RLS SHOULD rely on the authentication mechanisms provided by the underlying SIP/IP Core network to accomplish user identity verification.

When the SIP/IP Core network corresponds with 3GPP IMS or 3GPP2 MMD networks:

- The authentication mechanism is specified in [3GPP TS 33.203]/[3GPP2 S.R0086-A];
- The PS or RLS SHALL authenticate the SIP request originator as specified in [3GPP TS 24.229]/[3GPP2 X.S0013-004-A] section 5.7.1.4; and
- The PS or RLS acting on behalf of the Presence Source or the Watcher SHALL populate security related SIP header fields according to the procedures given in [3GPP TS 24.229]/[3GPP2 X.S0013-004-A] section 5.7.3.

An AS acting as originating UA SHALL follow the authentication procedures given in [3GPP TS 24.229]/[3GPP2 X.S0013-004-A] section 5.7.3.

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

7.3 Integrity and confidentiality protection

The access level security mechanism SHALL be provided by the SIP/IP Core network to support integrity and confidentiality protection of SIP signalling.

When the SIP/IP Core network corresponds with 3GPP IMS or 3GPP2 MMD networks, the integrity and confidentiality protection mechanism is specified in [3GPP TS 33.203]/[3GPP2 S.R0086-A].

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

8. Charging

8.1 Charging Architecture

Since both online and offline charging SHOULD be supported according to [PRESREQ], there are two different charging architectures, which can be simplified as shown in the following subsections.

8.1.1 Offline Charging Architecture

When the SIP/IP Core network corresponds with 3GPP IMS or 3GPP2 MMD networks the offline charging SHOULD be performed according to [3GPP TS 32.240] [3GPP TS 32.260] for 3GPP and [3GPP2 X.S0013-007-A] [3GPP2 X.S0013-008-A] for 3GPP2.

In the context of other realisations of the SIP/IP Core network similar charging functions SHOULD be provided.

8.1.2 Online Charging Architecture

When the SIP/IP Core network corresponds with 3GPP IMS or 3GPP2 MMD networks the online charging SHOULD be performed according to [3GPP TS 32.240] [3GPP TS 32.260] for 3GPP and [3GPP2 X.S0013-007-A] [3GPP2 X.S0013-008-A] for 3GPP2.

In the context of other realisations of the SIP/IP Core network similar charging functions SHOULD be provided.

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

9. Registration

When the SIP/IP Core corresponds with 3GPP IMS or 3GPP2 MMD networks, the Presence Source and the Watcher implemented by a UE SHALL use the 3GPP IMS or 3GPP2 MMD networks registration mechanisms as defined in [3GPP TS 24.229] and [3GPP2 X.S0013-004-A].

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

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

10. Content of the Presence Document

The presence data model and the content of the presence document is described in [PRESDDS].

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

11. SIP Methods

11.1 SUBSCRIBE Method

When SIP/IP Core network is realised with 3GPP IMS or 3GPP2 MMD networks, the supported headers of the SUBSCRIBE method and its responses SHALL correspond to those defined in [3GPP TS 24.229] and [3GPP2 X.S0013-004-A] respectively.

In the context of other realisations of the SIP/IP Core network the supported headers of the SUBSCRIBE method and its responses SHALL correspond to those defined in [RFC3265], [RFC3857] and [RFC3856].

11.2 PUBLISH Method

When SIP/IP Core network is realised with 3GPP IMS or 3GPP2 MMD networks, the supported headers of the PUBLISH method and its responses SHALL correspond to those defined in [3GPP TS 24.229] and [3GPP2 X.S0013-004-A] respectively.

In the context of other realisations of the SIP/IP Core network the supported headers of the PUBLISH method and its responses SHALL correspond to those defined in [RFC3903].

11.3 NOTIFY Method

When SIP/IP Core network is realised with 3GPP IMS or 3GPP2 MMD networks, the supported headers of the NOTIFY method and its responses SHALL correspond to those defined in [3GPP TS 24.229] and [3GPP2 X.S0013-004-A] respectively.

In the context of other realisations of the SIP/IP Core network the supported headers of the NOTIFY method and its responses SHALL correspond to those defined in [RFC3265], [RFC3857] and [RFC3856].

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

Appendix A. Static Conformance Requirements

The SCR's defined in the following tables include SCR for:

- Presence Source
- PS
- RLS
- Watcher
- XDM Client
- Presence XDMS
- RLS XDMS

Each SCR table indentifies a list of supported features as:

Item: Identifier for a feature.

Function: Short description of the feature.

Reference: Section(s) of this specification with more details on the feature.

Status: Whether support for the feature is mandatory or optional. MUST use "M" for mandatory support and "O" for optional support in this column.

Requirement: This column identifies other features required by this feature. If no other features are required, this column is left empty.

This section describes the dependency grammar notation to be used in the Requirement column of the SCR and CCR tables using ABNF [RFC4234].

TerminalExpression = ScrReference / NOT TerminalExpression / TerminalExpression LogicalOperator TerminalExpression / "(" TerminalExpression ")"

ScrReference = ScrItem / ScrGroup

ScrItem = SpecScrName "–" GroupType "–" DeviceType "–" NumericId / SpecScrName "–" DeviceType "–" NumericId

ScrGroup = SpecScrName ":" FeatureType / SpecScrName "– " GroupType "–" DeviceType "–" FeatureType

SpecScrName = 1*Character;

GroupType = 1*Character;

DeviceType = "C" / "S"; C – client, S – server

NumericId = Number Number Number

LogicalOperator = "AND" / "OR"; AND has higher precedence than OR and OR is inclusive

FeatureType = "MCF" / "OCF" / "MSF" / "OSF"; See Section A.1.6

Character = %x41-5A ; A-Z

Number = %x30-39 ; 0-9

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

A.1 Presence Source

Item	Function	Reference	Status	Requirement
SIMPLE-SRC-C-001	Support SIP PUBLISH to publish Presence Information	5.1.1	M	SIMPLE-SRC-C-006 OR SIMPLE-SRC-C-007
SIMPLE-SRC-C-002	application/pidf+xml PIDF	5.1.1	M	
SIMPLE-SRC-C-003	Presence Data Model	5.1.1	M	
SIMPLE-SRC-C-004	Partial Publication	5.1.1.1	O	SIMPLE-SRC-C-006 OR SIMPLE-SRC-C-007
SIMPLE-SRC-C-005	Content Indirection	5.1.1.2.1	O	
SIMPLE-SRC-C-006	IMS SIP PUBLISH Method	11.2	O	
SIMPLE-SRC-C-007	NON-IMS SIP PUBLISH Method	11.2	O	
SIMPLE-SRC-C-008	Direct Content	5.1.1.2.2	O	
SIMPLE-SRC-C-009	Source Throttle Publish	5.1.1.3	O	
SIMPLE-SRC-C-010	Presence entity attribute settings	5.1.1	M	SIMPLE-SRC-C-006
SIMPLE-SRC-C-011	Supporting other PIDF extensions	5.1.1	O	
SIMPLE-SRC-C-012	SIGCOMP	5.1.1.4	O	

A.2 Presence Server

Item	Function	Reference	Status	Requirement
SIMPLE-PS-S-001	Presence Data Model	5.4.3	M	
SIMPLE-PS-S-002	Publication of Presence Information	5.4.1	M	SIMPLE-PS-S-007 OR SIMPLE-PS-S-008
SIMPLE-PS-S-003	Presence Information Subscriptions	5.4.2	M	SIMPLE-PS-S-005 OR SIMPLE-PS-S-006
SIMPLE-PS-S-004	Presence Information Notifications	5.4	M	SIMPLE-PS-S-009 OR SIMPLE-PS-S-011
SIMPLE-PS-S-005	IMS SIP SUBSCRIBE Method	11	O	
SIMPLE-PS-S-006	NON-IMS SIP SUBSCRIBE Method	11	O	
SIMPLE-PS-S-007	IMS SIP PUBLISH Method	11	O	
SIMPLE-PS-S-008	NON-IMS SIP PUBLISH Method	11	O	
SIMPLE-PS-S-009	IMS SIP NOTIFY Method	11	O	
SIMPLE-PS-S-011	NON-IMS SIP NOTIFY Method	11	O	
SIMPLE-PS-S-012	Fetch Presence XDMS content	5.4	M	Presence_XDM-AU-S-001, Presence_XDM-AU-S-002, Presence_XDM-AU-S-003, Presence_XDM-AU-S-004, Presence_XDM-AU-S-005, Presence_XDM-AU-S-006, Presence_XDM-AU-S-007
SIMPLE-PS-S-013	Void			

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

Item	Function	Reference	Status	Requirement
SIMPLE-PS-S-014	Fetch Shared XDMS content	5.4	M	Shared_XDM-AU-S-001, Shared_XDM-AU-S-002, Shared_XDM-AU-S-003, Shared_XDM-AU-S-004, Shared_XDM-AU-S-005, Shared_XDM-AU-S-006, Shared_XDM-AU-S-007
SIMPLE-PS-S-015	Void			
SIMPLE-PS-S-016	Content Indirection of Presence Notification	5.4	O	
SIMPLE-PS-S-017	Direct Content of Presence Notification	5.4	O	
SIMPLE-PS-S-018	Watcher Information Subscriptions	5.4.4	M	SIMPLE-PS-S-005 OR SIMPLE-PS-S-006
SIMPLE-PS-S-019	Watcher Information Notifications	5.4.4	M	SIMPLE-PS-S-009 OR SIMPLE-PS-S-011
SIMPLE-PS-S-021	Partial Notifications	5.4	M	
SIMPLE-PS-S-022	Polite Blocking	5.4	M	

A.3 Watcher Information Subscriber

Item	Function	Reference	Status	Requirement
SIMPLE-WIS-C-001	IMS SIP SUBSCRIBE Method	11	O	
SIMPLE-WIS-C-002	NON-IMS SIP SUBSCRIBE Method	11	O	
SIMPLE-WIS-C-003	IMS SIP NOTIFY Method	11	O	
SIMPLE-WIS-C-004	NON-IMS SIP NOTIFY Method	11	O	
SIMPLE-WIS-C-005	Subscription for the Watcher information template package	5.3	O	
SIMPLE-WIS-C-006	SIGCOMP	5.3.2.1	O	

A.4 RLS Server

Item	Function	Reference	Status	Requirement
SIMPLE-RLS-S-001	Presence List Subscription	5.5	M	RLS_XDM-AU-S-001, RLS_XDM-AU-S-002, RLS_XDM-AU-S-003, RLS_XDM-AU-S-004, RLS_XDM-AU-S-007, SIMPLE-RLS-S-004 OR SIMPLE-RLS-S-005
SIMPLE-RLS-S-002	List Notifications	5.5	M	RLS_XDM-AU-S-001, RLS_XDM-AU-S-002, RLS_XDM-AU-S-003, RLS_XDM-AU-S-004, RLS_XDM-AU-S-007, SIMPLE-RLS-S-006 OR SIMPLE-RLS-S-007
SIMPLE-RLS-S-004	IMS SIP SUBSCRIBE Method	11	O	
SIMPLE-RLS-S-005	NON-IMS SIP SUBSCRIBE Method	11	O	
SIMPLE-RLS-S-006	IMS SIP NOTIFY Method	11	O	
SIMPLE-RLS-S-007	NON-IMS SIP NOTIFY Method	11	O	
SIMPLE-RLS-S-008	Partial Notifications	5.5	M	SIMPLE-RLS-S-006 OR SIMPLE-RLS-S-007

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

Item	Function	Reference	Status	Requirement
SIMPLE-RLS-S-009	Void			
SIMPLE-RLS-S-010	Fetch RLS XDMS content	5.5	M	RLS_XDM-AU-S-001, RLS_XDM-AU-S-002, RLS_XDM-AU-S-003, RLS_XDM-AU-S-004, RLS_XDM-AU-S-005, RLS_XDM-AU-S-006, RLS_XDM-AU-S-007, RLS_XDM-AU-S-008, RLS_XDM-AU-S-009
SIMPLE-RLS-S-011	Void			
SIMPLE-RLS-S-012	Fetch Shared XDMS content	5.5	M	Shared_XDM-AU-S-001, Shared_XDM-AU-S-002, Shared_XDM-AU-S-003, Shared_XDM-AU-S-004, Shared_XDM-AU-S-005, Shared_XDM-AU-S-006, Shared_XDM-AU-S-007

A.5 Watcher

Item	Function	Reference	Status	Requirement
SIMPLE-WATCH-C-001	Presence Data Model	5.2.3	M	
SIMPLE-WATCH-C-002	Presence Subscription	5.2.1	M	SIMPLE-WATCH-C-009 OR SIMPLE-WATCH-C-010
SIMPLE-WATCH-C-003	Presence List Subscription	5.2.1	O	SIMPLE-WATCH-C-009 OR SIMPLE-WATCH-C-010
SIMPLE-WATCH-C-004	Presence Notifications	5.2.1	M	SIMPLE-WATCH-C-011 OR SIMPLE-WATCH-C-012
SIMPLE-WATCH-C-005	Partial Notification	5.2.4	O	SIMPLE-WATCH-C-009 OR SIMPLE-WATCH-C-010
SIMPLE-WATCH-C-006	Content Indirection	5.1.1.2.1	O	
SIMPLE-WATCH-C-07	Rich Presence Information	5.1	O	
SIMPLE-WATCH-C-008	Presence-based Location Object	5.1	O	
SIMPLE-WATCH-C-009	IMS SIP SUBSCRIBE Method	11	O	
SIMPLE-WATCH-C-010	NON-IMS SIP SUBSCRIBE Method	11	O	
SIMPLE-WATCH-C-011	IMS SIP NOTIFY Method	11	O	
SIMPLE-WATCH-C-012	NON-IMS SIP NOTIFY Method	11	O	
SIMPLE-WATCH-C-013	SIGCOMP	5.2.7.1	O	

A.6 XDM Client

Item	Function	Reference	Status	Requirement
Presence_SIMPLE-XDMC-C-001	Mandatory XDMC functions	5.6	M	XDM_Core: MCF AND SHARED_XDM:MCF AND RLS_XDM:MCF AND PRESENCE_XDM:MCF
Presence_SIMPLE-XDMC-C-002	Optional XDMC functions	5.6	O	XDM_Core:OCF AND SHARED_XDM:OCF RLS_XDM:OCF AND PRESENCE_XDM:OCF

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

A.7 Presence XDMS

Item	Function	Reference	Status	Requirement
Presence_SIMPLE-PresenceXDMS-S-001	Mandatory Presence XDMS functions	5.7	M	XDM_Core:MSF AND PRESENCE_XDM:MSF
Presence_SIMPLE-PresenceXDMS-S-002	Optional Presence XDMS functions	5.7	O	XDM_Core:OSF AND PRESENCE_XDM:OSF

A.8 RLS XDMS

Item	Function	Reference	Status	Requirement
Presence_SIMPLE-RLSXDMS-S-001	Mandatory RLS XDMS functions	5.8	M	XDM_Core:MSF AND RLS_XDM:MSF
Presence_SIMPLE-RLSXDMS-S-002	Optional RLS XDMS functions	5.8	O	XDM_Core:OSF AND RLS_XDM:OSF

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

Appendix B. Presence Client Provisioning (Normative)

This Appendix specifies the parameters that are needed by the presence client. Existing parameters in [Provisioning Content] and [OMA-DM-v1-1-2] are re-used, those without corresponding parameters are defined and to be registered in OMNA through OMA official ergistration process.

The Management Object (MO) for the OMA SIMPLE Presence 1.1 enabler is defined in [PRESMO]. The MO MAY be used for initial provisioning of parameters when the DM Profile is to be used (as specified on [OMA-DM-v1-2]), and the MO SHOULD be used for continuous provisioning of parameters according to [OMA-DM-v1-1-2] or [OMA-DM-v1-2], if required by the service provider to update service configurations.

B.1 Presence Client provisioning parameters

The following table lists the parameters available in an instance of the Presence Application Characteristics:

Parameter Name	Man / Opt	Instances	Default
Standard Application Characteristic fields as defined in [Provisioning Content]			
APPID	Mandatory	1	“ap0002”
PROVIDER-ID	Optional	0 or 1	none
APPREF	Mandatory	1	none
TO-APPREF	Mandatory	1 or more	none
NAME	Optional	0 or 1	none
TO-NAPID	Optional	0 or more	none
Application Characteristic fields specifically required for the Presence Enabler			
CLIENT-OBJ-DATA-LIMIT	Mandatory	1	none
CONTENT-SERVER-URI	Optional	0 or 1	none
SOURCE-THROTTLE-PUBLISH	Optional	0 or 1	none
MAX-NUMBER-OF-SUBSCRIPTIONS-IN-PRESENCE-LIST	Optional	0 or 1	none
SERVICE-URI-TEMPLATE	Optional	0 or 1	none

The Presence Application Characteristics file for the OMA SIMPLE Presence 1.1 enabler is defined in [PRESAC].

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

Appendix C. Presence Signalling Flows (Informative)

The following signalling flows illustrate the implementation of the relevant use cases, derived from the [PRESREQ]. The supported headers of the SIP methods used in order to perform those functions are defined in section 11 and the body of the messages, when required, in section 11.

C.1 Subsystem Collaboration

This section presents message flow examples for the implementation of the basic mechanisms of the SIMPLE Presence Service.

C.1.1 Signalling flows for publishing Presence Information

C.1.1.1 Publishing Presence Information

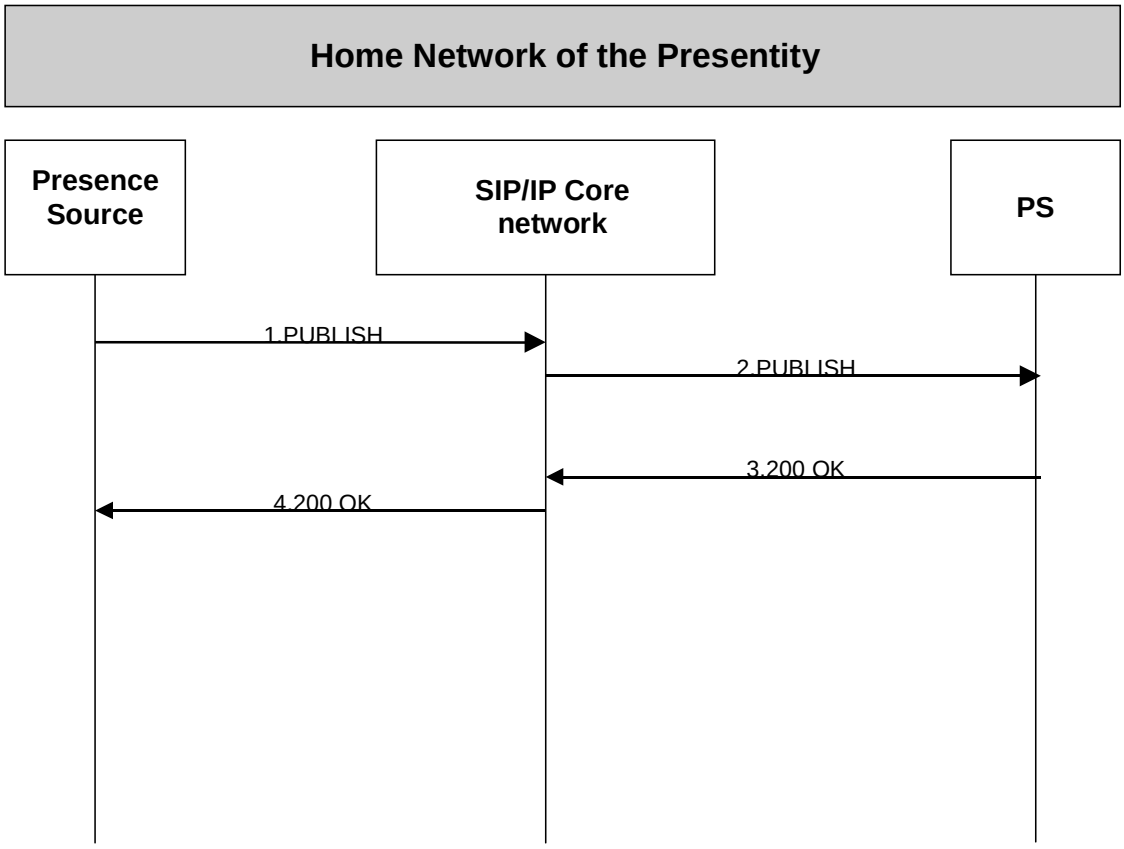

Figure 5- Publishing Presence Information

1. The Presence Source generates a SIP PUBLISH request, which contains a presence document. The means for the Presence Source to compose this presence document is outside the scope of this specification.
2. The SIP/IP Core network routes the request to the correct PS.
3. The PS authorises the presence publication, and checks the information the message contains. The PS then processes the Presence Information and sends a SIP 200 OK response back to Presence Source.
4. The SIP/IP Core network forwards the response back to the Presence Source.

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

C.1.1.2 Publishing Presence Information on behalf of another Presentity

C.1.1.2.1 Successful attempt

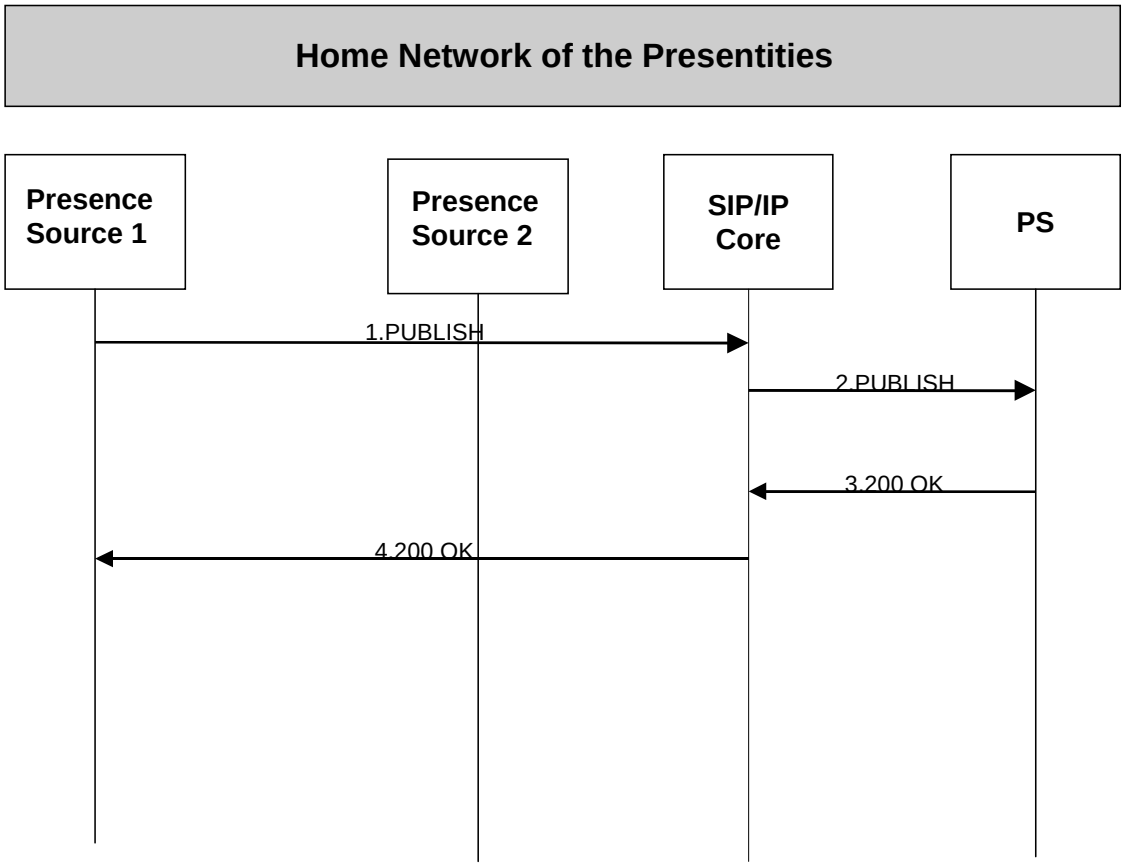

Figure 6 - Aggregating published Presence Information from multiple sources

1. Presence Source1 generates a SIP PUBLISH request, which contains Presence Information relating to Presence Source2's Presentity. The means for the Presence Source1 to compose the Presence Information is outside the scope of this specification.
2. The SIP/IP Core network forwards the SIP PUBLISH request to the appropriate PS.
3. The PS authorises the publication attempt and checks the content of the request. The PS then composes the Presence Information to the presence document of Presence Source2's Presentity. The PS sends a SIP 200 OK response back to the SIP/IP Core network.
4. The SIP/IP Core network forwards the SIP 200 OK response back to the Presence Source1.

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

C.1.1.2.2 Unsuccessful attempt

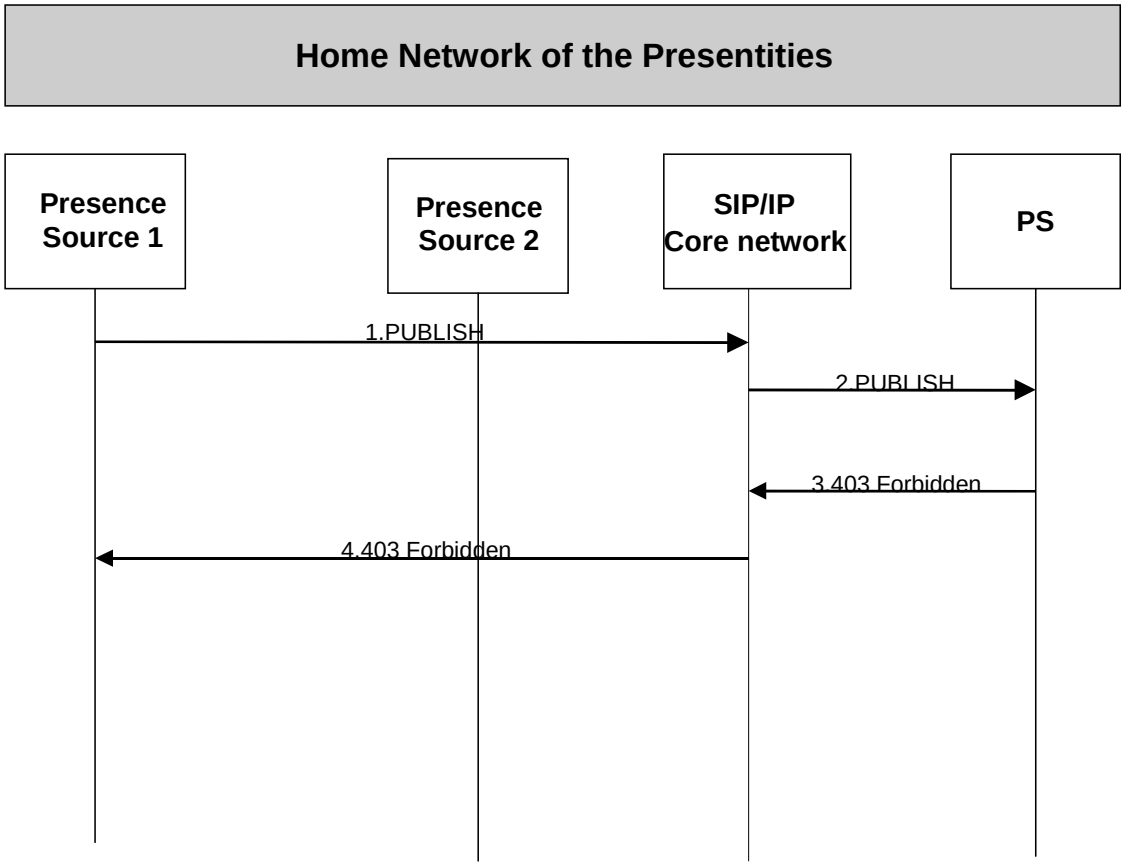

Figure 7 - Aggregating published Presence Information from multiple sources

1. Presence Source1 generates a SIP PUBLISH request, which contains Presence Information relating to Presence Source2's Presentity. The means for the Presence Source1 to compose the Presence Information is outside the scope of this specification.
2. The SIP/IP Core network forwards the SIP PUBLISH request to the appropriate PS.
3. The PS does not authorise the request and sends a SIP 403 Forbidden response back to the SIP/IP Core network.
4. The SIP/IP Core network forwards the SIP 403 Forbidden response back to the Presence Source1.

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

C.1.1.2.3 Aggregating published Presence Information from multiple sources

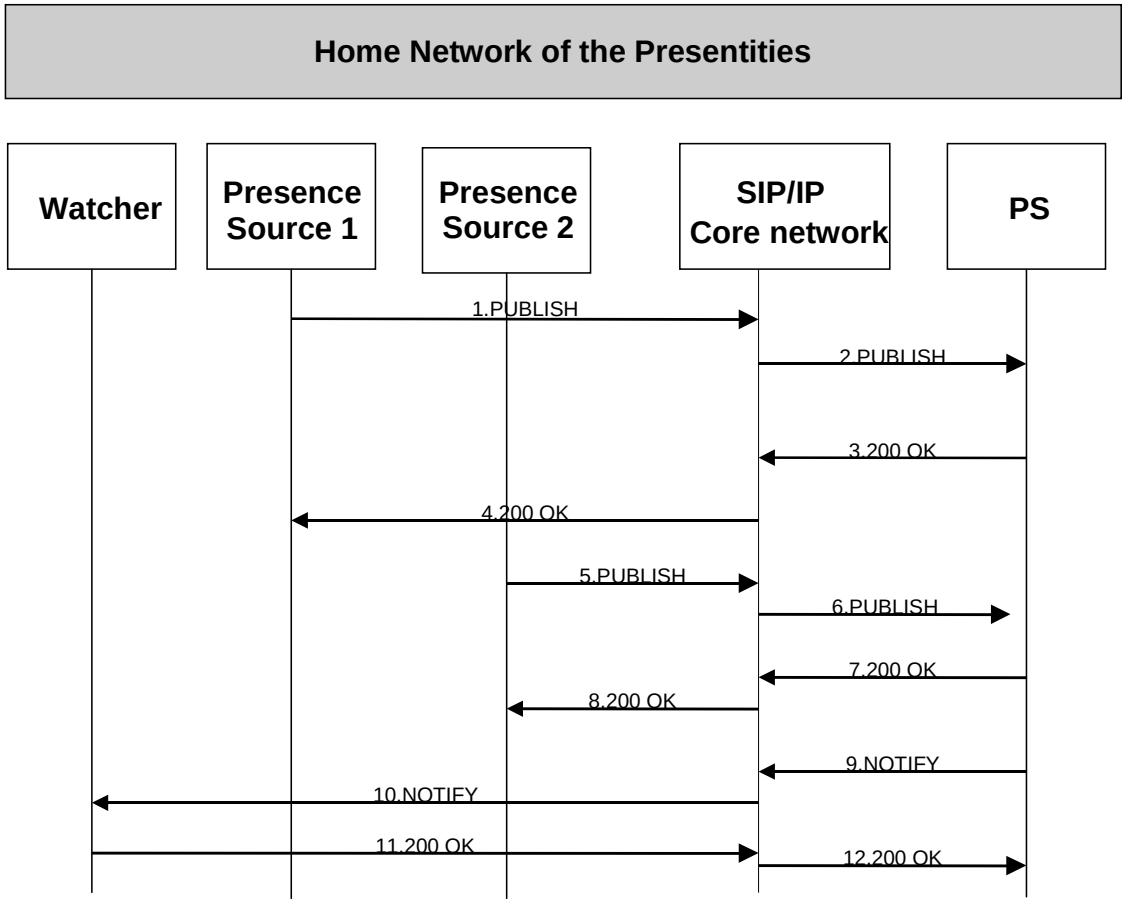

Figure 8- Aggregating published Presence Information from multiple sources

1. Presence Source1 generates a SIP PUBLISH request, which contains the Presence Information Presence Source1 wishes to publish on behalf of the Presentity.
2. The SIP/IP Core network forwards the SIP PUBLISH request to the appropriate PS.
3. The PS authorises the publication attempt and checks the content of the request. The PS then composes the Presence Information to the Presentity's presence document. The PS sends a SIP 200 OK response back to the SIP/IP Core network.
4. The SIP/IP Core network forwards the SIP 200 OK response back to the Presence Source1.
5. Presence Source2 generates a SIP PUBLISH request, which contains the Presence Information Presence Source2 wishes to publish on behalf of the Presentity.
6. The SIP/IP Core network forwards the SIP PUBLISH request to the appropriate PS.
7. The PS authorises the publication attempt and checks the content of the request. The PS then composes the Presence Information to the Presentity's presence document aggregating with the information Presence Source1 has published. The PS sends a SIP 200 OK response back to the SIP/IP Core network.
8. The SIP/IP Core network forwards the SIP 200 OK response back to the Presence Source2.

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

9. The PS determines which authorised Watchers are entitled to receive the updates of the Presence Information for this Presentity. For each appropriate Watcher, the PS sends a SIP NOTIFY request that contains the aggregated Presence Information from Presence Source1 and Presence Source2. The SIP NOTIFY request is sent along the path of the SUBSCRIBE dialog to the SIP/IP Core network of the Watcher.
10. The SIP/IP Core network forwards the SIP NOTIFY request to the Watcher.
11. The Watcher acknowledges the SIP NOTIFY request with a SIP 200 OK response to its SIP/IP Core network.
12. The SIP/IP Core network of the Watcher forwards the SIP 200 OK response to the PS.

C.1.2 Signalling flows for Watchers subscribing to presence event notification

C.1.2.1 Subscribing to Presence Information state changes - Proactive Authorization

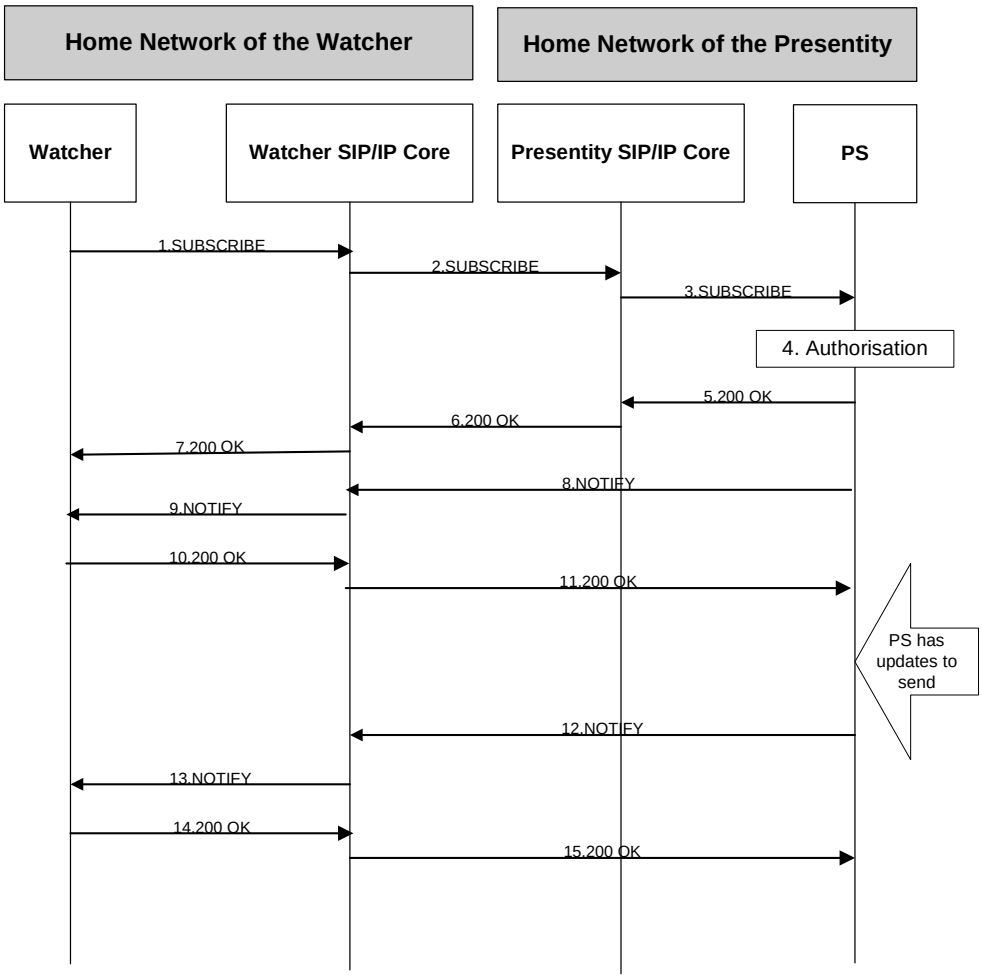

Figure 9 - Subscribing to Presence Information state changes (Watcher and Presentity are in different networks) – Proactive Authorization

1. A Watcher wishes to watch a Presentity's Presence Information, or certain parts of the Presentity's Presence Information. To initiate a subscription, the Watcher sends a SIP SUBSCRIBE request for the presence event package including an indication of the duration this subscription should last. The SIP SUBSCRIBE request may also include an indication of the Watcher's capability to handle partial notifications.

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

2. The SIP/IP Core network of the Watcher resolves the address of the Presentity and forwards the request to the SIP/IP Core network of the Presentity
3. The SIP/IP Core network of the Presentity routes the SUBSCRIBE request to the correct PS.
4. The PS performs the necessary authorisation checks on the originator to ensure it is allowed to watch the Presentity.

NOTE: In the case where the privacy/authorisation checks fail, then a negative acknowledgement is sent to the Watcher.

5. Once all privacy conditions are met, the PS issues a SIP 200 OK to the SIP/IP Core network.
6. The SIP/IP Core network of the Presentity forwards the response to the SIP/IP Core network of the Watcher.
7. The SIP/IP Core network of the Watcher forwards the response to the Watcher.
8. As soon as the PS sends a 200 OK response to accept the subscription, it sends a SIP NOTIFY request including the current full state of the Presentity's tuples that the Watcher has subscribed and been authorised to. The SIP NOTIFY request is sent to the Watcher SIP/IP Core network. Further notifications sent by the PS may either contain the complete set of Presence Information, or only those tuples that have changed since the last notification if the Watcher has indicated the capability to process partial notifications.
9. The SIP/IP Core network of the Watcher forwards the SIP NOTIFY request to the Watcher.
10. The Watcher acknowledges the receipt of the SIP NOTIFY request with a SIP 200 OK response sent to its SIP/IP Core network.
11. The SIP/IP Core network of the Watcher forwards the SIP 200 OK response to the PS.
12. Upon the Presence Information for the Presentity changes (the means how the Presence Information changes are outside the scope for this use case), the PS determines which authorized Watchers are entitled to receive notifications. For each appropriate Watcher, the PS sends a SIP NOTIFY request that contains the full or partial updates to the Presence Information. The SIP NOTIFY request is sent along the path of the SUBSCRIBE dialog to the SIP/IP Core network of the Watcher.
13. The Watcher’s SIP/IP Core network forwards the SIP NOTIFY request to the Watcher.
14. The Watcher acknowledges the SIP NOTIFY response with a SIP 200 OK response to its SIP/IP Core network.
15. The SIP/IP Core network of the Watcher forwards the SIP 200 OK response to the PS.

NOTE: Steps 2 and 3 as well as 5 and 6 are combined if the Watcher is in the same domain as the Presentity.

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

C.1.2.2 Fetching Presence Information state – Proactive authorization

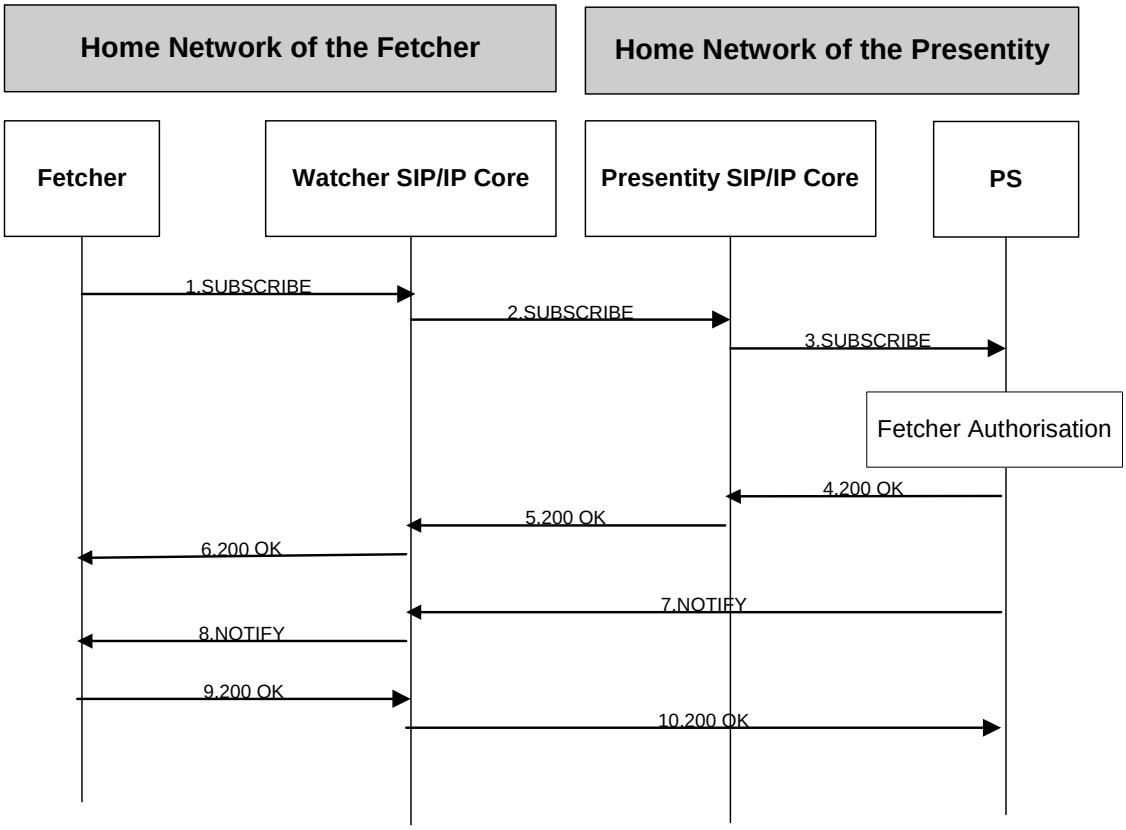

Figure 10 - Fetching Presence Information state (fetcher and Presentity are in different networks)

A Watcher requests Presence Information of a certain Presentity from the PS, acting as a fetcher. For the remaining use case, Watcher will be used uniformly.

1. The Watcher requests Presence Information of the Presentity using a SIP SUBSCRIBE request by setting the "Expires" header field to zero, as defined in [RFC3265].

2. The Watcher's SIP/IP Core network resolves the address of the SIP/IP Core network of the Presentity and forwards the request.

3. The SIP/IP Core network forwards the SIP SUBSCRIBE request to the appropriate PS.

4. The PS performs the necessary authorization checks on the originator to ensure it is allowed to request Presence Information of the Presentity. Assuming all privacy conditions are met, the PS issues a SIP 200 OK response to the SIP/IP Core network of the Presentity.

5. The SIP/IP Core network of the Presentity forwards the response to the SIP/IP Core network of the Watcher.

6. The SIP/IP Core network of the Watcher forwards the SIP 200 OK response to the Watcher

7. As soon as the PS sends a SIP 200 OK response to accept the request, it sends a SIP NOTIFY request with the current full state of the Presentity's tuples that the Watcher has requested and been authorized to. The SIP NOTIFY request is sent along the path of the SUBSCRIBE dialog to the SIP/IP Core network of the Watcher.

8. The SIP/IP Core network of the Watcher forwards the SIP NOTIFY request to the Watcher.

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

9 . The Watcher acknowledges the receipt of the SIP NOTIFY request with a SIP 200 OK responseto the SIP/IP Core network of the Watcher.

10. The Watcher's SIP/IP Core network forwards the SIP 200 OK response to the PS.

NOTE: Steps 2 and 3 as well as 5 and 6 are combined if the Watcher is in the same domain as the Presentity.

C.1.2.3 Subscribing to Presence Information state changes - Reactive Authorization

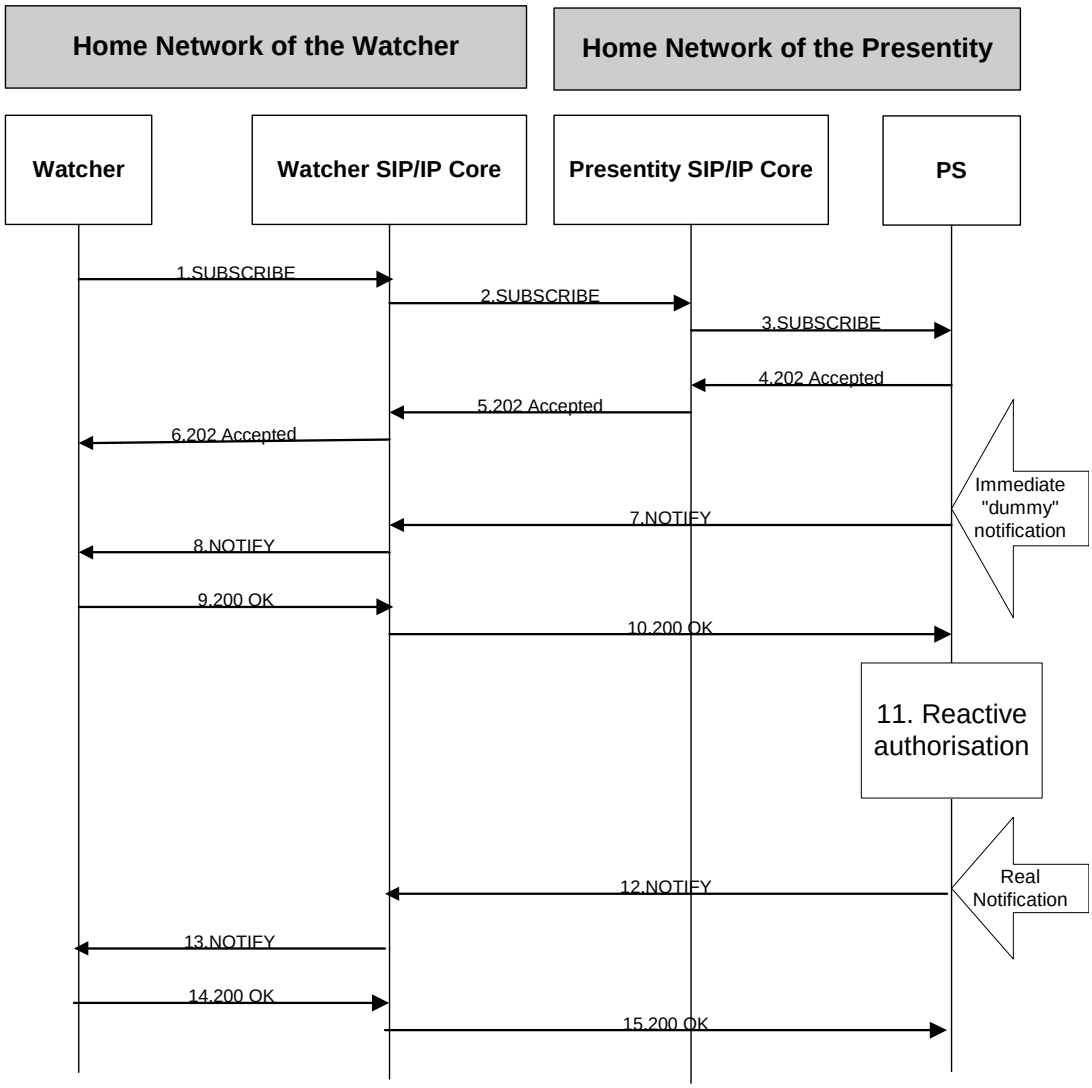

Figure 11 - Subscribing to Presence Information state changes (Watcher and Presentity are in different networks) - Reactive Authorisation

1. A Watcher wishes to watch a Presentity's Presence Information, or certain parts of the Presentity's Presence Information. To initiate a subscription, the Watcher sends a SIP SUBSCRIBE request for the presence event package including an indication of the duration this subscription should last. The SIP SUBSCRIBE request may also include an indication of the Watcher's capability to handle partial notifications.

2. The SIP/IP Core network of the Watcher resolves the address of the Presentity and forwards the request to the SIP/IP Core network of the Presentity.

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

3. The SIP/IP Core network of the Presentity routes the SUBSCRIBE request to the correct PS
4. The PS acknowledges the request with a SIP 202 Accepted response sent to the SIP/IP Core network of the Presentity.
5. The SIP/IP Core network of the Presentity forwards the response to the SIP/IP Core network of the Watcher
6. The SIP/IP Core network of the Watcher forwards the response to the Watcher..
7. As soon as the PS sends a SIP 202 Accepted response to accept the subscription, it sends a SIP NOTIFY request as mandated by [RFC3265]. At this time, the Presence Information may be inaccurate or not fully available for the Presentity. However a "dummy" SIP NOTIFY request must be sent, with a valid neutral or empty Presence Information and a valid Subscription-State header field (set to "pending") for the time being.
8. The SIP/IP Core network of the Watcher forwards the SIP NOTIFY request to the Watcher
9. The Watcher acknowledges the receipt of the SIP NOTIFY request with a SIP 200 OK response sent to its SIP/IP Core network.
10. The SIP/IP Core network of the Watcher forwards the SIP 200 OK response to the PS.
11. The PS authorizes the Watcher, after the Presentity modifies the Subscription Authorization Policy (see section 5.4.3.2).
12. The PS issues another SIP NOTIFY request, to amend the neutral state known to the Watcher with valid Presence Information.
13. The Watcher's SIP/IP Core network forwards the SIP NOTIFY request to the Watcher.
14. The Watcher acknowledges the SIP NOTIFY response with a SIP 200 OK response to its SIP/IP Core network
15. The SIP/IP Core network of the Watcher forwards the SIP 200 OK response to the PS.

NOTE 1: Steps 2 and 3 as well as 5 and 6 are combined if the Watcher is in the same domain as the Presentity.

NOTE 2: If the immediate Presence Information is accurate, then there is no need for another notification (shown in steps 12-15) until Presence Information state changes. In fact, the PS may choose to best describe the Presence Information as known in the immediate notification, and if upon completing the required steps to grant the real Presence Information, it matches the information previously sent, there is no need for the second SIP NOTIFY request.

C.1.2.4 Receiving a Presence Notification for an Existing Subscription

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

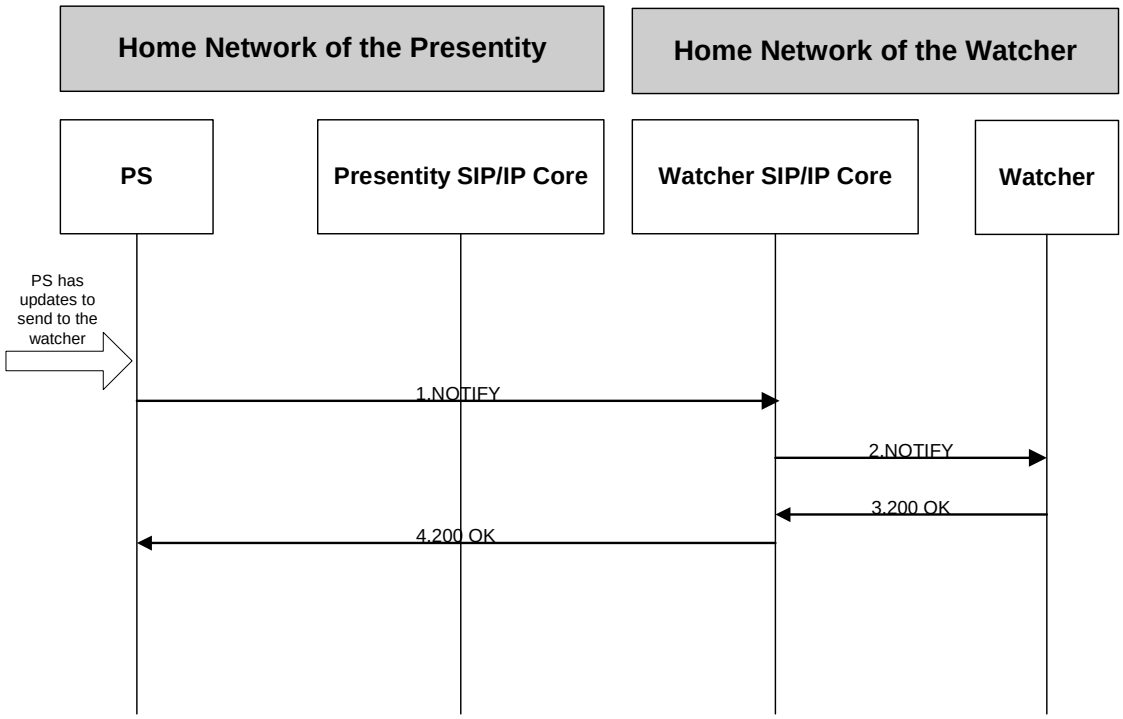

Figure 12- Receiving a presence notification

1. The PS determines which authorised Watchers are entitled to receive the updates of the Presence Information for this Presentity. For each appropriate Watcher, the PS generates a SIP NOTIFY request that contains either the full or partial updates of the Presence Information. The SIP NOTIFY request is sent inside the existing dialog created by the SIP SUBSCRIBE request to the SIP/IP Core network of the Watcher.
2. The SIP/IP Core network forwards the SIP NOTIFY request to the Watcher.
3. The Watcher acknowledges the SIP NOTIFY request with a SIP 200 OK response to its SIP/IP Core network.
4. The SIP/IP Core network of the Watcher forwards the SIP 200 OK response to the PS.

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

C.1.2.5 Partial Notifications

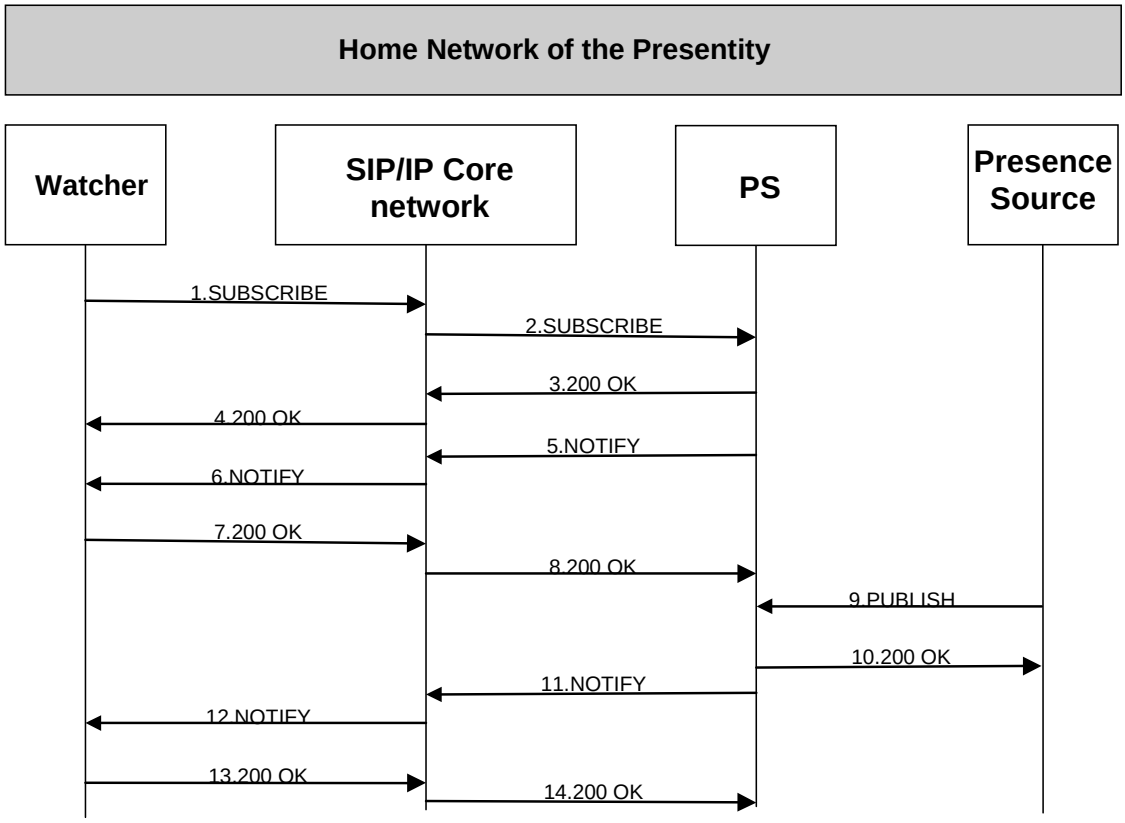

Figure 13 -Partial Notifications Information Flow

1. A Watcher sends a SIP SUBSCRIBE request to the PS indicating the support for the default Presence Information Data Format defined in [PIDF] and the partial PIDF defined in [PARFORMAT]. The Watcher also indicates the support for the partial notification mechanism according to [PARNOT].
2. The SIP/IP Core network forwards the SIP SUBSCRIBE request to the PS.
3. The PS authorizes the subscription and sends a SIP 200 OK response to the SIP/IP Core network.
4. The SIP/IP Core network forwards the SIP 200 OK response to the Watcher.
5. The PS, based on the Watcher's indication supporting partial notification mechanism, generates a SIP NOTIFY request, which includes a full state presence document formulated according to [PARNOT]. The SIP NOTIFY request is forwarded to the SIP/IP Core network.
6. The SIP/IP Core network forwards the SIP NOTIFY request to the Watcher.
7. The Watcher sends a SIP 200 OK response to the SIP/IP Core network to acknowledge the SIP NOTIFY request.
8. The SIP/IP Core network forwards the SIP 200 OK response to the PS.
9. After some time the Presentity's Presence Information changes (e.g. a tuple changes its <status>) so a Presence Source publishes the new state to the PS by generating a SIP PUBLISH request.
10. The PS acknowledges the SIP PUBLISH request with a SIP 200 OK response.

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

11. The PS generates a NOTIFY request which includes a partial presence document formulated according to [PARFORMAT] showing only the changed Presence Information.

12. The SIP/IP Core network forwards the SIP NOTIFY request to the Watcher.

13. The Watcher acknowledges the SIP NOTIFY request with a SIP 200 OK response.

14. The SIP/IP Core network forwards the SIP 200 OK response to the PS.

NOTE: If the Watcher and the Presentity reside at different domains the SIP/IP Core network of the Watcher will perform address resolution on the address of the Presentity to foward the SUBSCRIBE request to the SIP/IP Core network of the Presentity. Then the SIP/IP Core network of the Presentity will route the SUBSCRIBE request to the PS. (See step 2 and 3 as well as 5 and 6 in Section 12.1.2.1.)

C.1.2.6 Expiry of published Presence Information

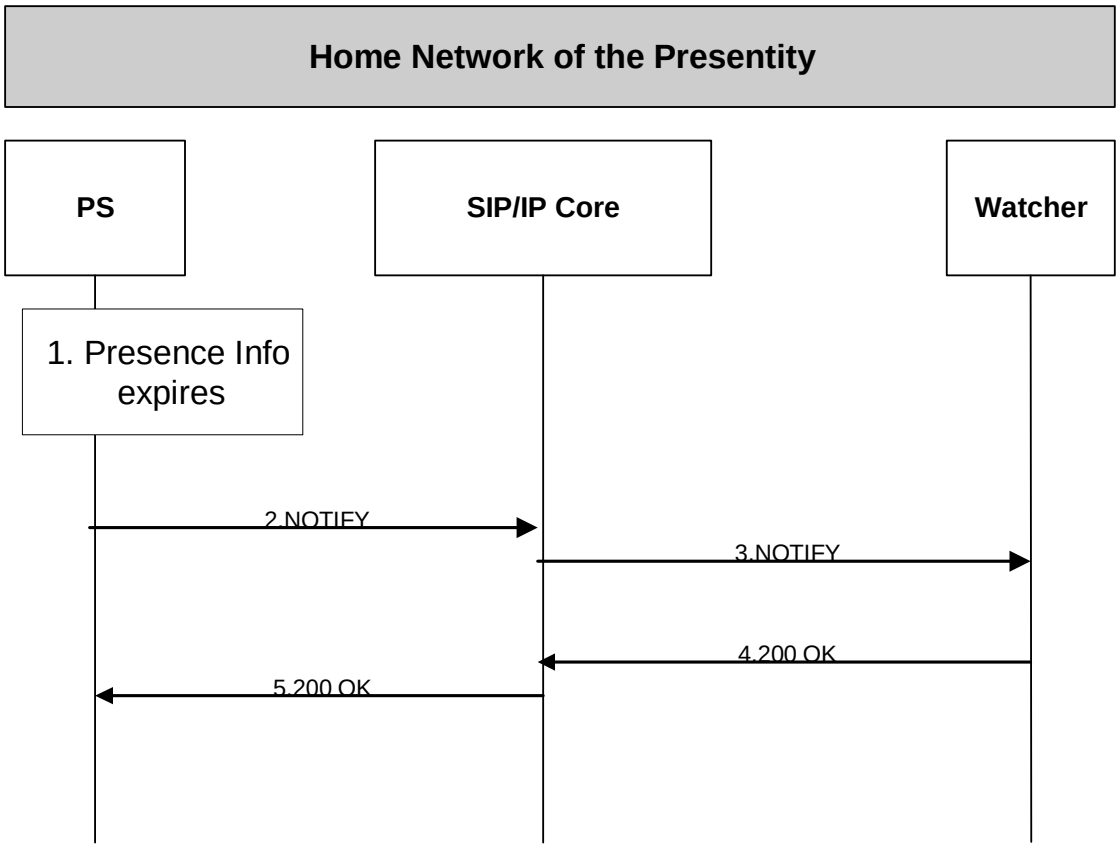

Figure 14- Expiry of published Presence Information

1. The lifetime of some Presence Information elapses and there is no refreshing transaction to update the lifetime of this Presence Information.

2. The PS issues a SIP NOTIFY request including the updated Presence Information.

3. The SIP/IP Core network forwards the SIP NOTIFY request to the Watcher.

4. The Watcher sends a 200 OK response to the SIP/IP Core network to acknowledge the SIP NOTIFY request.

5. The SIP/IP Core network forwards the 200 OK response to the PS.

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

C.1.2.7 Subscription Authorization Failure

A Presentity can deny a subscription request by either rejecting the request outright (so called “blocking”), or accepting the request but providing possibly inaccurate Presence Information (so called “polite blocking”).

C.1.2.7.1 Blocking

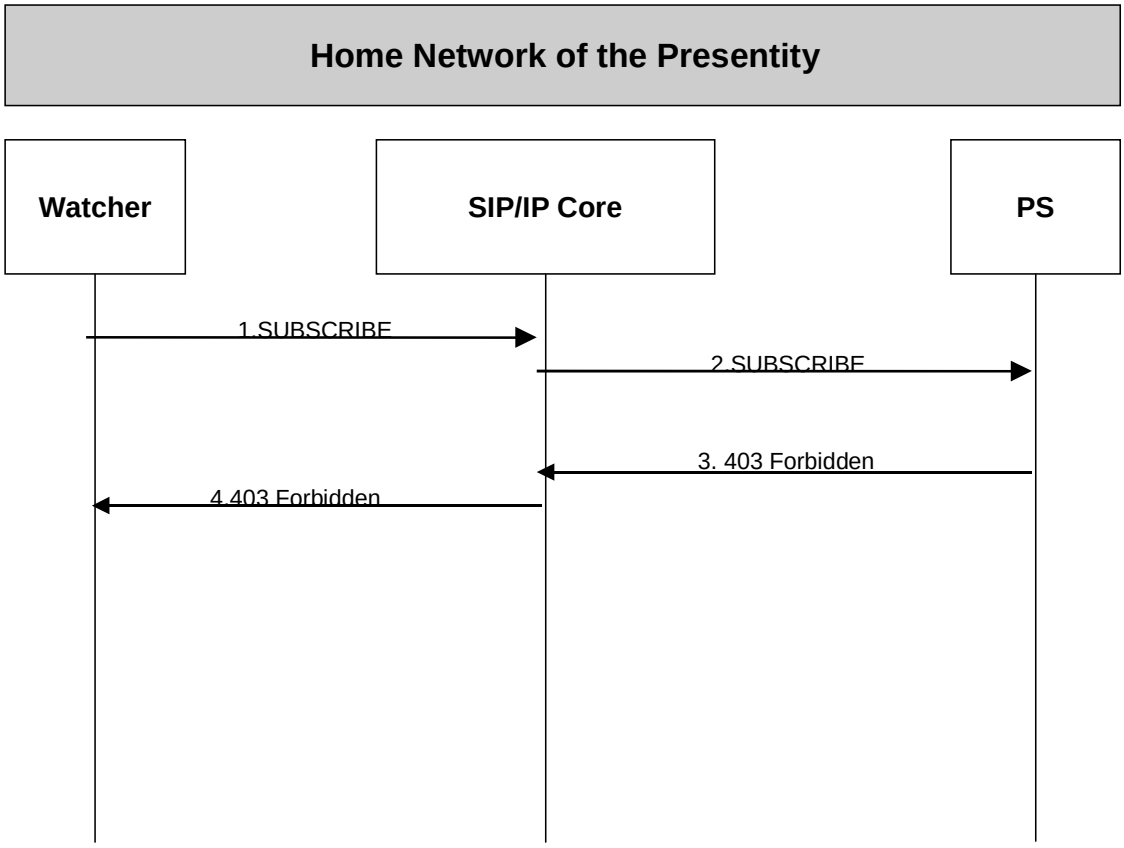

Figure 15- Blocking

1. A Watcher wishing to subscribe to Presence Information about a Presentity, sends a SUBSCRIBE request to the SIP/IP Core network.
2. The SIP/IP Core network forwards the SIP SUBSCRIBE request to the appropriate PS.
3. The PS performs a subscription authorization check on the Watcher to verify whether it is allowed to watch the Presentity. After applying the subscription authorization policies of the Presentity, the PS determines to reject the subscription request. The PS sends either a SIP 403 Forbidden response to the SIP/IP Core network.
4. The SIP/IP Core network forwards the SIP 403 Forbidden response to the Watcher.

NOTE: If the Watcher and the Presentity reside at different domains the SIP/IP Core network of the Watcher will perform address resolution on the address of the Presentity to foward the SUBSCRIBE request to the SIP/IP Core network of the Presentity. Then the SIP/IP Core network of the Presentity will route the SUBSCRIBE request to the PS. (See step 2 and 3 as well as 5 and 6 in Appendix D.1.2.1.)

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

C.1.2.7.2 Polite Blocking

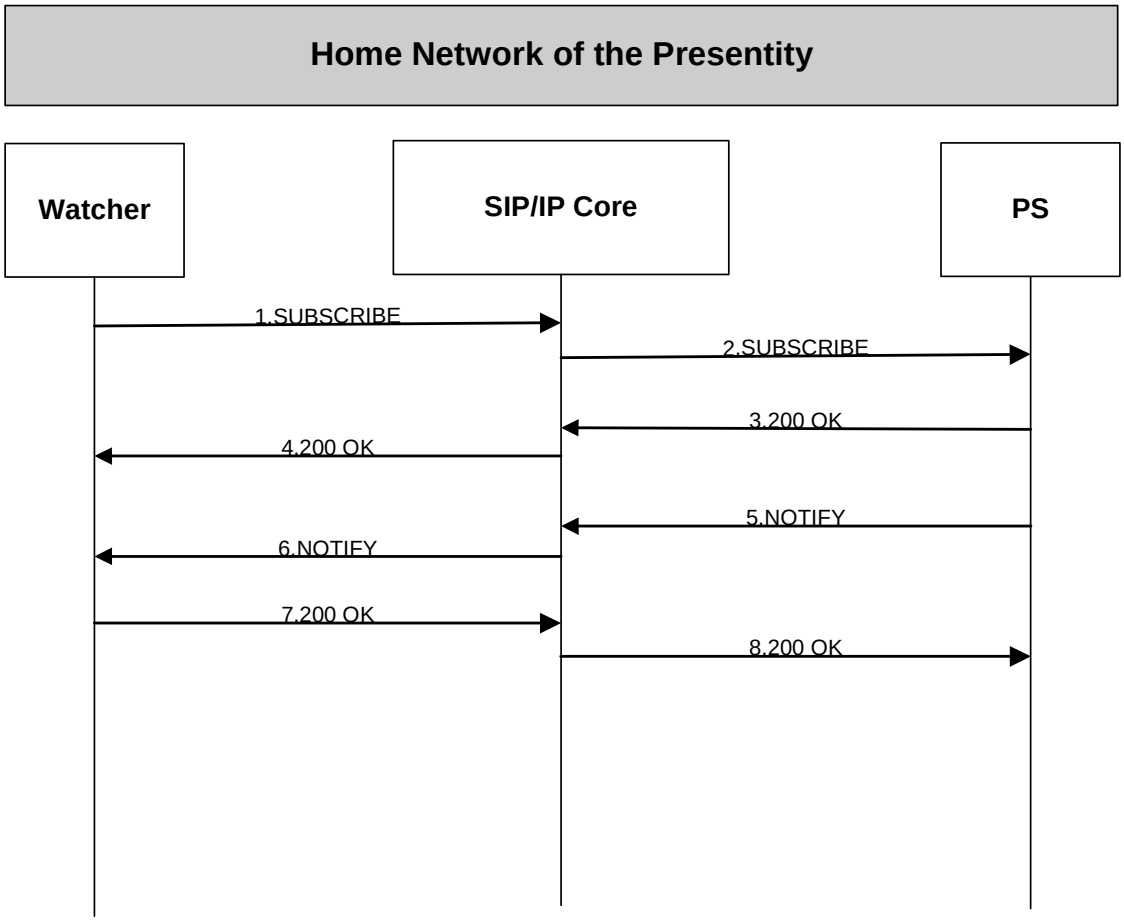

Figure 16- Polite Blocking

1. A Watcher wishing to subscribe to Presence Information about a Presentity, sends a SIP SUBSCRIBE request to the SIP/IP Core network.
2. The SIP/IP Core network forwards the SIP SUBSCRIBE request to the appropriate PS.
3. The PS performs a subscription authorization check on the Watcher to verify whether it is allowed to watch the Presentity. After applying the subscription authorization policies of the Presentity, the PS determines to reject the subscription request but give the appearance that the request has been granted (so called “polite blocking”) see section 5.4.3.2.1. The PS sends a 200 OK to the SIP/IP Core network.
4. The SIP/IP Core network forwards the SIP 200 OK response to the Watcher.
5. As soon as the PS sends the SIP 200 OK response, it sends a SIP NOTIFY request with the appropriate Presence Information as defined by the presence privacy policy.
6. The SIP/IP Core network forwards the SIP NOTIFY request to the Watcher.
7. The Watcher acknowledges the SIP NOTIFY request with a SIP 200 OK response.
8. The SIP/IP Core network forwards the SIP 200 OK response to the appropriate PS.

NOTE: If the Watcher and the Presentity reside at different domains the SIP/IP Core network of the Watcher will perform address resolution on the address of the Presentity to foward the SUBSCRIBE request to the SIP/IP Core

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

network of the Presentity. Then the SIP/IP Core network of the Presentity will route the SUBSCRIBE request to the PS. (See step 2 and 3 as well as 5 and 6 in Section 12.1.2.1.)

C.1.2.8 Subscription Filters

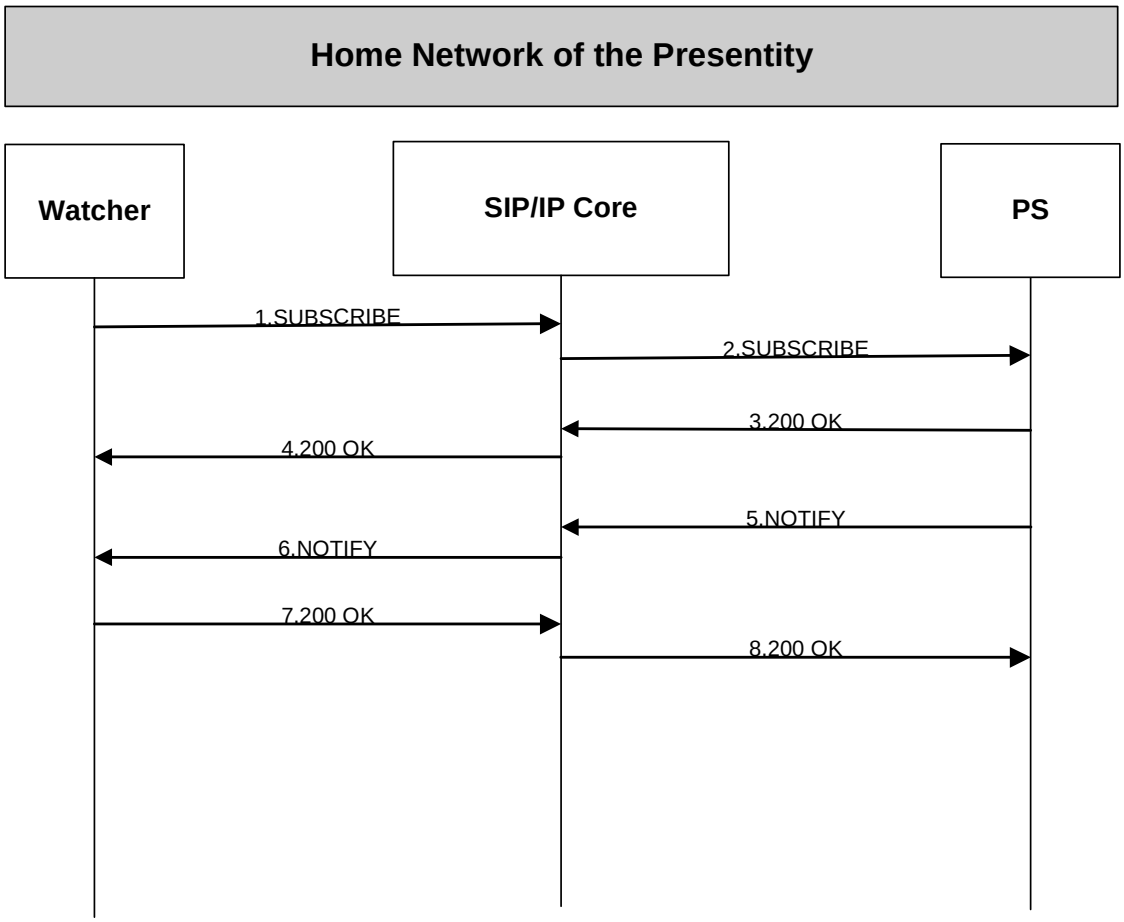

Figure 17 - Subscription Filters

In this example, a Presentity has a presence document that includes two presence tuples: one for Instant Messaging (IM) and another for gaming services.

1. A Watcher sends a SIP SUBSCRIBE request to the PS requesting the Presence Information related to all the messaging applications (e.g. MMS, SMS, IM) of the Presentity. This is done by including a filter in the body of the SIP SUBSCRIBE request according to [RFC4660] and [RFC4661].

2. The SIP/IP Core network forwards the SIP SUBSCRIBE request to the PS.

3. The PS authorizes the subscription and interprets the subscription filter and sends a SIP 200 OK response to the SIP/IP Core network indicating that the subscription has been accepted and the subscription filter understood.

4. The SIP/IP Core network forwards the SIP 200 OK response to the Watcher.

5. The PS sends a SIP NOTIFY request to the the SIP/IP Core network including only the Instant Messaging related tuple that was requested by the Watcher's subscription filter.

6. The SIP/IP Core network forwards the SIP NOTIFY request to the Watcher.

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

7. The Watcher acknowledges the SIP NOTIFY request with a SIP 200 OK response.

8. The SIP/IP Core network forwards the SIP 200 OK response to the PS.

NOTE: If the Watcher and the Presentity reside at different domains the SIP/IP Core network of the Watcher will perform address resolution on the address of the Presentity to foward the SUBSCRIBE request to the SIP/IP Core network of the Presentity. Then the SIP/IP Core network of the Presentity will route the SUBSCRIBE request to the PS. (See step 2 and 3 as well as 5 and 6 in Section 12.1.2.1.)

C.1.3 Signalling flows for Watchers canceling a subscription

C.1.3.1 Watcher Initiated Canceling

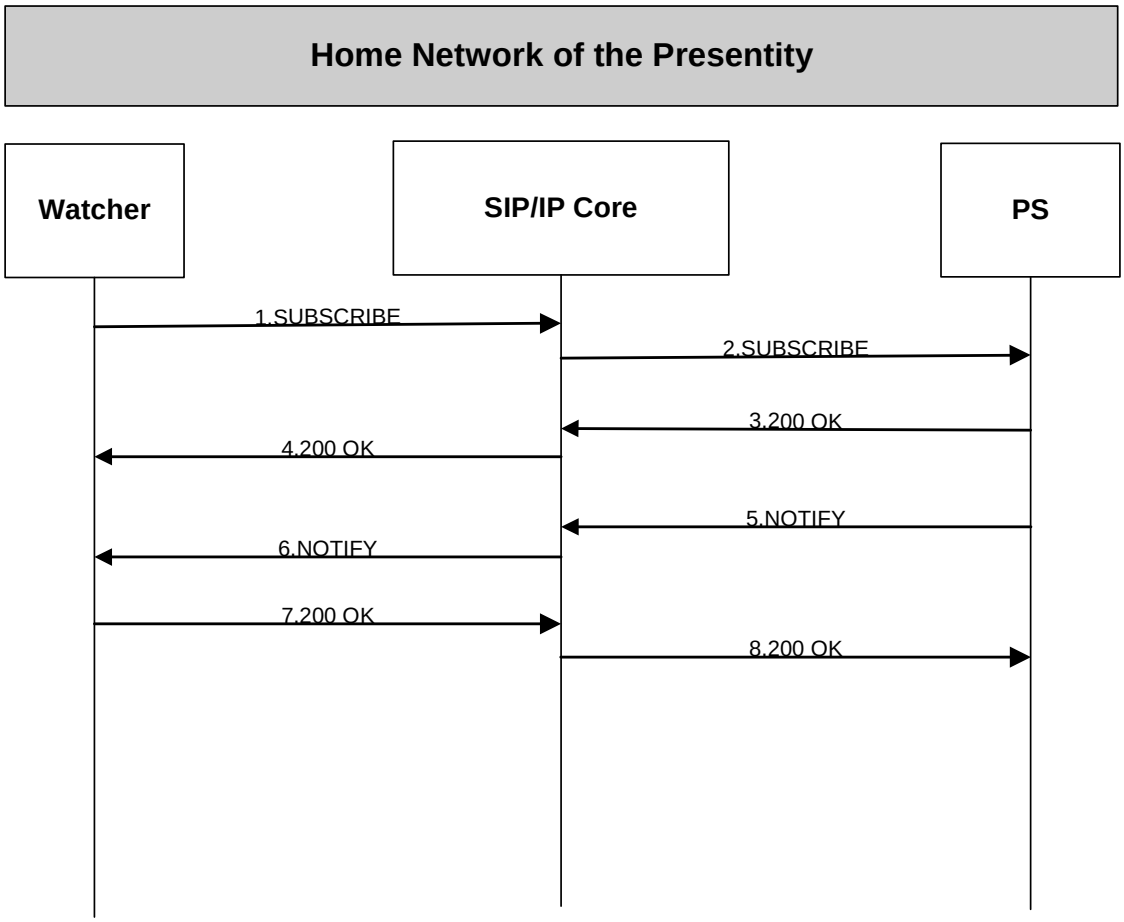

Figure 18 - Watcher Initiated cancelling

1. A Watcher sends a SIP SUBSCRIBE request to the SIP/IP Core network with the “Expires” header field set to 0 indicating the cancelling of the subscription, according to [RFC3265].

2. The SIP/IP Core network forwards the SIP SUBSCRIBE request to the PS.NOTE: Even when the Watcher and the Presentity reside at different domains the SIP/IP Core network of the Watcher will foward the SUBSCRIBE request directly to the PS since it has already performed the address resolution on the address of the Presentity during the initial subscription.

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

3. The PS accepts the SUBSCRIBE message with the "Expires" header set to 0 indicating the canceling a subscription operation, and sends a 200 OK to the SIP/IP Core network.
4. The SIP/IP Core network forwards the 200 OK to the Watcher.
5. The PS sends a SIP NOTIFY request to the SIP/IP Core network with a "Subscription-State" header field set to "terminated" indicating that the subscription has been terminated, according to [RFC3265].
6. The SIP/IP Core network forwards the SIP NOTIFY request to the Watcher.
7. The Watcher sends a SIP 200 OK response to the SIP/IP Core network to acknowledge the SIP NOTIFY request.
8. The SIP/IP Core network forwards the SIP 200 OK to the PS.

C.1.3.2 Presence Server Initiated Canceling

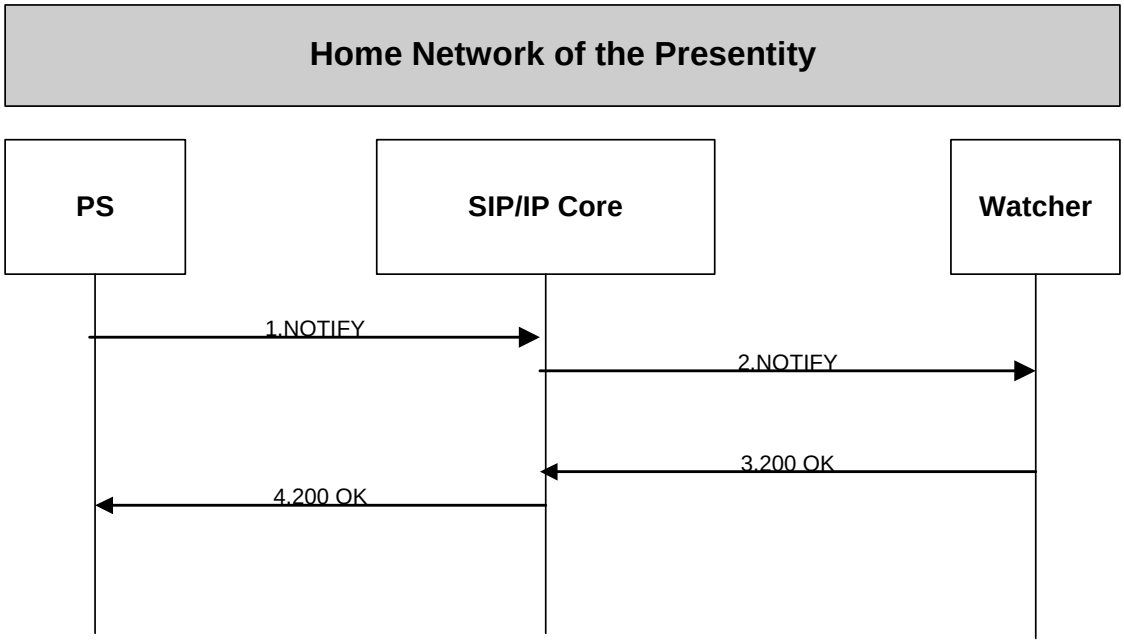

Figure 19 - Presence Server Initiated cancelling

1. The PS sends a SIP NOTIFY request with a "Subscription-State" header field set to "terminated" indicating that the PS wants to terminate a subscription, according to [RFC3265].
2. The SIP/IP Core network forwards the SIP NOTIFY request to the Watcher.

NOTE: Even when the Watcher and the Presentity reside at different domains the SIP/IP Core network of the Presentity will foward the NOTIFY request directly to the Watcher since it already has the address of the Watcher.

3. The Watcher sends a SIP 200 OK response to the SIP/IP Core network to acknowledge the SIP NOTIFY request.
4. The SIP/IP Core network forwards the SIP 200 OK to the PS.

C.1.4 Void

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

C.1.5 Subscribing to Watcher Information state changes

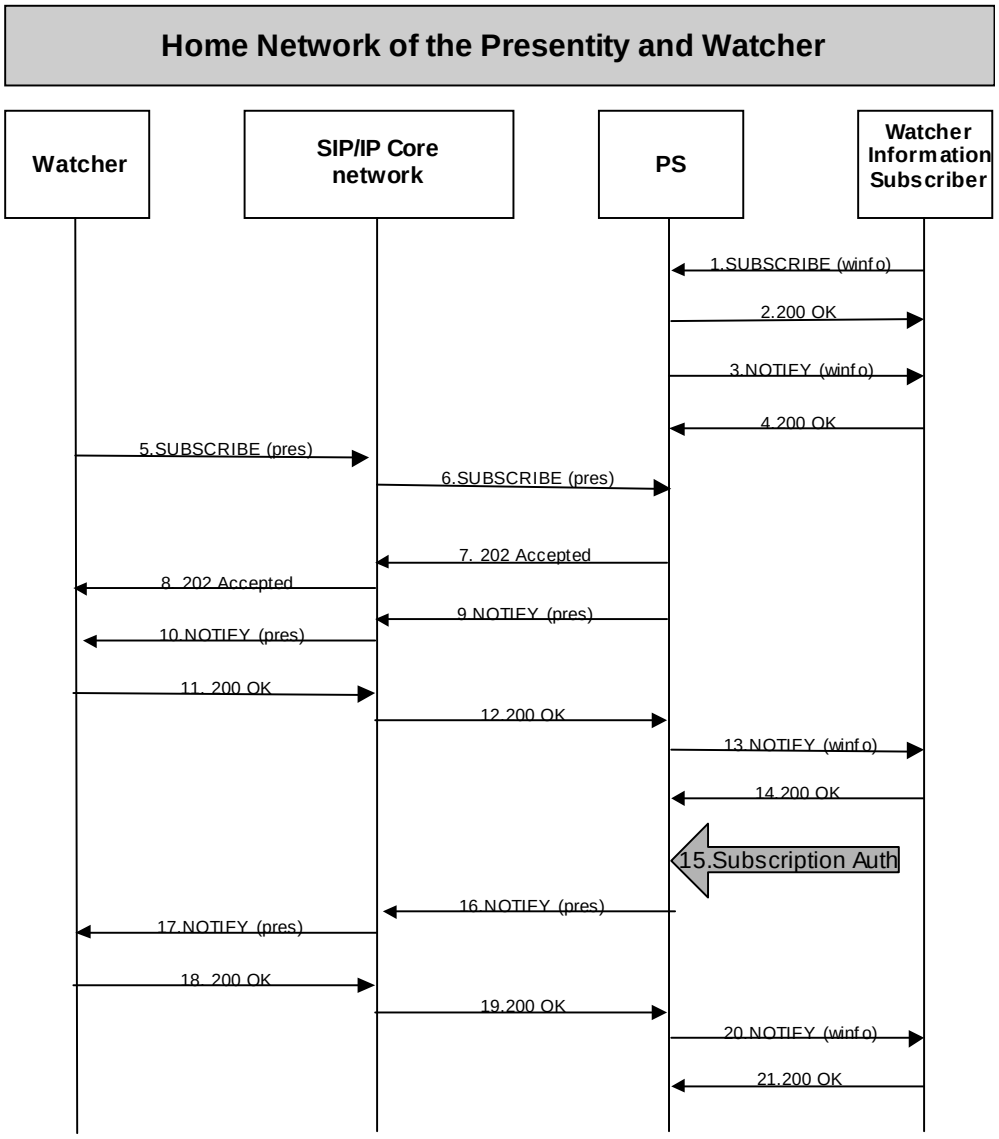

Figure 20- Watcher Information (Subscriptions/Notifications)

NOTE: The SIP/IP Core network between the PS and the Watcher Information Subscriber is not shown in the figure due to simplicity reasons.

In this use case we assume that the application of the presence subscription authorization rules for the Watcher results in placing the subscription into the state “pending”.

1. The Watcher Information Subscriber subscribes to the Watcher information (see section 5.3.1) of its own Presentity in order to receive notifications about new, unauthorized Watchers that subscribe to its Presence Information. This is performed by sending a SIP SUBSCRIBE request to the PS according to [RFC3857].

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

2. The PS after authorizing the subscription allows the Watcher Information Subscriber to subscribe to the Watcher information. The PS acknowledges the SIP SUBSCRIBE request by generating a SIP 200 OK response.
3. The PS generates a SIP NOTIFY request including the current state of the Watcher information of the Presentity.
4. The Watcher Information Subscriber acknowledges the SIP NOTIFY request by sending a SIP 200 OK response.
5. After time elapses, a Watcher attempts to subscribe to the Presentity's Presence Information by sending a SIP SUBSCRIBE request according to [RFC3856].
6. The SIP/IP Core network forwards the SIP SUBSCRIBE request to the PS.
7. The PS acknowledges the SIP SUBSCRIBE request and returns a SIP 202 Accepted response.
8. The SIP/IP Core network forwards the SIP 202 Accepted response to the Watcher.
9. The PS immediately sends a SIP NOTIFY request as mandated by [RFC3265], setting the "Subscription-State" header field to the value of "pending" indicating that the subscription has been received, but the Subscription Authorization Policy is insufficient to accept or deny the subscription at this time.
10. The SIP/IP Core network forwards the SIP NOTIFY request to the Watcher
11. The Watcher acknowledges the SIP NOTIFY request by sending a SIP 200 OK response.
12. The SIP/IP Core network forwards the SIP 200 OK response to the PS.
13. As the Watcher information state for the Presentity changes (a Watcher has requested to subscribe to the Presence Information), the PS sends a SIP NOTIFY request to indicate the change (a subscription for the Presentity's Presence Information is pending) to the Watcher Information Subscriber according to [RFC3857].
14. The Watcher Information Subscriber acknowledges the SIP NOTIFY request with a SIP 200 OK response.
15. The Presentity authorizes the subscription of the pending Watcher .
16. As the subscription state for the presence event package changes, the PS sends a SIP NOTIFY request to the Watcher indicating that the subscription is authorized. The SIP NOTIFY request also conveys the current Presence Information state of the Presentity.
17. The SIP/IP Core network forwards the SIP NOTIFY request to the Watcher
18. The Watcher acknowledges the SIP NOTIFY request by sending a SIP 200 OK response.
19. The SIP/IP Core network forwards the SIP 200 OK response to the PS.
20. As the subscription state for the presence event package changes, at the same time of step 16, the PS sends a SIP NOTIFY request to the winfo template package to the Watcher Information Subscriber indicating that the subscription is authorized.
21. The Watcher Information Subscriber acknowledges the SIP NOTIFY request with a SIP 200 OK response.

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

C.1.6 Sending different Presence Information to different Watchers

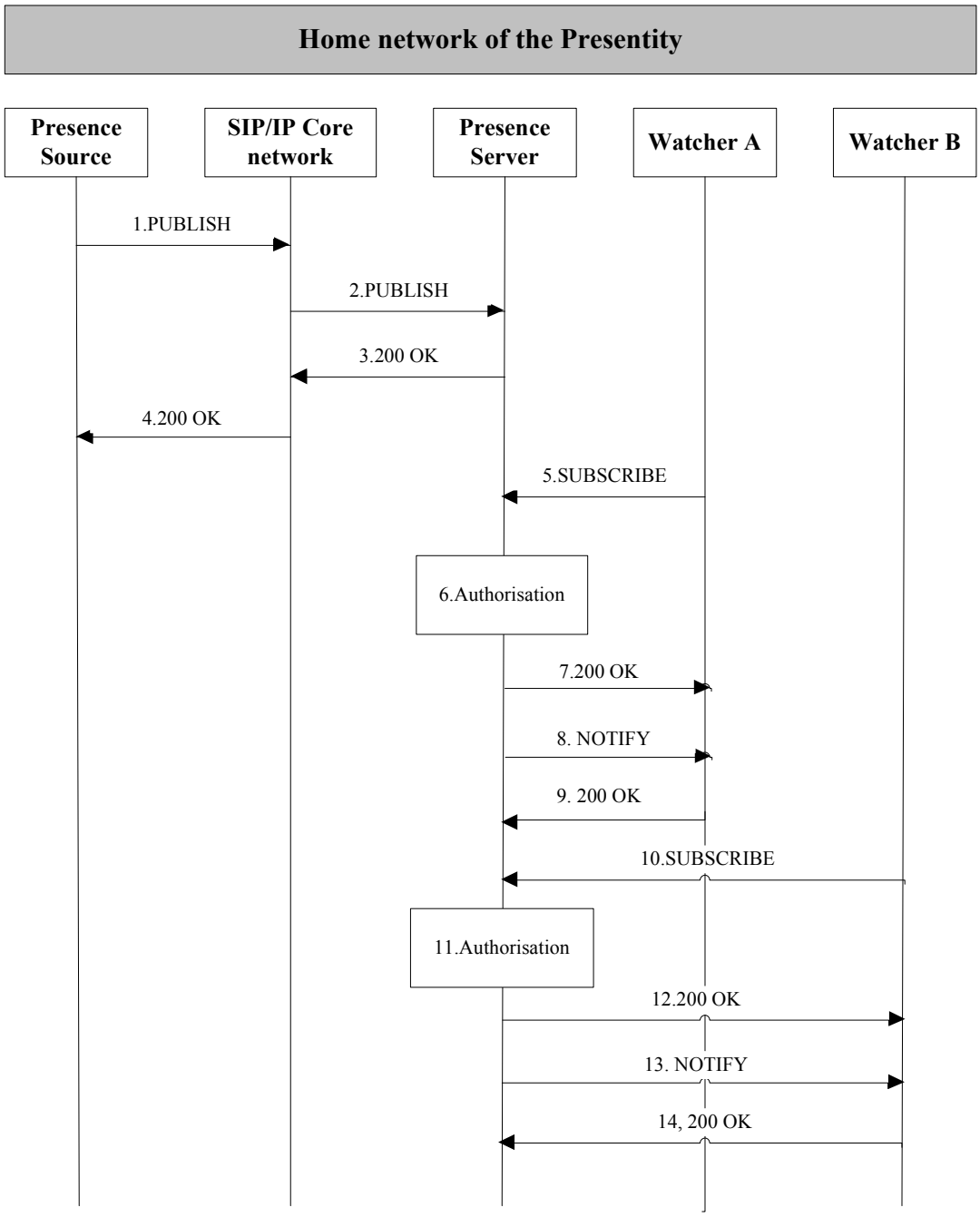

Figure 21 - Sending different Presence Information to different Watchers

NOTE: The SIP/IP Core network between the PS and the Watchers is not shown in the figure due to simplicity reasons.

1. The Presence Source generates a SIP PUBLISH request, which contains a presence document. This document contains more than one tuple that contain the same element with different value. The association of tuples to different Watchers and Watcher groups is based on the Presence authorisation policies.

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

2. The SIP/IP Core network routes the request to the corresponding PS.
3. The PS authorises the presence publication, and checks the information the message contains. The PS then processes the Presence Information and sends a SIP 200 OK response back to Presence Source.
4. The SIP/IP Core network forwards the response back to the Presence Source.
5. Watcher A wishing to subscribe to Presence Information about a Presentity, sends a SIP SUBSCRIBE request to the PS.
6. The PS performs the necessary authorisation checks on Watcher A to ensure it is allowed to watch the Presentity and to watch what specified tuples based on e.g. <class> element.
7. The PS sends a SIP 200 OK response back to Watcher A.
8. The PS generates a NOTIFY request which contains a presence document for Watcher A.
9. Watcher A sends a SIP 200 OK response to PS.
10. Watcher B wishing to subscribe to Presence Information about a Presentity, sends a SIP SUBSCRIBE request to the PS.
11. The PS performs the necessary authorisation checks on Watcher B to ensure it is allowed to watch the Presentity and to watch what specified tuples based on e.g. <class> element.
12. The PS sends a SIP 200 OK response back to Watcher B.
13. The PS generates a NOTIFY request which contains a presence document for Watcher B. Watcher B MAY receive different Presence Information than Watcher A.
14. Watcher B sends a SIP 200 OK response to PS.

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

Appendix D. Change History (Informative)

D.1 Approved Version History

Reference	Date	Description
OMA-TS-Presence_SIMPLE-V1_0-20060725-A	25 Jul 2006	TP approved: OMA-TP-2006-0223R04-INP_Presence_SIMPLE_V1_0_for_final_approval
OMA-TS-Presence_SIMPLE-V1_0_1-20061128-A	28 Nov 2006	Incorporated CRs: OMA-PAG-2006-0392R02 OMA-PAG-2006-0412 OMA-PAG-2006-0414 OMA-PAG-2006-0416 OMA-PAG-2006-0481R01 OMA-PAG-2006-0496 OMA-PAG-2006-0497 OMA-PAG-2006-0508 OMA-PAG-2006-0512 OMA-PAG-2006-0514 OMA-PAG-2006-0541 OMA-PAG-2006-0542 OMA-PAG-2006-0580 OMA-PAG-2006-0662 OMA-PAG-2006-0690 OMA-PAG-2006-0691 OMA-PAG-2006-0717R01 OMA-PAG-2006-0733 OMA-PAG-2006-0749R01
OMA-TS-Presence_SIMPLE-V1_0_1-20080627-A	27 Jun 2008	Status changed to Approved by TP TP ref# OMA-TP-2008-0250-INP_Presence_SIMPLE_V1_1_ERP_for_Final_Approval

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.