

WV-041 Features and Functions

Candidate Version 1.2 – 22 May 2004

Open Mobile Alliance
OMA-IMPS-WV-Features_Functions-V1_2-20040522-C

Continues the Technical Activities
Originated in the Wireless Village Initiative



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.

© 2004 Open Mobile Alliance Ltd. All Rights Reserved.

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

Contents

1. SCOPE	5
2. REFERENCES	6
2.1. NORMATIVE REFERENCES	6
2.2. INFORMATIVE REFERENCES	6
3. TERMINOLOGY AND CONVENTIONS	8
3.1. CONVENTIONS	8
3.2. DEFINITIONS	8
3.3. ABBREVIATIONS	8
4. INTRODUCTION	9
5. PRESENCE FEATURE	10
5.1. PRESENCE INFORMATION	10
5.1.1. Client Status Attributes	10
5.1.2. User Status Attributes	10
5.2. CONTACT LIST FEATURE	10
5.3. AUTHORIZATION OF PRESENCE ATTRIBUTES	10
5.3.1. Overview	10
5.3.2. Proactive Authorization	11
5.3.3. Reactive Authorization	11
5.3.4. Watcher List	12
5.3.5. Authorization Withdrawal and Removal	12
5.3.6. Combination of Proactive and Reactive Authorization	12
5.3.7. Retrieval of Watcher List Feature	12
5.4. DELIVERY OF PRESENCE VALUES	12
5.4.1. Subscribed Presence Feature	12
5.4.2. Get Presence Feature	12
5.4.3. Update Presence Feature	13
6. INSTANT MESSAGING FEATURES	14
6.1. DELIVERY	14
6.2. OFFLINE MESSAGING	14
6.3. ACCESS CONTROL	14
6.4. MESSAGE CONTENT	14
7. GROUP FEATURE	16
7.1. GROUP MODELS	16
7.1.1. Private Group Model	16
7.1.2. Public Group Model	16
7.1.3. Group Membership	16
7.2. DYNAMIC GROUP FEATURES	16
7.2.1. Join group feature	16
7.2.2. Leave group feature	16
7.2.3. Invite user to group feature	16
7.2.4. Search Group and Users Feature	17
7.2.5. Subscribe to Group Change Feature	17
7.3. STATIC GROUP FEATURES	17
7.3.1. Create group feature	17
7.3.2. Delete group feature	17
7.3.3. Management of Members' List Feature	17
7.3.4. Modify Group Properties Feature	17
7.3.5. Access Control Features	17
8. SHARED CONTENT FEATURE	18

9. ACCESS FEATURES	19
9.1. LOGIN AND LOGOUT FEATURE	19
9.2. SERVICE AND CAPABILITY FEATURE	19
9.3. KEEP ALIVE FEATURE	19
9.4. GET SERVICE PROVIDER INFORMATION FEATURE	19
10. COMMON FEATURES	20
10.1. GENERAL SEARCH FEATURE	20
10.2. GENERAL INVITATION FEATURE	20
11. SERVER INTEROPERABILITY FEATURES	21
11.1. SECURITY	23
11.2. TRANSACTION MANAGEMENT	23
11.3. SESSION MANAGEMENT	23
11.4. SERVICE MANAGEMENT	23
11.4.1. Service Discovery	23
11.4.2. Service Negotiation and Agreement	23
11.5. USER PROFILE MANAGEMENT	23
11.6. SERVICE RELAY – IMPS FEATURES	23
APPENDIX A. CHANGE HISTORY (INFORMATIVE)	24
A.1 APPROVED VERSION HISTORY	24
A.2 DRAFT/CANDIDATE VERSION 1.2 HISTORY	24

1. Scope

The Wireless Village Instant Messaging and Presence Service (IMPS) includes four primary features:

- Presence
- Instant Messaging
- Groups
- Shared Content

Presence is the key enabling technology for IMPS. It includes client device availability (my phone is on/off, in a call), user status (available, unavailable, in a meeting), location, client device capabilities (voice, text, GPRS, multimedia) and searchable personal statuses such as mood (happy, angry) and hobbies (football, fishing, computing, dancing). Since presence information is personal, it is only made available according to the user's wishes - access control features put the control of the user presence information in the users' hands.

Instant Messaging (IM) is a familiar concept in both the mobile and desktop worlds. Desktop IM clients, two-way SMS and two-way paging are all forms of Instant Messaging. Wireless Village IM will enable interoperable mobile IM in concert with other innovative features to provide an enhanced user experience.

Groups or chat are a fun and familiar concept on the Internet. Both operators and end-users are able to create and manage groups. Users can invite their friends and family to chat in group discussions. Operators can build common interest groups where end-users can meet each other online.

Shared Content allows users and operators to setup their own storage area where they can post pictures, music and other multimedia content while enabling the sharing with other individuals and groups in an IM or chat session.

These features, taken in part or as a whole, provide the basis for innovative new services that build upon a common interoperable framework.

2. References

2.1. Normative References

- [CREQ] "Specification of WAP Conformance Requirements". Open Mobile Alliance™. WAP-221-CREQ.
<http://www.openmobilealliance.org/tech/affiliates/wap/wapindex.html>
- [CSP SCR] "WV-048 Client-Server Protocol Static Conformance Requirement Version 1.2". Open Mobile Alliance.
[URL:http://www.openmobilealliance.org/release_program/enabler_releases.html](http://www.openmobilealliance.org/release_program/enabler_releases.html)
- [IMPP-CPIM] A Common Profile for Instant Messaging (CPIM), Internet Draft, August 2002.
[URL:http://www.ietf.org/internet-drafts/draft-ietf-impp-cpim-03.txt](http://www.ietf.org/internet-drafts/draft-ietf-impp-cpim-03.txt)
- [RFC822] "Standard for the Format of ARPA Internet Text Messages", August 1982.
[URL:http://www.ietf.org/rfc/rfc822.txt](http://www.ietf.org/rfc/rfc822.txt)
- [RFC2119] "Key words for use in RFCs to Indicate Requirement Levels". S. Bradner. March 1997.
[URL:http://www.ietf.org/rfc/rfc2119.txt](http://www.ietf.org/rfc/rfc2119.txt)
- [RFC2234] "Augmented BNF for Syntax Specifications: ABNF". D. Crocker, Ed., P. Overell. November 1997. [URL:http://www.ietf.org/rfc/rfc2234.txt](http://www.ietf.org/rfc/rfc2234.txt)
- [RFC2778] "A Model for Presence and Instant Messaging", February 2000.
[URL:http://www.ietf.org/rfc/rfc2778.txt?number=2778](http://www.ietf.org/rfc/rfc2778.txt?number=2778)
- [RFC2779] Instant Messaging / Presence Protocol Requirements, Feb. 2000.
[URL:http://www.ietf.org/rfc/rfc2779.txt?number=2779](http://www.ietf.org/rfc/rfc2779.txt?number=2779)
- [SSP SCR] "WV-055 SSP – Server-Server Protocol Static Conformance Requirement Version 1.2". Open Mobile Alliance.
[URL:http://www.openmobilealliance.org/release_program/enabler_releases.html](http://www.openmobilealliance.org/release_program/enabler_releases.html)
- [TS 22.121] Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); Service aspects; The Virtual Home Environment (3GPP TS 22.121 version 4.1.0 Release 4).
[URL:ftp://ftp.3gpp.org/Specs/archive/22_series/22.121/22121-410.zip](ftp://ftp.3gpp.org/Specs/archive/22_series/22.121/22121-410.zip)
- [TS 23.127] Universal Mobile Telecommunications System (UMTS); Virtual Home Environment/Open Service Architecture (3GPP TS 23.127 version 4.2.0 Release 4).
[URL:ftp://ftp.3gpp.org/Specs/archive/23_series/23.127/23127-420.zip](ftp://ftp.3gpp.org/Specs/archive/23_series/23.127/23127-420.zip)

2.2. Informative References

- [Arch] "WV-40 Architecture Model Version 1.2". Open Mobile Alliance.
[URL:http://www.openmobilealliance.org/release_program/enabler_releases.html](http://www.openmobilealliance.org/release_program/enabler_releases.html)
- [FeaFun] "WV-041 Features and Functions Version 1.2". Open Mobile Alliance.
[URL:http://www.openmobilealliance.org/release_program/enabler_releases.html](http://www.openmobilealliance.org/release_program/enabler_releases.html)
- [CSP] "WV-042 Client-Server Protocol Session and Transactions Version 1.2". Open Mobile Alliance.
[URL:http://www.openmobilealliance.org/release_program/enabler_releases.html](http://www.openmobilealliance.org/release_program/enabler_releases.html)
- [CSP DTD] "WV-043 Client-Server Protocol DTD and Examples Version 1.2". Open Mobile Alliance.
[URL:http://www.openmobilealliance.org/release_program/enabler_releases.html](http://www.openmobilealliance.org/release_program/enabler_releases.html)
- [CSP Trans] "WV-044 Client-Server Protocol Transport Bindings Version 1.2". Open Mobile Alliance.

	URL:http://www.openmobilealliance.org/release_program/enabler_releases.html
[CSP DataType]	"WV-045 Client-Server Protocol Data Types Version 1.2". Open Mobile Alliance. URL:http://www.openmobilealliance.org/release_program/enabler_releases.html
[CSP SMS]	"WV-046 Client-Server Protocol SMS Binding Version 1.2". Open Mobile Alliance. URL:http://www.openmobilealliance.org/release_program/enabler_releases.html
[CSP WBXML]	"WV-047 Client-Server Protocol Binary Definition and Examples Version 1.2". Open Mobile Alliance. URL:http://www.openmobilealliance.org/release_program/enabler_releases.html
[CSP SCR]	"WV-048 Client-Server Protocol Static Conformance Requirement Version 1.2". Open Mobile Alliance. URL:http://www.openmobilealliance.org/release_program/enabler_releases.html
[PA]	"WV-049 Presence Attributes Version 1.2". Open Mobile Alliance. URL:http://www.openmobilealliance.org/release_program/enabler_releases.html
[PA DTD]	"WV-050 Presence Attribute DTD and Examples Version 1.2". Open Mobile Alliance. URL:http://www.openmobilealliance.org/release_program/enabler_releases.html
[CLP]	"WV-051 Command Line Protocol Version 1.2". Open Mobile Alliance. URL:http://www.openmobilealliance.org/release_program/enabler_releases.html
[SSP]	"WV-052 SSP - Server-Server Protocol Semantics Document Version 1.2". Open Mobile Alliance. URL:http://www.openmobilealliance.org/release_program/enabler_releases.html
[SSP Syntax]	"WV-053 Server-Server Protocol XML Syntax Document Version 1.2". Open Mobile Alliance. URL:http://www.openmobilealliance.org/release_program/enabler_releases.html
[SSP Trans]	"WV-054 SSP - Transport Binding Version 1.2". Open Mobile Alliance. URL:http://www.openmobilealliance.org/release_program/enabler_releases.html
[SSP SCR]	"WV-055 SSP – Server-Server Protocol Static Conformance Requirement Version 1.2". Open Mobile Alliance. URL:http://www.openmobilealliance.org/release_program/enabler_releases.html
[WAPARCH]	“WAP Architecture, Version 12-July-2001”. Open Mobile Alliance™. WAP-210-WAPArch. http://www.openmobilealliance.org/tech/affiliates/wap/wapindex.html

3. Terminology and Conventions

3.1. Conventions

This is an informative document, which is not intended to provide testable requirements to implementations.

3.2. Definitions

None

3.3. Abbreviations

CLP	Command Line Protocol
CLI	Command Line Interface
WV	Wireless Village
CSP	Client Server Protocol
SSP	Server Server Protocol
MCN	Mobile Core Network
IM&P	Instant Messaging and Presence
IMPS	Instant Messaging and Presence Services
SMCNP	Server to Mobile Core Network Protocol

4. Introduction

The Instant Messaging and Presence Service (IMPS) consists of four main service features:

- Presence feature,
- Instant messaging feature,
- Group feature, and
- Shared content feature.

A service provider may create its own IMPS community by providing either a full range of services or a subset of services. The service provider may also support the existing instant messaging communities on the Internet via an open interface.

The specifications consider the existing, ongoing standard efforts in, for example, 3GPP, IETF and WAP Forum, while addressing mobile-specific requirements and solutions.

The IMPS system provides a unique address space for presence, instant messaging, chat and content which is interoperable with existing instant messaging systems.

5. Presence Feature

Presence features are provided by the presence service element. Presence features can be separated into three defined parts: the definition of presence information for interoperability, the authorization and delivery mechanisms for presence information, and the contact list feature.

5.1. Presence Information

Presence information is not easily defined due to the vast amount of information that can be considered as presence information. To ensure interoperability, a set of interoperable presence attributes is defined. This is accomplished by dividing the presence information into client status and user status classes described below and by defining the most common presence attributes within these classes.

The semantics for each defined presence attribute is described as well. The semantics definition allows the implementers to derive functionality from the value of the presence attributes instead of just presenting the value to the user. The presence delivery mechanism allows the delivery of presence attributes beyond the defined attributes, but semantics of those attributes are beyond the scope of the Wireless Village specifications.

5.1.1. Client Status Attributes

The client status attributes describe the status of the running WV client software as well as the hardware device. They include presence attributes that describe the status of the WV client and device in relation to the mobile or fixed network as well as more detailed information about the client itself, such as version and capabilities.

The network status of the client includes the registration and online status of the client to the network as well as the location and address information of the client.

5.1.2. User Status Attributes

The user status attributes describe the status of the WV user. They include attributes describing the user availability and preferred contact methods as well as the contact information of the user.

The user status attributes also include information that may be used to describe textual free-format status, status with content and the emotional state of the user, such as mood.

5.2. Contact List Feature

A *Contact List* is a user maintained list of WV users in the presence service element. In WV, the Contact List is used for various purposes: as a distribution list when sending instant messages or subscribing presence, as a mechanism for proactive presence authorization, etc.

Users can manage multiple Contact Lists for various purposes, such as a list of friends and a list of colleagues.

The management of Contact Lists includes features to create, delete and edit contact lists as well as the ability to obtain a list of Contact Lists. Users may also modify the contents of a Contact List and retrieve the contents of a Contact List from a presence service element.

5.3. Authorization of Presence Attributes

5.3.1. Overview

The authorization of presence values are divided into two models: *proactive authorization* in which the WV user authorizes presence attributes before anyone has requested the attributes, and *reactive authorization* in which the WV user authorizes presence attributes on request.

The model and tools for authorization of the presence attributes is presented in Figure 1.

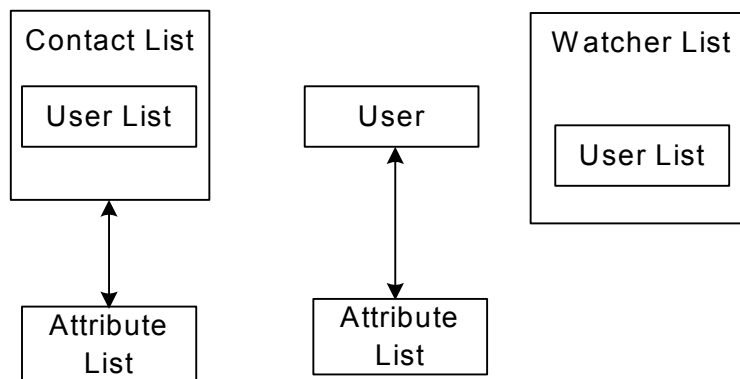


Figure 1. Authorization model for presence attributes

In the proactive authorization model, authorization is done proactively, without a specific request for information. In this case, the authorization may be targeted to either individual users or to a group of users through a Contact List. The reactive authorization applies to individual users only.

In the proactive authorization, the actual attributes that are authorized are defined in the attribute list. In reactive authorization, the requesting user either specifies the attributes he wants to receive or requests all attributes.

The term “publisher” represents the user who manages his or her own Contact Lists.

5.3.2. Proactive Authorization

In the proactive authorization model, the publisher creates the Contact List(s) and adds users into the Contact List(s). The members in a Contact List(s) are proactively authorized to access the publisher’s presence information contained in the default attribute list.

After creating a Contact List, the publisher may specify a list of presence attributes to be associated with the Contact List. The list of attributes of the Contact List is accessible by all members in that Contact List.

After adding a user to a Contact List, the publisher may specify a list of the presence attributes to be associated with that user, even if the Contact List has its own attributes list. The attributes list of the user is accessible only by that user.

When the user has his or her own list of attributes (i.e. A), while the Contact List has another list of attributes (i.e. B), the individual authorization always has priority over Contact List’s authorization, i.e. the individual’s attributes override the attributes of the Contact List.

When a user is in multiple Contact Lists that have separate attribute lists attached, the combination of the attributes in all attribute lists are authorized to this user.

The publisher manages the contact list and its members using functions such as “create Contact List”, “delete Contact List”, “get contact list”, “add contact list member”, and “remove contact list member”. The management functions also include the update of presence attributes for Contact Lists and users, and the removal of presence attributes for the users.

The publisher may also use some supporting functions to facilitate contact list management such as “create attribute lists”, “delete attribute lists”, “get attribute lists”, “update attribute list”, “attach and/or detach attribute lists to users and/or contact lists”.

5.3.3. Reactive Authorization

In the reactive authorization model, the requesting IM user may either request specific attributes or request all attributes. The presence service element sends an authorization request to the IM user who can grant or deny access to his presence attributes. The publisher specifies a list of attributes to which access is granted or denied. The attributes specified are added

to the list of attributes to which access is granted or denied as appropriate, overwriting any previous authorization for the specified attributes. The publisher can also specify that access to all presence attributes should be granted or denied.

The publisher can also cancel any previous authorizations or denials. This results in new notifications for any future requests.

5.3.4. Watcher List

Watcher List is a system-defined list of users with the functionality limited to holding the users that have subscribed to presence information.

All users that have subscribed to presence information are present in the Watcher List. Therefore it includes every user that has subscribed to one or more presence attributes, whether or not they were actually granted access to the attributes to which they subscribed. However, being present in the Watcher List does not mean that the authorization is still valid, or that the subscriber has access to any presence information. A user is removed from the watcher list when it sends an Unsubscribe Presence request. The user may remain in the watcher list after the subscription and session is not valid any more. The server may do garbage collection of users in the watcher list that has not had a valid subscription for a long time.

The server shall maintain one Watcher List for each user.

5.3.5. Authorization Withdrawal and Removal

Both proactive authorization and reactive authorization can be withdrawn by the authorizing user (publisher) at any time.

A subscribing user can request to be unsubscribed at any time. The server will then cancel the user's subscription and remove the subscriber from Watcher List.

5.3.6. Combination of Proactive and Reactive Authorization

The server may implement various combinations of the proactive and reactive authorization models. Proactive authorization has priority over reactive authorization. If some attributes are authorized proactively for the user, no reactive authorization is allowed, even if other proactively authorized attributes are requested.

5.3.7. Retrieval of Watcher List Feature

The publisher of the presence attributes is able to retrieve information about who is currently subscribing to their presence information. This is realized independent of whether the authorization is done proactively or reactively.

The Watcher List information List retrieval does not apply to the one-shot get presence feature described below.

5.4. Delivery of Presence Values

5.4.1. Subscribed Presence Feature

A user is able to subscribe to another user's presence information. The requesting user will initially receive new presence information and will always receive new presence information when the presence information of another party is updated. The authorization granted by the user may hide certain presence attribute values. A requesting user may unsubscribe to the presence information to stop the delivery of the other party's presence information to the requesting party.

5.4.2. Get Presence Feature

A user is able to get another user's current presence information once as widely as the presence owner has authorized it. This feature is used, for instance, when a user wants to occasionally check the status of another user.

5.4.3. Update Presence Feature

A user is able to change his or her own presence attribute values in the WV server. This feature is used when a value for the presence attributes originates from the WV client or the WV user him or herself.

6. Instant Messaging Features

Instant messaging features are provided by the instant messaging service element. The features include instant message origination and receiving, as well as delivery status reporting. Two separate receiving mechanisms are provided: direct push to the client as well as notification/pull. The instant messaging service is also used to send and receive instant messages through the group feature. Instant messaging using contact lists is also possible.

6.1. Delivery

IMPS users are able to send instant messages. The recipients of the message can be either one or more individual IMPS users, a group or IMPS users in a particular Contact List.

IMPS users are able to receive instant messages from individual senders, or from a group. Two receiving methods are provided:

Push-type delivery. The IM service element pushes the instant message directly to the recipient. This mechanism is usually used with short textual messages.

Notification/pull –type delivery. The IM service element sends a notification of the message to the recipient. The recipient then retrieves the message from the IM service element. This mechanism is usually used with multimedia and other large content. The notification/pull –type delivery mechanism can also be used to indicate messages that are outside of the Wireless Village system.

The receiving method the terminal chooses to use is initially provided in its login phase. The receiving method may be altered during later phases.

In the notification/pull –type delivery, the WV user may decide to forward the message to another recipient as well as to reject the message when receiving the notification.

While submitting the instant message the originator may request a delivery report that indicates the success or failure of the delivery of the message to the recipient(s). In the case of group messaging, the delivery report indicates the status of delivery to the group, but not the status of the delivery from the group to the joined users of that group.

6.2. Offline Messaging

When a WV user sends a message to another WV user, the receiving user may be offline, i.e., not logged onto the WV server. This is indicated by a presence attribute that the user may check before sending the message.

When a WV user sends a message and the other WV user is offline, the WV server implementation may support a store-and-forward functionality. If there is no such support in the WV server, the message is lost.

If the WV server supports a store-and-forward functionality, the messages are available (within a reasonable period) in the WV server awaiting the login of the recipient. When the user logs in, the WV server may either push each message independently to the user after login, or wait the user to retrieve a list of the waiting messages to retrieve each message separately.

6.3. Access Control

IMPS users are able to block messages or invitations from users using a blocked list as well as allow messages or invitations using a granted list. This blocking applies to both point-to-(multi)point messaging or invitations as well as messaging via the group feature. The blocked list and granted lists may be used in parallel with clear priority rules.

6.4. Message Content

Instant messaging technology allows the delivery of any content, including multimedia content. In order to ensure minimum interoperability, the following requirements are set:

The mandatory content type is plain Unicode text with UTF-8 encoding. The characters (glyphs) that are supported are at least those in ISO 8859-1 (Latin-1).

The suggested content types are:

- Multimedia Message [TS23.140]
- Enhanced Short Message [TS23.040]
- Business Card [vCard 2.1]
- Calendar Entry [vCalendar 1.0]

The purpose of the suggested content types is to further guide manufacturers to maximize interoperability while not making the implementation of the content and the related functionality mandatory. Definition and use of other content types are beyond the scope of Wireless Village specifications.

7. Group Feature

The concept of a user group means a chat room–type discussion forum formed either by a service provider or an individual WV user to exchange information such as opinions, comments, thoughts, etc., about a particular issue, which is the topic of the group. The group is a basic feature that allows the service providers to create communities of IMPS users.

Messaging to and from a group is done via the instant messaging features described earlier. Using the instant messaging features, the messages are directed toward a group instead of individual recipients. The key difference between group messaging and ordinary point-to-point messaging is that a group acts as a distribution mechanism for the messages. Consequently, every users that wants to receive messages from a group and participate in a discussion must join the group.

The users joined to a group may participate in the discussions using their WV user name, or they may pick a suitable screen name when joining to the group to maintain anonymity.

7.1. Group Models

7.1.1. Private Group Model

A private group is a user group that is created by an individual WV user. The creator of the group is able to control how the group is accessible for other users, i.e., whether the private group is open for anyone or a restricted one that only specified users may join. The visibility of the group may be restricted from other users by setting the group's properties.

7.1.2. Public Group Model

A public group is a users group that is created by a service provider. The service provider can control the group in the same way the owner of a private group can.

7.1.3. Group Membership

A public or private user group may have a list of members. This list may be used to restrict access to the group, for example a group may be a restricted group allowing only members to join the group. In addition the list of members may be used to assign roles to the WV users, such as administrator or moderator.

7.2. Dynamic Group Features

These features include those features that are used frequently when chatting in a group.

7.2.1. Join group feature

A user is able to join a public or private group if allowed by group properties and other access control features. This enables the user to communicate with other members joined to the group. A user may use a screen name instead of a user name while in the group.

7.2.2. Leave group feature

A user may leave a group at any time. Leaving a group indicates the end of the user's messaging within the group. In order to restart messaging, the user needs to rejoin the group. The group service element may also force the user to leave the group if there is a change in the access control information for the group.

7.2.3. Invite user to group feature

A user may invite other users to the group and provide the reason the invitation was sent. An invitee may accept or reject the invitation; the sender will get information about the reason for rejection. The invite–user-to-a-group feature is part of the common invitation feature.

7.2.4. Search Group and Users Feature

A user may search user groups based on the groups' properties. In addition, a user may search groups that are owned by a particular user or groups that a particular user is currently joined to. The search features are part of the common search feature described below.

7.2.5. Subscribe to Group Change Feature

A user may subscribe to automatic notifications about changed group information, i.e. joined/left users or changes in common or own group properties. The user may cancel the subscription.

7.3. Static Group Features

The static group features are those that allow the users to create, manage and delete groups as well as obtain information from the group.

7.3.1. Create group feature

A user is able to create a private user group and specify the initial group properties if the service provider offers such a feature.

7.3.2. Delete group feature

An owner or user with sufficient privileges is able to delete a private user group.

7.3.3. Management of Members' List Feature

An owner or user with sufficient privileges may add users to the list of members or delete users from the list.

7.3.4. Modify Group Properties Feature

A user with sufficient privileges may modify properties of a private group, for instance specifying the maximum number of users and the topic of discussion.

7.3.5. Access Control Features

The service provider, or in the case of a private group a user with sufficient privileges, may define the group as restricted in the group's properties so that only the users in the members' list can join the group.

In addition, the service provider or user may maintain a separate reject list that indicates those users not allowed to join the group.

8. Shared Content Feature

The shared content feature allows IMPS users to share content, such as images and documents, while sending messages or chatting in a group.

In the current specification release, the shared content is realized with the common invitation function described in detail below. Using the invitation function, the users can send a URL of the content they are willing to share. Similarly, they can cancel the invitation content when they no longer want to share the content. Currently there are no mechanisms to upload or download content.

9. Access Features

9.1. Login and Logout Feature

The WV client is required to log into a WV server to be able to use WV services. In the login phase the user is authenticated and a *session* is established. When the client no longer wants to use the WV services the client may log out of the service.

The WV server may disconnect the session from the server side.

9.2. Service and Capability Feature

When a WV client has logged into a WV server, the capabilities and services are negotiated between the client and the server before the WV services may be used.

In the capabilities negotiation phase the WV client indicates its capabilities to the WV server. The server uses these capabilities to adapt the communications and delivered content to the client. The client capabilities include:

- Preferred delivery method (push or notification/pull)
- Accepted content types
- Accepted transfer encoding
- Accepted content length
- Supported transport bindings

In the service negotiation phase the WV client indicates the features and functions it plans to use within the session and that it requires the WV server to support. The WV server then responds with the features and functions it agrees to support based on availability and the user's profile.

9.3. Keep Alive Feature

A keep alive message is sent according to an agreed keep alive timer whenever there is no other communication within the session. The purpose of the keep alive feature is to indicate to the WV server that the WV client is still online and ready for communication.

9.4. Get Service Provider Information Feature

The get service provider information feature is used to retrieve information about the WV service provider, including the name and logo of the service provider, as well as descriptive text and a URL to the Web pages of the service provider.

The get service provider information feature is a tool for branding of WV services.

10. Common Features

10.1. General Search Feature

The general search feature is intended to enable users to search the information and users from the provided WV services. In this specification version the search feature is limited to a search of users and groups.

The users can be searched by providing (part of) the user's name, first name, last name, email address or user alias.

The groups can be searched by providing (part of) the group id, name and topic. In addition it is possible to search groups that are owned by a particular WV user, or groups a particular user is currently joined to.

10.2. General Invitation Feature

The general invitation feature enables a WV user to invite some other user or user(s) to some WV related activity such as:

- Invitation to a group chatting,
- Invitation to sharing of presence information and,
- Invitation to share identified content

In the invitation request the user can provide an explanation or reason for the invitation. The recipient user is expected to respond indicating his acceptance or rejection of the invitation as well as a free-format explanation or reason for the response.

The WV user may also cancel her previously sent invitation to indicate that she is no longer interested in continuing the indicated WV activities.

11. Server Interoperability Features

The term “Server” represents the logical server cluster in one service provider domain. The term “Server” is interpreted as the single access point, which may be physically a Local Director, a Proxy, a Routing Proxy, or anything else that represents the domain. The term “Server” is NOT interpreted as any physical server entity deployed within the domain.

The term “Home Domain” is the domain where the client subscribes to, and is authenticated and authorized to use the IMPS services.

The term “Primary Service Element” (PSE) means the primary SE of an IMPS service for a client. PSE may be in the Home Domain of the client or in a remote domain.

Wireless Village supports server interoperability at different levels. At the lowest level, two users located at two different home domains are able to communicate with each other, as shown in Figure 2. At the highest level, Wireless Village supports a complete set of IMPS services assembled from complementary IMPS services across service provider domains, as shown in Figure 3. Wireless Village defines the rules for the PSE to take appropriate actions to achieve the interoperability and provide distributed IMPS services.

In order for the service providers to have the flexibility to choose the appropriate level of interoperability and set up different service agreements between themselves, Wireless Village mandates a minimum set of interoperable features and functions. To guarantee interoperability it is required that the two interacting servers provide the same subset of services.

In the example in Figure 2, client 1 is located in home domain A, and client 2 is located in home domain B. Domain A implements IM and Group service elements, and domain B implements the full set of Wireless Village service elements. The common subset of services is IM and Group, i.e. client 1 and client 2 are interacting across domains via the minimum set of interoperable IM and Group features and functions.

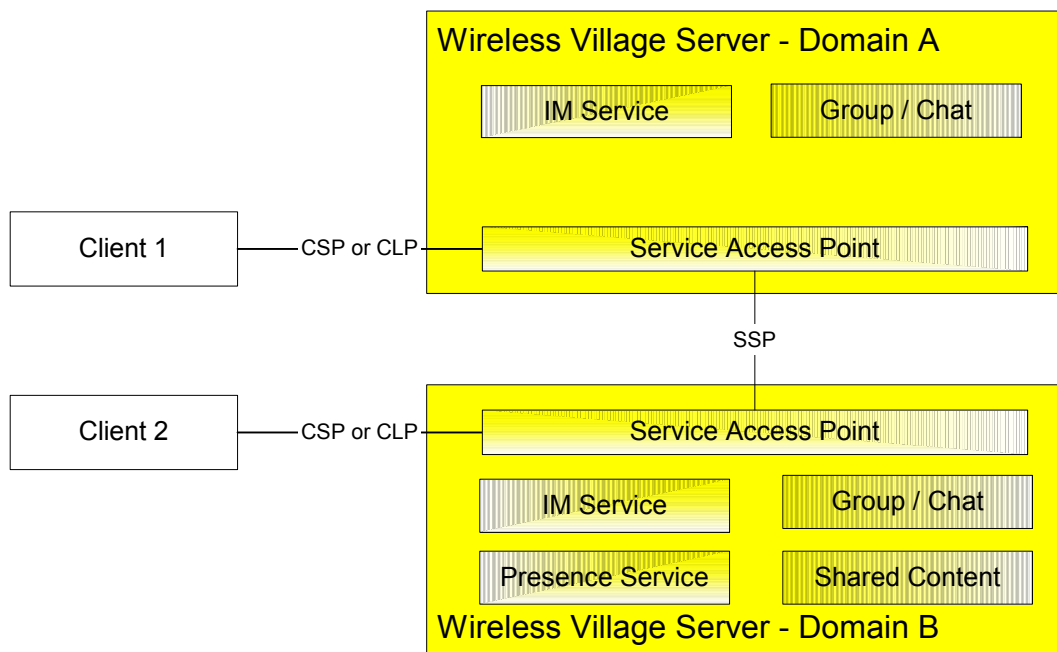


Figure 2. The minimal interoperability.

The full set of interoperability features includes the Interoperability Management and the IMPS Service Relay. Interoperability Management includes a Security Model, Transaction Management, Session Management, Service Management and User Profile Management. The IMPS Service Relay includes Common IMPS Features, Contact List Features, Presence Features, Instant Messaging Features, Group Features and Shared Content Features.

In the example in Figure 3, client 1 is located in home domain A, and Client 2 is located in home domain B. Domain A implements the presence and group service elements and domain B the IM and shared content service elements. The Wireless Village interoperability model allows client 1 and 2 to use the complete set of features and interact with each other via the SSP.

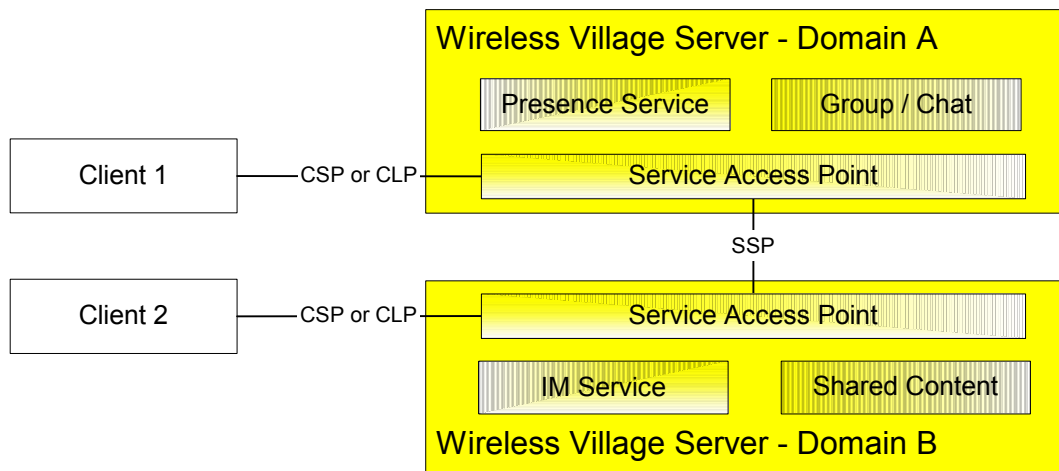


Figure 3. Complementary services.

In Wireless Village Interoperability, the Home Domains must have a direct SSP connection to interoperate with each other. However, Wireless Village supports the routing of “Service Relay” between the Home Domain and the PSE. The route from Home Domain B to its PSE is shown in Figure 4, where the PSE domain that provides the actual service element, e.g. IM service, is at the end of the route. Each intermediate domain relays the service request to the next node. The intermediate nodes act as the “logical” Service Provider role for each downstream domain, and act as the “logical” Service Requestor role for each upstream domain.

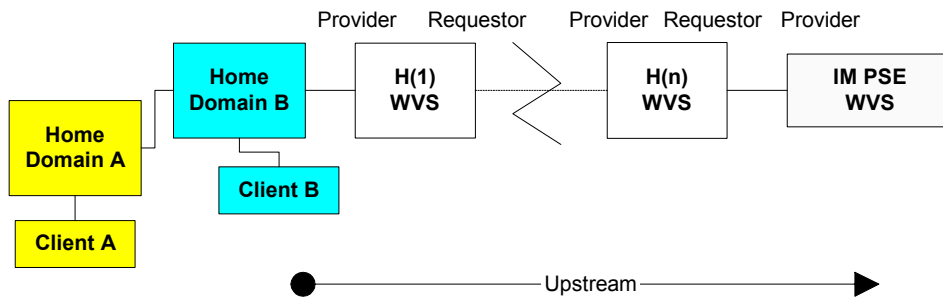


Figure 4. The SSP Service Relay

At each domain the SAP should maintain a Service Table that keeps track of the service agreements to appropriately relay the SSP service request on a per-service basis and forward the SSP service result on a per-domain basis. Being the “logical” Service Provider, the SAP should maintain a Session Record for each Service Requestor. Being the “logical” Service Requestor, the SAP should maintain a Transaction Record for each Service Provider. The SAP should maintain a Transaction Table to map each requested transaction from its Service Requestor of the initiated transaction to its Service Provider. The Transaction Table should have a unique match for each transaction. Therefore, the Service Relay flow and Result Forward flow at each SAP is clearly and uniquely identified by the transaction flows.

The SAP at the Home Domain shall appropriately map the CSP/CLP service request from the client to the SSP service request, and/or map the SSP service result of the CSP/CLP service result to the client.

11.1. Security

The scope of security in server interoperability is the server-to-server communication at the IMPS application level, i.e., to ensure that the data sent and/or received on behalf of an End User in a given IMPS domain is actually originating from and/or terminating at the servers in that domain.

Other security requirements, such as data integrity and confidentiality in the transport layer and other underlying layers, are out of the scope of server interoperability in WV. Whenever possible the service providers have to ensure that current security approaches in the underlying layers shall be used to secure those layers.

11.2. Transaction Management

Transaction management defines the necessary common information elements in the service requests and service responses at the transaction level, regulates the behaviour in the transaction flows, and handles the exception and error conditions at the transaction level.

11.3. Session Management

Session management authenticates and authorizes the servers in other domains, and maintains the session and security. Features and functions include session establishment, session termination and session maintenance. Access control is supported in the session management features.

11.4. Service Management

After the servers trust each other, they are able to find the IMPS features and functions supported by each other, and set up a service agreement to provide each other with complementary IMPS services.

11.4.1. Service Discovery

Service Discovery enables one server to find the total collection of IMPS capability features and functions supported by another server.

11.4.2. Service Negotiation and Agreement

A service provider is able to control which SSP features are made available to another domain by using the Service Negotiation and Agreement feature.

11.5. User Profile Management

User Profile Management enables servers to exchange user profile information between each other including those services a user subscribes to, the service status (active / inactive), privacy status with regard to network service capabilities (e.g. user location, user interaction), terminal capabilities, *etc.*

The features of User Profile Management are “Get-User-Profile” and “Update-User-Profile”.

The “Get-User-Profile” feature allows one server to get user profile information from another server.

The “Update-User-Profile” feature allows one server to update user profile information in another server

11.6. Service Relay – IMPS Features

The Service Relay of the IMPS Features includes Common IMPS Features, Contact List Features, Presence Features, Instant Messaging Features, Group Features and Shared Content Features.

Appendix A. Change History (Informative)

A.1 Approved Version History

Reference	Date	Description
OMA-WV-Features_Functions-V1_1-20021001-A	01 Oct 2002	Version 1.1

A.2 Draft/Candidate Version 1.2 History

Document Identifier	Date	Sections	Description
Candidate Versions OMA-IMPS-WV- Features_Functions-V1_2	02 Feb 2003	n/a	Status changed to Candidate by TP TP ref # OMA-TP-2003-0109-IMPS-V1_2-Candidate-Package
	22 May 2004	Overall 3.1	The 2004 spec template applied and the document reference and hyperlinks corrected. Convention description corrected as this document is informative.

