Features and Functions

Version 1.1

WV Internal Tracking Number: WV-021

Notice

Implementation of all or part of any Specification may require licenses under third party intellectual property rights, including without limitation, patent rights (such a third party may or may not be a Supporter). The Sponsors of the Specification are not responsible and shall not be held responsible in any manner for identifying or failing to identify any or all such third party intellectual property rights.

THIS DOCUMENT AND THE INFORMATION CONTAINED HEREIN ARE PROVIDED ON AN "AS IS" BASIS WITHOUT WARRANTY OF ANY KIND AND ERICSSON, MOTOROLA and NOKIA DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL ERICSSON, MOTOROLA or NOKIA BE LIABLE TO ANY PARTY FOR ANY LOSS OF PROFITS, LOSS OF BUSINESS, LOSS OF USE OF DATA, INTERRUPTION OF BUSINESS, OR FOR DIRECT, INDIRECT, SPECIAL OR EXEMPLARY, INCIDENTAL, PUNITIVE OR CONSEQUENTIAL DAMAGES OF ANY KIND IN CONNECTION WITH THIS DOCUMENT OR THE INFORMATION CONTAINED HEREIN, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE. The above notice and this paragraph must be included on all copies of this document that are made.

Intellectual Property Rights have been asserted or conveyed in some manner toward these Wireless Village specifications. The Wireless Village initiatives' intellectual property rights guidelines are defined in Section 5.1 of the Wireless Village Specification Supporter Agreement. The Wireless Village initiative takes no position regarding the validity or scope of any intellectual property right or other rights that might be claimed to pertain to the implementation or use of the technology, or the extent to which any license under such rights might or might not be available. A public listing of all claims against the Wireless Village specifications, as well as an excerpt of Section 5.1 of the Wireless Village Specification Supporter Agreement, can be found at:

http://www.wireless-village.org/ipr.html

Table of Contents

1. Revision History 1
2. References 2
3. Service Overview 3
4. Presence Feature 4
4.1 Presence Information 4
4.1.1 Client Status Attributes 4
4.1.2 User Status Attributes 4
4.2 Contact List Feature 4
4.3 Authorization of Presence Attributes 5
4.3.1 Overview 5
4.3.2 Proactive Authorization 5
4.3.3 Reactive Authorization 6
4.3.4 Watcher List 6
4.3.5 Authorization Withdrawal and Removal 6
4.3.6 Combination of Proactive and Reactive Authorization 7
4.3.7 Retrieval of Watcher List Feature 7
4.4 Delivery of Presence Values 7
4.4.1 Subscribed Presence Feature 7
4.4.2 Get Presence Feature 7
4.4.3 Update Presence Feature 7
5. Instant Messaging Features 8
5.1 Delivery 8
5.2 Offline Messaging 8
5.3 Access Control 9
5.4 Message Content 9
6. Group Feature 10
6.1 Group Models 10
6.1.1 Private Group Model 10
6.1.2 Public Group Model 10
6.1.3 Group Membership 10
6.2 Dynamic Group Features 10
6.2.1 Join group feature 10
6.2.2 Leave group feature 11
6.2.3 Invite user to group feature 11
6.2.4 Search Group and Users Feature 11
6.2.5 Subscribe to Group Change Feature 11
6.3 Static Group Features 11
6.3.1 Create group feature 11
6.3.2 Delete group feature 11
6.3.3 Management of Members' List Feature 11
6.3.4 Modify Group Properties Feature 11
6.3.5 Access Control Features 12
7. Shared Content Feature 13
8. Access Features 14
8.1 Login and Logout Feature 14
8.2 Service and Capability Feature 14
8.3 Keep Alive Feature 14
8.4 Get Service Provider Information Feature 14
9. Common Features 15
9.1 General Search Feature 15
9.2 General Invitation Feature 15

10. Server Interoperability Features 16
10.1 Security 19
10.2 Transaction Management 19
10.3 Session Management 19
10.4 Service Management 19
10.4.1 Service Discovery 19
10.4.2 Service Negotiation and Agreement 19
10.5 User Profile Management 19
10.6 Service Relay – IMPS Features 20

1. REVISION HISTORY

Date	Issue	Description	Author
February 13th	TBD	Initial release	WV TechComm
July 31, 2002	V1.1	Version 1.1	WV TechComm

2. REFERENCES

[RFC2778] "A Model for Presence and Instant Messaging", Day M., Rosenberg J., Sugano H, February 2000.

[RFC2779] "Instant Messaging / Presence Protocol Requirements", Day M., Aggarwal S, Mohr G., Vincent J. February 2000.

[CPIM] "Common Presence and Instant Messaging", Crocker D., Diacakis A., Mazzoldi F., Huitema C., Klyne G., Rosenberg J., Sparks R. Sugano H. November 2001.

[TS23.140] 3rd Generation Partnership Project; Technical Specification Group Terminals; Multimedia Messaging Service (MMS); Functional description; Stage 2 (3GPP TS 23.140 version 4.6.0, Release 4)

[TS22.140] 3rd Generation Partnership Project; Technical Specification Group Terminals; Technical Realization of the Short Message Service (SMS); (3GPP TS 23.040 version 4.4.0, Release 4)

[vCard 2.1] vCard, The Electronic Business Card, Version 2.1, A versit Consortium Specification, September 18, 1996, Copyrights © 1996, International Business Machines Corp., Lucent Technologies, Inc., and Siemens. All rights reserved.

[vCalendar 1.0] vCalendar, The Electronic Calendaring and Scheduling Exchange Format, Version 1.0, A versit Consortium Specification, September 18, 1996, Copyrights © 1996, International Business Machines Corp., Lucent Technologies, Inc., and Siemens. All rights reserved.

3. SERVICE OVERVIEW

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

1. Presence feature,
2. Instant messaging feature,
3. Group feature, and
4. 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.

4. 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.

4.1. 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.

4.1.1 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.

4.1.2 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.

4.2. 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.

4.3. AUTHORIZATION OF PRESENCE ATTRIBUTES

4.3.1 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.

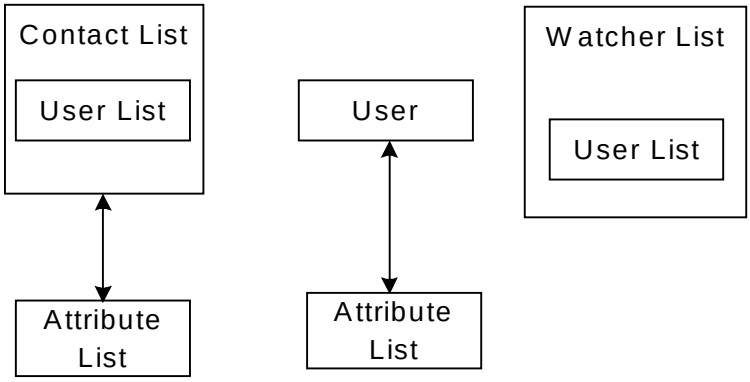

Figure 1. Authorization model for presence attributes

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.

4.3.2 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".

4.3.3 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 and, if authorized, adds the user to the Watcher List.

If the user does not indicate specific attributes in his reactive authorization request, the Default Public Attribute List will be used for this user. Otherwise the specific attribute list shall be associated with the subscriber.

There is no mechanism enabling partial authorization of requested attributes.

4.3.4 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.

The server shall maintain one Watcher List for each user.

4.3.5 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.

4.3.6 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.

4.3.7 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.

4.4. DELIVERY OF PRESENCE VALUES

4.4.1 Subscribed Presence Feature

A user is able to subscribe to another user's presence information for a time period that may be indefinite. 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 during the time period to stop the delivery of the other party's presence information to the requesting party.

4.4.2 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.

4.4.3 Update Presence Feature

A user is able to change his or her own presence attrib ute 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.

5. 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.

5.1. 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.

5.2. 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.

5.3. ACCESS CONTROL

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

5.4. 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 [TS 23.140]
- Enhanced Short Message [TS 23.040]
- 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.

6. 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.

6.1. GROUP MODELS

6.1.1 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.

6.1.2 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.

6.1.3 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.

6.2. DYNAMIC GROUP FEATURES

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

6.2.1 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.

6.2.2 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.

6.2.3 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.

6.2.4 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.

6.2.5 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.

6.3. 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.

6.3.1 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.

6.3.2 Delete group feature

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

6.3.3 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.

6.3.4 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.

6.3.5 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.

7. 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 when they no longer want to share the content. Currently there are no mechanisms to upload or download content.

8. ACCESS FEATURES

8.1. 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.

8.2. 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.

8.3. 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.

8.4. 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.

9. COMMON FEATURES

9.1. 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.

9.2. 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.

10. 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.

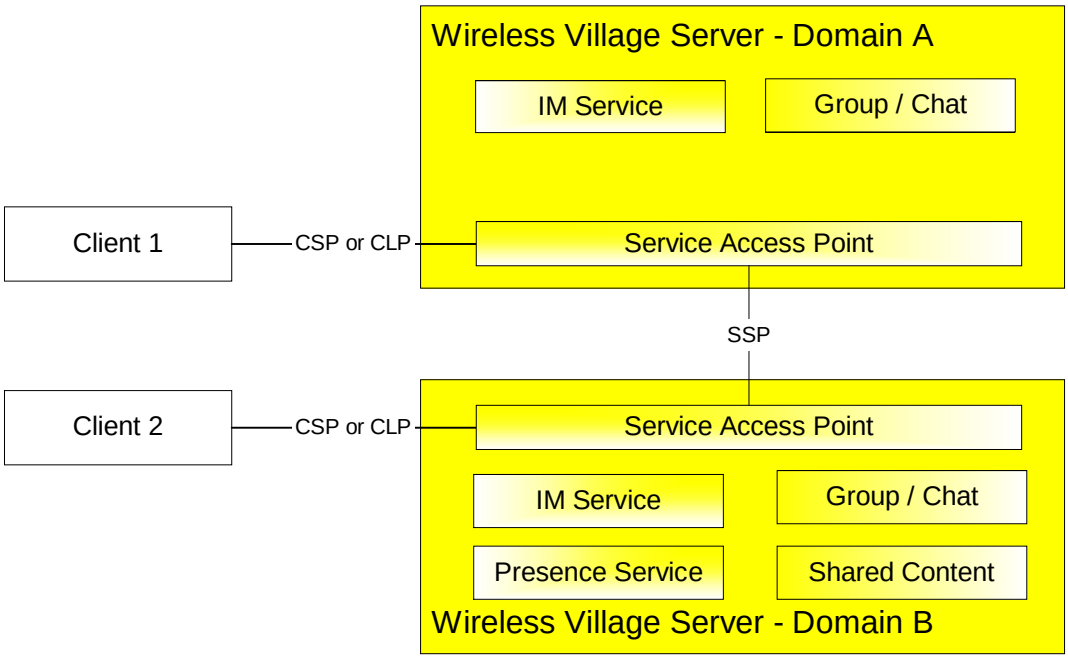

Figure 2. The minimal interoperability.

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.

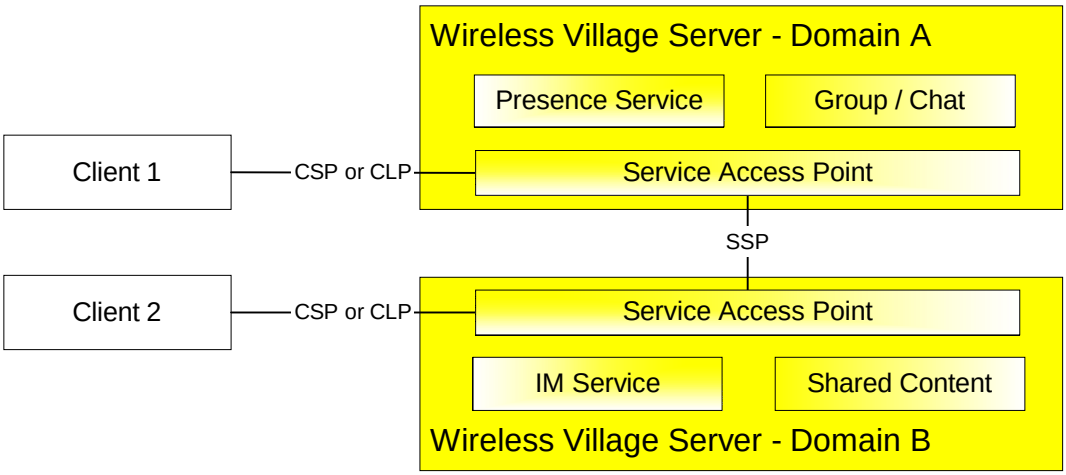

Figure 3. Complementary services.

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.

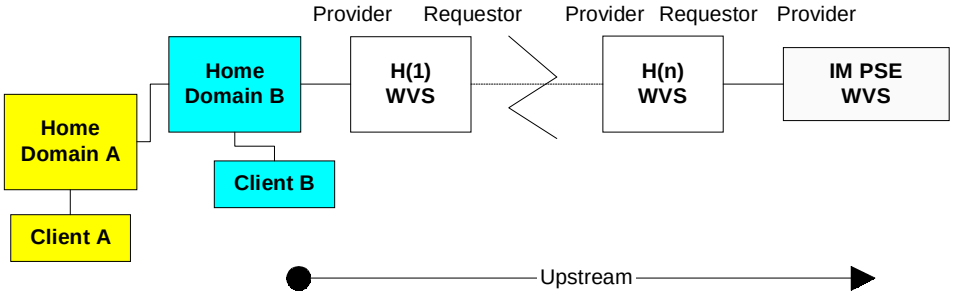

Figure 4. The SSP Service Relay

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.

10.1. 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.

10.2. 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.

10.3. 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.

10.4. 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.

10.4.1 Service Discovery

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

10.4.2 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.

10.5. 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

10.6. 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.