Features and Functions

V1.0

WV Internal Tracking Number: WV-002

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.

Table of Contents

1. 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.

2. Service Overview

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

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

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

3. Presence Feature

The presence feature is provided by the presence service element. It can be defined into three parts: the definition of presence information for interoperability, the authorization and delivery mechanisms for presence information and the contact list feature.

3.1 Presence Information

The presence information is not easily defined due to vast amount of information that can be considered as presence information. However, to ensure interoperability, a set of interoperable presence attributes are defined. This is

accomplished by dividing the presence information into client status and user status classes described below and defining the most common presence attributes within the classes.

The semantics for each defined presence attribute is described as well. The semantics definition allow the implementors 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 Wireless Village specifications.

3.1.1 Client Status Attributes

The client status attributes describe the status of the running WV client software as well as the hardware device. It includes 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 of 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 location and address information of the client.

3.1.2 User Status Attributes

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

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

3.2 Contact List Feature

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

Users can manage multiple contact lists for various purposes, such as list of friends and list of colleagues.

The management of contact lists include features to create, delete and manage contact lists as well as obtain a list of contact lists. The users may also modify the content of a contact list and retrieve the content of a contact list from the presence service element.

3.3 Authorisation of Presence Attributes

3.3.1 Overview

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

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

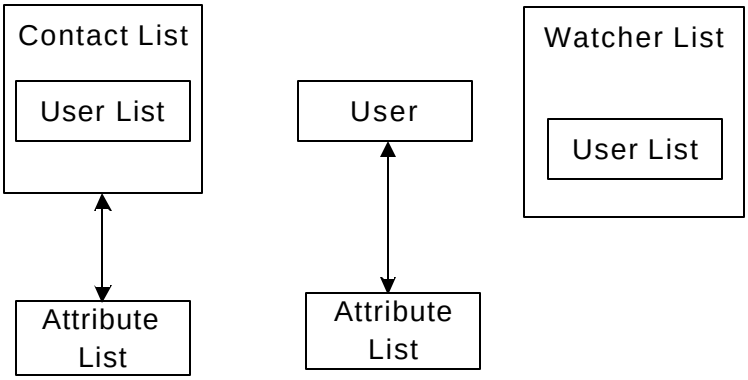

Figure 1. Authorization model for presence attributes

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

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

We use the term “publisher” to represent the user who manages its own contact lists.

3.3.2 Proactive Authorisation

In the proactive authorization, the publisher creates the contact list(s) and adds the other users into the contact list(s). The members in the contact list(s) are proactively authorized to access the publisher’s presence information.

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

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

When the user has its own list of attributes (i.e. A), while its contact list has the list of attributes (i.e. B), the individual authorization always has priority over contact list's authorization, i.e. the individual 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 in such ways 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 detatch attribute lists to users and/or contact lists".

3.3.3 Reactive Authorisation

In the reactive authorisation, the requesting IM user may request either specific attributes or request for all attributes. The presence service element sends an authorisation request to the IM user and, if authorised, 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 of partial authorization of the requested attributes.

3.3.4 Watcher List

Watchers list is a system-defined list of users with the functionality limited to hold users that have subscribed to presence information including the subscribed attributes.

All users that have subscribed to presence information are present in the Watchers list, i.e. a user that is present in a contact list and has subscribed to one or more presence attributes is always present in the watchers list. A user

whose reactive authorization request is accepted shall also be present in the watchers list.

The server shall maintain one Watcher List for each user.

3.3.5 Authorization Withdrawal and Removal

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

The authorized user (subscriber) can request the publisher to remove the authorization at any time. The publisher shall withdraw the authorization upon the removal request from the subscriber.

3.3.6 Combination of Proactive and Reactive Authorisation

The server may implement various combinations of the proactive and reactive authorisation models. The proactive authorisation has priority over reactive authorisation. If some attributes are authorised proactively for the user, no reactive authorisation is done, even if other attributes are requested than were authorised proactively.

3.3.7 Retrieval of Watcher List Feature

The publisher of the presence attributes is able to retrieve information who is currently subscribing their presence information. This is realised independently whether the authorisation is done proactively or reactively.

The retrieval does not apply to the one-shot get presence feature described later on.

3.4 Delivery of Presence Values

3.4.1 Subscribed Presence Feature

A user is able to subscribe another user's presence information to a time period which may be infinite. The requesting user will receive new presence information initially and always when the presence information of other party is updated. The authorisationmay hide certain presence attribute values. A user is able to unsubscribe the presence information during the time period to stop the delivery of other party's presence information.

3.4.2 Get Presence Feature

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

3.4.3 Update Presence Feature

A user is able to change its 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 itself.

4. Instant Messaging Feature

The instant messaging feature is provided by the instant messaging service element. The features include origination, 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 group feature. Also, instant messaging using contact lists is possible.

4.1 Delivery

The IMPS users are certainly able to send instant messages. The recipient of the message can be either one or more individual IMPS users, a group or IMPS users in particular contact list.

The IMPS users are able to receive instant messages from individual senders, or from a group. Two different 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 at login phase. It may, however, be altered at later phase.

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

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

4.2 Offline Messaging

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

When a WV user sends the message and the other WV user is offline, it is up to the WV server implementation to support store and forward type functionality. If there is no such support in the WV server, the message is simply lost.

If the WV server supports store and forward type of functionality, the messages are available (within a reasonable period) in the WV server waiting the recipient to log in. 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 messages waiting and retrieve each message separately.

4.3 Access Control

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

4.4 Message Content

The instant messaging technology allows the delivery of any content, including multimedia content. However, in order to ensure minimum interoperability, the following requirement 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 (MMS v1.0)
- Enhanced Short Message (SMS v4.4.0)
- Business Card (vCard 1.0)
- Calendar Entry (vCalendar 2.1)

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

5. Group Feature

The concept of user group means a chat room –type discussion forum formed either by service provider or 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 which allows the service providers to create communities of IMPS users.

The messaging to and from group is done via instant messaging features described earlier. In the messaging features, the messages are directed towards group instead of individual recipients. The key difference between group messaging and ordinary point-to-point messaging is that group acts as distribution mechanism to the messages. Consequently, each users that wants to receive messages from a group and participate discussed must join the group.

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

5.1 Group Models

5.1.1 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 closed one and only specified users may join it. The visibility of the group may be restricted from other users in group properties.

5.1.2 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 as the owner of the group in case of private group.

5.1.3 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 instance, a group may be a closed group and only members may join to the group. In addition, the list of members may be used to assign roles to the WV users, such as administrator or moderator.

5.2 Dynamic Group Features

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

5.2.1 Join group feature

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

5.2.2 Leave group feature

A user may leave a group at any time he wants to. Leaving of a group indicates end of messaging within the group. In order to restart messaging, the user needs to rejoin to 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.

5.2.3 Invite user to group feature

A user may invite other users to the group and tell the reason why the invite was send. An invitee may accept or reject the invite and the sender gets information about the reason of rejection. The invite user to a group is part of the common invitation feature.

5.2.4 Search Group and Users Feature

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

5.2.5 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 also cancel the subscription.

5.3 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.

5.3.1 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.

5.3.2 Delete group feature

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

5.3.3 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.

5.3.4 Modify Group Properties Feature

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

5.3.5 Access Control Features

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

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

6. Shared Content Feature

The shared content feature allows the 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 realised with the common invitation function described in detail later. With 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 want no more to share the content. Currently, there are no mechanisms to upload or download the content.

7. Access Features

7.1 Login and Logout Feature

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

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

7.2 Service and Capability Feature

When the WV client has logged in to the WV server, the capabilities and services are negotiated between the client and the server before the use of the WV services.

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 included are:

- 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 it requires the WV server to support. The WV server then responds the features and functions it agrees to support based on availability and user profile.

7.3 Keep Alive Feature

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

7.4 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 URL to the Web pages of the service provider.

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

8. Common Features

8.1 General Search Feature

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

The users can be searched by providing (part of) their user name, their first name, their 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 where a particular user is currently joined in.

8.2 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 an identified content

In the invitation request, the user can provide explanation or reason for the invitation. The recipient user is expected to respond indicating his acceptance or

rejection for the invitation as well as again free-format explanation or reason for the response.

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

9. 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, or a Proxy, or a Routing Proxy, or anything else that represents the domain. The term “Server” is NOT interpreted as any physical server entity of the deployment 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) is 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 that a complete set of IMPS services are 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 them, Wireless Village mandates a minimum set of interoperable features and functions. To guarantee inte acting servers provide the same sub

In the example in Figure 2, c nt 2 is located in home domain B ervice elements, and domain B im ervice elements. The common subs 1 and client 2 are interacting cross domains via the minimum set of interoperable IM and Group features and functions.

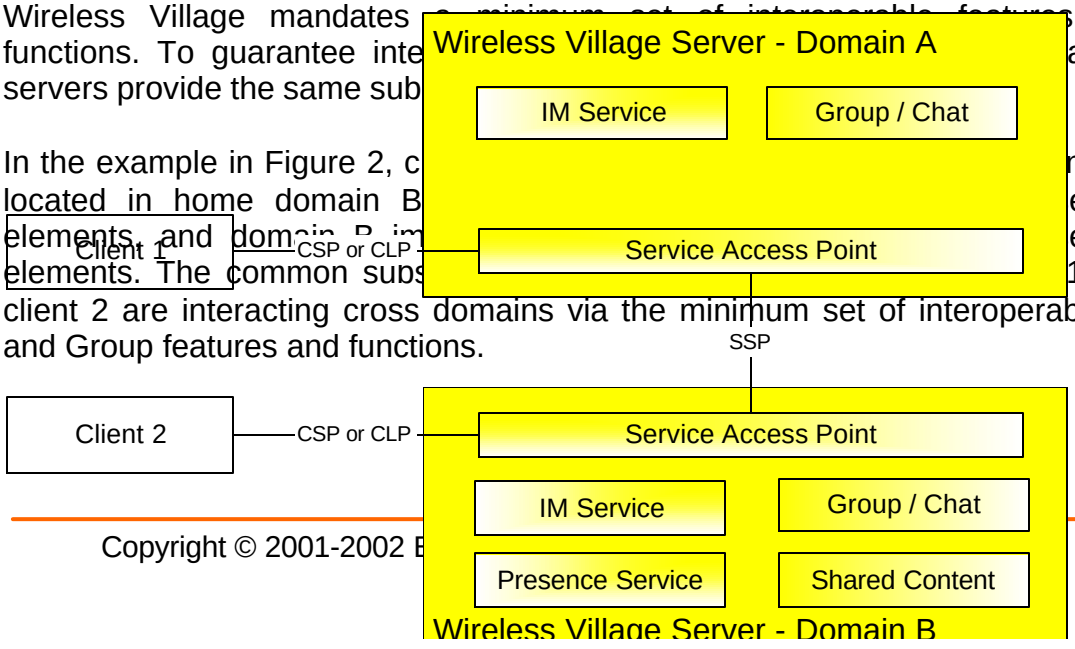

Figure 2. The minimal interoperability.

The full set of interoperability features includes the Interoperability Management and the IMPS Service Relay. The 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 utilize the complete set of features and interact with each other via the SSP.

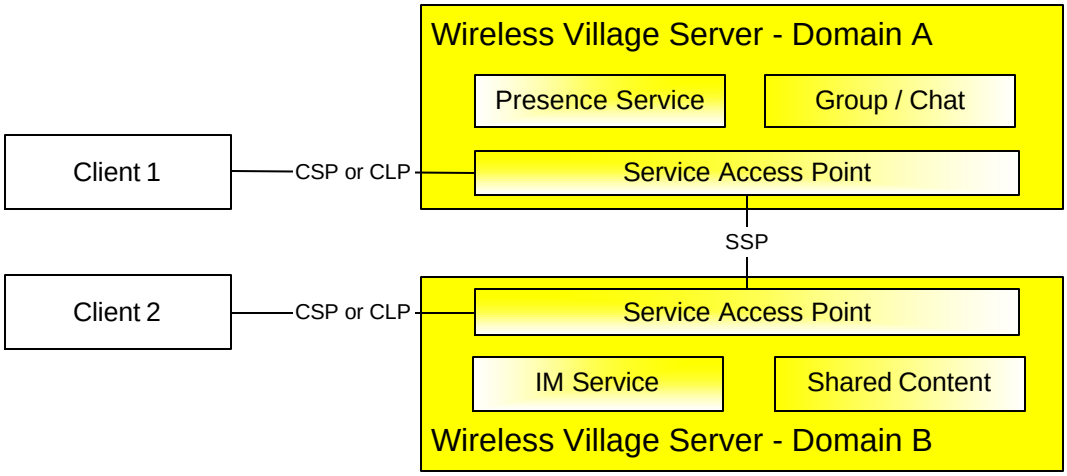

Figure 3. Complementary services.

In Wireless Village Interoperability, the Home Domains must have direct SSP connection if they want 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. All intermediate domains are relaying the service request to the next hop. The intermediate nodes act the "logical" Service Provider role for each downstream domain, and act the “logical” Service Requestor role for each upstream domain.

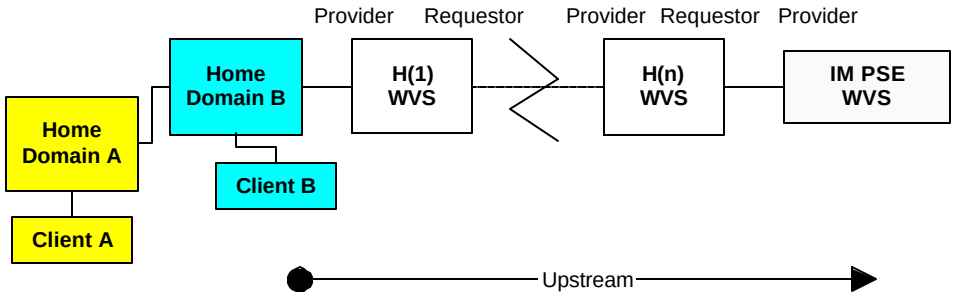

Figure 4. The SSP Service Relay

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 to the initiated transaction to its Service Provider. The Transaction Table should be the uniquely one-one match. Therefore, the Service Relay flow and Result Forward flow at each SAP is clearly and uniquely identified by the transaction flows.

The SAP at 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 to CSP/CLP service result to the client.

9.1 Security

The scope of security in the 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 to the servers in that domain.

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

9.2 Transaction Management

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

9.3 Session Management

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

9.4 Service Management

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

9.4.1 Service Discovery

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

9.4.2 Service Negotiation and Agreement

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

9.5 User Profile Management

User Profile Management enables the servers to exchange user profile information between each other including to which a user subscribes, 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”.

“Get-User-Profile” is for one server to get user profile information from another server.

“Update-User-Profile” is for one server to update user profile information in another server

9.6 Service Relay – IMPS Features

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