IMPS Architecture

Candidate Version 1.3 – 11 Oct 2005

Open Mobile Alliance

OMA-AD-IMPS-V1_3-20051011-C

Contents

Figures

1. Scope (Informative)

Instant Messaging and Presence Service (IMPS) is an OMA enabler that is designed for exchanging instant messages and presence information not only between mobile devices but also between mobile and fixed devices. The origins of this enabler lie in the Wireless Village initiative. When Wireless Village was incorporated into OMA, the version 1.1 of its specifications became the OMA IMPS 1.1 enabler. Afterwards the IMPS 1.2 enabler was finalized within OMA.

The IMPS 1.3 enabler is a significant enhancement of the IMPS 1.2 enabler and is not designed to be backwardly compatible with previous IMPS versions.

The 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. IMPS 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

No normative references.

2.2   Informative References

[CSP]	"Client-Server Protocol Session and Transactions Version 1.3", OMA-TS-IMPS-CSP-V1_3. Open Mobile Alliance™. URL:http://www.openmobilealliance.org/
[CSP DTD]	"Client-Server Protocol XML Syntax, OMA-TS-IMPS-CSP-XMLS-V1_3. Version 1.3". Open Mobile Alliance™. URL:http://www.openmobilealliance.org/
[CSP Trans]	"Client-Server Protocol Transport Bindings Version 1.3", OMA-TS-IMPS-CSP_Transport-V1_3. Open Mobile Alliance™. URL:http://www.openmobilealliance.org/
[CSP DataType]	"Client-Server Protocol Data Types Version 1.3", OMA-TS-IMPS-CSP_Data_Types-V1_3. Open Mobile Alliance™. URL:http://www.openmobilealliance.org/
[CSP SMS]	"Client-Server Protocol Plain Text Syntax Version 1.3", OMA-TS-IMPS-CSP_PTS-V1_3. Open Mobile Alliance™. URL:http://www.openmobilealliance.org/
[CSP WBXML]	" Client-Server Protocol Binary XML Definition and Examples 1.3", OMA-TS-IMPS-CSP_WBXML-V1_3. Open Mobile Alliance™. URL:http://www.openmobilealliance.org/
[IMPS RD]	OMA IMPS Delta Requirements, Version 1.3, OMA-RD_IMPSDelta-V1_3. Open Mobile Alliance™. URL:http://www.openmobilealliance.org/
[ISO-8859-1]	"Information Processing -- 8-bit single-byte coded graphic character sets -- Part 1: Latin alphabet No. 1", ISO 8859-1:1987.
[PA]	" Presence Attributes Version 1.3", OMA-TS-IMPS-PA-V1_3. Open Mobile Alliance™. URL:http://www.openmobilealliance.org/
[PA DTD]	" Presence Attributes XML Syntax Version 13", OMA-TS-IMPS-PA_XMLS-V1_3. Open Mobile Alliance™. URL:http://www.openmobilealliance.org/
[SSP]	" Server-Server Protocol Semantics Document Version 1.3", OMA-TS-IMPS-SSP-V1_3. Open Mobile Alliance™. URL:http://www.openmobilealliance.org/
[SSP Syntax]	" Server-Server Protocol XML Syntax Document Version 1.3", OMA-TS-IMPS-SSP_XMLS-V1_3. Open Mobile Alliance™. URL:http://www.openmobilealliance.org/
[SSP Trans]	" Server-Server Protocol Transport Binding Version 1.3", OMA-TS-IMPS-SSP_Transport-V1_3. Open Mobile Alliance™. URL:http://www.openmobilealliance.org/
[TS23.040]	3GPP, Technical realization of the Short Message Service (SMS);(Release 6), TS 23.040 V6.5.0 September 2004,URL: http://www.3gpp.org/ftp/Specs/html-info/23040.htm
[TS23.140]	3GPP, Technical realization of the Multimedia Messaging Service (MMS), Functional description, Stage 2, (Release 6), TS 23.140 V6.8.0 December 2004, URL: http://www.3gpp.org/ftp/Specs/html-info/23140.htm
[vCard 2.1]	"vCard - The Electronic Business Card", version 2.1,The Internet Mail Consortium (IMC), September 18, 1996, URL: http://www.imc.org/pdi/vcard-21.doc
[vCalendar 1.0]	"vCalendar - The Electronic Calendaring and Scheduling Format", version 1.0, The Internet Mail Consortium (IMC), September 18, 1996, URL: http://www.imc.org/pdi/vcal-10.doc

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

Publisher   The user that owns the presence information.

Subscriber   The user who requests to receiver the presence information of another user.

3.3 Abbreviations

CLI   Command Line Interface

CSP   Client Server Protocol

SSP   Server Server Protocol

IMPS   Instant Messaging and Presence Services

SMCNP   Server to Mobile Core Network Protocol

4. Introduction   (Informative)

The Instant Messaging and Presence Services (IMPS), intends to define and promote a set of universal specifications for mobile instant messaging and presence services. The specifications will be used for exchanging messages and presence information between mobile devices, mobile services and Internet-based instant messaging services, all fully interoperable and leveraging existing web technologies.

This document describes the architecture of the IMPS system. In Appendix A of this document, features and functionalitties of IMPS are described.

5. Architectural Model

This section and its subsections describe IMPS architecture and its relation to mobile networking and the Internet. The IMPS system is a client-server-based system, where the server is the IMPS server and clients can be either mobile terminals, or other services/applications, or fixed PC-clients.

5.1 Dependencies

This enabler has no dependencies on any other enablers.

5.2 Architectural Diagram

Figure 1 illustrates IMPS architecture. The functional entities are described in the next section.
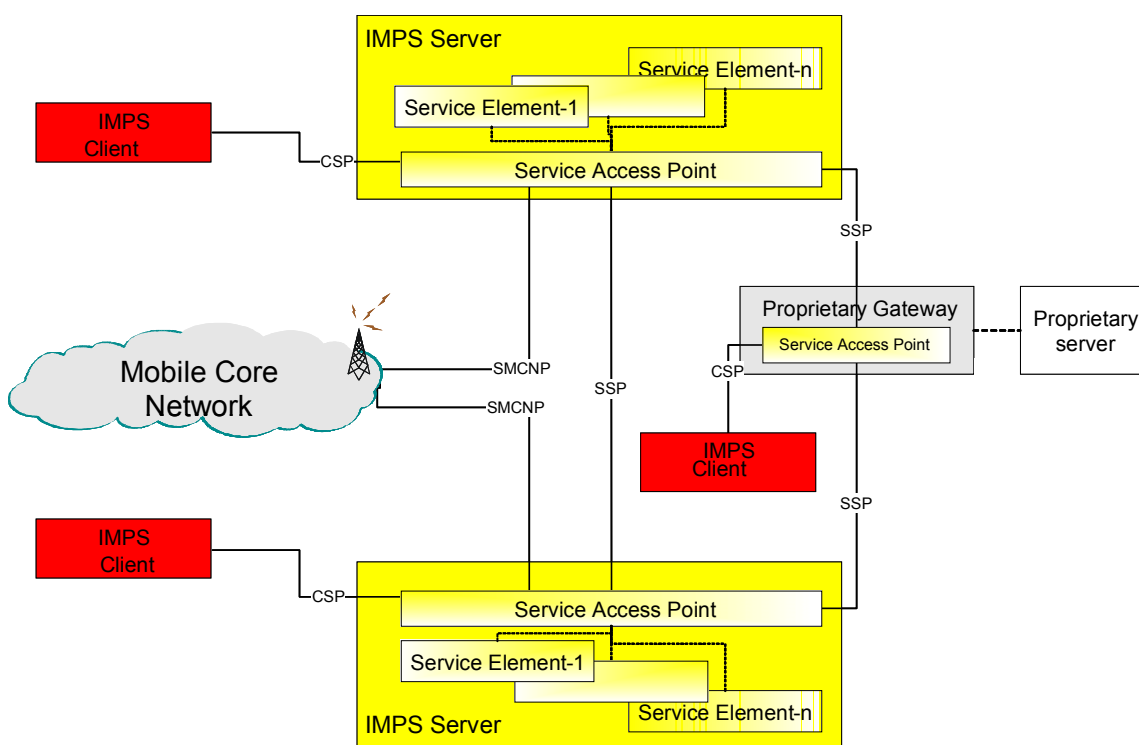
Figure 1: IMPS system architecture

"IMPS client" includes but is not limited to mobile hand-held and fixed terminals.

5.3 Functional Components and Interfaces

5.3.1 IMPS Server

The IMPS Server is the central point in an IMPS system, its functional elements are illustrated in Figure 2. It is composed of four Application Service Elements that are accessible via the Service Access Point. The Application Service Elements are:

- Presence Service Element

- Instant Messaging Service Element

- Group Service Element

- Content Service Element
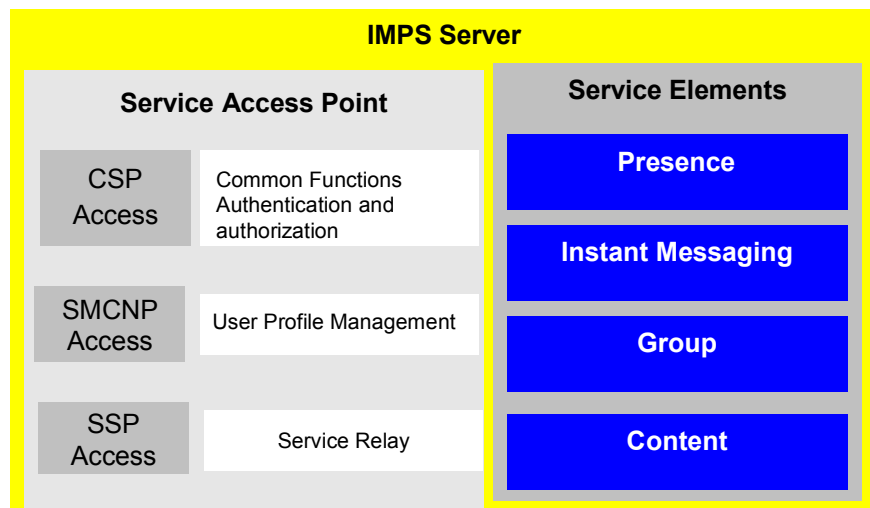
Figure 2: Functional Elements of IMPS Server

5.3.2   Presence Service Element

The Presence Service Element provides functionality for presence information management. This includes update, retrieve, set and store presence and location information. Presence information can be manipulated implicitly by the system, or explicitly by the user.

A user can subscribe to receive the presence information of other users, as specified in a contact list. Contact List Management is also a part of the presence service.

Presence information can be obtained from different internal and external sources. Through the Service Access Point (described below) the Presence Service Element can connect to the Mobile Core Network to access network presence and service information. Network presence defines the properties of the mobile devices, as well as the underlying network functionality. The Network service features define the properties related to the wireless devices on the wireless network, and determine the ability to communicate with a particular wireless device.

5.3.3   Instant Messaging Service Element

The Instant Messaging Service Element provides functionality for sending and receiving instant messages. An instant message may be sent to, or received from, a specific IMPS-user, or users of other instant messaging systems. It is also possible to send instant messages to a group of IMPS-users. IMPS supports several message types such as plain text, video, picture and sound.

5.3.4   Group Service Element

The Group Service Element provides functionality for use and management of groups. The groups can be private or public. A common usage of the Group Service is a chat room. It is also possible to bind content to the Groups.

5.3.5   Content Service Element

The Content Service Element provides functionality for sharing content such as images and documents between IMPS users. The shared content feature allows the IMPS users to share content while sending messages or chatting in a group. In this IMPS enabler, the shared content is realized by allowing a user to send a URL of the content he or she is willing to share. There are no mechanisms to upload or download content (see also section B.4 of Appendix B).

5.3.6   Service Access Point

The Service Access Point (SAP) serves as the interface between the IMPS server and its environment. It has interfaces to the IMPS clients, other IMPS servers, the Mobile Core Network and Proprietary Gateways to non-IMPS servers.

The functionality of the Service Access Point is:

- • Authentication and Authorization

- • Service Discovery and Service Agreement

- • User Profile Management

- • Service Relay

Some potentially useful functions, such as a service administration and monitoring interface, a provisioning interface, and a billing interface, etc., are subject to service deployment. Those functions are outside the scope of the standard and will not be addressed within IMPS specifications.

5.3.6.1   Authentication and Authorization

Authentication is used to verify the identity of an entity (user, network, or application). Authorization is the activity of determining what an authenticated entity (user, network, or application) is allowed to do.

There are several types of mechanisms for authentication and authorization:

- • Application-Network Authentication / Authorization.

- • User-Application Authentication / Authorization.

- • Application-Application Authentication / Authorization

- • User-Network Authentication (only for Authentication)

5.3.6.2   Service Discovery and Service Agreement

Service Discovery enables the application to identify the collection of service capability features that it can use. The service discovery process includes service capability registration and service capability notification. This is done both between Client – Server and Server –Server.

A **Service Agreement** (also known as a Service negotiation) must be established before the server can interact with the Network Service Capability or other servers' service capabilities, and provides the client with the services.

Upon successful agreement, the server may obtain information about the network capability and service capability features. The client may obtain the service capability features provided by the server. The services include the network services and IMPS services (presence service, IM service, group service and shared content service).

5.3.6.3   User Profile Management

One or more User Profile(s) describe(s) how the user wishes to manage and interact with their communication services (Figure 3). The User Profile information consists of various user interfaces and service related information including the list of services to which the end-user is subscribed, preferences associated with those services, service status (active / inactive), privacy status with regards to network service capabilities (e.g. user location, user interaction), terminal capabilities and terminal interface preferences etc.

User Profile Management allows the application to retrieve and update the user profile.
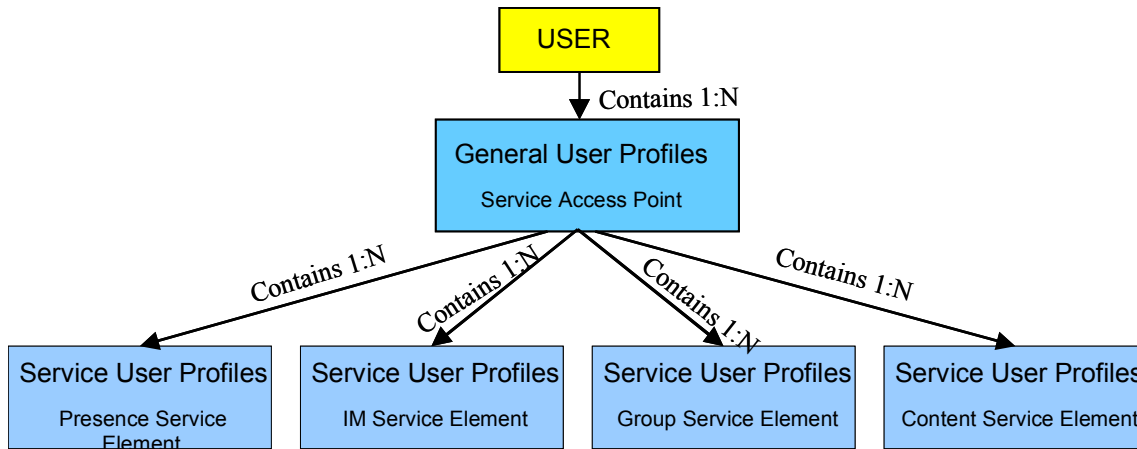
Figure 3: User Profiles

5.3.6.4   Service Relay

The Service Access Point must provide the Service Relay function to route all service requests and responses among the servers using the Server-to-Server Protocol (SSP). The Service Relay requires that the SAP performs CSP to SSP conversion and may have to transcode the contents of a service request and response.

5.3.7   IMPS Client

The IMPS client includes but is not limited to mobile hand-held and fixed terminals. IMPS clients will be interoperable with each other via SAP using the Client Server Protocol.

5.3.8   Interfaces and protocols

IMPS is a bearer-independent enabler, where different bindings can be defined between the IMPS-specific application protocols and other underlying protocols, as shown in Figure 4. CSP and SSP are the IMPS-specific application protocols.

CSP provides access for IMPS Clients within mobile and desktop terminals to the IMPS Server. CSP can use different transport bearers depending on the capability of the client. The transport-layer in IMPS can be supported via either HTTP or WSP/WTP, whereas secure transport can be provided using TLS, WTLS or IPSec protocols.

SSP connects IMPS servers. This can be used within one service provider domain or between different service providers. In this way the system will be interoperable so that a user that subscribes to IMPS services at Service Provider A can communicate with a user that is a customer of Service Provider B. The SSP is also used when connecting an IMPS server to Proprietary IMPS service via a Proprietary Gateway.

IMPS bearers for CSP include SMS, 2.5G/3G wireless IP or Mobile IP, but, when CSP is transported over SMS, other transport or security protocols are not needed. Instead a fixed IP connectivity is generally used as a bearer for SSP.

The Server to Mobile Core Network Protocol (SMCNP) is a reference point between the IMPS server and the underlying mobile networks. The SMCNP is implementation-dependent and not specified in this enabler.

Syntaxes:
PTS, XML, WBXML

Application layer (IMPS):
CSP, SSP

Transport layer:
HTTP, WSP/WTP

Security:
TLS, WTLS, IPSec

Bearers:
SMS, 2.5G/3G wireless IP, Mobile IP, fixed IP
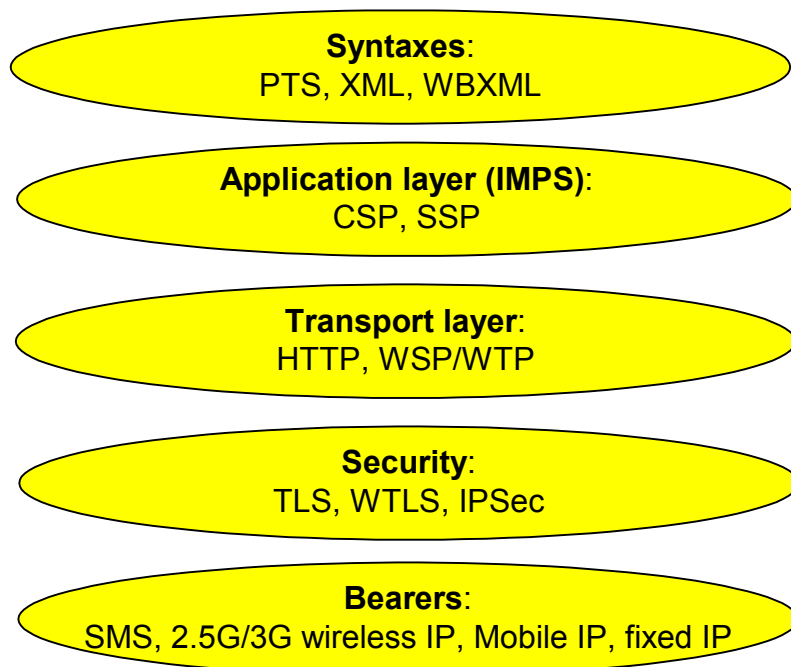
Figure 4: Interfaces and Protocols

Appendix A.   Change History   (Informative)

A.1   Approved Version History

Reference	Date	Description
n/a	n/a	No prior version

A.2   Draft/Candidate Version 1.3 History

Document Identifier	Date	Sections	Description
Draft version OMA-IMPS-Architecture-V1_3	28 Jan 2005		First draft, based on OMA-IMPS-WV-Arch-V1_2.
	21 Apr 2005		Working draft.
	25 Apr 2005		Version submitted for consistency review.
Draft versions OMA-AD-IMPS-V1_3	01 Jul 2005		Comments from consistency review incorporated.
	29 Jul 2005		Comments from consistency review incorporated.
Draft version OMA-AD-IMPS-Architecture-V1_3	29 Aug 2005		Version submitted for TP Candidate approval.
Candidate version OMA-AD-IMPS-V1_3	11 Oct 2005		Status changed to Candidate by TP TP ref # OMA-TP-2005-0279R01-IMPS-V1_3-for-Candidate-approval. Appendix A: Change History updated.

Appendix B.   IMPS Functions and Features   (Informative)

B.1   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.

B.1.1   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 IMPS specifications.

Client Status Attributes

The client status attributes describe the status of the running IMPS client software as well as the hardware device. They include presence attributes that describe the status of the IMPS 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.

User Status Attributes

The user status attributes describe the status of the body 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.

B.1.2   Contact List Feature

A *Contact List* is a user maintained list of IMPS users in the presence service element. In IMPS, 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.

B.1.3   Authorization of Presence Attributes

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

The authorization MAY be targeted to either individual users or to a group of users through a Contact List, or to the general public through the Default Attribute list. The actual attributes that are authorized MUST be defined in an attribute list.

B.1.4   Delivery of Presence Values

Subscribed Presence Feature

A user known as the subscriber is able to subscribe to the presence information of another user's known as the publisher. The subscriber, as long as he is authorized, will receive updated presence information when the presence information of the publisher is updated. The authorization granted by the publisher can expose the authorized subset of presence attributes. A subscriber can cancel the subscription to the presence information to stop the delivery of the publisher's presence information.

Get Presence Feature

A user is able to get another user's currently authorized subset of presence information upon request.This feature is used, for instance, when a user wants to occasionally check the status of another user.

Update Presence Feature

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

B.2   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.

B.2.1   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 IMPS 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 IMPS 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.

B.2.2   Offline Messaging

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

When an IMPS user sends a message and the other IMPS user is offline, the IMPS server implementation may support a store-and-forward functionality. If there is no such support in the IMPS server, the message is not delivered.

If the IMPS server supports a store-and-forward functionality, the messages are available in the IMPS server awaiting the login of the recipient. When the user logs in, the IMPS 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.

B.2.3   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.

B.2.4   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 IMPS specifications.

B.3   Group Feature

The concept of a user group means a chat room–type discussion forum formed either by a service provider or an individual IMPS 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 user 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 IMPS user name, or they may pick a suitable screen name when joining to the group to maintain anonymity.

B.3.1   Group Models

Private Group Model

A private group is a user group that is created by an individual IMPS 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.

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.

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 IMPS users, such as administrator or moderator.

B.3.2   Dynamic Group Features

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

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.

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.

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.

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.

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.

B.3.3   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.

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.

Delete group feature

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

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.

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.

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.

B.4 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.

B.5 Access Features

B.5.1 Login and Logout Feature

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

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

B.5.2 Service and Capability Feature

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

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

B.5.3 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 IMPS server that the IMPS client is still online and ready for communication.

B.5.4   Get Service Provider Information Feature

The get service provider information feature is used to retrieve information about the IMPS 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 IMPS services.

B.6   Common Features

B.6.1   General Search Feature

The general search feature is intended to enable users to search the information and users from the provided IMPS 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 IMPS user, or groups a particular user is currently joined to.

B.6.2   General Invitation Feature

The general invitation feature enables a IMPS user to invite some other user or user(s) to some IMPS 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 IMPS user may also cancel her previously sent invitation to indicate that she is no longer interested in continuing the indicated IMPS activities.

B.7   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.

IMPS 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 5. At the highest level, IMPS supports a complete set of IMPS services assembled from complementary IMPS services across service provider domains, as shown in 6. IMPSdefines 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, IMPS 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 5, 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 IMPS 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.
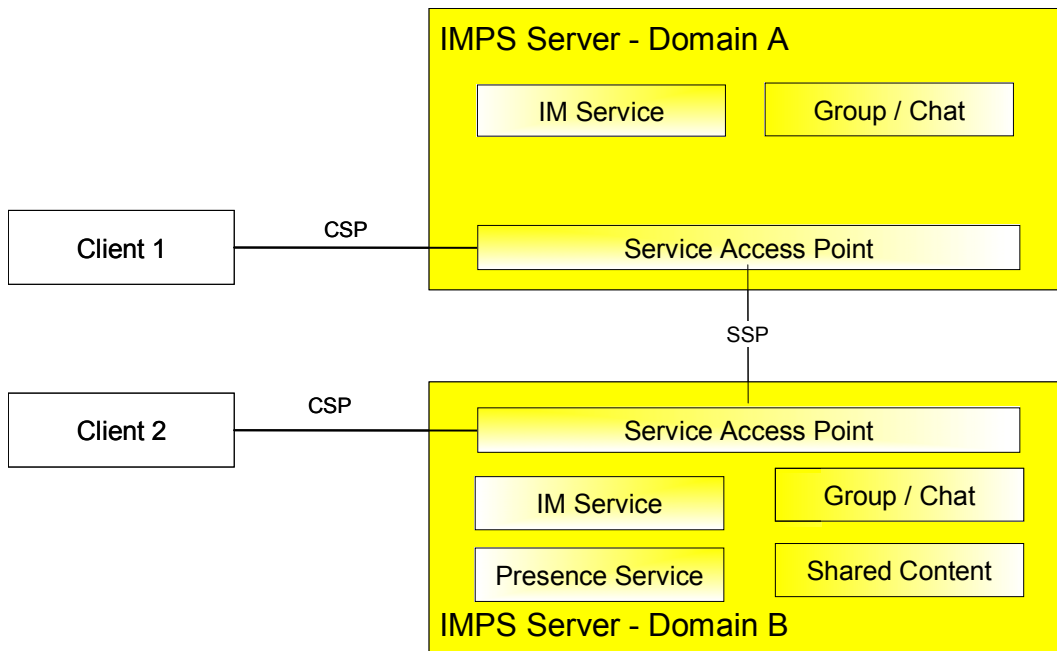
**Figure 5: The minimal interoperability.**

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 6, 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 IMPS interoperability model allows client 1 and 2 to use the complete set of features and interact with each other via the SSP.
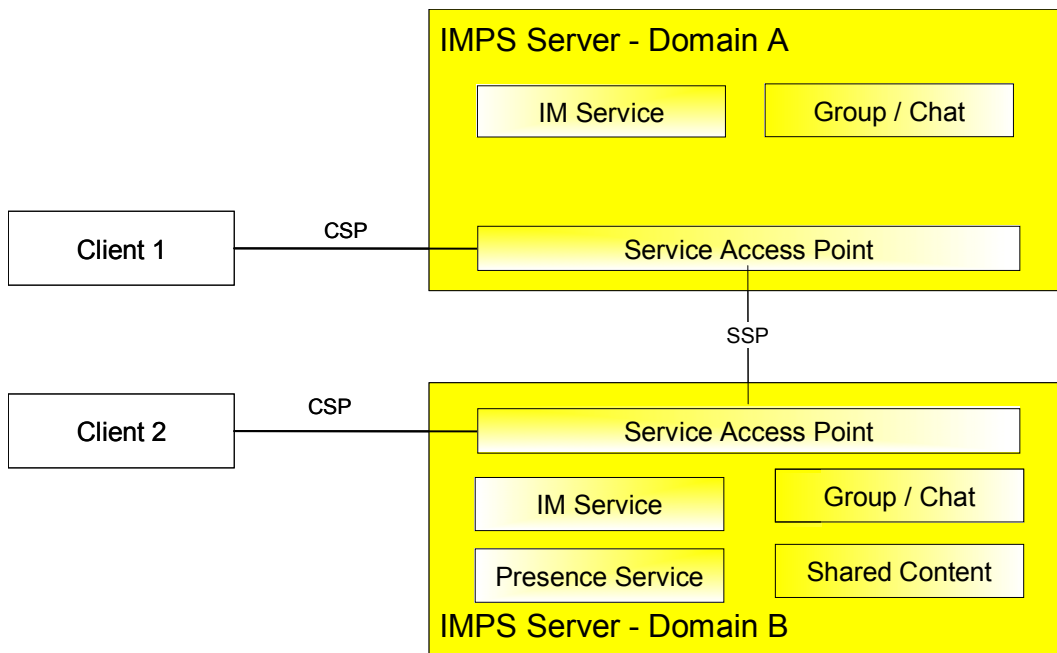
Figure 6: Complementary services

In IMPS Interoperability, the Home Domains must have a direct SSP connection to interoperate with each other. However, IMPS 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 7, 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.
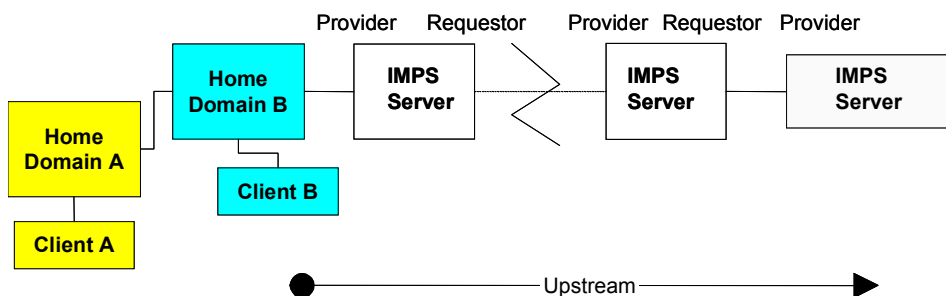
Figure 7: The SSP Service Relay

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 service request from the client to the SSP service request, and/or map the SSP service result of the CSP service result to the client.

B.7.1   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 IMPS. Whenever possible the service providers have to ensure that current security approaches in the underlying layers shall be used to secure those layers.

B.7.2   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.

B.7.3   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.

B.7.4   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.

Service Discovery

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

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.

B.7.5   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

B.7.6   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.

B.8 New IMPS 1.3 features

The new IMPS 1.3 features are described in details in [IMPS RD].

- Segmentation for clients with limited memory

- Addition of a contact by IMPS User ID

- Addition of a contact by MSISDN

- Search By Contact Details

- Send when a user is not on another user contact list

- Send an offline instant message

- Extend IM to private group conversation

- Participate in private group conversation

- Add/Update public profile

- Search by public profile

- Locate friend and show map

- Auto-Registration

- Auto Login

- System Message

- Advanced search

- Multiple applications / sessions

- Remote user session management

- Sending an announcement in a chatting

- Original name of multimedia message in IM