WV-052 SSP – Server-Server Protocol Semantics Document

Candidate Version 1.2 – 22 May 2004

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

Continues the Technical Activities
Originated in the Wireless Village Initiative

Contents

1. Scope

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

- Presence
- Instant Messaging
- Groups
- Shared Content

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

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

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

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

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

2. References

2.1 Normative References

[CREQ] "Specification of WAP Conformance Requirements". Open Mobile Alliance™. WAP-221-CREQ. URL:http://www1.wapforum.org/tech/terms.asp?doc=WAP-221-CREQ-20010425-a.pdf

[CSP SCR] "WV-048 Client-Server Protocol Static Conformance Requirement Version 1.2". Open Mobile Alliance. URL:http://www.openmobilealliance.org/release_program/enabler_releases.html

[FIPS 180-1] "Secure Hash Standard", April 1995 URL:http://csrc.nist.gov/publications/fips/fips180-1/fip180-1.pdf

[IMPP-CPIM] A Common Profile for Instant Messaging (CPIM), Internet Draft, August 2002. URL:http://www.ietf.org/internet-drafts/draft-ietf-impp-cpim-03.txt

[E.164] ITU-T Recommendation E.164 (05/97) The international Public Telecommunication Numbering Plan. URL:http://www.itu.int/rec/recommendation.asp?type=items&lang=e&parent=T-REC-E.164-199705-I

[RFC1321] "The MD5 Message-Digest Algorithm", April 1992. URL:http://www.ietf.org/rfc/rfc1321.txt?number=1321

[RFC2045] Multipurpose Internet Mail Extensions (MIME) Part one: Format of Internet Message Bodies. Section 6.8 "Base64 Content-Transfer-Encoding", November 1996. URL:http://www.ietf.org/rfc/rfc2045.txt?number=2045

[RFC2046] Borenstein N., and N. Freed, "MIME (Multipurpose Internet Mail Extensions) Part Two: Media Types", November 1996. URL:http://www.ietf.org/rfc/rfc2046.txt?number=2046

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

[RFC2234] "Augmented BNF for Syntax Specifications: ABNF". D. Crocker, Ed., P. Overell. November 1997. URL:http://www.ietf.org/rfc/rfc2234.txt

[RFC822] "Standard for the Format of ARPA Internet Text Messages".August 1982. URL:http://www.ietf.org/rfc/rfc0822.txt?number=822

[SSP SCR] "WV-055 SSP – Server-Server Protocol Static Conformance Requirement Version 1.2". Open Mobile Alliance. URL:http://www.openmobilealliance.org/release_program/enabler_releases.html

[XML] "Extensible Markup Language 1.0 (Second Edition)", W3C recommendation, October 2000. URL:http://www.w3.org/TR/2000/REC-xml-20001006.pdf

2.2 Informative References

[Arch] "WV-040 System Architecture Model Version 1.2". Open Mobile Alliance. *URL:http://www.openmobilealliance.org/release_program/enabler_releases.html*

[FeaFun] "WV-041 Features and Functions Version 1.2". Open Mobile Alliance. *URL:http://www.openmobilealliance.org/release_program/enabler_releases.html*

[CSP] "WV-042 Client-Server Protocol Session and Transactions Version 1.2". Open Mobile Alliance. *URL:http://www.openmobilealliance.org/release_program/enabler_releases.html*

[CSP DTD] "WV-043 Client-Server Protocol DTD and Examples Version 1.2". Open Mobile Alliance. *URL:http://www.openmobilealliance.org/release_program/enabler_releases.html*

[CSP Trans] "WV-044 Client-Server Protocol Transport Bindings Version 1.2". Open Mobile Alliance. *URL:http://www.openmobilealliance.org/release_program/enabler_releases.html*

[CSP DataType] "WV-045 Client-Server Protocol Data Types Version 1.2". Open Mobile Alliance. *URL:http://www.openmobilealliance.org/release_program/enabler_releases.html*

[CSP SMS] "WV-046 Client-Server Protocol SMS Binding Version 1.2". Open Mobile Alliance. *URL:http://www.openmobilealliance.org/release_program/enabler_releases.html*

[CSP WBXML] "WV-047 Client-Server Protocol Binary Definition and Examples Version 1.2". Open Mobile Alliance. *URL:http://www.openmobilealliance.org/release_program/enabler_releases.html*

[CSP SCR] "WV-048 Client-Server Protocol Static Conformance Requirement Version 1.2". Open Mobile Alliance. *URL:http://www.openmobilealliance.org/release_program/enabler_releases.html*

[PA] "WV-049 Presence Attributes Version 1.2". Open Mobile Alliance. *URL:http://www.openmobilealliance.org/release_program/enabler_releases.html*

[PA DTD] "WV-050 Presence Attribute DTD and Examples Version 1.2". Open Mobile Alliance. *URL:http://www.openmobilealliance.org/release_program/enabler_releases.html*

[CLP] "WV-051 Command Line Protocol Version 1.2". Open Mobile Alliance. *URL:http://www.openmobilealliance.org/release_program/enabler_releases.html*

[SSP] "WV-052 SSP - Server-Server Protocol Semantics Document Version 1.2". Open Mobile Alliance. *URL:http://www.openmobilealliance.org/release_program/enabler_releases.html*

[SSP Syntax] "WV-053 Server-Server Protocol XML Syntax Document Version 1.2". Open Mobile Alliance. *URL:http://www.openmobilealliance.org/release_program/enabler_releases.html*

[SSP Trans] "WV-054 SSP - Transport Binding Version 1.2". Open Mobile Alliance. *URL:http://www.openmobilealliance.org/release_program/enabler_releases.html*

[SSP SCR] "WV-055 SSP – Server-Server Protocol Static Conformance Requirement Version 1.2". Open Mobile Alliance. *URL:http://www.openmobilealliance.org/release_program/enabler_releases.html*

[WAPARCH] "WAP Architecture, Version 12-July-2001". Open Mobile Alliance™. WAP-210-WAPArch. *URL:http://www1.wapforum.org/tech/terms.asp?doc=WAP-210-WAPArch-20010712-a.pdf*

3. Terminology and Conventions

3.1 Conventions

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in [RFC2119].

All sections and appendixes, except “Scope” and “Introduction”, are normative, unless they are explicitly indicated to be informative.

3.2 Definitions

The following definitions are for terms specific to the Wireless Village and general terms that may have some special context within the documentation. These definitions are provided to enhance the use of this documentation.

Home Domain	refers to the home IMPS system, which the user subscribes to, and in which the user is authenticated and authorized to use IMPS services
Primary Service Element	refers to a Service Element of an IMPS service for a client. A PSE may be in the Home Domain of the client, or in the other domain.
Complementary Service	refers to a situation in which the Primary Service Element (PSE) is NOT in the Home Domain. Instead, the PSE is in another domain.
Provider Server	the WV server, which provides the services for the Requestor Server in the frame of a session after the successful service agreement is negotiated.
Requestor Server	the WV server, which requests the services from the Provider Server in the frame of a session after the successful service agreement is negotiated.
Service Request	it is initiated from the Requestor Server to the Provider Server
Service Notification	it is initiated from the Provider Server to the Requestor Server

The terms MAY, SHOULD, MUST are consistent with the definitions in RFC 2119.

3.3 Abbreviations

ARPA	Advanced Research Projects Agency
	An agency of the United States Department of Defense, ARPA underwrote the development of the Internet beginning in 1969. A precursor to IETF.
DTD	Document Type Definition
HTTP	Hypertext Transfer Protocol
IANA	Internet Assigned Number Authority
IETF	Internet Engineering Task Force
	A society of engineers and developers dedicated to designing and advancing standards for internet use.
WAP	Wireless Application Protocol
	A specification for a set of communication protocols to standardize the way that wireless devices, such as cellular telephones and radio transceivers, can be used for Internet access

4. Introduction

The Wireless Village (WV) Server-Server Protocol (SSP) provides the communication and interaction means between different IMPS service domains. SSP allows the WV clients to subscribe to the IMPS services provided by different service providers that are distributed across the network. SSP allows the WV clients to communicate with existing proprietary Instant Messaging networks through the Proprietary Gateway. The interoperability between different devices and service providers is achieved in a way that user #1 that subscribes to Wireless Village services at Service Provider A can communicate with user #2 that is a client of Service Provider B. The goal of SSP is to support the distributed interoperable complementary IMPS services across service provider domains.

5. Server-Server Protocol

5.1 SSP Interoperability Model

The term "Home Domain" is the domain 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 be in a remote domain.

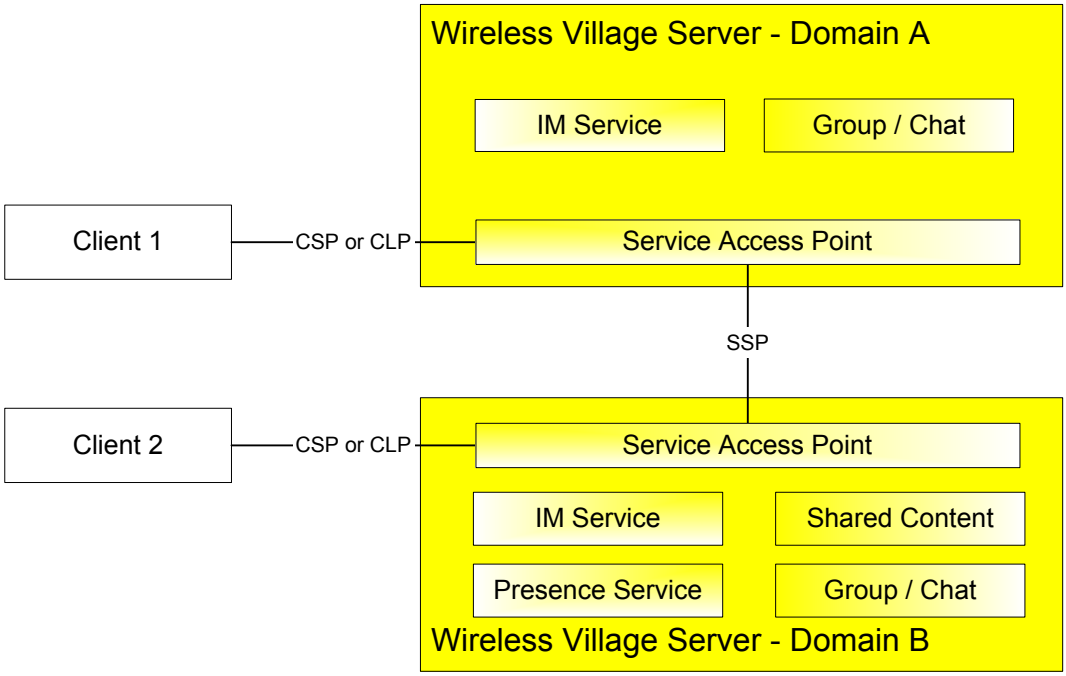

Figure 1. The SSP Minimum Interoperability Model

SSP 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 1. At the highest level, SSP supports a complete set of IMPS services that are assembled from complementary IMPS services across service provider domains, as shown in Figure 2. SSP defines the rules for the PSE to take appropriate actions to achieve the interoperability and provide distributed IMPS services.

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

In the example in Figure 1, 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 in SSP.

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.

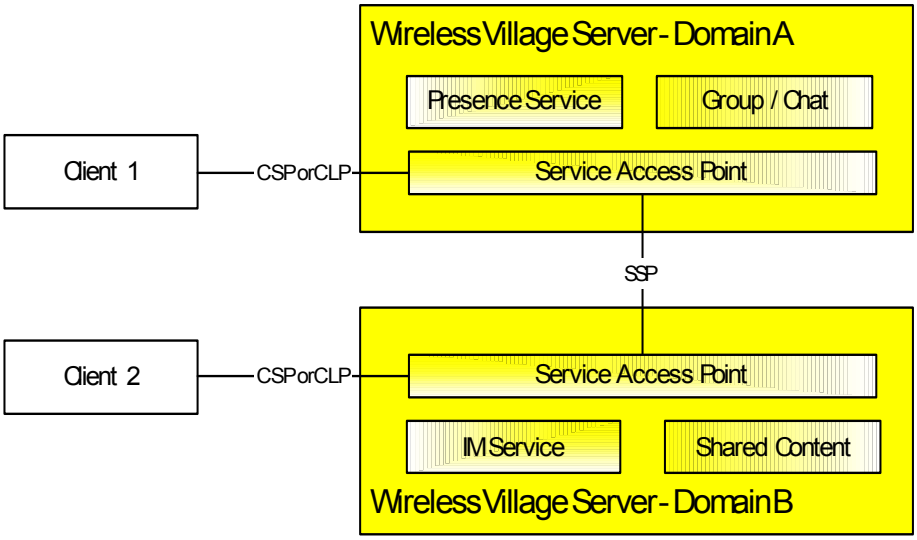

Figure 2. The SSP Full Interoperability Model

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 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.

In SSP Interoperability, the Home Domains must have direct SSP connection to interoperate with each other. However, SSP 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 3, 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 as the "logical" Service Provider role for each downstream domain, and act as the "logical" Service Requestor role for each upstream domain.

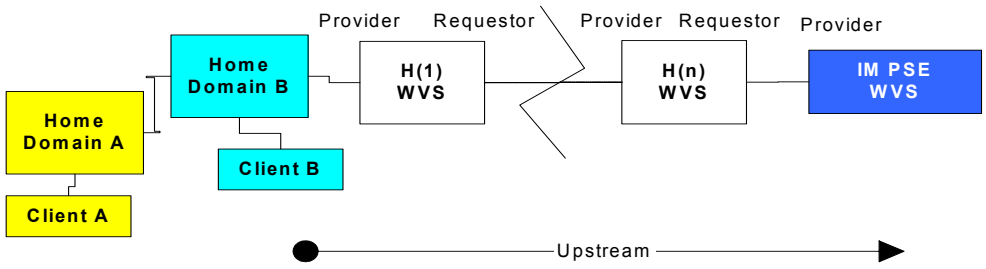

Figure 3. The SSP Service Relay

At each Wireless Village server, the Service Access Point (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 a 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.

5.2 SSP Interoperability Rules

In SSP Interoperability, the Home Domains must have direct SSP connections to interoperate with each other. However, SSP supports the routing of "Service Relay" between the Home Domain and the PSE. The basic IOP rules are:

Rule 1: At the Home Domain, each user-initiated service request and the relayed service request from another Home Domain shall be routed / relayed from this Home Domain to its PSE for the first and primary processing. PSE is the primary and default service element to provide the user with the service.

Rule 2: If PSE needs more information from another SE in another Home Domain, but the service agreement between them does not support such information exchange, the PSE shall relay the service request to that Home Domain for further processing. Before a service request is relayed to a SE in another Home Domain, all information elements of local scope must be replaced with those of global scope. For example, a local User-ID is replaced with a global User-ID. Moreover, if the information element is a reference to a local object, it must be replaced by the actual information, e.g. a reference to a Contact-List must be replaced by a list of global User-ID's.

Rule 3: At the PSE, each PSE-initiated transaction shall be routed / relayed from the PSE back to its Home Domain, from which the PSE-initiated transaction is triggered (by the user-initiated or relayed service request). The PSE-initiated transaction shall be next relayed from the Home Domain to the destination Home Domain via the direct SSP connection between them (e.g. Figure 7 in section 5.4.4). If two Home Domains provide each other with the complementary PSE, the direct routing / relay is allowed from the complementary PSE to the destination domain (e.g. Figure 6 in section 5.4.3).

An intermediate domain shall route / relay the service request to the PSE and from the PSE based on its service agreement. A routing table is allowed in the intermediate domain. The routing table shall be offline configured based on the service agreement. If the routing table is used in PSE, it shall override the routing Rule 3 (e.g. Figure 8 in section 5.4.6).

5.3 SSP Service Agreement and Routing

The exchange of messages between Wireless Village domains is normally performed in one hop over an established direct SSP connection. However, Wireless Village does support routing of messages between the Home Domain and the PSE. The SSP routing between domains is based on the SSP IOP rules and the business agreements between the domains. The business agreements must be established among all domains that are involved in the handling of SSP service relays between two end points.

After the business agreements are made between the domains, each domain shall be able to route and relay the services between the domains along the path. The routing table is created based on the business and service agreement.

In conclusion, the SSP IOP routing is defined by offline business agreements and service agreements that contains routing agreements and configuration. Each Wireless Village Server (WVS) holds a static list of direct connected neighbors. The list specifies the agreed domains that may be forwarded to one of the direct connected WVS's.

5.4 SSP Interoperability Case Study

There are different situations in SSP interoperability. This section illustrates different interoperability models and the transaction flows based on the IOP rules described in 5.2.

5.4.1 Case 1 – Two Users are Located in different Home Domains. Each Home Domain has its own SE. Two Home Domains are Connected

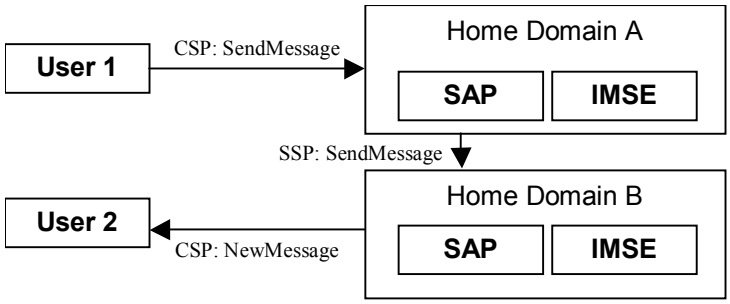

Figure 4. The SSP IOP Case One

In the example in Figure 4, client 1 is located in home domain A, and client 2 is located in home domain B. A's IM PSE is located in Domain A, and B's PSE is located in Domain B. This is the minimal interoperability case. The transaction flow of sending a message from client 1 to client 2 is:

1. C1 -> DA: CSP-SendMessage
2. DA -> DB: SSP-SendMessage
3. DB -> C2, SSP-NewMessage (after checking block list etc.)

5.4.2 Case 2 – Two Users are Located in the same Home Domain

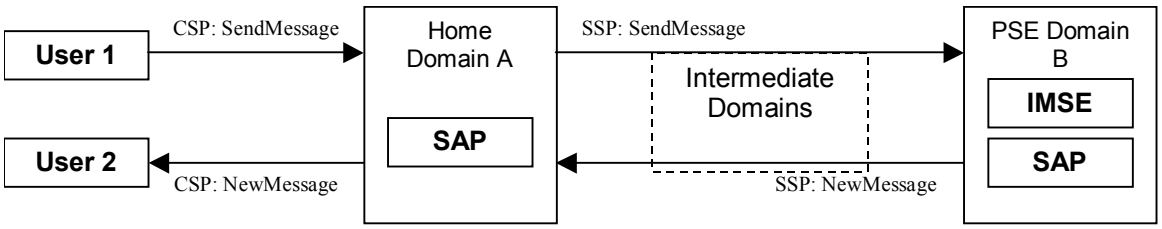

Figure 5. The SSP IOP Case Two

In the example in Figure 5, both client 1 and 2 are located in home domain A. The IM PSE is located in Domain B. Domain A and B are connected via some intermediate domains. The transaction flow of sending a message from client 1 to client2 is:

1. C1 -> DA: CSP-SendMessage
2. DA -> DB: SSP-SendMessage (through intermediate domains via routing)
3. DB -> DA, SSP-NewMessage (after checking block list etc.)
4. DA -> C2, CSP-NewMessage

If Domain A and Domain B are directly connected, there will be one SSP-SendMessage from A to B, and one SSP-NewMessage from B to A.

If Domain A and Domain B are connected through several intermediate domains, there will be several SSP-SendMessages from A to B, one for each hop. Each intermediate domain will relay the SSP-SendMessage to the next hop. There will also be several SSP-NewMessages from B to A, one for each hop. Each intermediate domain will forward the SSP-NewMessage to the next hop.

5.4.3 Case 3 – Domain A and C have Direct SSP Connection while Domain C Provides A with Complementary PSE

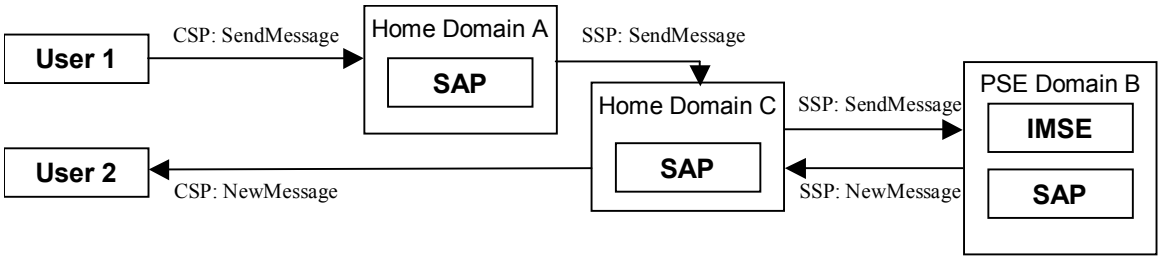

Figure 6. The SSP IOP Case Three

In the example in Figure 6, Domain A and C have a direct SSP connection, and Domain C provides A with complementary IM PSE in Domain B. The transaction flow of sending a message from client 1 to client 2 is:

1. C1 -> DA: CSP-SendMessage
2. DA -> DC: SSP-SendMessage
3. DC -> DB: SSP-SendMessage (through intermediate domains via routing)
4. DB -> DC, SSP-NewMessage (after checking block list etc.)
5. DC -> C2, CSP-NewMessage

5.4.4 Case 4 – Two Users are Located in different Home Domains. Each Home Domain has its complementary PSE. Two Home Domains are Connected

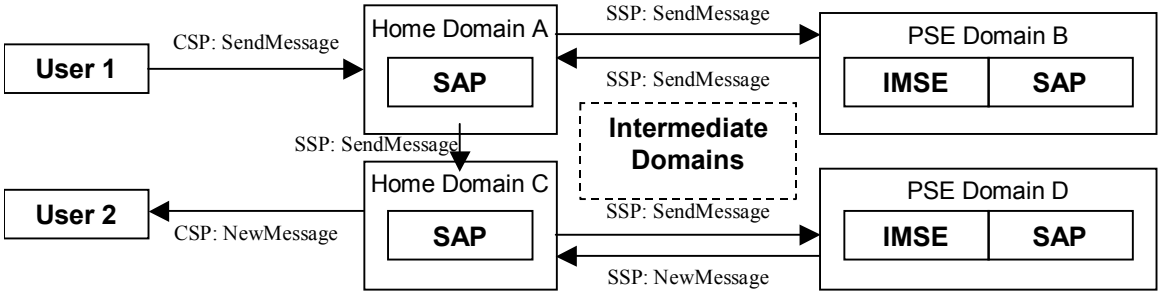

Figure 7. The SSP IOP Case Four

In the example in Figure 7, client 1 is located in home domain A, and client 2 is located in home domain C. A's IM PSE is located in Domain B, and C's PSE is located in Domain D. Home domain A and home domain C are connected via some intermediate domains. The transaction flow of sending a message from client 1 to client 2 is:

1. C1 -> DA: CSP-SendMessage
2. DA -> DB: SSP-SendMessage (through intermediate domains via routing)
3. DB -> DA: SSP-SendMessage (through intermediate domains via routing)
4. DA -> DC: SSP-SendMessage
5. DC -> DD: SSP-SendMessage (through intermediate domains via routing)
6. DD -> DC, SSP-NewMessage (after checking block list etc.)
7. DC -> C2, CSP-NewMessage

5.4.5 Special Case Processing

The special cases include the situations in which offline agreement overrides the IOP Rule 3. The following example illustrates the processing for this type of special case.

5.4.6 Two Users are Located in different Home Domains. Both Home Domains Share the same PSE

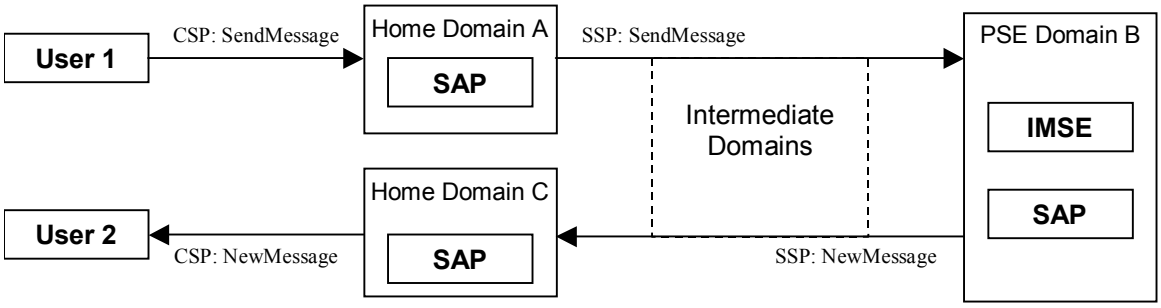

Figure 8. The SSP IOP Special Case

In the example in Figure 8, client 1 is located in home domain A, client 2 is located in home domain C. Both Domain A and Domain C share the IM PSE located in Domain B. Domain A and B are connected via some intermediate domains. Domain C and B are connected via some intermediate domains. The transaction flow of sending a message from client 1 to client2 is:

6. C1 -> DA: CSP-SendMessage
7. DA -> DB: SSP-SendMessage (through intermediate domains via routing)
8. DB -> DC, SSP-NewMessage (after checking block list etc.)
9. DC -> C2, CSP-NewMessage

Note that the transaction flow is based on the offline configuration in PSE Domain B, which allows the direct relay from A to B to C without the direct SSP connection between Home Domain A and C based on their off-line routing agreement. IOP Rule 3 does not apply to this case.

If Domain A and Domain B are directly connected, there will be one SSP-SendMessage from A to B. If Domain A and Domain B are connected through several intermediate domains, there will be several SSP-SendMessages from A to B, one for each hop. Each intermediate domain will relay the SSP-SendMessage to the next hop.

If Domain C and Domain B are directly connected, there will be one SSP-NewMessage from B to C. If Domain C and Domain B are connected through several intermediate domains, there will be several SSP-NewMessages from B to C, one for each hop. Each intermediate domain will forward the SSP-NewMessage to the next hop.

5.5 SSP Protocol Stack

The SSP protocol stack is divided into three layers as follows.

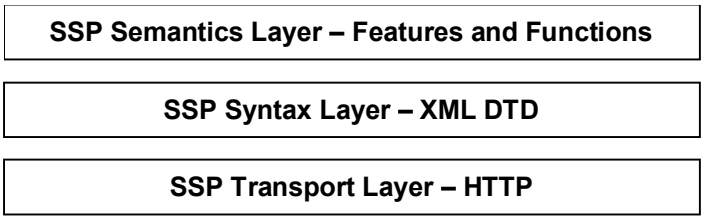

Figure 9. The SSP Protocol Stack

SSP Semantics Layer defines the complete set of features and functions that SSP intends to address in the full interoperability model among the WV domains. The nature of the features and functions, i.e. mandatory or optional or conditional, is also defined in the SSP Semantics Layer. The details of the features and functions are described in the transactions, primitives and information elements in the SSP Semantics Layer.

SSP Syntax Layer defines the "communication language" for the WV SAP's to understand the information between each other and accomplish the interoperability of the features and functions defined in SSP Semantics Layer. SSP Syntax Layer is the set of XML DTD specification.

SSP Transport Layer defines the "communication method" that conveys the "communication language" between the WV SAP's to achieve the interoperability. SSP Transport Layer v1.0 is HTTP.

This document describes the SSP Semantics Layer.

The term "Server" in this document represents the logical server cluster in one service provider domain. The term "Server" is interpreted as the single access point of the domain, 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.

6. Protocol Introduction

SSP is based on the architecture model described in the *"System Architecture Model"* document [Arch] and focuses on the communication and interaction among the WV domains. The semantics of SSP is consistent with the functional description of the Service Access Point (SAP) in the architecture model. The semantics of SSP implements the server interoperability described in the "*Features and Functions*" document [FeaFun]. The semantics of SSP supports the semantics of Client to Server Protocol (CSP) [CSP] in a distributed environment to achieve full interoperability.

6.1 Basics

6.1.1 Session

The server interoperability is accomplished in the frame of two SSP sessions. An SSP session is the period during which the servers conduct interactions and interoperations for the Service Provider to provide the Service Requestor with the negotiated IMPS services.

Each Provider Server maintains one session for each Requestor Server. There are two sessions between two domains. Each server maintains one session to provide the other with its own negotiated IMPS services.

6.1.2 Transaction

The SSP semantics are accomplished by "transactions". An SSP transaction is the sequence of interactions to complete a specific SSP feature or function. The SSP transactions include one-way transactions, two-way transactions, and multi-way transactions. A one-way transaction consists of a service request. A two-way transaction consists of a service request and a service response. A multi-way transaction consists of a sequence of service requests and responses.

6.1.3 Message

Both service requests and service responses are called SSP "messages". An SSP message is the syntax unit in one interaction.

An SSP message must contain some meta-information including the protocol information (e.g. version), the session information (e.g. Session-ID), the transaction information (e.g. Transaction-ID) and the attribute information (e.g. one-way / two-way, request / response). The "response" message in a two-way transaction must contain the same Transaction-ID as the corresponding "request" message. All transactions during one session must contain the same Session-ID.

6.1.4 Primitive

Each SSP message includes one or more SSP "primitives" with appropriate parameters. An SSP primitive is the semantics unit in one message.

Each service request message contains one functional primitive. Each service response message includes a status primitive as well as the optional, one or more SSP primitive(s).

6.2 Session Pair vs. Connections

There are two sessions between two domains. Each domain maintains one session to provide the other with its own negotiated IMPS services. The two sessions are established through session establishment.

There are at least two physical connections, namely the connection pair, to carry the service traffic of the session pair. The servers may establish more than one connection pair to support the same session pair.

The physical connection carries the service requests from the Requestor server to the Provider Server in one direction, and / or the notifications from the Provider Server to the Requestor Server in the other direction.

Connections are reusable. Each session may use some or all of the connections to transport its transactions. Each connection may be used by only one session, or reused by both sessions.

An SSP transaction (request and response) must be completed using the same connection pair.

Please refer to the SSP Transport Binding Document [SSP Trans] about how the connection (pair) is bound to the underlying transport.

6.3 Addressing

SSP addressing schema uses the uniform Wireless Village addressing model in a unique Wireless Village address space. SSP addressing schema is consistent with that in CSP.

The definition of SSP address is based on the URI [RFC2396]. The addressable entities are:

- User
- Contact List
- Group (public and private)
- Content (public and private)
- Message
- Service (SSP unique)

The other address spaces may be used to interoperate with other systems. The use of other address spaces is up to the implementation and out of scope of Wireless Village.

6.3.1 General SSP Addressing Schema

The general SSP addressing schema is based on URI [RFC2396]. The "wv" schema in the URI indicates the Wireless Village address space. The generic syntax is defined as follows:

```
WV-Address          = Service-ID | Message-ID | Other-Address
Other-Address       = ["wv:"] [User-ID] ["/" Resource] "@" Domain
Global-User-ID      = User-ID "@" Domain
Resource            = Group-ID | Contact-List-ID | Content-ID
Domain              = sub-domain *("." sub-domain)
```

where User-ID refers to the identification of the Wireless Village user inside the domain. Domain is a set of the Wireless Village entities that have the same "Domain" part in their Wireless Village addresses. Domain identifies the point of the Wireless Village server domain to which the IMPS service requests must be delivered if the requests refer to this domain. Resource further identifies the public or private resource within the domain. The sub-domain is defined in [RFC822]. The Service-ID is globally unique to identify a Server (either a WV server or a Proprietary Gateway), which is defined in section 6.3.7.

When the Global-User-ID is present without the Resource, the address refers to the user. In SSP, the user is always identified in the global scope.

When the Global-User-ID is present with Resource, the address refers to the private resource of the user. When the User-ID is not present, the Domain and the Resource must always be present, and then the address refers to a public resource within the domain.

The domain must always be present in SSP addressing to globally identify the user or resources, and used for address resolution of those network entities.

The schema part is optional. When it is not present, the default schema "wv:" is assumed.

The addresses are case insensitive.

6.3.2 Address encoding

As per URI [RFC2396], certain reserved characters must be escaped if they occur within the User-ID, Resource, or Domain portions of a Wireless Village address. This includes the characters ";", "?", ":", "&", "=", "+", "$" and ",". For example, a valid Wireless Village address for the user "$mith" in the "server.com" domain is:

```
wv:%24mith@server.com
```

Certain characters are not permitted to occur in the User-ID portion of Wireless Village addresses (see 6.3.3 below). This includes the characters "/", "@", "+", " " and TAB. This restriction is independent of the encoding of a User-ID within a Wireless Village address. For example, this Wireless Village address is not permissible:

```
wv:john%40aol.com@server.com
```

This address is not permissible because after URI-decoding, the User-ID portion contains a forbidden character ("@"). If a server's internal representation of a username permits the occurrence of forbidden characters, such characters must be double-escaped when they occur in a Wireless Village address, such that they do not occur unescaped in the User-ID portion after URI-decoding, or they must be escaped via some other scheme that does not employ forbidden characters.

6.3.3 User Addressing and Global-User-ID

SSP uses User-ID's to uniquely identify a WV User. The User-ID refers to either the Internet-type address or to a mobile number of the user. If it refers to the mobile number of the user, the user name always starts either with digit or with '+' sign. User name referring to Internet-type address may not start with '+' sign or digit.

The syntax of the User-ID is defined as follows:

```
User-ID                = Mobile-Identity | Internet-Identity
Internet-Identity      = *alpha
Mobile-Identity        = (digit | "+") *digit
digit                  = "0" | "1" | "2" |"3" |"4" |"5" |"6" |"7" |"8" | "9"
alpha                  = Any non-control ASCII character (decimal 32 - 126,
                         inclusive) except specials
specials               = "/" | "@" | "+" | " " | TAB
```

When the User-ID refers to the mobile number address, the User-ID preceded with a '+' sign refers to the international numbering in The International Public Telecommunication Numbering Plan [E.164]. Without a '+' sign, it refers to the national numbering in the [E.164].

Examples of the User-ID's are:

Local-User-ID: wv:Jon.Smith

```
wv:+358503655121
wv:0503655121
```

Global-User-ID: wv:Jon.Smith@imps.com

```
wv:+358503655121@imps.com
wv:0503655121@imps.com
```

SSP always uses Global-User-ID to identify the users.

The users may also be identified by screen names, nicknames and aliases. These identifiers explicitly and implicitly refer to the User-ID.

ScreenName – the combination of a name a user chooses in a group session, and the Group-ID itself. The user may have different ScreenNames on different occasions as well as on different groups. The ScreenName is always connected to a group.

NickName – A name that is used internally in a client to hide the UserID of contacts. When ContactList is stored on the server, the NickName must have a space, but it is not possible to address a NickName.

Alias – The name a user suggest others to use as NickName. Part of the User Presence.

The definition of User-ID in SSP is consistent with that in CSP.

6.3.4 Contact List Addressing and Contact-List-ID

SSP uses Contact-List-ID's to uniquely identify any contact list of any user. The syntax of Contact-List-ID is defined as follows:

```
Contact-List-ID = *alpha
```

Examples of the contact list address with Contact-List-ID are:

```
wv:john/colleagues@imps.com
wv:/managers@imps.com
```

SSP always identifies the contact list globally.

The definition of Contact-List-ID in SSP is consistent with that in CSP.

6.3.5 Group Addressing and Group-ID

SSP uses Group-ID's to uniquely identify any group. The syntax of the Group-ID is defined as follows:

```
Group-ID = *alpha
```

Examples of the group address with Group-ID are:

```
wv:john/mygroup@imps.com
wv:/technical_forum@imps.com
```

SSP always identifies the group globally.

The definition of Group-ID in SSP is consistent with that in CSP.

6.3.6 Content Addressing and Content-ID

SSP uses Content-ID's to uniquely identify any content. The syntax of the Content-ID is defined as follows:

```
Content-ID = *alpha
```

Examples of the content address with the Content-ID are:

```
wv:john/WV_presentation@imps.com
wv:/wvspec@imps.com
```

SSP always identifies the content globally.

The definition of Content-ID in SSP is consistent with that in CSP.

6.3.7 Client Addressing and Client-ID

The Client-ID uniquely identifies the WV client as an application as well as its addressing that allows the access to the WV services. The client-ID is intended to allow:

- Multiple accesses from the same user
- Direct application-to-application communication

The Client-ID consists of

- Optional application identifier such as a URL identifying the application and its addressing,
- Optional mobile device identity (such as international mobile number [E.164]).

The definition of Client-ID in SSP is consistent with that in CSP.

6.3.8 Service Addressing and Service-ID

The Service-ID in SSP is equivalent in the semantic role to the User-ID in CSP. The Service-ID in SSP uniquely identifies a Server. The syntax of Service-ID is defined as follows.

```
Service-ID = "wv:"@ Domain
```

Domain is a set of the WV entities that have the same Domain part in their WV addresses. The Domain is associated with one WV server (the unique access point) to which the IMPS service requests must be delivered if the addressed network entities refer to this Domain.

The Service-ID is used in the session establishment (refer to section 9.1.1, 9.2.2 and 9.3.1) and other SSP management functions.

The Service-ID is used as part of the meta-information in the SSP transactions (refer to section 8.1).

An examples of the Service-ID is:

```
Service-ID:          wv:@imps.com
```

6.3.9 Message and Message-ID

The Message-ID in SSP is globally unique to identify a message. The syntax of Message-ID is defined as follows:

```
Message-ID = Local-Message-ID "@" Domain
```

Where the "Local-Message-ID" uniquely identifies a message within the IMSE domain, and subject to the implementation.

An example of the Message-ID is:

```
12345678@imps.com.
```

The definition of Message-ID in SSP is consistent with that in CSP.

6.4 Data Types

SSP defines four basic data types, namely "*Char*", "*Integer*", "*String*" and "*Boolean*", and three structured date types namely "*Enum*", "*DateTime*" and "*Structure*".

An information element is "*String*" type by default unless specified.

6.4.1 Char

A "*Char*" type element is a single character encoded in UTF-8.

6.4.2 Integer

An "*Integer*" type element is a 32-bit decimal number ranging in [0, 2^{32} - 1].

6.4.3 String

A "*String*" type element is a sequence of "*Char*" elements.

6.4.4 Boolean

A "*Boolean*" type element is either "True" or "False".

6.4.5 Enum

An "*Enum*" type element is one of the pre-defined set of values.

6.4.6 DateTime

A "*DateTime*" type element follows the ISO-8601 specification and is expressed in a "*String*" type element. The date and time format shall be complete date and time using the basic format. There shall be no time-zone indication, but the time may indicate if the time is Coordinated Universal Time (UTC) or local time. The examples are:

```
Local time: 20011019T125031
UTC: 20011019T095031Z
```

6.4.7 Structure

A "*Structure*" type element is the combination of other types of elements as specified.

6.5 Infrastructure Elements

Infrastructure elements are required in the end-to-end solution of server interoperability. Infrastructure elements may not be carried within information elements in SSP protocol. However, the implementation shall be able to support the infrastructure elements to ensure the server interoperability.

6.5.1 Host-ID

The Host-ID is the primary (Master) host address of the SAP of the WV server or Proprietary Gateway. The Host-ID must be used for establishing the session with this WV server or Proprietary Gateway.

The Host-ID is referenced in the form of DNS host name. The Host-ID may be stored inside the environment for DNS A RR host address resolution, or may be retrieved from the Service-ID by the DNS SRV RR based address resolution.

The Host-ID cannot be changed during a session.

An example of Host-ID is:

```
host1.imps.com
```

6.5.2 Redirect (Host) Name

When the WV server in a domain can be accessed through several SAP's distributed in different physical hosts, this WV server may provide a list of those hosts for the other WV server to share the load at the session establishment. This list is called Redirect List and contains the redirect host DNS names. A Redirect (Host) Name in SSP uniquely identifies a physical host in the WV Server or a Proprietary Gateway domain.

The Redirect (Host) Names may be configured statically based on offline agreement between two domains. The Redirect (Host) Addresses may be notified dynamically during session establishment over Master Connection Pair (9.1.1).

An example of a Redirect (Host) Address is:

```
host2.serviceprovider.com.
```

6.6 Features and Functions

SSP supports the server interoperability features and functions defined and described in features and functions document.

6.6.1 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 at the server in that domain.

SSP supports the security requirement in the server interoperability through the CALLBACK connection establishment and access control across session management and transaction management. Please refer to section 6.1.1 for details of CALLBACK connection establishment.

SSP supports the security requirement in the server interoperability through the underlying transport layer whenever possible.

The individual domain security enhances the overall security level in the server interoperability.

6.6.2 Connection Management

SSP connection management ensures the authenticated connections to transport SSP transactions during SSP sessions. Connection management includes connection establishment, connection termination and connection maintenance.

SSP supports CALLBACK connection establishment.

SSP supports the implicit connection termination and connection maintenance through session management. SSP session maintenance covers connection maintenance, and SSP session termination covers connection termination. Connection termination causes the session termination if no more connection exists.

6.6.3 Transaction Management

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

6.6.4 Session Management

SSP supports the authentication among the WV SAP's. The WV SAP's must authenticate each other before they can provide each other with the IMPS services.

SSP supports the authorization and access control among the WV SAP's so that the servers and the gateways are allowed to access the IMPS services provided by each other.

SSP session management includes session establishment, session termination and session maintenance. The CALLBACK connection establishment shall be used in the session establishment. The access control is supported in the whole session management.

6.6.5 Service Management

SSP supports service discovery among the WV domains. The services include Common Services, Presence Service, Instant Messaging (IM) Service, Group Service and Shared Content Service that are defined in the "*Features and Functions*" document. However, those services are discovered in the element level rather than the protocol level. SSP only provides a protocol method and facilitates the message exchange to support the service discovery.

SSP supports the service negotiation and agreement among the WV domains. The service agreement may be made either online or offline. The service agreement must be made before they can provide each other with the IMPS services.

6.6.6 User Profile Management

SSP supports the exchange of user profile information among the WV domains including the list of services 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, the user account status etc.

User Profile Management features can support various functions based on the exchange of user profile information.

6.6.7 Service Relay

SSP supports the service relay among the WV domains including the functional relay of the common IMPS features, presence features, IM features, group features and shared content features that are defined in "*Features and Functions*" document. The goal of SSP is to support the distributed interoperable complementary IMPS services across service provider domains.

Due to the nature of the server interoperation, the SSP has its own requirement on meta-information and information elements in the primitives at transaction level. The complete primitives and transaction flows at SSP semantics level have been defined in the following sections including functional relay services.

Please refer to the CSP document so as to conclude how to relay the complete IMPS features from client-server interaction (CSP) to server-server interoperation (SSP).

7. 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.

7.1 Trust Models

A TRUST model is assumed between the WV SAP and the Service Elements within a single IMPS domain.

A TRUST model is assumed for the network infrastructure such as DNS.

The TRUST model is mutual, *i.e.*, A trusts B if and only if B trusts A.

The TRUST model is created between domain A and domain B if and only if they have been authenticated and authorized by each other. A TRUST model must be created between two domains before they can provide each other with interoperable complementary IMPS services.

7.2 Access Control

The authentication and authorization between the servers in different domains are accomplished by the access control at each server. The scope of access control covers online session management, transaction management and offline configuration agreement.

The online session management includes the initial CALLBACK connection establishment, authentication and authorization to start a session, session maintenance and session termination.

The transaction management supports the access control by the transaction authentication based on the information elements specified in each service request and service response.

The offline configuration agreement includes, but is not limited to, server identity registration, Host-ID, account creation, password protection, configurable parameters, SAP Service Routing Table, etc. through provisioning and / or administration interface.

7.3 Transport Security

The security requirement in the transport layer and other underlying layers, such as data integrity and confidentiality, is out of the scope of SSP. However, whenever possible, current security approach including SSL / TLS, PGP, PKI, digital certificates, etc. in the underlying transport layer should be used to ensure the secure transmission in the underlying layers to prevent from out-of-scope security issues. The deployed security technology is negotiated between the service providers through the offline configuration agreement.

7.4 Individual Domain Security

The security of an individual domain enhances the inter-domain security. A single IMPS domain is encouraged to use firewalls or other precautions to ensure the highest possible level of security.

8. TRANSACTION MANAGEMENT

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

8.1 Meta-Information

The SSP service requests must contain the meta-information as defined in table 1.

Information Element	Req	Type	Description
Client-Originated	M	Boolean	Indicates whether the request is originated from the client ("True") or from the service element ("False").
Session-ID	M	String	Identifies the session managed by the **Provider Server**.
Transaction-ID	M	String	Identifies the transaction originated from the transaction initiator (either requestor server, or provider server).
Service-ID	M	String	Identifies the initiator domain (and the service element if needed).
User-ID	C	String	Identifies the user represented by the requestor server domain. It is present if the request is originated from a client.
Client-ID	O	String	Identifies the Client-ID of the user. It optionally present if the request is originated from a client.

Table 1. Information elements in Meta-information primitive

The Session-ID is unique for each session at the Provider Server.

The Transaction-ID is unique for each transaction originated from the server that initiates the transaction.

An SSP service response in a two-way transaction must contain the same Session-ID and the Transaction-ID as those in the service request.

Some implementation notes are as follows.

1. The SAP at the service provider server should maintain a **Session Record** for each service requestor.
2. The SAP at the service requestor should maintain a **Transaction Record** for each service provider.
3. The SAP at each server 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 hop is clearly and uniquely identified by the transaction flows.

8.2 Status Primitive

The status primitive in the service response is defined as follows in table 2.

Information Element	Req	Type	Description
Session-ID	M	String	Identifies the session. It should be consistent with the Session-ID in the Meta-Information in the request.
Transaction-ID	M	String	Identified the transaction. It should be consistent with the Transaction-ID in the Meta-Information in the

			request.
Status code	M	String	Status code of the processing result.
Status description	O	String	Textual description of the status.

Table 2. Information elements in Status primitive

8.3 Asynchronous Transaction

The server shall support asynchronous transactions.

8.4 General Error Handling

In two-way transactions, after a transaction is initiated, the originating server is expecting the response from the processing server. In multi-way transactions, after a transaction is initiated, one server is expecting the response from the other server.

Whenever an error occurs, the processing server shall handle the exception based on its own policy. In addition, the processing server shall inform the other server involved in this transaction of such an exception by sending the Status primitive with an appropriate Status Code and optional Status Description. More precisely if the processing server sends Status Code 2XX then it SHALL be sent in the response primitive specified for the transaction. Otherwise Status primitive SHALL be used.

8.5 Invalid Transaction

A transaction is considered “valid” if the transaction completes within a reasonable period. The transaction validity time is the sum of the network latency, transaction processing time and an adjustable offset. Those three elements must be configurable at each service domain by the operator. Each operator shall define and configure the reasonable value of the three elements based on the network, hardware and software capacity to ensure the quality and performance of the service as well as the security.

A transaction is considered “invalid” if the transaction cannot complete within the validity time.

If an invalid transaction occurs, the service requestor shall not receive a response from the provider domain. The service requestor shall repeat the transaction for reasonable times until the transaction completes or the repeat times expire. If the transaction completes, the session shall go on for the future transactions. If the repeat times expire, the session shall be terminated by the requestor for security reason. In addition, the requestor-maintained session, which provides the other side with its own service, shall be terminated also.

The repeat times must be configurable at each service domain by the operator. Each operator shall define and configure a reasonable value of repeat times to ensure the quality and performance of the service as well as the security. The repeat times may be zero (0) if security is the major concern.

8.6 Unknown Transaction

A transaction is considered “unknown” if (1) the request message has syntactic error (e.g. not XML well-formed, XML invalid, data value error); or (2) any of the information elements of the Meta-Information is invalid; or (3) the service request refers to a service that doesn't correspond to the service agreement between the service requester and provider; or (4) the service response cannot be associated with the original service request.

If an unknown transaction happens in a service request, the provider domain shall return a status code indicating an “Unknown Transaction” error. If the unknown transaction happens frequently, the provider domain shall terminate the session as well as the session maintained by the requestor for security reasons.

The definition of “Unknown Transaction Frequency” is up to each server implementation. However, the value of “Unknown Transaction Frequency” must be configurable at each service domain by the operator. Each operator shall define and configure a reasonable value of “Unknown Transaction Frequency” to ensure the quality and performance of the service as

well as the security. The server may terminate the sessions immediately after an unknown transaction happens if security is the major concern.

If an unknown transaction happens in a service response, the requestor shall perform the same behavior as that in handling "invalid transaction".

8.7 General Status Code

All SSP transactions may return the following status codes:

- Continue (100) – for all complementary transactions
- Queued (101) – for all complementary transactions
- Started (102) – for all complementary transactions
- Server queued (104)
- Bad Request (400)
- Service not supported (405) – for all complementary transactions
- Service Unavailable (503)
- Invalid Timeout (504)
- Service not agreed (506) – except transactions required for the service agreement
- Internal Server Error (500)
- Invalid server session (620) – except transactions allowed outside of a session
- Multiple errors (900)
- Not logged in (604)
- Bad parameter (402)
- Forbidden (403)
- Not found (404)

9. Session Management

SSP session management includes session establishment, session termination and session maintenance. The CALLBACK connection establishment is used in the session establishment. The access control is supported in the whole session management.

9.1 Access Control

9.1.1 Session Establishment

The session is established through the connection establishment and initial authentication and authorization between the servers in different domains.

The CALLBACK connection establishment is used in the session establishment. The basic session establishment with the CALLBACK connection is as follows.

Prerequisites:

- A-Host-ID represents the unique access point to domain A.
- B-Host-ID represents the unique access point to domain B.
- Offline configuration agreement has been established between Server A and Server B.
- In Server A, Server B's identity is registered with at least { B-Host-ID, B-Service-ID, B-password } tuple. An empty B-password is valid.
- In Server B, Server A's identity is registered with at least { A-Host-ID, A-Service-ID, A-password } tuple. An empty A-password is valid.
- Both servers has registered and supported a common digest schema such as MD5 or SHA.

The basic steps are:

1. Server A originates a connection 1 to Server B based on its own registration record about Server B, containing { A-Service-ID, A-secret-token} tuple.
2. Server B looks for { A-Service-ID} in its own registration record. If it is not found, Server B closes the connection.
3. Server B initiates connection 2 to the Server A containing { B-Service-ID, B-secret-token }.
4. Server A looks for { B-Service-ID } in its own registration record. If it is not found, Server A closes the connection.
5. Server A sends the LoginRequest to Server B through connection 1, containing { A-Service-ID, A-password-digest }. The "A-password-digest" is generated with A-password and B-secret-token based on the common digest schema in the registration record.
6. Server B sends the LoginRequest to Server A through connection 2, containing { B-Service-ID, B-password-digest }. The "B-password-digest" is generated with B-password and A-secret-token based on the common digest schema in the registration record.
7. Server B verifies the A-password-digest. If the verification fails, it closes the connection.
8. Server B responds to Server A with the LoginResponse through connection 2, containing the status of the transaction and the new session information maintained by Server B. The LoginResponse may contain an optional list of Redirect (Host) Names. This is also called the **Redirect List**.
9. Server A verifies the B-password-digest. If the verification fails, it closes the connection.

10. Server A responds to Server B with the `LoginResponse` through connection 1, containing the status of the transaction and the new session information maintained by Server A. The `LoginResponse` may contain an optional list of Redirect (Host) Names. This is also called the Redirect List.

The `secret-token` is a random string generated by the connection originator at each server.

After step 10 succeeds, two domains are authenticated with each other. The session pair between Server A and Server B are established with trust over two connections, i.e. the **connection pair**. The connection pair (1 and 2) between A-Host-ID and B-Host-ID is called "**Master Connection Pair**".

The "**Redirect List**" reflects the server's desire and capability to handle the redirect. If the server does not include the "Redirect List" in its `LoginResponse`, the server does not support the redirect, and the server intends to use the "Master Connection Pair" to support the session. In this case, the other server shall not try the connection pair establishment unless a new redirect process takes place. Therefore, even if the server does not have its own "Redirect List", but if the server supports the redirect of the other server, it MUST provide a "Redirect" List in the `LoginResponse`. In this case, the "Redirect List" contains only its original `Host-ID`.

If the "Redirect List" is included in both of the `LoginResponses`, i.e. in both Step 8 and Step 10, the redirect takes place. Otherwise the Master Connection Pair (1 and 2) shall be used to support the session.

If the "Redirect List" is included in the `LoginResponse` in Step 8 and Step 10, both of the domains want to use the new "Redirect List" as the physical connections to support the session. The connection pair(s) shall be handed over to the actual physical nodes, and the Master Connection Pair (1 and 2) shall be disconnected. If there is more than one Redirect (Host) Names in either of the "Redirect List", a mesh of redirect connection pairs shall be initiated to support the session pair. A mesh means that every single host connects to all remote hosts.

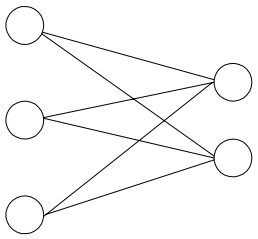

Figure 10. Mesh of redirect connection pairs

After establishing a session there may be an optional online service negotiation and service agreement depending on the offline agreement between two domains. If the online service negotiation and service agreement is needed, it shall be the first transaction in the session pair.

Two servers will provide each other with the IMPS services after the authorization (i.e. online service negotiation and service agreement) if needed, or otherwise right after the session establishment.

There are at least two connections, the connection pair, to carry the session pair. The servers may establish more than one connection pair to support the same session pair. The redirect connection pair between two redirect physical hosts in two domains is established through the same steps except that the redirect connection pair shall be bound to the existing session pair between two domains. The "Redirect List" in Step 8 and Step 10 of session establishment may have set up a mesh of more than one redirect connection pair. Within the session, if additional (mesh of) redirect connection pair(s) is needed, the same Session Establishment steps with the "Redirect List" in Step 8 and Step 10 shall be repeated except that the Master Connection Pair shall be bound to the existing session pair and no new session shall be created. The "Redirect List" shall initiate the establishment of a new mesh of redirect connection pairs. Note that the "Redirect List" is only allowed over the Master Connection Pair. Also note that no new session shall be established when setting up redirect connection pairs. There is always one session pair between two domains no matter how many redirect connection pairs are created. When creating redirect connection pairs online service negotiation and service agreements may not be made.

Connections are reusable. Each session may use some or all of the connections to transport its transactions. Each connection may be used by only one session, or reused by both sessions. In the simplest case, one possiblity is that Connection 1 will be

used for the service session provided and managed by Server B, and connection 2 will be used for the service session provided and managed by Server A.

SSP Transport Binding document [SSP Trans] shall define how to bind session pairs to reusable connections by the underlying transport.

9.1.2 Session Maintenance

Server A and Server B shall maintain the session and keep the session alive by exchanging the live traffic if needed during the session. The initial interval is negotiated during session establishment. The interval may be adjusted by negotiating a new interval when exchanging the live traffic.

The session maintenance may be required periodically as an intermediary (e.g. proxy) may break the connection, resulting in terminating the session, if there is no data traffic for a reasonable time period. The session maintenance may also be required periodically in the case where the server policy requires the termination of the session if there is no transaction activity for a reasonable time period. If session maintenance is required for one session, it is usually also required for the other (reciprocal) session.

The interval must be configurable at each service domain by the operator. The operators shall define and configure a reasonable value of “interval” to ensure the quality and performance of the service as well as the security. The interval configuration must be adjustable on-the-fly.

The session maintenance shall be performed over all of the connections used by the current session, thus covering the connection maintenance.

9.1.3 Session Termination

The session shall be able to be terminated by either Server A or Server B at any time. Both of the sessions managed by Server A and Server B must be terminated to ensure security.

A session may be terminated normally. For example, if the service agreement expires, or the session expires. If any of the service agreements expires, or any of the sessions expire, both of the sessions are terminated.

A session may be terminated abnormally. For example, if an invalid session occurs, or the connection (due to the underlying transport) breaks. If all of the connections of one session break, both of the sessions are terminated. However, even if some connections are terminated due to load balancing or some other reason, as long as there is at least one connection for each session, the session pair SHALL NOT be terminated.

The session termination covers and implies the connection termination. Whenever the session is terminated, all of the connections used by this session shall also be terminated.

9.1.4 Session Re-establishment

If the sessions are terminated, two servers may re-establish the session based on their offline service agreement. The session re-establishment means creating a new session pair, and follows the same steps in establishing the session.

9.2 Primitives

9.2.1 The "SendSecretToken" Primitive

The "`SendSecretToken`" primitive is issued by the requestor server to send the secret token for the provider server as the first step of the CALLBACK connection establishment.

Information Element	Req	Type	Description
Message-Type	M	SendSecretToken	Message identifier
Transaction-ID	M	String	Identifies the transaction originated from the initiating provider server.

Service-ID	M	String	Identifies the requestor server.
Protocol	M	"WV-SSP"	SSP protocol.
Protocol-Version	M	"1.2"	SSP protocol version.
SecretToken	M	String	Secret token originated by the requestor.

Table 3. Information elements in SendSecretToken Primitive

9.2.2 The "LoginRequest" Primitive

The `LoginRequest` primitive is issued from the requestor server to create a new session or a new connection pair inside the existing session with the provider server. The `LoginRequest` primitive specifies initial status of the requestor server. The `LoginRequest` primitive MAY also contain the `time-to-live` attribute, which specifies the time that the session or the connection will expire. If `time-to-live` attribute is omitted, the requestor server requests an infinite session or connection until the service agreement expires.

Information Element	Req	Type	Description
Message-Type	M	LoginRequest	Message identifier
Session-ID	C	String	Identifies the session. It is present when creating additional redirect connection pairs within the existing session.
Transaction-ID	M	String	Identifies the transaction. It should be consistent with the Transaction-ID in the SendSecretToken originated from the provider server.
Service-ID	M	String	Identifies the requestor server.
Redirect-HostID	O	String	Identifies the requestor host if the connection is a redirected connection pair.
Password-Digest	M	String	The password digest generated with password and secret token based on a common digest schema (MD5 or SHA).
Time-To-Live	O	Integer in Seconds	Interval for a valid session or connection before expired. If omitted, the requestor server requests an infinite session or connection.

Table 4. Information elements in LoginRequest Primitive

9.2.3 The "LoginResponse" Primitive

The `LoginResponse` primitive is issued from the provider server to accept the session creation or connection pair creation with the requestor server. In the response the provider server MAY specify the `time-to-live` of the current session. This `time-to-live` may be different from that in the `LoginRequest` from the requestor server.

Information Element	Req	Type	Description
Message-Type	M	LoginResponse	Message identifier
Status-Info	M	Structure of Status-Primitive	The necessary status information in a service response defined in 8.2.
Time-To-Live	O	Integer in Seconds	Interval for a valid session or connection before expired. This time may be any value

			other than zero.
List-of-Hosts	O	Structure	"Redirect" list, which indicates the actual connection addresses in its own domain.

Table 5. Information elements in LoginResponse Primitive

9.2.4 The "LogoutRequest" Primitive

The `LogoutRequest` primitive allows the requestor server to close the session with the provider server.

Information Element	Req	Type	Description
Message-Type	M	LogoutRequest	Message identifier
Session-ID	M	String	Identifies the session.
Transaction-ID	M	String	Identifies the transaction.

Table 6. Information elements in LogoutRequest

9.2.5 The "Disconnect" Primitive

The `Disconnect` primitive allows the provider server to indicate that it accepts the `LogoutRequest` from the requestor server and closes the session.

If the provider server does not receive any session maintenance update within the time-to-live interval (see `KeepAlive` primitive) from requestor server, the provider server will also close this session by sending the `Disconnect` message to the requestor server.

Information Element	Req	Type	Description
Message-Type	M	Disconnect	Message identifier
Session-ID	C	String	Identifies the session. Present if the provider server initiates the Disconnect.
Transaction-ID	C	String	Identifies the transaction. Present if the provider server initiates the Disconnect.
Status-Info	C	Structure of Status-Primitive	The status information (see 8.2). Present if the requestor server Logout.

Table 7. Information Elements in Disconnect Primitive

9.2.6 The "KeepAliveRequest" Primitive

The "`KeepAliveRequest`" primitive allows the requestor server to maintain the session and update the time-to-live interval with the provider server. The session maintenance shall be performed over all of the connections used by this session, thus implies and covers the connection maintenance for each connection. The TTL may have different values for different connections.

Information Element	Req	Type	Description
Message-Type	M	KeepAliveRequest	Message identifier
Session-ID	M	String	Identifies the session.
Transaction-ID	M	String	Identifies the transaction.
Time-to-live	O	Integer in Seconds	Indicates the time-to-live of the session over this connection.

Table 8. Information Elements in KeepAliveRequest Primitive

9.2.7 The "KeepAliveResponse" Primitive

The `KeepAliveResponse` primitive allows the provider server to maintain the session and update the time-to-live interval with the requestor server. The session maintenance shall be performed over all of the connections used by this session, thus implies and covers the connection maintenance for each connection. The TTL may have different value for different connection.

Information Element	Req	Type	Description
Message-Type	M	KeepAliveResponse	Message identifier
Status-Info	M	Structure of Status-Primitive	The status information (see 8.2).
Time-to-live	O	Integer in Seconds	Indicates the time-to-live of the session over this connection.

Table 9. Information Elements in KeepAliveResponse Primitive

9.3 Transactions

9.3.1 The "Login" Transaction

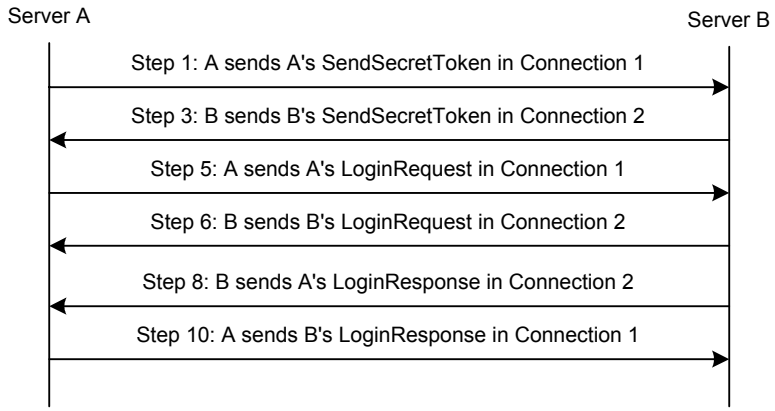

Figure 11. The "Login" Transaction

Session establishment and additional redirect connection establishment are achieved through a "**Login"** transaction.

The Server A performs Step 1 and sends A's `SendSecretToken` to Server B through Connection 1. After the Server B performs Step 2, the Server B performs Step 3 and sends B's `SendSecretToken` to Server A through Connection 2. After the Server A performs Step 4, the Server A performs Step 5 and sends A's `LoginRequest` to Server B through Connection 1. The Server B performs Step 6 and sends B's `LoginRequest` to Server A through Connection 2. Finally, the Server B performs Steps 7 & 8, and replies with A's `LoginResponse` to Server A through Connection 2, and A performs Steps 9 & 10 and replies with B's `LoginResponse` to Server B through Connection 1.

Step 1, Step 6 and Step 10 share the same `Transaction-ID` that is generated by Server A in step 1.

Step 3, Step 5 and Step 8 share the same `Transaction-ID` that is generated by Server B in step 3.

After step 10 succeeds, two domains are authenticated with each other. The session pair between Server A and Server B is established with trust over two connections, i.e. the connection pair. The connection pair (1 and 2) between A-Host-ID and B-Host-ID is called "Master Connection Pair".

The "Redirect List" reflects the server's desire and capability to handle the redirect. If the server does not include the "Redirect List" in its LoginResponse, the server does not support the redirect, and the server intends to use the "Master Connection Pair" to support the session. In this case, the other server shall not try a connection pair establishment unless a new redirect process takes place. Therefore if the server does not have its own "Redirect List", but if the server supports the redirect of the other server, it MUST provide a "Redirect" List in the LoginResponse. In this case, the "Redirect List" contains its original Host-ID only.

If the "Redirect List" is included in both of the `LoginResponses`, i.e. in both Step 8 and Step 10, the redirect takes place. Otherwise the Master Connection Pair (1 and 2) shall be used to support the session.

If the "Redirect List" is included in the `LoginResponse` in Step 8 and Step 10, both of the domains should use the new "Redirect List" as the physical connections to support the session. The connection pair(s) shall be handed over to the actual physical nodes, and the Master Connection Pair (1 and 2) shall be disconnected. If there are more than one Redirect (Host) Names in either of the "Redirect List", a mesh of redirect connection pairs shall be initiated to support the session pair.

There are at least two connections, the connection pair, to carry the session pair. The servers may establish more than one connection pair to support the same session pair. The redirect connection pair between two redirect physical hosts in two domains is established through the same steps except that the redirect connection pair shall be bound to the existing session pair between the two domains. The "Redirect List" in Step 8 and Step 10 of session establishment may have set up a mesh of more than one redirect connection pair. Within the session, if additional (mesh of) redirect connection pair(s) is needed, the same Session Establishment steps with the "Redirect List" in Step 8 and Step 10 shall be repeated except that the Master Connection Pair shall be bound to the existing session pair and no new session shall be created. The "Redirect List" shall initiate the establishment of a new mesh of redirect connection pairs. Note that the "Redirect List" is only allowed over Master Connection Pair. Also note that no new session shall be established when setting up redirect connection pairs. There is always one session pair between two domains no matter how many redirect connection pairs are created. While creating redirect connection pairs an online service negotiation and service agreement may not be made.

Primitive	Direction
SendSecretToken	Requestor Server ← Provider Server
LoginRequest	Requestor Server → Provider Server
LoginResponse	Requestor Server ← Provider Server

Table 10. Primitive Directions for Login Transaction

9.3.2 The "Logout" Transaction

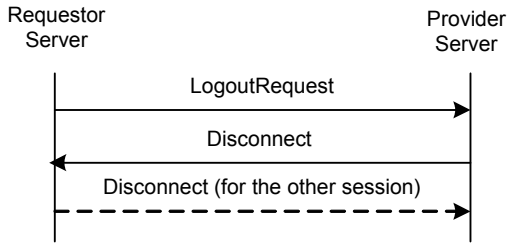

Figure 12. The "Logout" Transaction

Session termination is achieved through "**Logout**" and "**Disconnect**" transactions. All of the connections used by this session shall be terminated as well after the session is finished.

The requestor server can logout from the provider server and close the session through a "Logout" transaction. In addition the requestor also shall terminate the other session through a "Disconnect" transaction that is illustrated in the dashed line.

The requestor server sends a `LogoutRequest` request to the provider server. After the provider server finishes processing the request, it sends a `Disconnect` response to the requestor server to indicate the close of the session.

Primitive	Direction
LogoutRequest	Requestor Server → Provider Server
Disconnect	Requestor Server ← Provider Server

Table 11. Primitive Directions for Logout Transaction

9.3.3 The "Disconnect" Transaction

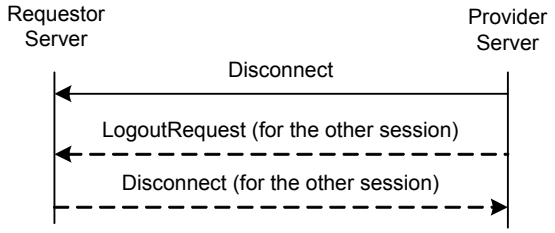

Figure 13. The "Disconnect" Transaction

The provider server may close the session through a "**Disconnect**" transaction. Under such conditions the provider also shall terminate the other session through a "Logout" transaction that is illustrated in the dash lines.

Primitive	Direction
Disconnect	Requestor Server ← Provider Server

Table 12. Primitive Directions for Disconnect Transaction

9.3.4 The "KeepAlive" Transaction

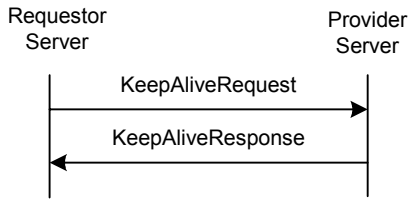

Figure 14. The "KeepAlive" Transaction

Session maintenance is achieved through the "**KeepAlive**" transaction. A "KeepAlive" transaction shall be performed over all of the connections used by this session, thus implies and covers the connection maintenance for each connection. The TTL may have different value for different connection.

The requestor server updates the time-to-live interval and keeps the session and the connection(s) alive through the "KeepAlive" transaction(s).

The requestor server sends a `KeepAliveRequest` request to the provider server. After the provider server finishes processing the request, it sends a `KeepAliveResponse` response to the requestor server to indicate the status of the session over this connection. The `KeepAliveRequest` may carry a new time-to-live interval. The time-to-live value returned in the `KeepAliveResponse` response may differ from that in the request.

The "KeepAlive" transaction may be required periodically in case an intermediary (e.g. proxy) breaks the connection, resulting in terminating the session, if there is no data traffic for a reasonable time period.

The "KeepAlive" transaction may be required periodically in case the server policy requires the termination of the session if there is no transaction activity for a reasonable time period.

If "KeepAlive" is required for one session, it is usually also required for the other, complementary, session.

Primitive	Direction
KeepAliveRequest	Requestor Server → Provider Server
KeepAliveResponse	Requestor Server ← Provider Server

Table 13. Primitive Directions for KeepAlive Transaction

9.4 Status Code

9.4.1 "Login" Transaction

- `Unknown Service-ID (606)`
- `Redirection refused (607)`
- `Invalid password. (608)`

9.4.2 "Logout" / "Disconnect" Transaction

- `Session Expired (600)`
- `Connection expired (609)`

10.Service Management

The service management in SSP enables the Wireless Village servers to mutually agree on the usable Wireless Village services. The usable services offered by a server are arranged in a negotiation tree.

10.1 Service Structure

The Wireless Village services are organized in a hierarchy:

- Features – a specific set of related functionality
- Functions – defines a set of related transactions for each feature
- Transactions – defines a set of related primitives for each function
- Information Elements – the lowest level building blocks of the transactions

A Wireless Village server may support all or a subset of the features. However, if a WV server supports a feature, some functions and transactions must be supported to ensure minimal interoperability [SSP SCR]. The remaining functions and transactions are optional. Moreover, there are multiple choices in the semantics for some of the functions and transactions, e.g. the general search transaction with search-type USER-ID is mandatory while all other search types are optional.

The optional functions, transactions, and choices offered by a server are arranged in a service tree, as shown in Figure 14. Each node in the tree specifies the functions, transactions, and choices that must be supported by the server that includes that node in its **Service-List**.

Each node in the service tree defines a group of one or several transactions or choices. The content of each node and how the tree should be interpreted are described below. The transactions that are not described are considered mandatory functions that must be always supported in the servers.

10.2 General

If a **Feature** node is included in the Service-List, all mandatory requirements for that specific feature must be supported as specified in [SSP SCR].

If a lower level node is included in the Service-List, all transactions or choices specified by that node must be supported.

10.3 SAP Feature

- **Service Negotiation** node includes the following transactions
  - GetAvailableService
  - ServiceIndication
  - SetServiceAgreement
- **User Profile** management node includes the following transactions
  - GetUserProfile
  - UpdateUserProfile
  - Service Relay node indicates if the SAP supports service relay including routing

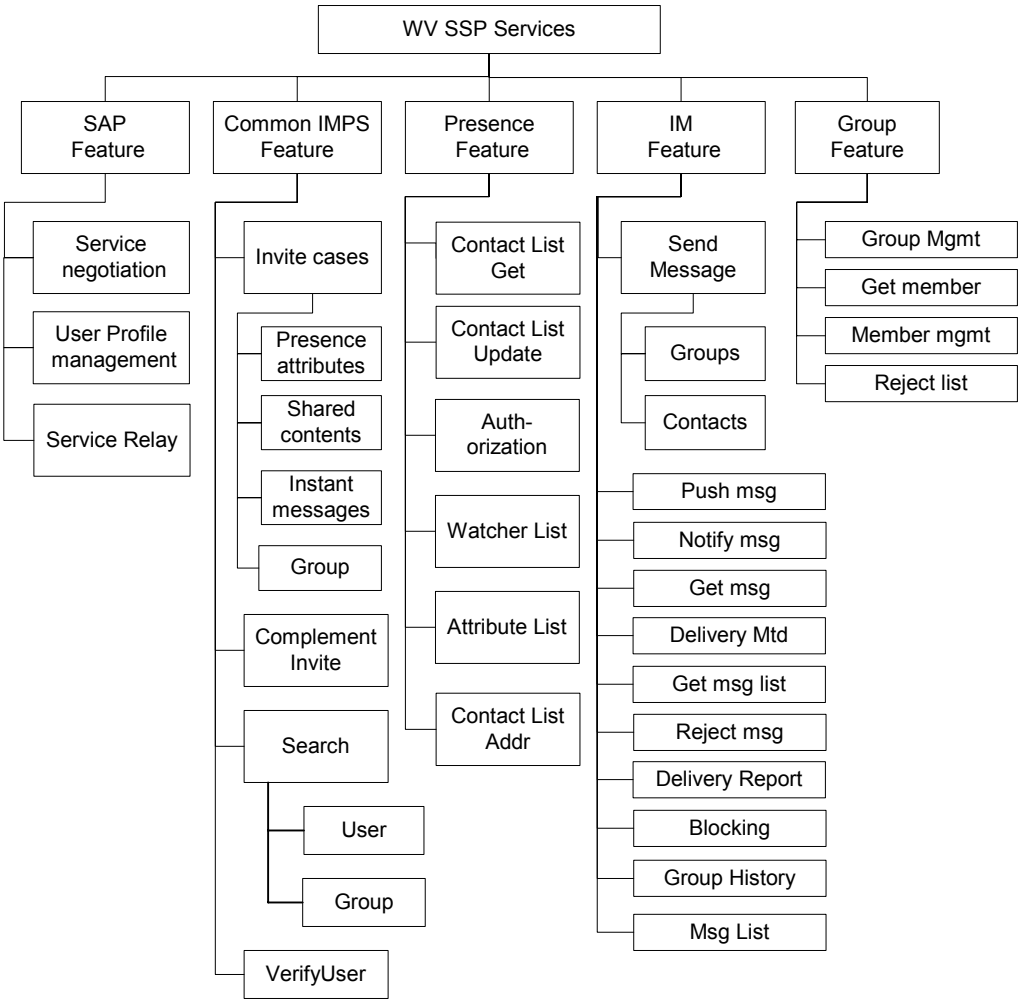

Figure 15: SSP Service tree

10.4 Common IMPS feature

- **Invite** node includes the Invitation/Cancel-Invitation transactions
  - All supported invite types must be included in the Service List (Presence, IM, Shared Content, Group)
- Complementary Invite node includes the Complementary Invitation/Cancel-Invitation transactions
  - If the Complementary invite node is included in the Service-List, the Invite cases node must be included as well.
- **Search** node includes the optional choices for the GeneralSearch. All supported search types must be included in the Service List i.e.
  - User: Support Presence attributes criteria
  - Group: Support Group related criteria
- **VerifyUser** node includes the following transactions:
  - VerifyWVID

10.5 Presence Feature

- ***Contact List Get*** node includes the following transactions:
  - GetContactList
  - GetListMember
  - GetListProperties
- ***Contact List Update*** node includes the following transactions:
  - CreateContactList
  - DeleteContactList
  - AddListMember
  - RemoveListMember
  - SetListProperties
- ***Authorization*** node includes the following transactions
  - ReactiveAuthorizarion
  - CancelAuthorization
  - GetReactiveAuthStatus
- ***Watcher List*** node includes the following transaction
  - GetWatcherList
- ***Attribute List*** node includes the following transactions
  - CreateAttributeList
  - DeleteAttributeList
  - GetAttributeList
- ***Contact List Addr*** node indicates if the contacts list is valid for addressing users in the following transactions
  - Subscribe
  - UnSubscribe
  - GetPresence
  - UpdatePresence
  - Suspend Presence

10.6 IM Feature

- ***Send Msg*** node includes the optional choices for the SendMessage and ForwardMessage transactions. All supported ID types must be included in the Service List i.e.
  - Group-ID: Support recipient as Group-ID and addressing by screen name
  - ContactList-ID: Support recipients listed by Contact List ID
- ***Push Msg*** node includes the following transaction

  - PushMessage
- ***Notify Msg*** node includes the following transaction
  - MessageNotification
- ***Get Msg*** node includes the following transaction
  - GetMessage
- ***Delivery Mtd*** node includes the following transaction
  - SetMessageDeliveryMethod
- ***Get Msg List*** node includes the following transaction
  - GetMessageList without group functionality
- ***Reject Msg*** node includes the following transaction
  - RejectMessage
- ***Delivery Report*** node includes the following transaction
  - NotifyDeliveryStatusReport
- ***Blocking*** node includes the following transactions
  - BlockUser
  - GetBlockedList
- ***Group History*** node indicates if the IM service element supports group chat cashing functionality.
- ***Msg List*** node includes the optional choices for the GetMessageList transaction (Undelivered messages)

10.7 Group Feature

- ***Group Mgmt*** node includes the following transactions
  - CreateGroup
  - DeleteGroup
- ***Get Member node*** includes the following transaction
  - GetJoinedMember
- ***Member mgmt*** node includes the following transactions
  - AddGroupMember
  - GetGroupMember
  - RemoveGroupMember
  - MemberAccess
- ***Reject list*** node includes the following transactions
  - RejectList

10.8 Primitives

10.8.1 The "GetServiceRequest" Primitive

The `GetServiceRequest` primitive is issued from the requestor server to discover the available services provided by the provider server.

Information Element	Req	Type	Description
Message-Type	M	GetServiceRequest	Message identifier
Meta-Information	M	Structure of Meta-information	The necessary meta-information in a service request defined in 8.1.

Table 14. Information elements in GetServiceRequest Primitive

10.8.2 The "ServiceList" Primitive

The `ServiceList` primitive is issued from the provider server to indicate its available services.

Information Element	Req	Type	Description
Message-Type	M	ServiceList	Message identifier
Meta-Information	C	Structure of Meta-information	The necessary meta-information in a service request defined in 8.1. Present if the provider initiates ServiceIndication.
Status-Info	C	Structure of Status-Primitive	The status information (see 8.2). Present if the requestor initiates GetServiceRequest.
Service-List	M	Structure	List of available services in a tree structure.

Table 15. Information elements in ServiceList Primitive

10.8.3 The "ServiceNegotiation" Primitive

The `ServiceNegotiation` primitive is issued from the requestor server to negotiate the desired services that will be committed and provided by the provider server. The provider server sends the `ServiceAgreement` primitive to confirm the agreed services with the requestor server.

Information Element	Req	Type	Description
Message-Type	M	ServiceNegotiation	Message identifier
Meta-Information	M	Structure of Meta-information	The necessary meta-information in a service request defined in 8.1.
Desired-Service-List	M	Structure	List of desired services in a tree structure
Desired-Sub-Protocol	O	String	Desired sub-protocol and its version for proprietary protocol extensions
Time-to-live	O	Integer in Seconds	Indicates the desired time-to-live of the service agreement

Table 16. Information elements in ServiceNegotiation Primitive

10.8.4 The "ServiceAgreement" Primitive

After the provider server receives the `ServiceNegotiation` primitive from the requestor server, the provider server shall send the `ServiceAgreement` primitive to confirm the agreed services with the requestor server.

Information Element	Req	Type	Description
Message-Type	M	ServiceAgreement	Message identifier
Status-Info	M	Structure of Status-Primitive	The status information (see 8.2).
Agreed-Service-List	M	Structure	List of agreed services in a tree structure
Agreed-Sub-Protocol	O	String	Agreed sub-protocol and its version for proprietary protocol extensions
Agreed-Time-to-live	O	Integer in Seconds	Indicates the agreed time-to-live of the service agreement

Table 17. Information elements in ServiceAgreement Primitive

10.9 Transactions

10.9.1 The "GetAvailableService" Transaction

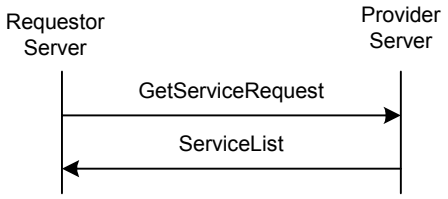

Figure 16. The "GetAvailableService" Transaction

SSP supports service discovery among the WV domains. The services include Common Features, Presence Service, Instant Messaging (IM) Service, Group Service and Shared Content Service that are defined in "*Features and Functions*" document.

The requestor server discovers the available services provided by the provider server through a "**GetAvailableService**" Transaction.

The requestor server sends a `GetServiceRequest` request to the provider server inquring about the available services. After the provider server finishes processing the request, it sends a `ServiceList` response to the requestor server with the available service information.

Primitive	Direction
GetServiceRequest	Requestor Server → Provider Server
ServiceList	Requestor Server ← Provider Server

Table 18. Primitive Directions for GetAvailableService Transaction

10.9.2 The "ServiceIndication" Transaction

Figure 17. The "ServiceIndication" Transaction

The provider server also informs the requestor server of any change in the available services through a "**ServiceIndication**" Transaction. It depends on the offline service agreement between two domains to decide what the subsequent actions to be taken are.

The provider server sends a `ServiceList` request to the requestor server and indicates the available services on-the-fly.

Primitive	Direction
ServiceList	Requestor Server ← Provider Server

Table 19. Primitive Directions for ServiceIndication Transaction

10.9.3 The "SetServiceAgreement" Transaction

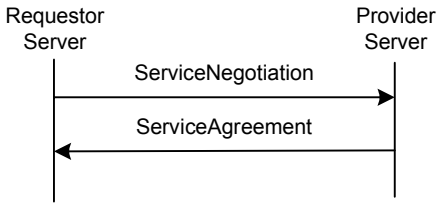

Figure 18. The "SetServiceAgreement" Transaction

The service agreement between the requestor and provider servers is established through a "**SetServiceAgreement**" Transaction.

The `ServiceNegotiation` request is issued from the requestor server to request and negotiate the agreement on the services that will be committed to and provided by the provider server. The provider server sends the `ServiceAgreement` response to confirm the agreement with the requestor server.

After a service agreement is confirmed, the servers may perform interoperable IMPS services.

Primitive	Direction
ServiceNegotiation	Requestor Server → Provider Server
ServiceAgreement	Requestor Server ← Provider Server

Table 20. Primitive Directions for SetServiceAgreement Transaction

10.10 Status Code

- `Version Not Supported (505)`

11. Interoperability Management – User Profile Management

These transactions are needed for the complementary services.

11.1 User Profile

User Profile consists of general user information and service-specific user information. The general user information includes the services to which the user subscribes, the service status (active / inactive), the privacy status with regard to network service capabilities (e.g. user location, user interaction), terminal capabilities, user account status, etc. The service-specific user information includes the user-related information for each specific service element.

The general user information is defined as follows:

General UP Attribute	Value	Description
User.Account.Status	"ON" | "OFF"	Status of user account – active or inactive
User.Privacy.Location	"ON" | "OFF"	Status of location privacy – private or not
User.Privacy.Interaction	"ON" | "OFF"	Status of Interaction privacy – private or not
Services.Common	"YES" | "NO"	Whether or not Common service is subscribed
Services.Common.PSE	Domain	PSE of Common service. See 6.3.1 for Domain definition.
Services.Common.Status	"ON" | "OFF"	Status of Common service – active or inactive
Services.IM	"YES" | "NO"	Whether or not IM service is subscribed
Services.IM.PSE	Domain	PSE of IM service. See 6.3.1 for Domain definition.
Services.IM.Status	"ON" | "OFF"	Status of IM service – active or inactive
Services.Presence	"YES" | "NO"	Whether or not Presence service is subscribed
Services.Presence.PSE	Domain	PSE of Presence service. See 6.3.1 for Domain definition.
Services.Presence.Status	"ON" | "OFF"	Status of Presence service – active or inactive
Services.Group	"YES" | "NO"	Whether or not Group service is subscribed
Services.Group.PSE	Domain	PSE of Group service. See 6.3.1 for Domain definition.
Services.Group.Status	"ON" | "OFF"	Status of Group service – active or inactive

Services.Content	"YES" | "NO"	Whether or not Content service is subscribed
Services.Content.PSE	Domain	PSE of Content service. See 6.3.1 for Domain definition.
Services.Content.Status	"ON" | "OFF"	Status of Content service – active or inactive
Terminal.Delivery	"PUSH" | "NOTIFY"	Preferred message delivery method in client
Terminal.Content.type	MIME {, MIME }	Supported MIME types in client. See RFC 2045, RFC 2046 and WAP Forum for standard MIME.
Terminal.Content.encoding	encoding {, encoding }	Supported transfer encoding in client. See RFC 2045 for standard "transfer-encoding".
Terminal.Content.length	Integer in Byte	Supported message size in client for "PUSH"
Terminal.Content.protocol	Protocol {, Protocol }	Supported out-band protocol in client for binary message retrieval.
x.key	String	A service provider may define new key-values. These service provider specific keys are prefixed with x[.].

Table 21. General User Profile

Each piece of user profile information is organized in a "(name, value)" pair. The General User Profile is the list of "(name, value)" pairs, which are separated with "; ". An example of a General User Profile is as follows:

(User.Account.Status, ON); (Services.IM, ON); (Services.IM.PSE, im.wv.com); (Services.IM.Status, ON); (Terminal.Delivery, PUSH); (Terminal.Content.type, text/plain; charset=US-ASCII, text/xml; charset=UTF-8, image/wbmp); (Terminal.Content.encoding, BASE64); (Terminal.Content.length, 256); (Terminal.Content.protocol, HTTP, SIP, RTP, RTSP)); (x.MaxNumberOfConatctLists, 100)

11.2 Primitives

11.2.1 The "GetUserProfileRequest" Primitive

The `GetUserProfileRequest` primitive is issued to discover the available user profile information.

Information Element	Req	Type	Description
Message-Type	M	GetUserProfileRequest	Message identifier
Meta-Information	M	Structure of Meta-information	The necessary meta-information in a service request defined in 8.1.
User-ID-List	M	Structure	Identifies the users whose User Profiles are requested. If it is empty, all users' User Profiles are requested.

Table 22. Information elements in GetUserProfileRequest Primitive

11.2.2 The "UserProfile" Primitive

The `UserProfile` primitive is issued from the provider server to provide the user profile information.

Information Element	Req	Type	Description
Message-Type	M	UserProfile	Message identifier
Status-Info	M	Structure of Status-Primitive	The status information (see 8.2).
User-Profile-List	M	Structure of User-Profile	A list of User Profiles. Each User profile contains User-ID and a list of (name, value) pairs.

Table 23. Information elements in UserProfile Primitive

11.2.3 The "UpdateUserProfileRequest" Primitive

The `UpdateUserProfileRequest` primitive is issued to update the user profile information.

Information Element	Req	Type	Description
Message-Type	M	UpdateUserProfileRequest	Message identifier
Meta-Information	M	Structure of Meta-Information	The meta-information (see 8.1).
Updated-User-Profile-List	M	Structure of User-Profile	A list of User Profiles. Each User profile contains User-ID and a list of (name, value) pairs.

Table 24. Information elements in UpdateUserProfileRequest Primitive

11.3 Transactions

11.3.1 The "GetUserProfile" Transaction

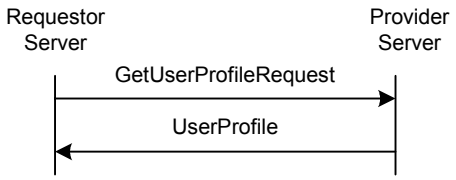

Figure 19. The "GetUserProfile" Transaction

SSP supports the exchange of user profile information among the WV domains including the list of services 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 user profile information is discovered through a "**GetUserProfile**" transaction.

The `GetUserProfileRequest` request is issued from the requestor server to request the user profile information from the provider server. The provider server sends the `UserProfile` response to provide the requestor server with the user profile information.

Primitive	Direction
GetUserProfileRequest	Requestor Server → Provider Server
UserProfile	Requestor Server ← Provider Server

Table 25. Primitive Directions for GetUserProfile Transaction

11.3.2 The "UpdateUserProfile" Transaction

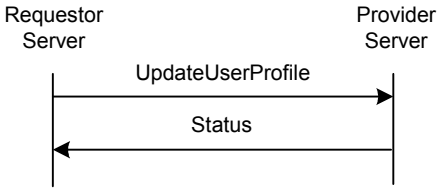

Figure 20. The "UpdateUserProfile" Transaction

The requestor server may update the user profile information in the provider server through an "**UpdateUserProfile**" Transaction.

The requestor server sends an `UpdateUserProfile` request to the provider server and provides the updated user profile information. After the provider server finishes processing the request, it sends a `Status` response to the requestor server and confirms that it has updated the user profile information.

Primitive	Direction
UpdateUserProfile	Requestor Server → Provider Server
Status	Requestor Server ← Provider Server

Table 26. Primitive Directions for UpdateUserProfile Transaction

11.4 Status Code

- `Unknown user (531)`

12.Service Relay – Common IMPS Features

SSP supports the service relay among the WV servers and the SSP Gateways including the functional relay of the common IMPS features, contact list, presence features, IM features, group features and shared content features that are defined in the "*Features and Functions*" document.

12.1 Overview

This chapter focuses on the functional relay of common IMPS features. Because of the server interoperation nature, the SSP has its own requirement on meta-information and information elements in the primitives at transaction level. The complete primitives and transaction flows of common IMPS features at SSP semantics level are defined in the following two sections.

Please refer to the CSP document to determine how to relay the common IMPS features from client-server interaction (CSP) to server-server interoperation (SSP).

12.2 Primitives

12.2.1 The "SearchRequest" Primitive

The `SearchRequest` primitive allows a user to search for users or groups based on different properties of the user or group. The user may limit the number of search results retrieved at one time. The user may continue the search and go through all the results.

The search is performed using a list of one or more **Search-Pairs**. A Search-Pair consists of a **Search-Element** and a **Search-String**. The Search-Element indicates which property of the user / group shall be searched for the Search-String. When more than one search pair is specified in the primitive, a logical AND operation is assumed among the different pairs. Every Search-Element may be present only once within the same search request.

The search result is restricted in the same manner presence information is restricted when requested. If the searching user is not proactively authorized to see certain presence values for a user included in the search result, that presence value shall not be included. If the unauthorized presence attribute is part of the search criteria, that user shall not be included in the search result at all. Users that want to have certain presence attributes searchable should expose them through their default attribute list.

The result of a user search is always user-ID. Similarly, the result of a group search is always group-ID.

Search-Element for User Search (the result is always user-ID) is listed as follows:

Search-Element	Description
USER_ID	The *Search-String* is a substring of a user-ID.
USER_FIRST_NAME	The *Search-String* is a substring of a user's firstname.
USER_LAST_NAME	The *Search-String* is a substring of a user's lastname.
USER_EMAIL_ADDRESS	The *Search-String* is a substring of a user's e-mail address.
USER_ALIAS	The *Search-String* is a substring of a user's alias.
USER_MOBILE_NUMBER	The *Search-String* is a mobile number. [E.164].
USER_ONLINE_STATUS	The *Search-String* is an online status value.

Search-Element for Group Search (the result is always group-ID) is listed as follows:

Search-Element	Description
GROUP_ID	The *Search-String* is a substring of a group-ID.
GROUP_NAME	The *Search-String* is a substring of a group's name (part of group properties).
GROUP_TOPIC	The *Search-String* is a substring of a group's topic (part of group properties).
GROUP_USER_ID_JOINED	The *Search-String* is a substring of a user-ID.
GROUP_USER_ID_OWNER	The *Search-String* is a user-ID. Search result contains the list of groups owned by the specified user.
GROUP_USER_ID_AUTOJOIN	The *Search-String* is a user-ID. Search result contains the list of groups that have the AutoJoin property set to "T" for the specified user.

Information Element	Req	Type	Description
Message-Type	M	SearchRequest	Message identifier
Meta-Information	M	Structure of Meta-Information	The meta-information (see 8.1).
Search-Pair-List	C	Structure	Search criteria in terms of properties. It is present only in the 1st search request.
Search-Limit	C	Integer	Indicates the number of maximum search results that can be received at one time. It is Present only in the 1st search request.
Search-ID	C	String	Uniquely identifies a search transaction. The server assigns this ID when the first search is performed, thus it is not present in the 1st search request.
Search-Index	C	Integer	Indicates that the results shall be sent starting from this particular index. It is present only when the search is continued.

Table 27. Information elements in SearchRequest Primitive

12.2.2 The "SearchResponse" Primitive

Information Element	Req	Type	Description
Message-Type	M	SearchResponse	Message identifier
Status-Info	M	Structure of Status-Primitive	The status information (see 8.2).
Search-ID	**C**	String	Uniquely identifies a search transaction. The server assigns this ID when the 1st search is performed successfully.
Search-Findings	M	Integer	Indicates the number of current findings.
Completed	M	Boolean	Indicates if the client can expect new results.

			'No' if server may provide new results (still searching), 'Yes' if new results will not be provided.
Search-Index	M	Integer	Indicates the index of the last result. This provides the user with the information of where to continue the next search.
Search-Results	C	Structure	Search results.

Table 28. Information elements in SearchResponse Primitive

12.2.3 The "StopSearchRequest" Primitive

The `StopSearchRequest` primitive allows a user in the requestor server to indicate to the provider server that the search and / or its result is not needed any more from a previously issued search request.

Information Element	Req	Type	Description
Message-Type	M	StopSearchRequest	Message identifier
Meta-Information	M	Structure of Meta-Information	The meta-information (see 8.1).
Search-ID	M	String	Identifies the search to be invalidated.

Table 29. Information elements in StopSearchRequest Primitive

12.2.4 The "InviteRequest" Primitive

The `InviteRequest` primitive allows the user in the requestor server to invite a list of other users to join a discussion / chat group, or to exchange messages, or to share presence information, or to share content.

The invited user may be a single user identified by its User-ID or Screen-Name. A list of users may be invited using a Contact-List-ID or Group-ID. If Invite-Type is GM, the Invited-User is the group ID.

Information Element	Req	Type	Description
Message-Type	M	InviteRequest	Message identifier
Meta-Information	M	Structure of Meta-Information	The meta-information (see 8.1).
Invite-ID	M	String	Identifies this invitation.
Invite-Type	M	Enum {"GR", "IM", "PR", "SC","GM"}	Inviting for Group/chat (GR), Messaging (IM), Presence (PR), Content (SC)) or Group Membership (GM).
Inviting-User	M	Structure	Identifies the requesting user who sends the invitation (User-ID and / or Screen-Name)
Invited-User	M	Structure	Identifies the user(s) to be invited (User-ID and / or Screen-Name, or Contact-List-ID). If Invite-Type is GM, identifies the group ID.
Invite-Group-ID	C	String	Identifies the group. It is mandatory if InviteGroup (GR) or Group Membership (GM). Otherwise, not present.

Invite-Presence-Attribute-List	CO	Structure	Identifies the Presence Attributes that the inviter wants to share with the invitees. It is optional if InvitePresence (PR). Otherwise, not present.
Invite-Content-ID-List	CO	Structure	Identifies the related shared content as a list of URLs. It is optional if InviteContent (SC). Otherwise, not present.
Invite-Reason	O	String	Textual description of the invitation.
Validity	O	Integer in seconds	Indicates the interval over which the invitation is valid.

Table 30. Information elements in InviteRequest Primitive

12.2.5 The "InviteResponse" Primitive

The `InviteResponse` primitive allows the provider server to return the result of the invitation to the requestor server, representing the inviting user.

Information Element	Req	Type	Description
Message-Type	M	InviteResponse	Message identifier.
Status-Info	M	Structure of Status-Primitive	The status information (see 8.2).
Invite-ID	M	String	Identifies this invitation.
Inviting-User	M	Structure	Identifies the requesting user who sends the invitation (User-ID and / or Screen-Name)
Invite-Acceptance	M	Boolean	Indicates if the user accepts the invitation or not.
Responding-User	M	Structure	Identifies the responding invited user (User-ID and / or Screen-Name). If Invite-Type was GM, identifies the group ID.
Invite-Response	O	String	Textual description, why the invited user accepted/rejected the invitation.

Table 31. Information elements in InviteResponse Primitive

Each tuple { Invite-Acceptance, Responding-User, Invite-Response } represents the response from one invitee. There may be multiple tuples { Invite-Acceptance, Responding-User, Invite-Response } in one "InviteResponse" primitive if the provider server is able to collect the response from the invited users in a reasonable time and combine the multiple responses in one primitive in order to reduce the traffic overhead between the servers.

12.2.6 The "InviteUserRequest" Primitive

The `InviteUserRequest` primitive allows the provider server to invite the user(s) in the requestor server to join a discussion / chat group, or to exchange messages, or to share presence information, or to share content or to become a group member.

Information Element	Req	Type	Description
Message-Type	M	InviteUserRequest	Message identifier
Meta-Information	M	Structure of Meta-	The meta-information (see 8.1).

		Information	
Invite-ID	M	String	Identifies this invitation.
Invite-Type	M	Enum { “GR”, “IM”, “PR”, “SC” , “GM” }	Inviting for Group/chat (GR), Messaging (IM), Presence (PR), Content (SC) or Group Membership (GM).
Inviting-User	M	Structure	Identifies the requesting user who sends the invitation (User-ID and / or Screen-Name)
Invited-User	M	Structure	Identifies the user(s) to be invited (User-ID and / or Screen-Name, or List-of-User-IDs)
Invite-Group-ID	C	String	Identifies the group. It is mandatory if InviteGroup (GR) or Group Membership (GM). Otherwise, not present.
Invite-Presence-Attribute-List	CO	Structure	Identifies the Presence Attributes that the inviter wants to share with the invitees. It is optional if InvitePresence (PR). Otherwise, not present.
Invite-Content-ID-List	CO	Structure	Identifies the related shared content as a list of URLs. It is optional if InviteContent (SC). Otherwise, not present.
Invite-Reason	O	String	Textual description of the invitation.
Validity	O	Integer in seconds	Indicates the interval in which the invitation is valid.

Table 32. Information elements in InviteUserRequest Primitive

12.2.7 The “InviteUserResponse” Primitive

The `InviteUserResponse` primitive allows the requestor server, representing the invited users, to return the result of the invitation to the provider server.

Information Element	Req	Type	Description
Message-Type	M	InviteUserResponse	Message identifier
Status-Info	M	Structure of Status-Primitive	The status information (see 8.2).
Invite-ID	M	String	Identifies this invitation.
Inviting-User	M	Structure	Identifies the requesting user who sends the invitation (User-ID, Screen-Name)
Invite-Acceptance	M	Boolean	Indicates if the user accepts the invitation or not.
Responding-User	M	Structure	Identifies the responding invited user (User-ID and / or Screen-Name). If Invite-Type was GM, identifies the group

			ID.
Invite-Response	O	String	Textual description, why the invited user accepted/rejected the invitation.

Table 33. Information elements in InviteUserResponse Primitive

Each tuple { Invite-Acceptance, Responding-User, Invite-Response } represents the response from one invitee. There may be multiple tuples { Invite-Acceptance, Responding-User, Invite-Response } in one "InviteUserResponse" primitive if the requestor server, which represents the invited users, is able to collect the response from the invited users in a reasonable time and combine the multiple responses in one primitive in order to reduce the traffic overhead between the servers.

12.2.8 The "CancelInviteRequest" Primitive

The `CancelInviteRequest` primitive allows the user in the requestor server to cancel its previous invitation.

Information Element	Req	Type	Description
Message-Type	M	CancelInviteRequest	Message identifier
Meta-Information	M	Structure of Meta-Information	The meta-information (see 8.1).
Invite-ID	M	String	Identifies the invitation.
Canceling-User	M	Structure	Identifies the requesting user who cancels the invitation (User-ID and / or Screen-Name)
Canceled-User	M	Structure	Identifies the user(s) to whom the invitation will be canceled (User-ID and / or Screen-Name, or Contact-List-ID)
Canceled-Content-ID-List	C	Structure	Identifies the related shared content as a list of URLs which will be canceled.
Cancel-Reason	O	String	Textual description of the cancel.

Table 34. Information elements in CancelInviteRequest Primitive

12.2.9 The "CancelInviteUserRequest" Primitive

The `CancelInviteUserRequest` primitive allows the provider server to cancel its previous invitation to the users in the requestor server.

Information Element	Req	Type	Description
Message-Type	M	CancelInviteUserRequest	Message identifier
Meta-Information	M	Structure of Meta-Information	The meta-information (see 8.1).
Invite-ID	M	String	Identifies the invitation.
Canceling-User	M	Structure	Identifies the requesting user who cancels the invitation (User-ID and / or Screen-Name)
Canceled-User	C	Structure	Identifies the user(s) to whom the invitation will be canceled (User-ID and / or Screen-Name, or List-of-User-

			IDs). Not present if the invitation was to a group membership
Canceled-Content-ID-List	C	Structure	Identifies the related shared content as a list of URLs which will be canceled.
Cancel-Reason	O	String	Textual description of the cancel.

Table 35. Information elements in CancelInviteUserRequest Primitive

12.2.10 The "VerifyIDRequest" Primitive

The `VerfiyIDRequest` primitive allows the requestor server to verify that userid(s) are valid in the provider server.

Information Element	Req	Type	Description
Message-Type	M	VeifyIDRequest	Message identifier
Meta-Information	M	Structure of Meta-Information	The meta-information (see 8.1).
WV-ID-List	M	Structure	The list contains the WV-ID'sto be verified, and optionally the time when the WV ID was created

Table 36. Information elements in VerfifyIDRequest Primitive

12.2.11 The "VerifyIDResponse" Primitive

The `VerifyIDResponse` primitive allows the provider server to return the result of the verification, and the list of valid WV IDs along with the time when the valid WV ID was created.

Information Element	Req	Type	Description
Message-Type	M	VerifyUseridResponse	Message identifier.
Status-Info	M	Structure of Status-Primitive	The status information (see 8.2).
WV-ID-List	M	Structure	The list contains the valid WV Ids along with the time when the valid WV ID was created.

Table 37. Information elements in VerifyIDResponse Primitive

12.2.12The "GetReactiveAuthStatusRequest" Primitive

The "*GetReactiveAuthStatusRequest*" primitive is used for the requestor server to retrieve the current status of reactive authorizations.

Information Element	Req	Type	Description
Message-Type	M	CancelAuthRequest	Message identifier
Meta-Information	M	Structure of Meta-Information	The meta-information (see 5.1).
User-ID-List	O	Structure	Identifies the user(s) to retrieve the reactive authorization status for.

Table x. Information elements in CancelAuthRequest Primitive

12.2.13 The "GetReactiveAuthStatusResponse" Primitive

The "*GetReactiveAuthStatusResponse*"primitive is used for the provider server to send the current reactive authorization status to the requestor server.

Information Element	Req	Type	Description
Message-Type	M	CancelAuthRequest	Message identifier
Meta-Information	M	Structure of Meta-Information	The meta-information (see 5.1).
ReactiveAuthStatus-List	M	Structure	List of users and presence attributes and corresponding state of the reactive authorization function.

Table x. Information elements in CancelAuthRequest Primitive

12.3 Transactions

12.3.1 The "GeneralSearch" Transaction

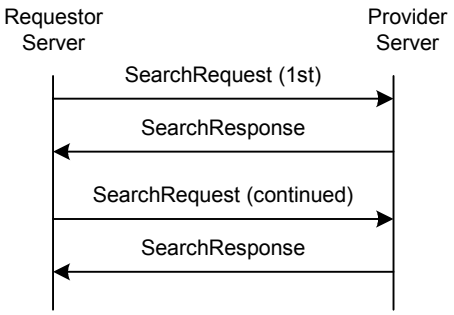

Figure 21. The "GeneralSearch" Transaction

The requestor server sends the `SearchRequest` message to the provider server including the **Search-Pair-List**, the **Search-Online-Status** (T-Online, F-Offline, N/A-both), the type of the search and the **Search-Limit** (maximum number of results at a time). The provider server responds with the `SearchResponse` message, which includes the Status of the search. If the search is successful, it includes the **Search-ID**, the **Search-Index** (a continuation index to indicate where the search should be continued), the **Search-Findings** (the number of items found that match the criteria so far), and the **Search-Results** (the actual data).

The requestor server may continue the search. In this case the `SearchRequest` message includes only the Search-ID and the Search-Index. The provider server responds with the `SearchResponse`, but the message includes only the **Result**, the Search-Index, the Search-Findings and the Search-Results.

The requestor server may modify the Search-Index value, so that the search may be continued at a different place. The Search-Index is valid until a new search is performed or the session ends (a previous search is invalidated when a new search is started).

Primitive	Direction
SearchRequest	Requestor Server → Provider Server
SearchResponse	Requestor Server ← Provider Server

Table 38. Primitive Directions for GeneralSearch Transaction

12.3.2 The "StopSearch" Transaction

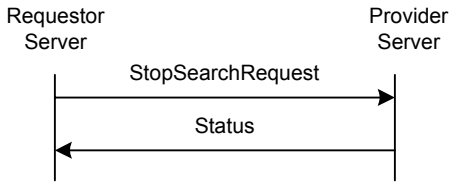

Figure 22. The "StopSearch" Transaction

The "**StopSearch**" transaction allows the requestor server to indicate to the provider server that the search and / or the results are not needed from a previously issued search request. The requestor server sends the `StopSearchRequest` message to the provider server including the Search-ID. The provider server invalidates the indicated search, and replies with a Status message. The invalidated Search-ID cannot be used after invalidation.

Primitive	Direction
StopSearchRequest	Requestor Server → Provider Server
Status	Requestor Server ← Provider Server

Table 39. Primitive Directions for StopSearch Transaction

12.3.3 The "Invitation" Transaction

A user may invite other user(s) to join a discussion / chat group, or to exchange messages, or to share presence values list, or to share content.

There are two service models with corresponding transaction flows.

12.3.3.1 Basic Invitation transaction

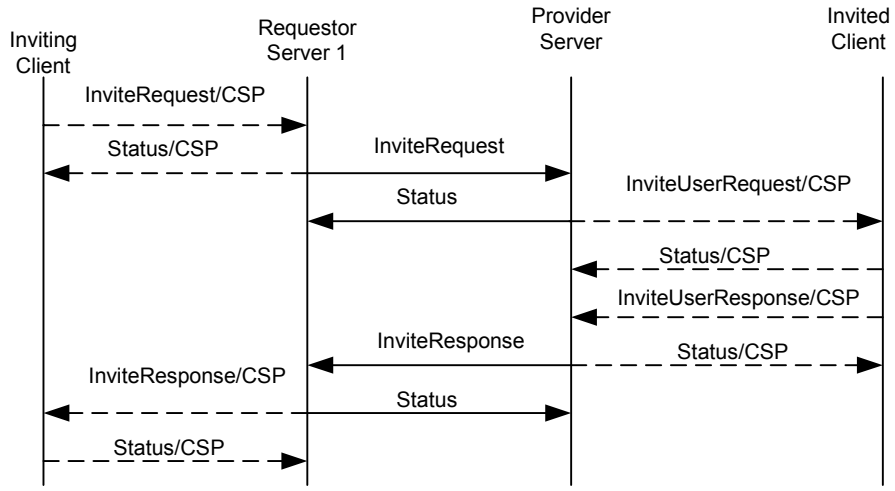

Figure 23. The "Basic Invitation" Transaction

The requestor server 1 is the Home Domain of the inviting user, the provider server is the Home Domain of the invited user.

Primitive	Direction
InviteRequest	Requestor Server 1 → Provider Server
Status	Requestor Server 1 ← Provider Server
InviteResponse	Requestor Server 1 ← Provider Server
Status	Requestor Server 1 → Provider Server

Table 40. Primitive Directions for Basic Invitation Transaction

12.3.3.2 Complementary Invitation transaction

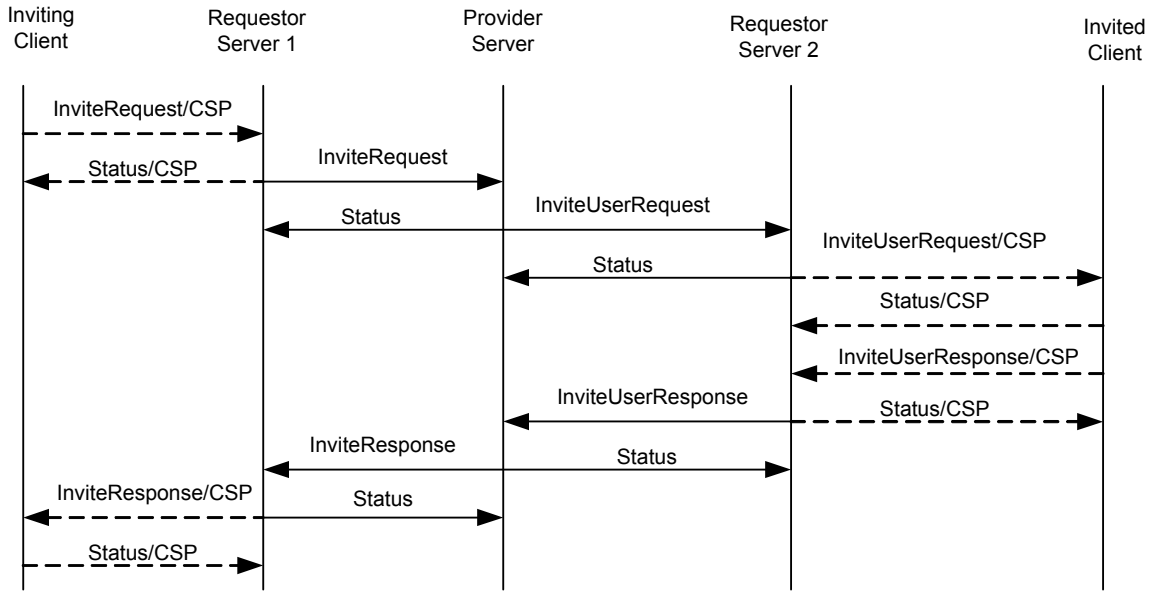

Figure 24. The "Complementary Invitation" Transaction

In this service model the requestor server 1 is the Home Domain of the inviting user, the provider server is the PSE of the invited user in another Domain, and the requestor server 2 is the Home Domain of the invited user. The transaction flow is as follows.

Primitive	Direction
InviteRequest	Requestor Server 1 → Provider Server
Status	Requestor Server 1 ← Provider Server
InviteUserRequest	Provider Server → Requestor Server 2
Status	Provider Server ← Requestor Server 2
InviteUserResponse	Provider Server ← Requestor Server 2
Status	Provider Server → Requestor Server 2
InviteResponse	Requestor Server 1 ← Provider Server
Status	Requestor Server 1 → Provider Server

Table 41. Primitive Directions for Complementary Invitation transaction

The general description of the transactions

The requestor server 1, which represents the inviting user, sends the provider server the `InviteRequest` message with the ID of the invitation, the invitation type, the inviting User-ID and/or Screen-Name, the list of user(s) to be invited specified by User-IDs and/or Screen-Names, the ID of the subject, and optionally the reason for the invitation (a short text).

The provider server responds to the requestor server 1 with a `Status` message. The provider server also sends `InviteUserRequest` message to every requestor server 2, which represents one or several of the invited users. The `InviteUserRequest` message contains the ID of the invitation, the invitation type, the inviting User-ID and/or Screen-Name, the list of user(s) to be invited specified by User-IDs and/or Screen-Names, the ID of the subject, and optionally the reason for the invitation (a short text).

Each requestor server 2 responds to the provider server with a `Status` message.

The invited user may accept or reject the invitation, and the requestor server 2, which represents the invited users, responds to the provider server with the `InviteUserResponse` message with the ID of the invitation, the acceptance indicator, the User-ID and/or Screen-Name of the responding invited user, and optionally the short response text.

The provider server responds to the requestor server 2 with a Status message. The provider server will send the `InviteResponse` message to the requestor server 1, which represents the inviting user. The `InviteResponse` message contains the ID of the invitation, the acceptance indicator, the User-ID and/or Screen-Name of the responding invited user, and optionally the short response text.

The requestor server 1 responds to the provider server with a `Status` message.

Each tuple { Invite-Acceptance, Responding-User, Invite-Response } represents the response from one invitee. There may be multiple tuples { Invite-Acceptance, Responding-User, Invite-Response } in one `InviteUserResponse` or `InviteResponse` primitive if the requestor server 2 or the provider server is able to collect the responses from the invited users in a reasonable time and combine the multiple responses in one primitive in order to reduce the traffic overhead between the servers.

While in general there is no mandatory requirement about how an invited user shall act according to the acceptance indicator within its response in the scope of this function, it is recommended that the invited user should act consistently in accordance with its response.

The subject of the invitation may be a group, messaging, a shared content, or presence. In case of presence the user may include a list of presence attributes that he/she is willing to share with the other party. Note that there is no actual presence

attribute sharing that has been done, the transaction is only informational. Similarly, in case of group, messaging, or shared content invitations the actual action is not taken, it is up to the user to share presence attributes manually (the invitation is only informational).

12.3.4 The "CancelInvitation" Transaction

A user may cancel any previous invitations.

12.3.4.1 Basic Cancel Invitation transaction

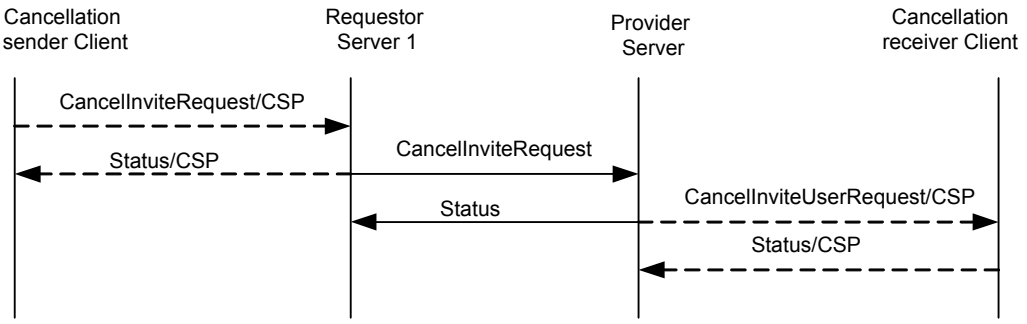

Figure 25. The "Basic CancelInvitation" Transaction

The requestor server 1 is the Home Domain of the invitation canceling user, the provider server is the Home Domain of the invitation cancellation receiver user.

Primitive	Direction
CancelInviteRequest	Requestor Server 1 → Provider Server
Status	Requestor Server 1 ← Provider Server

Table 42. Primitive Directions for Basic CancelInvitation Transaction

12.3.4.2 Complementary Cancel Invitation transaction

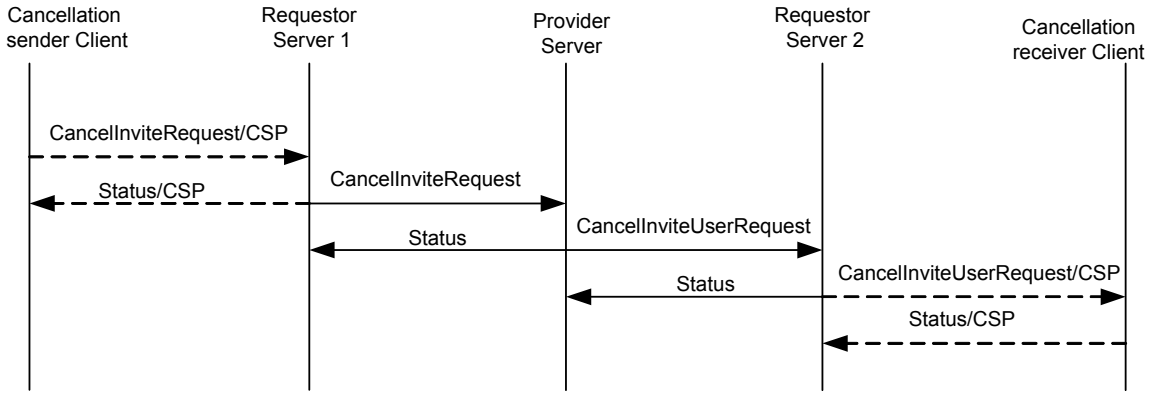

Figure 26. The "Complementary CancelInvitation" Transaction

In this service model the requestor server 1 is the Home Domain of the invitation canceling user, the provider server is the PSE of the invitation cancellation recipient in another Domain, and the requestor server 2 is the Home Domain of the invitation cancellation recipient. The transaction flow is as follows.

Primitive	Direction
CancelInviteRequest	Requestor Server 1 → Provider Server

Status	Requestor Server 1 ← Provider Server
CancelInviteUserRequest	Provider Server → Requestor Server 2
Status	Provider Server ← Requestor Server 2

Table 43. Primitive Directions for Complementary CancelInvitation Transaction

The general description of the transactions

The requestor server 1, which represents the inviting user, sends the provider server the `CancelnviteRequest` message with the ID of the invitation, the inviting User-ID and/or Screen-Name, the list of user(s) to be notified about the cancellation specified by User-IDs and/or Screen-Names, and optionally the reason for the cancellation (a short text).

The provider server responds to the requestor server 1 with a `Status` message. The provider server also sends `CancelnviteUserRequest` message to every requestor server 2, which represents one or several of the invited users. The `CancelnviteUserRequest` message contains the ID of the invitation, the inviting User-ID and/or Screen-Name, the list of user(s) to be notified about the cancellation specified by User-IDs and/or Screen-Names, and optionally the reason for the invitation (a short text).

The requestor server 2, which represents the canceled users, responds to the provider server with the Status message.

Note that the "CancelInvitation" transaction makes sense only for the scope of presence sharing and content sharing invitations.

12.3.5 The "VerifyID" Transaction

Figure 27. The "VerifyWVID" Transaction

The "VerifyWVIDUserid" transaction is used by the requestor server to verify that a list of WV IDsUser-ID is in use are valid at the provider server, i.e. the Home Domain of the WV User-IDs. The transaction is used before the WV IDUser-ID is stored in the requestor sever to ensure that all locally stored WV IDsUser-ID's are valid. The VerifyWVIDUserid response contains the result of the verification, and a list of WV IDs along withsubset of User-ID'(s) in use and the time when the valid WV User-ID was created. The time information is used to verify that the locally stored WV User-ID belongs to the same end-user on both the requestor and provider server or if it has been recycled on the provider side and given to a new end-user. If the time is not present in the request it is assumed that the requestor server just want to verify if the WV that the User-IDs isare validin use.

Primitive	Direction
VerifyIDRequest	Requestor Server → Provider Server
VerifyIDResponse	Requestor Server ← Provider Server

Table 44. Primitive Directions for the VerifyUserid Transaction

12.3.9 The "GetReactiveAuthStatus" Transaction

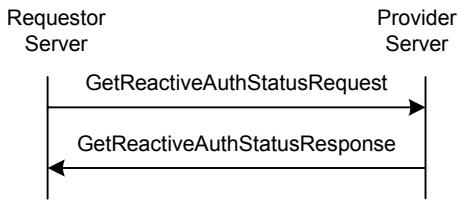

Figure 28. The "GetReactiveAuthStatus" Transaction

The purpose of the "*GetReactiveAuthStatus*" transaction is for the requestor server to retrieve the status of the reactive authorization function for a particular user.

The requestor server sends a "*GetReactiveAuthStatusRequest*" to the provider server for the reactive authorization status of the publishing users. A "*GetReactiveAuthStatusResponse*" message from the provider server will contain the current status of the reactive authorization function.

Primitive	Direction
GetReactiveAuthStatusRequest	Requestor Server → Provider Server
GetReactiveAuthStatusResponse	Requestor Server ← Provider Server

Table 45. Primitive Directions for GetReactiveAuthStatus Transaction

12.4 Status Code

12.4.1 "GeneralSearch" Transaction

- `Unable to parse criteria. (Invalid Search-Element) (402)`
- `Initial search request was not sent (Invalid Search-ID) (424).`
- `Invalid Search-Index (out of range) (425)`
- `Search timeout (in case of continued search the subsequent request primitive is late). (535)`
- `Server search limit is exceeded (610)`
- `Too many hits (536)`
- `Too broad search criteria (537)`

12.4.2 "StopSearch" Transaction

- `Service Not Supported (405)`
- `Invalid Search-ID (424)`

12.4.3 "Invitation" Transaction

- `Invalid invitation type(402).`

- Unknown user (ID or screen-name) (531).
- Group does not exist (800).
- Invalid invite-ID. (423)
- Delivery to recipient not available. (410)
- Delivery to recipient domain not available. (516)
- Recipient unknown (Contact list). (700)
- Invalid or unsupported presence value. (751)

12.4.4 “CancelInvitation” Transaction

- Invalid invitation type (402).
- Invalid invitation ID (423).
- Unknown user (ID or screen-name) (531).
- Delivery to recipient not available. (410)
- Delivery to recipient domain not available. (516)
- Recipient unknown (Contact list). (700)
-

12.4.5 VerifyWVID” Transaction

- Domain not found (404).
- Service Not Supported (405)
- Unknown user (531).
- Contact list does not exist (700).
- Group does not exist (800).
- General address error (901)

13.Service Relay – Contact List Features

13.1 Overview

A "***contact list***" is a list created and maintained by a User so that the User may send messages to the "*contact list*" as a recipient. The message will be delivered to every member in the particular "*contact list*". However, except the owner User, the other members of the "c*ontact list*" do not have any knowledge about the "contact list". Nor do the members of the list conduct any group functions.

In concept, the "*contact list*" is a special case and subset of Private Group, and is also a special case of Restricted Group. In practice, the "*contact list*" has two cases:

Address book – the "*contact list*" contains a list of addresses, nicknames, and other relevant information of family members, friends, colleagues or other frequently contacted persons.

Presence – the "*contact list*" is closely tied to the presence service. It allows proactive presence authorization (the people on the list can get these presence attributes), and presence update (presence attributes of the people on the list).

A user may have any number of contact lists, thus the contact lists has their own IDs. The users do not know about (and cannot access) each other's contact list(s).

There are two properties for Contact List:

Display-Name: a free text string given by user that can be presented in the user interface of the client.

Default: a Boolean set by user that indicates that the particular contact list is the default contact list.

When the user creates his/her first contact list, the server automatically sets that contact list as the default. The server may also create the first list automatically.

When the user has more than one contact lists in the system, the user may set any of his/her contact lists as the default contact list. When the user sets "Default" property of a contact list to "True", the "Default" property of the previously default contact list must be automatically set to "False" by the server.

Watchers list is a system defined contact list with the functionality limited to holding 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. 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.

The server shall maintain one Watcher List for each user.

This chapter focuses on the functional relay of Contact List features. Because of the server interoperation nature, the SSP has its own requirements on meta-information and information elements in the primitives at the transaction level. The complete primitives and transaction flows of Contact List features at SSP semantics level have been defined in the following two sections.

Please refer to the CSP document understand how to relay the Contact List features from client-server interaction (CSP) to server-server interoperation (SSP).

The transactions below belong to the complementary service.

13.2 Primitives

13.2.1 The "CreateContactListRequest" Primitive

The `CreateContactListRequest` primitive is used to create a contact list.

In addition to the "Contact-List-ID" which identifies the contact list, the `CreateContactListRequest` primitive contains the initial properties (Display-Name, Default) and a "User-List" which identifies the initial users to be added to the contact list (User-ID, Nickname).

Information Element	Req	Type	Description
Message-Type	M	CreateContactListRequest	Message identifier
Meta-Information	M	Structure of Meta-Information	The meta-information (see 8.1).
Contact-List-ID	M	String	Identifies the contact list.
Contact-List-Props	O	Structure	The initial properties of the contact list (Display-Name, Default).
User-List	O	Structure	Identifies the initial users to be added to the contact list (User-ID, Nickname).

Table 46. Information elements in CreateContactListRequest Primitive

13.2.2 The "DeleteContactListRequest" Primitive

The `DeleteContactListRequest` primitive is used to delete the contact list(s).

Information Element	Req	Type	Description
Message-Type	M	DeleteContactListRequest	Message identifier
Meta-Information	M	Structure of Meta-Information	The meta-information (see 8.1).
Contact-List-ID-List	M	Structure	Identifies the contact list(s).

Table 47. Information elements in DeleteContactListRequest Primitive

13.2.3 The "GetContactListRequest" Primitive

The `GetContactListRequest` primitive allows a user in the requestor server to retrieve the list of all Contact-List-IDs.

Information Element	Req	Type	Description
Message-Type	M	GetContactListRequest	Message identifier
Meta-Information	M	Structure of Meta-Information	The meta-information (see 8.1).

Table 48. Information elements in GetContactListRequest Primitive

13.2.4 The "GetContactListResponse" Primitive

The `GetContactListResponse` primitive returns a list of all Contact-List-IDs.

Information Element	Req	Type	Description
Message-Type	M	GetContactListResponse	Message identifier

Status-Info	M	Structure of Status-Primitive	The status information (see 8.2).
Contact-List-ID-List	C	Structure	The list of the Contact-List-IDs.
Default-C-List-ID	C	String	Identifies the default contact list.

Table 49. Information elements in GetContactListResponse Primitive

13.2.5 The "GetListMemberRequest" Primitive

The `GetListMemberRequest` primitive is used to retrieve the all members of a contact list.

Information Element	Req	Type	Description
Message-Type	M	GetListMemberRequest	Message identifier
Meta-Information	M	Structure of Meta-Information	The meta-information (see 8.1).
Contact-List-ID	M	String	Identifies the contact list.

Table 50. Information elements in GetListMemberRequest Primitive

13.2.6 The "AddListMemberRequest" Primitive

The `AddListMemberRequest` primitive is used to add the members to a contact list.

Information Element	Req	Type	Description
Message-Type	M	AddListMemberRequest	Message identifier
Meta-Information	M	Structure of Meta-Information	The meta-information (see 8.1).
Contact-List-ID	M	String	Identifies the contact list.
User-List	M	Structure	Identifies the users to be added to the contact list (User-ID, Nickname).

Table 51. Information elements in AddListMemberRequest Primitive

13.2.7 The "RemoveListMemberRequest" Primitive

The `RemoveListMemberRequest` primitive is used to remove members from the contact list.

Information Element	Req	Type	Description
Message-Type	M	RemoveListMemberRequest	Message identifier
Meta-Information	M	Structure of Meta-Information	The meta-information (see 8.1).
Contact-List-ID	M	String	Identifies the contact list.
User-List	M	Structure	Identifies the users to be removed from the contact list (User-ID, Nickname).

Table 52. Information elements in RemoveListMemberRequest Primitive

13.2.8 The "ContactListMemberResponse" Primitive

The `ContactListMemberResponse` primitive returns a list of all members in the contact list.

Information Element	Req	Type	Description
Message-Type	M	ContactListMemberResponse	Message identifier
Status-Info	M	Structure of Status-Primitive	Status information (see 8.2).
User-List	M	Structure	Identifies the users in the contact list (User-ID, Nickname).

Table 53. Information elements in ContactListMemberResponse Primitive

13.2.9 The "GetListPropsRequest" Primitive

The `GetListPropRequest` primitive is used to retrieve the properties of a contact list.

Information Element	Req	Type	Description
Message-Type	M	GetListPropsRequest	Message identifier
Meta-Information	M	Structure of Meta-Information	The meta-information (see 8.1).
Contact-List-ID	M	String	Identifies the contact list.

Table 54. Information elements in GetListPropsRequest Primitive

13.2.10 The "SetListPropsRequest" Primitive

The `SetListPropRequest` primitive is used to set the properties of a contact list.

Information Element	Req	Type	Description
Message-Type	M	SetListPropsRequest	Message identifier
Meta-Information	M	Structure of Meta-Information	The meta-information (see 8.1).
Contact-List-ID	M	String	Identifies the contact list.
Contact-List-Props	M	Structure	The properties (Display-Name, Default) to be set.

Table 55. Information elements in SetListPropsRequest Primitive

13.2.11 The "ContactListPropsResponse" Primitive

The `ContactListPropsResponse` primitive returns a list of all members in a contact list.

Information Element	Req	Type	Description
Message-Type	M	ContactListPropsResponse	Message identifier
Status-Info	M	Structure of Status-Primitive	Status information (see 8.2).
Contact-List-Props	M	Structure	The properties of the contact list (Display-Name, Default).

Table 56. Information elements in ContactListPropsResponse Primitive

13.2.12 The "CreateAttrListRequest" Primitive

The `CreateAttrListRequest` primitive is used to create an attribute list, and attach the attribute list to some contact list(s) and / or user(s).

Information Element	Req	Type	Description
Message-Type	M	CreateAttrListRequest	Message identifier
Meta-Information	M	Structure of Meta-Information	The meta-information (see 8.1).
Presence-Attribute-List	M	Structure	A list of presence attributes.
Default-List	M	"Yes" | "No"	Indicates if the attributes are targeted to the default attribute list instead of a separate attribute list.
Contact-List-ID-List	C	Structure	Contact list(s) which the attribute list should be attached to.
User-ID-List	C	Structure	User(s) which the attribute list should be attached to.

Table 57. Information elements in CreateAttrListRequest Primitive

13.2.13 The "DeleteAttrListRequest" Primitive

The `DeleteAttrListRequest` primitive is used to delete an attribute list(s).

Information Element	Req	Type	Description
Message-Type	M	DeleteAttrListRequest	Message identifier
Meta-Information	M	Structure of Meta-Information	The meta-information (see 8.1).
Default-List	M	"Yes" | "No"	Indicates if the default attribute list should be cleared.
Contact-List-ID-List	C	Structure	Identifies the contact list(s) to remove the attribute list association
User-ID-List	C	Structure	Identifies the user(s) to remove the attribute list association

Table 58. Information elements in DeleteAttrListRequest Primitive

13.2.14 The "GetAttrListRequest" Primitive

The `GeAttrListRequest` primitive is used to retrieve the published or subscribed attributes associated with specific contact list(s) and / or user(s). If the user(s) or contact list(s) are not specified, the response shall include all user-specific and contact list-specific attributes.

Information Element	Req	Type	Description
Message-Type	M	GetAttrListRequest	Message identifier
Meta-Information	M	Structure of Meta-Information	The meta-information (see 8.1).
Default-List	M	"Yes" | "No"	Indicates if the default attribute list should be retrieved ("YES") or not.

Contact-List-ID-List	O	Structure	Identifies the contact list(s) to retrieve the attribute list association
User-ID-List	O	Structure	Identifies the user(s) to retrieve the attribute list association

Table 59. Information elements in GetAttrListRequest Primitive

13.2.15 The "GetAttrListResponse" Primitive

The `GetAttrListResponse` primitive returns the presence attributes.

Information Element	Req	Type	Description
Message-Type	M	GetAttrListResponse	Message identifier
Status-Info	M	Structure of Status-Primitive	The status information (see 8.2).
Attribute-Association-List	O	Structure	A list of attribute list associations with the user and / or the contact list.
Default-Association-List	O	Structure	The list of presence attributes associated with the default list.

Table 60. Information elements in GetAttrListResponse Primitive

13.3 Transactions

13.3.1 The "CreateContactList" Transaction

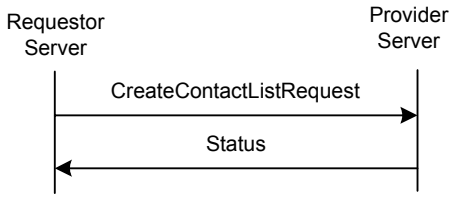

Figure 29. The "CreateContactList" Transaction

The requestor server sends a `CreateContactListRequest` to the provider server. The provider server shall create the contact list and respond with a `Status` message to the requestor server.

A user is able to create more than one contact list. There may be system specific limitations for the maximum number of lists per user. After a contact list is created, a user may create an attribute list for the contact list.

Primitive	Direction
CreateContactListRequest	Requestor Server → Provider Server
Status	Requestor Server ← Provider Server

Table 61. Primitive Directions for CreateContactList Transaction

13.3.2 The "DeleteContactList" Transaction

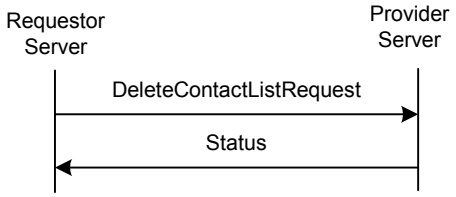

Figure 30. The "DeleteContactList" Transaction

The requestor server sends a `DeleteContactListRequest` to the provider server. The provider server shall delete the contact lists(s) and respond with a `Status`. The server should not unsubscribe the members implicitly; if a contact list that has been subscribed to is deleted, the presence subscriptions should not be cancelled for the particular users.

A user may delete more than one contact list in one transaction.

Primitive	Direction
DeleteContactListRequest	Requestor Server → Provider Server
Status	Requestor Server ← Provider Server

Table 62. Primitive Directions for DeleteContactList Transaction

13.3.3 The "GetContactList" Transaction

Figure 31. The "GetContactList" Transaction

The "**GetContactList**" transaction allows the requestor server to retrieve the list of all Contact-List-IDs of the user. The requestor server sends a `GetContactListRequest` request. The provider server returns a `GetContactListResponse` primitive with a list of all Contact-List-ID's and the default contact list ID of the user.

Primitive	Direction
GetContactListRequest	Requestor Server → Provider Server
GetContactListResponse	Requestor Server ← Provider Server

Table 63. Primitive Directions for GetContactList Transaction

13.3.4 The "GetListMember" Transaction

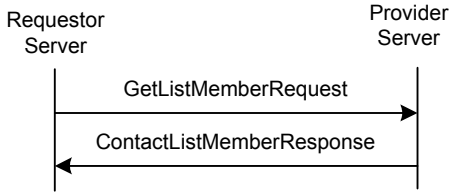

Figure 32. The "GetListMember" Transaction

The "**GetListMember**" transaction is used to retrieve all members of a contact list. The requestor server sends a `GetListMemberRequest` to the provider server. The provider responds to the requestor server with a `ContactListMemberResponse` containing the list of all members of the contact list.

Primitive	Direction
GetListMemberRequest	Requestor Server → Provider Server
ContactListMemberResponse	Requestor Server ← Provider Server

Table 64. Primitive Directions for GetListMember Transaction

13.3.5 The "AddListMember" Transaction

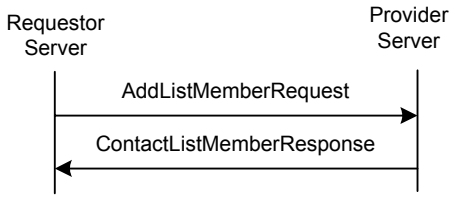

Figure 33. The "AddListMember" Transaction

The requestor server sends an `AddListMemberRequest` to the provider server to add one or more members in a contact list. The provider server shall respond to the requestor server with a `ContactListMemberResponse` containing the list of all members of the contact list.

Primitive	Direction
AddListMemberRequest	Requestor Server → Provider Server
ContactListMemberResponse	Requestor Server ← Provider Server

Table 65. Primitive Directions for AddListMember Transaction

13.3.6 The "RemoveListMember" Transaction

Figure 34. The "RemoveListMember" Transaction

The requestor server sends a `RemoveListMemberRequest` to the provider server. The provider server shall delete the specified user(s) from the specified contact list, and return a list of all members of the contact list in the `ContactListMemberResponse`.

Primitive	Direction
RemoveListMemberRequest	Requestor Server → Provider Server
ContactListMemberResponse	Requestor Server ← Provider Server

Table 66. Primitive Directions for RemoveListMember Transaction

13.3.7 The "GetListProperties" Transaction

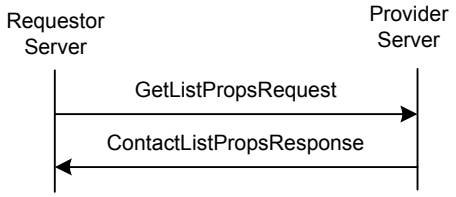

Figure 35. The "GetListProperties" Transaction

The "**GetListProperties**" transaction is used to retrieve the properties of a contact list (Display-Name, Default). The requestor server sends a `GetListPropsRequest` to the provider server. The provider responds with a `ContactListPropsResponse` to the requestor server containing the properties.

Primitive	Direction
GetListPropsRequest	Requestor Server → Provider Server
ContactListPropsResponse	Requestor Server ← Provider Server

Table 67. Primitive Directions for GetListProperties Transaction

13.3.8 The "SetListProperties" Transaction

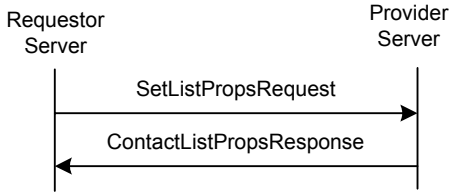

Figure 36. The "SetListProperties" Transaction

The "**SetListProperties**" transaction is used to set the properties of a contact list (Display-Name, Default), i.e. to set the display name, or to set a default contact list. The requestor server sends a `SetListPropsRequest` to the provider server. The provider responds with a `ContactListPropsResponse` to the requestor server containing the new properties.

Primitive	Direction
SetListPropsRequest	Requestor Server → Provider Server
ContactListPropsResponse	Requestor Server ← Provider Server

Table 68. Primitive Directions for SetListProperties Transaction

13.3.9 The "CreateAttributeList" Transaction

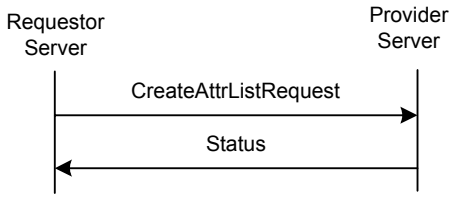

Figure 37. The "CreateAttributeList" Transaction

A user may create a specific attribute list for a contact list, or a member in a contact list through "**CreateAttributeList**" transaction. The requestor server sends a `CreateAttrListRequest` to the provider server. The provider server shall create an attribute list, and attach the attribute list to specified contact list(s) and / or user(s).

In order to modify an attribute list, it can be overwritten by creating a new one for the same user or contact list. (It is not necessary to delete it first.)

Primitive	Direction
CreateAttrListRequest	Requestor Server → Provider Server
Status	Requestor Server ← Provider Server

Table 69. Primitive Directions for CreateAttributeList Transaction

13.3.10 The "DeleteAttrList" Transaction

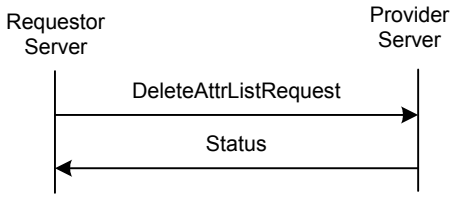

Figure 38. The "DeleteAttrList" Transaction

A user may delete an attribute list from a user and / or a contact list through "**DeleteAttrList**" transaction. The requestor server sends a `DeleteAttrListRequest` to the provider server. The provider server shall remove the associations of the attribute lists with the contact list(s) and / or user(s). If an attribute list is not associated with any contact list or user, it shall be cleared from the provider server (garbage collection).

Primitive	Direction
DeleteAttrListRequest	Requestor Server → Provider Server
Status	Requestor Server ← Provider Server

Table 70. Primitive Directions for DeleteAttrList Transaction

13.3.11 The "GetAttrList" Transaction

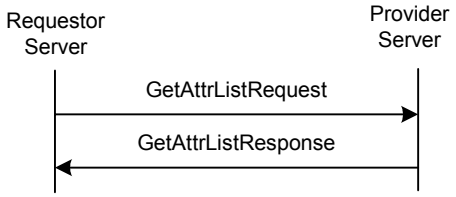

Figure 39. The "GetAttrList" Transaction

The "**GetAttrList**" transaction is used to retrieve the published or subscribed attributes associated with specific contact list(s) and / or user(s). The provider server returns the requested attributes. If the user(s) or contact list(s) are not specified in the request, the response shall include all user-specific and contact list-specific attributes.

Primitive	Direction
GetAttrListRequest	Requestor Server → Provider Server
GetAttrListResponse	Requestor Server ← Provider Server

Table 71. Primitive Directions for GetAttrList Transaction

13.4 Status Code

13.4.1 Contact List Transactions

- Unknown user ID (531)
- Contact list does not exist (700)
- Contact list already exists (701)
- Invalid or unsupported contact list property. (752)

13.4.2 Attribute List Transactions

- Unknown user ID (531)
- Contact list does not exist (700).
- Unknown presence attribute (not defined in [PA]) (750).

14.Service Relay – Presence Features

14.1 Overview

This chapter focuses on the functional relay of Presence features. Because of the server interoperation nature, the SSP has its own requirements on meta-information and information elements in the primitives at transaction level. The complete primitives and transaction flows of Presence features at SSP semantics level have been defined in the following two sections.

Please refer to the CSP document to understand how to relay the Presence features from client-server interaction (CSP) to server-server interoperation (SSP).

14.2 Primitives

14.2.1 The "SubscribeRequest" Primitive

The `SubscribeRequest` primitive is used to create subscriptions to obtain notifications about changes of the PRESENCE INFORMATION and attributes of other PRINCIPALS. The scope of subscription is either a single user or a contact list that refers to a list of users. If the requesting client subscribes to a contact list, the requesting client may request the server to automatically subscribe to the presence attributes when a new user is added to this contact list, and automatically unsubscribe to the presence attributes when the contact list is deleted or when a user is removed from the contact list. Note that the automatic subscription / unsubscription is merely a characteristics of the subscription / unsubscription itself.

Information Element	Req	Type	Description
Message-Type	M	SubscribeRequest	Message identifier
Meta-Information	M	Structure of Meta-Information	The meta-information (see 8.1).
User-ID-List	C	Structure	Identifies the IM users to be subscribed.
Contact-List-ID-List	C	Structure	Identifies the set of users.
Presence-Attribute-List	O	Structure	A list of presence attributes to which are subscribed. An empty list or missing list indicates all presence attributes are desired.
Auto-Subscribe	M	Boolean	'Yes' means that the automatic subscription to the presence attributes is enabled when a new user is added to the contact list, and the automatic unsubscription to the presence attributes is also enabled when the contact list is deleted or when a user is removed from the contact list. 'No' means that the automatic subscription / unsubscription is disabled.

Table 72. Information elements in SubscribeRequest Primitive

14.2.2 The "AuthorizationRequest" Primitive

The `AuthorizationRequest` primitive allows the provider server to perform the reactive authorization with the requestor server that represents the publishing users.

Information Element	Req	Type	Description
Message-Type	M	AuthorizationRequest	Message identifier
Meta-Information	M	Structure of Meta-Information	The meta-information (see 8.1).

Authorizing-User-ID	M	String	Identifies the user who can grant the authorization to the requesting users.
List-of-Subscribing-User-ID-and-Presence-Attribute-List	M	Structure	A list of elements in which each node specifies the user-ID and the presence attributes subscribed to. An empty attribute list indicates that all presence attributes are desired.

Table 73. Information elements in AuthorizationRequest Primitive

There may be multiple tuples { Authorizing-User-ID, List-of-Subscribing-User-ID-and-Presence-Attribute-List } in one `AuthorizationRequest` primitive if the provider server is able to combine the multiple reactive authorizations in one primitive in order to reduce the traffic overhead between the servers.

14.2.3 The "AuthorizationResponse" Primitive

The `AuthorizationResponse` primitive returns the authorization result from the responding authorizing users.

There may be multiple tuples { Authorizing-User-ID, Subscribing-User-IDs, Authorization-Result } in one `AuthorizationResponse` primitive if the provider server is able to collect the responses from the authorizing users in a reasonable time and combine the multiple responses in one primitive in order to reduce the traffic overhead between the servers.

Information Element	Req	Type	Description
Message-Type	M	AuthorizationResponse	Message identifier
Meta-Information	M	Structure of Meta-Information	The meta-information (see 8.1).
Authorizing-User-ID	M	String	Identifies the user who can grant the authorization to the requesting users.
Subscribing-User-ID-List	M	Structure	Identifies the requesting users who want to subscribe
Authorization-Result(s)	M	Structure	Authorization results from the authorizing user per subscribing user.

Table 74. Information elements in AuthorizationResponse Primitive

14.2.4 The "UnsubscribeRequest" Primitive

The `UnsubscribeRequest` primitive is used to cancel the current subscription.

Information Element	Req	Type	Description
Message-Type	M	UnsubscribeRequest	Message identifier
Meta-Information	M	Structure of Meta-Information	The meta-information (see 8.1).
User-ID-List	C	Structure	Identifies the IM users to be unsubscribed.
Contact-List-ID-List	C	Structure	Identifies the set of users.

Table 75. Information elements in UnsubscribeRequest Primitive

14.2.5 The "PresenceNotification" Primitive

The `PresenceNotification` primitive allows the provider server to send the notifications about changes of presence information to the requestor server.

Information Element	Req	Type	Description
Message-Type	M	PresenceNotification	Message identifier
Meta-Information	M	Structure of Meta-Information	The meta-information (see 8.1).
Subscribing-User-ID-List	M	Structure	Identifies the users who subscribed to the presence change.
Presence-Value-List	M	Structure	List of User IDs and corresponding presence values.

Table 76. Information elements in PresenceNotification Primitive

14.2.6 The "GetWatcherListRequest" Primitive

The `GetWatcherListRequest` primitive allows the requestor server to retrieve the list of users that subscribed to its presence information.

Information Element	Req	Type	Description
Message-Type	M	GetWatcherListRequest	Message identifier
Meta-Information	M	Structure of Meta-Information	The meta-information (see 8.1).

Table 77. Information elements in GetWatcherRequest Primitive

14.2.7 The "GetWatcherListResponse" Primitive

The `GetWatcherListResponse` primitive allows the provider server to return the subscriber list to the requestor server.

Information Element	Req	Type	Description
Message-Type	M	GetWatcherListResponse	Message identifier
Status-Info	M	Structure of Status-Primitive	Status information (see 8.2).
User-ID-List	C	Structure	Identifies the subscribers.

Table 78. Information elements in GetWatcherListResponse Primitive

14.2.8 The "GetPresenceRequest" Primitive

The `GetPresenceRequest` primitive allows the requestor server to retrieve the updated presence information. If the presence attribute list is missing from the request, the server sends all available presence information.

Information Element	Req	Type	Description
Message-Type	M	GetPresenceRequest	Message identifier
Meta-Information	M	Structure of Meta-Information	The meta-information (see 8.1).
User-ID-List	C	Structure	Identifies the publishing users.
Contact-List-ID-List	C	Structure	Identifies the set of publishing users.

Presence-Attribute-List	O	Structure	A list of presence attributes to be retrieved. An empty or missing list indicates all presence attributes are desired.

Table 79. Information elements in GetPresenceRequest Primitive

14.2.9 The "GetPresenceResponse" Primitive

The `GetPresenceResponse` primitive allows the provider server to send the updated presence information to the requestor server.

Information Element	Req	Type	Description
Message-Type	M	GetPresenceResponse	Message identifier
Status-Info	M	Structure of Status-Primitive	Status information (see 8.2).
Presence-Value-List	O	Structure	List of User IDs and corresponding presence values.

Table 80. Information elements in GetPresenceResponse Primitive

14.2.10 The "UpdatePresenceRequest" Primitive

The `UpdatePresenceRequest` primitive allows the requestor server to update presence information for the publishing user. Only the updated attributes and their values need to be carried in this primitive, the omitted attributes are not modified.

Information Element	Req	Type	Description
Message-Type	M	UpdatePresenceRequest	Message identifier
Meta-Information	M	Structure of Meta-Information	The meta-information (see 8.1).
Presence-Value-List	M	Structure	A list of presence values to update.

Table 81. Information elements in UpdatePresenceRequest Primitive

14.2.11 The "CancelAuthRequest" Primitive

The `CancelAuthRequest` primitive allows the publishing user to cancel its previous reactive authorizations, and remove the subscriber from its Watcher List.

Information Element	Req	Type	Description
Message-Type	M	CancelAuthRequest	Message identifier
Meta-Information	M	Structure of Meta-Information	The meta-information (see 8.1).
Canceled-User-ID-List	M	Structure	Identifies the users who will be cancelled authorization.

Table 82. Information elements in CancelAuthRequest Primitive

14.2.12 The "SuspendRequest" Primitive

The "*SuspendRequest*" primitive is used to suspend presence notifications..

Information Element	Req	Type	Description
Message-Type	M	SuspendRequest	Message identifier
Meta-Information	M	Structure of Meta-Information	The meta-information (see 5.1).
User-ID-List	C	Structure	Identifies the IM users whos presence notifications to be suspended.
Contact-List-ID-List	C	Structure	Identifies the set of users.

Table 82 Information elements in SuspendRequest Primitive

14.3 Transactions

14.3.1 The "Subscribe" Transaction

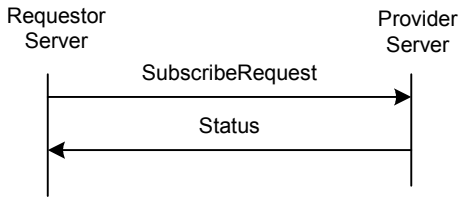

Figure 40. The "Subscribe" Transaction

The subscription for obtaining the notification about the changes of the presence information is accomplished through a "**Subscribe**" transaction.

The requestor server sends a `SubscribeRequest` request to the provider server for subscribing to the notification about the changes of the presence information of some publishing users. The provider server shall determine whether or not the reactive authorization is needed based on whether or not the subscribing user is proactively authorized in the publishing user's contact list. The provider server shall return a `Status` message indicating that the provider server has accepted and processed the request.

The provider server shall perform "**ReactiveAuthorization**" transactions with the publishing users if the individual reactive authorizations are needed.

If the subscription succeeds, the requestor server shall receive immediately the current presence information through a "**PresenceNotification**" transaction. The requestor server shall also receive the presence changes in the future.

The scope of the subscription is either a single user or a contact list referring to multiple users. The requesting user may subscribe to only part of the presence information and, correspondingly, the user whose presence information is subscribed may allow only part of the presence information to be delivered. The subscription may be persistent through different sessions.

Primitive	Direction
SubscribeRequest	Requestor Server → Provider Server
Status	Requestor Server ← Provider Server

Table 83. Primitive Directions for Subscribe Transaction

14.3.2 The "ReactiveAuthorization" Transaction

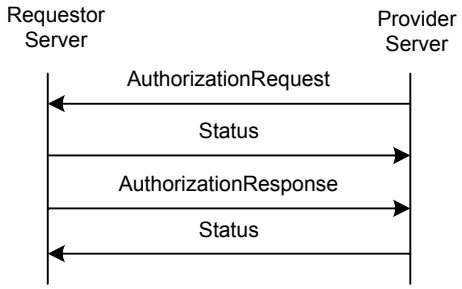

Figure 41. The "ReactiveAuthorization" Transaction

If the reactive authorization is needed in the "Subscribe" transaction from the subscribing user, the provider server shall perform the "ReactiveAuthorization" transactions with the requestor servers that represent the publishing users. The publishing user may accept or reject the request for authorization to subscribe to its presence information.

There may be multiple tuples { Authorizing-User-ID, List-of-Subscribing-User-ID-and-Presence-Attribute-List } in one `AuthorizationRequest` primitive if the provider server is able to combine the multiple reactive authorizations in one primitive in order to reduce the traffic overhead between the servers.

There may be multiple tuples { Authorizing-User-ID, Subscribing-User-IDs, Authorization-Result } in one `AuthorizationResponse` primitive if the provider server is able to collect the response from the authorizing users in a reasonable time and combine the multiple responses in one primitive in order to reduce the traffic overhead between the servers.

A new authorization will overwrite the existing one. Any attribute previously granted or denied that is not specified in the new authorization will not be changed. An exception is an empty list, which will overwrite all authorizations.

This transaction belongs to the complementary service.

Primitive	Direction
AuthorizationRequest	Requestor Server ← Provider Server
Status	Requestor Server → Provider Server
AuthorizationResponse	Requestor Server → Provider Server
Status	Requestor Server ← Provider Server

Table 84. Primitive Directions for ReactiveAuthorization Transaction

14.3.3 The "Unsubscribe" Transaction

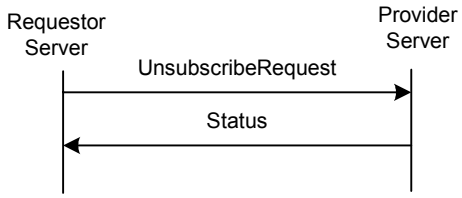

Figure 42. The "Unsubscribe" Transaction

The cancellation of a current subscription is accomplished through an "**Unsubscribe**" transaction. The provider server shall return a `Status` message indicating that the provider server has accepted and processed the request.

Primitive	Direction
UnsubscribeRequest	Requestor Server → Provider Server
Status	Requestor Server ← Provider Server

Table 85. Primitive Directions for Unsubscribe Transaction

14.3.4 The "PresenceNotification" Transaction

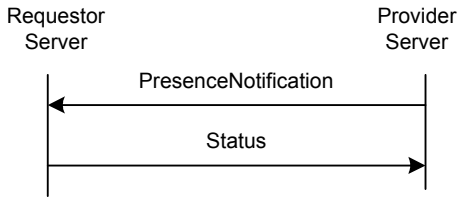

Figure 43. The "PresenceNotification" Transaction

The requestor server is informed of the change of the presence information through a "**PresenceNotification**" transaction originated by the provider server.

Primitive	Direction
PresenceNotification	Requestor Server ← Provider Server
Status	Requestor Server → Provider Server

Table 86. Primitive Directions for PresenceNotification Transaction

14.3.5 The "GetWatcherList" Transaction

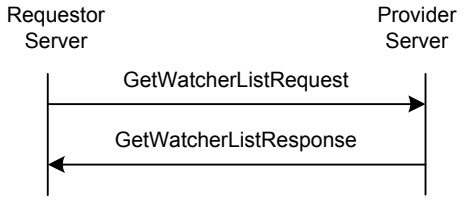

Figure 44. The "GetWatcherList" Transaction

The purpose of the `GetWatcherList` transaction is to allow the requestor server to retrieve the list of users that subscribed to its presence information.

The requestor server sends a `GetWatcherListRequest` to the provider server. A `GetWatcherListResponse` message from the provider server contains a list of subscribers.

This transaction belongs to the complementary service.

Primitive	Direction
GetWatcherListRequest	Requestor Server → Provider Server
GetWatcherListResponse	Requestor Server ← Provider Server

Table 87. Primitive Directions for GetWatcherList Transaction

14.3.6 The "GetPresence" Transaction

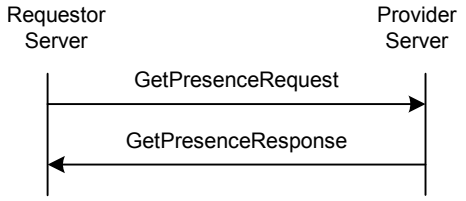

Figure 45. The "GetPresence" Transaction

The purpose of the `GetPresence` transaction is to allow the requestor server to retrieve the presence information of other users.

The requestor server sends a `GetPresenceRequest` to the provider server for the updated presence information of the publishing users. A `GetPresenceResponse` message from the provider server will contain result code(s) and if the request was successful it will relay the requested PRESENCE INFORMATION.

Primitive	Direction
GetPresenceRequest	Requestor Server → Provider Server
GetPresenceResponse	Requestor Server ← Provider Server

Table 88. Primitive Directions for GetPresence Transaction

14.3.7 The "UpdatePresence" Transaction

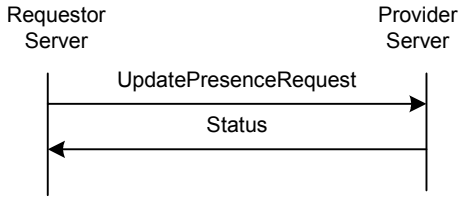

Figure 46. The "UpdatePresence" Transaction

An owner of the presence data or a user with sufficient privileges may update presence attributes and their values through a "**UpdatePresence**" transaction.

The requestor server sends an `UpdatePresenceRequest` message to the provider server. The provider server returns a Status response.

Primitive	Direction
UpdatePresenceRequest	Requestor Server → Provider Server
Status	Requestor Server ← Provider Server

Table 89. Primitive Directions for UpdatePresence Transaction

14.3.8 The "CancelAuthorization" Transaction

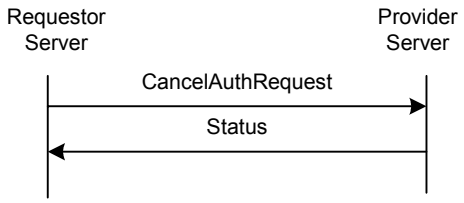

Figure 47. The "CancelAuthorization" Transaction

A publishing user may cancel the reactive authorization and subscription, and remove the subscriber from the Watcher List through "**CancelAuthorization**" transaction.

Please note that the proactive authorization is cancelled by removing the subscriber from the contact list, or by removing the associated attribute list, or by making the associated attribute list empty.

The requestor server sends a `CancelAuthRequest` message to the provider server. The provider server returns a`Status` esponse.

This transaction belongs to the complementary service.

Primitive	Direction
CancelAuthRequest	Requestor Server → Provider Server
Status	Requestor Server ← Provider Server

Table 90. Primitive Directions for CancelAuthorization Transaction

14.3.9 The "Suspend" Transaction

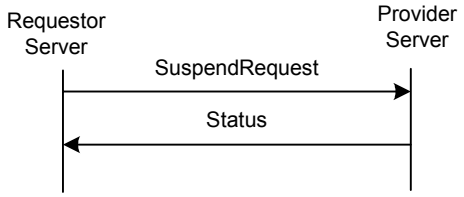

Figure 48. The "Suspend" Transaction

The suspension of presence notification to current subscription is accomplished through a Suspend transaction. The notifications are delivered again when a new Subscribed is preformed. The difference of Suspend and Unsubscribe is that the user remains in the watcher list when a suspend is requested but is removed with an Unsubscribe. The provider server shall return a "Status" message indicating that the provider server has accepted and processed the request.

Primitive	Direction
SuspendRequest	Requestor Server → Provider Server
Status	Requestor Server ← Provider Server

Table 90. Primitive Directions for Suspend Transaction

14.4 Status Code

14.4.1 “ReactiveAuthorization” Transaction

- Unknown presence attribute (not defined in [PA]). (750)
- Unknown authorization request or user ID. (531)

14.4.2 “GetPresence” Transaction

- Unknown presence attribute (not defined in [PA]) (750)
- Unknown user ID. (531)
- Contact list does not exist. (700)

14.4.3 “UpdatePresence” Transaction

- Unknown presence attribute (not defined in [PA]) (750)
- Unknown presence value (not defined in [PA]) (751)

14.4.4 Other Presence Transactions

- Unknown user ID (531)
- Unknown contact list (700).
- Unknown presence attribute (not defined in [PA]). (750)
- Unknown presence value (not defined on the [PA])(751).
- Automatic subscription / unsubscription is not supported (760)

15.Service Relay – Instant Messaging Features

15.1 Overview

This chapter focuses on the functional relay of IM features. Because of server interoperation, the SSP has its own requirements on meta-information and information elements in the primitives at transaction level. The complete primitives and transaction flows of IM features at SSP semantics level have been defined in the following two sections.

Please refer to the CSP document to understand how to relay the IM features from client-server interaction (CSP) to server-server interoperation (SSP).

15.2 Primitives

15.2.1 The "SendMessageRequest" Primitive

The `SendMessageRequest` primitive allows the requesting server to send the instant messages to the users through the requested server.

Information Element	Req	Type	Description
Message-Type	M	SendMessageRequest	Message identifier
Meta-Information	M	Structure of Meta-Information	The meta-information (see 8.1).
Delivery-Report-Request	M	"Yes" | "No"	Indicates if the user wants delivery report.
Message-Info	M	Structure	Message information data, including { Message-ID or Message-URI, Content-type / MIME, encoding, size, sender and recipients (User-ID and/or Client-ID and/or Screen-Name and/or Group-ID and/or Contact-List-ID), date and time, validity }. Message-ID is NOT present if the request is relayed from the user's Home Domain to its PSE. Otherwise, Message-ID is present.
Content	C	String or Binary data	The content of the instant message.

Table 91. Information elements in SendMessageRequest Primitive

15.2.2 The "SendMessageResponse" Primitive

The `SendMessageResponse` primitive allows the requested server to inform the requesting server of the message sending result.

Information Element	Req	Type	Description
Message-Type	M	SendMessageResponse	Message identifier
Status-Info	M	Structure of Status-Primitive	Status information (see 8.2).
Message-ID	C	String	Server generated message id for this message.

Table 92. Information elements in SendMessageResponse Primitive

15.2.3 The "ForwardMessageRequest" Primitive

The `ForwardMessageRequest` primitive allows the requesting server to forward the non-retrieved instant messages.

Information Element	Req	Type	Description
Message-Type	M	ForwardMessageRequest	Message identifier
Meta-Information	M	Structure of Meta-Information	The meta-information (see 8.1).
Message-ID	M	String	Identifies the message (either Message-ID or Message-URI).
Recipients	M	Structure	Identifies the users to whom the message is forwarded (User-ID-List, Contact-List-ID-List, Screen-Name-List and Group-ID-List)

Table 93. Information elements in ForwardMessageRequest Primitive

15.2.4 The "NewMessage" Primitive

The `NewMessage` primitive allows the provider server to deliver the instant message to the users through the requestor server.

Information Element	Req	Type	Description
Message-Type	M	NewMessage	Message identifier.
Meta-Information	C	Structure of Meta-Information	The meta-information (see 8.1). Present if in PushMessage transaction.
Status-Info	C	Structure of Status-Primitive	Status information (see 8.2). Present if in GetMessage transaction.
Recipient-User-ID-List	M	Structure	Identifies the recipients with a list of User-ID's.
Message-Info	M	Structure	Message information data, including { Message-ID or Message-URI, Content-type / MIME, encoding, size, sender and recipients (User-ID and optionally the Client-ID and/or Screen-Name and/or Group-ID and/or Contact-List-ID), date and time, validity }.
Content	M	String or Binary data	Message data.

Table 94. Information elements in NewMessage Primitive

15.2.5 The "MessageDelivered" Primitive

The `MessageDelivered` primitive allows the requestor server to confirm that the message has been delivered.

Information Element	Req	Type	Description
Message-Type	M	MessageDelivered	Message identifier.
Meta-Information	C	Structure of Meta-Information	The meta-information (see 8.1). Present if in GetMessage transaction.
Status-Info	C	Structure of Status-Primitive	Status information (see 8.2). Present if in PushMessage transaction.
Message-ID	M	String	ID of message that has been delivered

Table 95. Information elements in MessageDelivered Primitive

15.2.6 The "MessageNotification" Primitive

The `MessageNotification` primitive allows the provider server to notify the user of the new messages through the requestor server.

Information Element	Req	Type	Description
Message-Type	M	MessageNotification	Message identifier
Meta-Information	M	Structure of Meta-Information	The meta-information (see 8.1).
Recipient-User-ID-List	M	Structure	Identifies the recipients with a list of User-ID's.
Message-Info	M	Structure	Message information data, including { Message-ID or Message-URI, Content-type / MIME, encoding, size, sender and recipients (User-ID and optionally the Client-ID and/or Screen-Name and/or Group-ID and/or Contact-List-ID), date and time, validity }.

Table 96. Information elements in MessageNotification Primitive

15.2.7 The "GetMessageRequest" Primitive

The `GetMessageRequest` primitive allows the requestor server to get the instant message from the provider server.

Information Element	Req	Type	Description
Message-Type	M	GetMessageRequest	Message identifier
Meta-Information	M	Structure of Meta-Information	The meta-information (see 8.1).
Message-ID	M	String	ID of message to retrieve

Table 97. Information elements in GetMessageRequest Primitive

15.2.8 The "SetMessageDeliveryMethod" Primitive

The `SetMessageDeliveryMethod` primitive allows user in the requestor server to set the instant message delivery method.

Information Element	Req	Type	Description
Message-Type	M	SetMessageDelivery Method	Message identifier
Meta-Information	M	Structure of Meta-Information	The meta-information (see 8.1).
Message-Delivery-Method	M	"Notify/Get" | "Push"	Determines the type of message delivery. Push means that complete message is transferred in the notification. Notify/Get means that only the message-ID or message-URI is transferred in the notification the message is then retrieved using a GetMessage transaction.
Accepted-Content-Length	O	Integer	Maximum size of message that can be pushed to the user.

Group-ID	O	String	Group ID if Delivery method refers to a group.

Table 98. Information elements in SetMessageDeliveryMethod Primitive

15.2.9 The "GetMessageListRequest" Primitive

If the provider server offers a space where messages are stored, the user can retrieve an undelivered message list or group history list. The `GetMessageListRequest` primitive allows the requestor server to get the stored Message-ID's or Message-URI's so that they can be used in GetMessage or RejectMessage transactions. If "Group-ID" is present, the user will have the group history list. Otherwise, the user will have the undelivered message list.

Information Element	Req	Type	Description
Message-Type	M	GetMessageListRequest	Message identifier
Meta-Information	M	Structure of Meta-Information	The meta-information (see 8.1).
Group-ID	C	String	List the messages to the group(s) (to retrieve the history).
Message-Count	O	Integer	The maximum number of message-info structures to be returned.

Table 99. Information elements in GetMessageListRequest Primitive

15.2.10 The "GetMessageListResponse" Primitive

The `GetMessageListResponse` primitive allows the provider server to return a list of message information.

Information Element	Req	Type	Description
Message-Type	M	GetMessageListResponse	Message identifier.
Status-Info	M	Structure of Status-Primitive	Status information (see 8.2).
Message-Info-List	M	Structure	Message information data, including { Message-ID or Message-URI, Content-type / MIME, encoding, size, sender and recipients (User-ID and/or Client-ID and/or Screen-Name and/or Group-ID and/or Contact-List-ID), date and time, validity }.

Table 100. Information elements in GetMessageListResponse Primitive

15.2.11 The "RejectMessageRequest" Primitive

The `RejectMessageRequest` primitive allows the requestor server to remove the unwanted and / or stored messages in the provider server.

Information Element	Req	Type	Description
Message-Type	M	RejectMessageRequest	Message identifier
Meta-Information	M	Structure of Meta-Information	The meta-information (see 8.1).

Message-ID-List	M	Structure	Identifies the messages (either Message-ID-List or Message-URI-List).

Table 101. Information elements in RejectMessageRequest Primitive

15.2.12 The "DeliveryStatusReport" Primitive

The `DeliveryStatusReport` primitive allows the provider server to give the sender the message delivery status report. The delivery report can also inform the client about an unsuccessful delivery attempt due to detected error conditions on the receiving side.

Information Element	Req	Type	Description
Message-Type	M	DeliveryStatusReport	Message identifier.
Meta-Information	M	Structure of Meta-Information	Meta-information (see 8.1).
Delivery-Result	M	Structure of Status-Primitive	The delivery result shares the same structure as Status (see 8.2).
Delivery-Time	O	DateTime	Date and time of delivery
Message-Info	M	Structure	Message information data, including { Message-ID or Message-URI, Content-type / MIME, encoding, size, sender and recipients (User-ID and/or Client-ID and/or Screen-Name and/or Group-ID and/or Contact-List-ID), date and time, validity }.

Table 102. Information elements in DeliveryStatusReport Primitive

15.2.13 The "BlockUserRequest" Primitive

The `BlockUserRequest` primitive allows the blocking groups or users (specified by UserID or ScreenName) in the requesting server to prevent message or invitations delivery from certain sources. None of the message or invitations from the blocked entity will be delivered to the blocking user.

Information Element	Req	Type	Description
Message-Type	M	BlockUserRequest	Message identifier
Meta-Information	M	Structure of Meta-Information	The meta-information (see 8.1).
Block-Entity-List	O	Structure	A list of entities to be added to the block list.
Unblock-Entity-List	O	Structure	A list of entities to be removed from the block list.
Block-List-Status	M	"Active" | "Inactive"	Indicates if the block list is in use ("Active") or not ("Inactive").
Grant-Entity-List	O	Structure	The list of entities to be added to the grant list.
Ungrant-Entity-List	O	Structure	The list of entities to be removed from the grant list.

Grant-List-Status	M	"Active" | "Inactive"	Indicates if the grant list is in use ("Active") or not ("Inactive").

Table 103. Information elements in BlockUserRequest Primitive

15.2.14 The "GetBlockedRequest" Primitive

The `GetBlockedRequest` primitive allows the blocking user in the requestor server to get its own list of blocked and granted entities, and the status of the grant list and block list.

Information Element	Req	Type	Description
Message-Type	M	GetBlockedRequest	Message identifier
Meta-Information	M	Structure of Meta-Information	The meta-information (see 8.1).

Table 104. Information elements in GetBlockedRequest Primitive

15.2.15 The "GetBlockedResponse" Primitive

The `GetBlockedResponse` primitive allows the provider server to return a list of blocked entities and granted users, and the list status.

Information Element	Req	Type	Description
Message-Type	M	GetBlockedResponse	Message identifier
Status-Info	M	Structure of Status-Primitive	Status information (see 8.2).
Block-Entity-List	C	Structure	The list of currently blocked entities.
Block-List-Status	M	"Active" | "Inactive"	If the block list is in use ("Active") or not ("Inactive").
Grant-Entity-List	C	Structure	The list of currently granted entities.
Grant-List-Status	M	"Active" | "Inactive"	If the grant list is in use ("Active") or not ("Inactive").

Table 105. Information elements in GetBlockedResponse Primitive

15.3 Transactions

15.3.1 The "SendMessage" Transaction

Figure 49. The "SendMessage" Transaction

The purpose of "**SendMessage**" transaction is to allow the requestor server to send the instant messages through the provider server. The user may send message to a group or to other user(s) at any suitable time.

The requestor server sends a `SendMessageRequest` message to the provider server. The provider server returns a `SendMessageRsponse` response containing the result and the message ID.

Primitive	Direction
SendMessageRequest	Requestor Server → Provider Server
SendMessageResponse	Requestor Server ← Provider Server

Table 106. Primitive Directions for SendMessage Transaction

15.3.2 The "ForwardMessage" Transaction

The purpose of "**ForwardMessage**" transaction is to allow the requestor server to forward instant messages through the provider server.

The requestor server sends a `ForwardMessageRequest` message to the provider server. The provider server returns a `Status` response containing the result.

This transaction belongs to the complementary service.

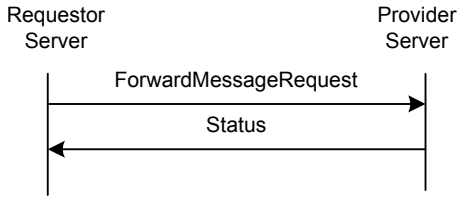

Figure 50. The "ForwardMessage" Transaction

Primitive	Direction
ForwardMessageRequest	Requestor Server → Provider Server
Status	Requestor Server ← Provider Server

Table 107. Primitive Directions for ForwardMessage Transaction

15.3.3 The "PushMessage" Transaction

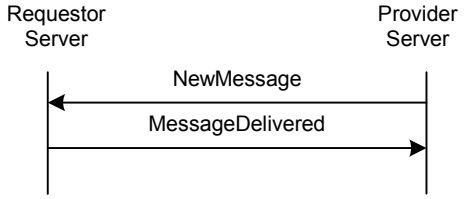

Figure 51. The "PushMessage" Transaction

The purpose of "**PushMessage**" transaction is to allow the provider server to deliver the messages to users through the requestor server.

The provider server sends a `NewMessage` primitive to the requestor server. The requestor server returns a `MessageDelivered` response containing the result and the message ID.

This transaction belongs to the complementary service.

Primitive	Direction
NewMessage	Requestor Server ← Provider Server
MessageDelivered	Requestor Server → Provider Server

Table 108. Primitive Directions for PushMessage Transaction

15.3.4 The "MessageNotification" Transaction

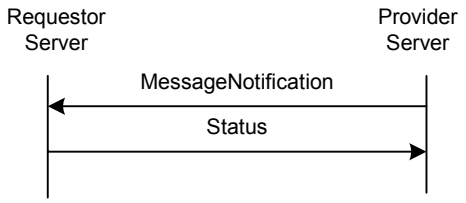

Figure 52. The "MessageNotification" Transaction

The purpose of "**MessageNotification**" transaction is to allow the provider server to notify the users of new messages through the requestor server.

The provider server sends a `MessageNotification` primitive to the requestor server. The requestor server returns a `Status` response.

This transaction belongs to the complementary service.

Primitive	Direction
MessageNotification	Requestor Server ← Provider Server
Status	Requestor Server → Provider Server

Table 109. Primitive Directions for MessageNotification Transaction

15.3.5 The "GetMessage" Transaction

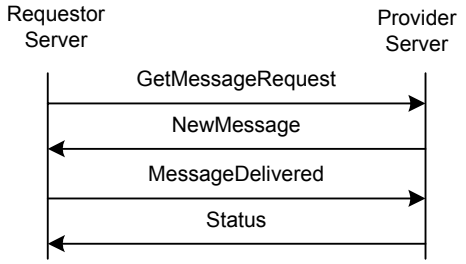

Figure 53. The "GetMessage" Transaction

The purpose of the "**GetMessage**" transaction is to allow the requestor server to retrieve a new message from the provider server.

The requestor server sends a `GetMessageRequest` message with a message ID to the provider server. The provider server returns a `NewMessage` response containing the new message.

This transaction belongs to the complementary service.

Primitive	Direction
GetMessageRequest	Requestor Server → Provider Server
NewMessage	Requestor Server ← Provider Server
MessageDelivered	Requestor Server → Provider Server
Status	Requestor Server ← Provider Server

Table 110. Primitive Directions for GetMessage Transaction

15.3.6 The "SetMessageDeliveryMethod" Transaction

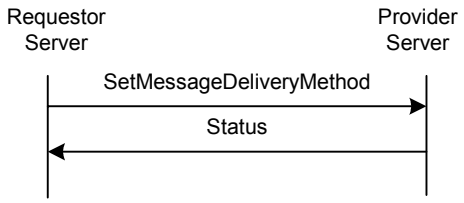

Figure 54. The "SetMessageDeliveryMethod" Transaction

The purpose of the "**SetMessageDeliveryMethod**" transaction is to allow the user in the requestor server to set the appropriate message delivery method from the provider server.

The requestor server sends a `SetMessageDeliveryMethod` request to the provider server. The provider server returns a `Status` response.

This transaction belongs to the complementary service.

Primitive	Direction
SetMessageDeliveryMethod	Requestor Server → Provider Server
Status	Requestor Server ← Provider Server

Table 111. Primitive Directions for SetMessageDeliveryMethod Transaction

15.3.7 The "GetMessageList" Transaction

Figure 55. The "GetMessageList" Transaction

The purpose of the "**GetMessageList**" transaction is to allow the requestor server to get the stored Message-ID's or Message-URI's so that they can be used in GetMessage or RejectMessage transactions. This transaction can be used to retrieve the message history of the group if the GetMessageListRequest contains the Group ID.

The requestor server sends a `GetMessageListRequest` to the provider server. The provider server returns a `GetMessageListResponse`.

This transaction belongs to the complementary service if the undelivered messages are requested.

Primitive	Direction
GetMessageListRequest	Requestor Server → Provider Server
GetMessageListResponse	Requestor Server ← Provider Server

Table 112. Primitive Directions for GetMessageList Transaction

15.3.8 The "RejectMessage" Transaction

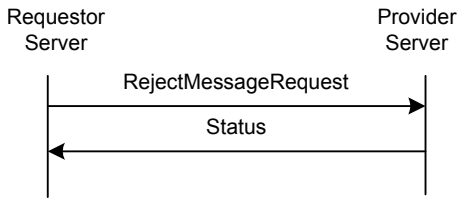

Figure 56. The "RejectMessage" Transaction

This transaction belongs to the complementary service.

Primitive	Direction
RejectMessageRequest	Requestor Server → Provider Server
Status	Requestor Server ← Provider Server

Table 113. Primitive Directions for RejectMessage Transaction

15.3.9 The "NotifyDeliveryStatusReport" Transaction

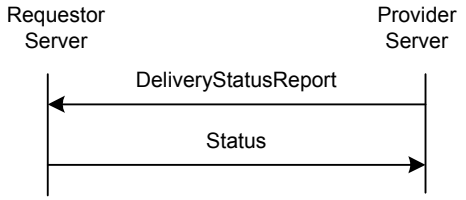

Figure 57. The "NotifyDeliveryStatusReport" Transaction

Primitive	Direction
DeliveryStatusReport	Requestor Server ← Provider Server
Status	Requestor Server → Provider Server

Table 114. Primitive Directions for NotifyDeliveryStatusReport Transaction

15.3.10 The "BlockUser" Transaction

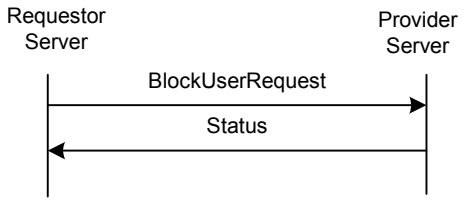

Figure 58. The "BlockUser" Transaction

A user may block/un-block any other user at any suitable time. The purpose of the "**BlockUser**" transaction is to allow the blocking user in the requestor server to prevent getting the messages or invitations from the blocked users in the provider server.

The requestor server sends a `BlockUserRequest` request to the provider server containing the list of users to be blocked / unblocked . The provider server returns a `Status` response.

This transaction belongs to the complementary service.

Primitive	Direction
BlockUserRequest	Requestor Server → Provider Server
Status	Requestor Server ← Provider Server

Table 115. Primitive Directions for BlockUser Transaction

15.3.11 The "GetBlockedList" Transaction

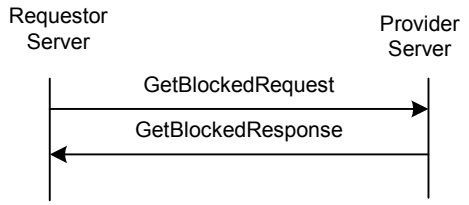

Figure 59. The "GetBlockedList" Transaction

A user may get its own list of blocked users at any suitable time. The purpose of the "**GetBlockedList**" transaction is to allow the blocking user in the requestor server to get its own list of blocked users and granted users.

The requestor server sends a `GetBlockedRequest` request to the provider server. The provider server returns a `GetBlockedResponse` response containing the list of blocked users.

This transaction belongs to the complementary service.

Primitive	Direction
GetBlockedRequest	Requestor Server → Provider Server
GetBlockedResponse	Requestor Server ← Provider Server

Table 116. Primitive Directions for GetBlockedList Transaction

15.4 Status Code

15.4.1 "SendMessage" Transaction

- `Unknown content-type (415)`
- `Message queue full (507)`
- `Recipient user does not exist. (531)`
- `Recipient user blocked the sender (532)`
- `Recipient user is not logged in (533)`
- `Contact list does not exist. (700)`
- `Recipient group does not exist (800)`
- `Sender has not joined the group (or kicked) (808)`
- `Private messaging is disabled in the group (812)`
- `Private messaging is disabled for the recipient (813)`
- `Domain not supported. (516)`

15.4.2 “SetMessageDeliveryMethod” Transaction

- Group does not exist. (800)

15.4.3 “GetMessageList” Transaction

- Group does not exist. (800)
- Group is not joined (808)
- History is not supported (821)

15.4.4 “RejectMessage” Transaction

- Invalid Message-ID (426)

15.4.5 “NewMessage” Transaction

- Invalid Message-ID (426)
- Client will not accept the message delivery. (410)
- Client does not support the content type. (415)

15.4.6 “GetMessage” Transaction

- Invalid Message-ID (426)

15.4.7 “NotifyDeliveryStatusReport” Transaction

- Unsupported content-type. (415)
- Domain not supported. (516)
- Contact list does not exist. (700)
- Recipient user does not exist. (531)
- Recipient user blocked the sender. (532)
- Recipient user is not logged in. (533)
- Message queue full. (507)
- Recipient group does not exist. (800)
- Sender has not joined the group (or kicked). (808)
- Private messaging is disabled in the group. (812)
- Private messaging is disabled for the recipient. (813)

15.4.8 “ForwardMessage” Transaction

- Message queue full. (507)
- Recipient user does not exist. (531)
- Recipient user blocked the sender. (532)
- Recipient user is not logged in. (533)
- Contact list does not exist. (700)
- Recipient group does not exist. (800)

- Sender has not joined the group (or kicked). (808)
- Private messaging is disabled in the group. (812)
- Private messaging is disabled for the recipient. (813)
- Invalid Message-ID. (426)
- Unsupported content-type. (415)
- Domain not supported. (516)

15.4.9 Block Transactions

- Unknown user ID (531)
- Unknown group-ID (800)

16.Service Relay – Group Features

This chapter focuses on the functional relay of Group features. Because of the server interoperation nature, the SSP has its own requirement on meta-information and information elements in the primitives at transaction level. The complete primitives and transaction flows of Group features at SSP semantics level has been defined in the following two sections.

Please refer to the CSP document so as to conclude how to relay the Group features from client-server interaction (CSP) to server-server interoperation (SSP).

16.1 Primitives

16.1.1 The “CreateGroupRequest” Primitive

The `CreateGroupRequest` primitive is used for the user in the requestor server to create a private user group at any suitable time. The `CreateGroupRequest` primitive contains the User-ID, Group-ID, the initial properties of the group, the user's intention of joining to the created group, getting the group change notifications and optionally to define the screen name as well. The provider server creates the group with the specified properties, and responds with a`Status` essage.

Information Element	Req	Type	Description
Message-Type	M	CreateGroupRequest	Message identifier
Meta-Information	M	Structure of Meta-Information	The meta-information (see 8.1).
Group-ID	M	String	Identifies the group
Group-Props	M	Structure	The properties of the group.
Join-Group	M	Boolean	A flag indicating that the user creating the group joins the group at the same time.
Screen-Name	O	Structure	Screen name of the user in the group.
Subscribe-Notif	M	Boolean	A flag indicating that the user wants to activate the group change notifications while joining the group.

Table 117. Information elements in CreateGroupRequest Primitive

16.1.2 The “DeleteGroupRequest” Primitive

The `DeleteGroupRequest` primitive allows the user with sufficient access rights in the requestor server to delete a private user group at any suitable time. The `DeleteGroupRequest` primitive contains the Group-ID. The provider server removes all currently joined users from the group (ServerInitiatedLeaveGroup transaction), deletes the specified group, and responds with a Status message.

Information Element	Req	Type	Description
Message-Type	M	DeleteGroupRequest	Message identifier
Meta-Information	M	Structure of Meta-Information	The meta-information (see 8.1).
Group-ID	M	String	Identifies the group

Table 118. Information elements in DeleteGroupRequest Primitive

16.1.3 The "JoinGroupRequest" Primitive

The `JoinGroupRequest` primitive allows the user in the requestor server to join a discussion group at any suitable time. The `JoinGroupRequest` primitive contains the Group-ID, its screen name shown during the discussion, the joined users' list request and the user's intention of getting the group change notifications.

Information Element	Req	Type	Description
Message-Type	M	JoinGroupRequest	Message identifier
Meta-Information	M	Structure of Meta-Information	The meta-information (see 8.1).
Group-ID	M	String	Identifies the group
Joined-Request	M	"Yes" | "No"	Indicates if the user wants the list of currently joined users ("Yes") or not ("No").
Screen-Name	O	String	Screen name of the user in the group.
Subscribe-Notif	M	Boolean	A flag indicating that the user wants to activate the group change notifications while joining the group.
Own-Prop-List	O	Structure	The list of the user's properties in that group.

16.1.4 The "JoinGroupResponse" Primitive

The `JoinGroupResponse` primitive allows the provider server to return the processing result with the list of currently joined users (if requested), and optionally a welcome note.

Information Element	Req	Type	Description
Message-Type	M	JoinGroupResponse	Message identifier
Status-Info	M	Structure of Status-Primitive	Status information (see 8.2).
Joined-User-Screen-Name-List	C	Structure	The list of currently joined users identified by their Screen-Name's. Present if it was requested.
Welcome-Text	O	String	A short text to be shown to the user when he/she has joined the group.

Table 119. Information elements in JoinGroupResponse Primitive

16.1.5 The "LeaveGroupRequest" Primitive

The `LeaveGroupRequest` primitive allows the user in the requestor server to leave a discussion group at any suitable time. The `LeaveGroupRequest` primitive contains the Group-ID.

Information Element	Req	Type	Description
Message-Type	M	LeaveGroupRequest	Message identifier
Meta-Information	M	Structure of Meta-Information	The meta-information (see 8.1).

Group-ID	M	String	Identifies the group

Table 120. Information elements in LeaveGroupRequest Primitive

16.1.6 The "LeaveGroupIndication" Primitive

The `LeaveGroupIndication` primitive allows the provider server to return the group leaving result requested from the requestor server. The `LeaveGroupIndication` primitive is also used for the provider server to initiate the group leaving due to user kickout, group deletion etc.

Information Element	Req	Type	Description
Message-Type	M	LeaveGroupIndication	Message identifier
Meta-Information	C	Structure of Meta-Information	Meta-information (see 8.1). Present if in ServerInitiatedLeaveGroup transaction
Status-Info	C	Structure of Status-Primitive	Status information (see 8.2). Present if in LeaveGroup transaction.
Reason-text	M	String	Indicate why the user has to leave.
Group-ID	C	String	Identification of the group that has been left. Present if in ServerInitiatedLeaveGroup transaction.

Table 121. Information elements in LeaveGroupIndication Primitive

16.1.7 The "GetJoinedMemberRequest" Primitive

The `GetJoinedMemberRequest` primitive allows the requestor server to retrieve the joined member list of a group. This primitive (and transaction) has no corresponding CSP primitive (and transaction).

Information Element	Req	Type	Description
Message-Type	M	GetJoinedMemberRequest	Message identifier
Meta-Information	M	Structure of Meta-Information	The meta-information (see 8.1).
Group-ID	M	String	Identifies the group

Table 122. Information elements in GetJoinedMemberRequest Primitive

16.1.8 The "GetJoinedMemberResponse" Primitive

The `GetJoinedMemberResponse` primitive allows the provider server to return the result with a list of joined group members.

Information Element	Req	Type	Description
Message-Type	M	GetJoinedMemberResponse	Message identifier
Status-Info	M	Structure of Status-Primitive	Status information (see 8.2).
Joined-User-List	M	Structure	A list of joined members identified by their { User-ID, Screen-Name } pairs.

Table 123. Information elements in GetJoinedMemberResponse Primitive

16.1.9 The "GetGroupMemberRequest" Primitive

The `GetGroupMemberRequest` primitive allows the user with sufficient access rights in the requestor server to retrieve the member list of a group. The `GetGroupMemberRequest` primitive contains the Group-ID.

Information Element	Req	Type	Description
Message-Type	M	GetGroupMemberRequest	Message identifier
Meta-Information	M	Structure of Meta-Information	The meta-information (see 8.1).
Group-ID	M	String	Identifies the group

Table 124. Information elements in GetGroupMemberRequest Primitive

16.1.10 The "GetGroupMemberResponse" Primitive

The `GetGroupMemberResponse` primitive allows the provider server to return the result with a list of all group members.

Information Element	Req	Type	Description
Message-Type	M	GetGroupMemberResponse	Message identifier
Status-Info	M	Structure of Status-Primitive	Status information (see 8.2).
User-ID-List-Adm	O	Structure	The list of users that are in the "Administrator" list.
User-ID-List-Mod	O	Structure	The list of users that are in the "Moderator" list.
User-ID-List	O	Structure	The list of users that are ordinary members.

Table 125. Information elements in GetGroupMemberResponse Primitive

16.1.11 The "AddGroupMemberRequest" Primitive

The `AddGroupMemberRequest` primitive allows the user with sufficient access rights in the requestor server to add the other user(s) to a group. The `AddGroupMemberRequest` primitive contains the Group-ID and the list of user(s) to be added. All of the newly added users are the ordinary members.

Information Element	Req	Type	Description
Message-Type	M	AddGroupMemberRequest	Message identifier
Meta-Information	M	Structure of Meta-Information	The meta-information (see 8.1).
Group-ID	M	String	Identifies the group
User-ID-List	O	Structure	The list of users to be added.

Table 126. Information elements in AddGroupMemberRequest Primitive

16.1.12 The "RemoveGroupMemberRequest" Primitive

The `RemoveGroupMemberRequest` primitive allows the user with sufficient access rights in the requestor server to remove users from a group. The `RemoveGroupMemberRequest` primitive contains the Group-ID and the list of user(s) to be removed.

Information Element	Req	Type	Description
Message-Type	M	RemoveGroupMemberRequest	Message identifier
Meta-Information	M	Structure of Meta-Information	The meta-information (8.1).
Group-ID	M	String	Identifies the group
User-ID-List	M	Structure	A list of removed users.

Table 127. Information elements in RemoveGroupMemberRequest Primitive

16.1.13 The "MemberAccessRequest" Primitive

The `MemberAccessRequest` primitive allows the user with sufficient access rights in the requestor server to change the access privileges of other users.

Information Element	Req	Type	Description
Message-Type	M	MemberAccessRequest	Message identifier
Meta-Information	M	Structure of Meta-Information	The meta-information (8.1).
Group-ID	M	String	Identifies the group
User-ID-List-Adm	O	Structure	The list of users to be set in the "Administrator" list.
User-ID-List-Mod	O	Structure	The list of users to be set in the "Moderator" list.
User-ID-List	O	Structure	The list of users to be set as ordinary members.

Table 128. Information elements in MemberAccessRequest Primitive

16.1.14 The "GetGroupPropsRequest" Primitive

The `GetGropPropsRequest` primitive allows the user with sufficient access rights in the requestor server to retrieve the properties of a group, and its own properties in that particular group. The `GetGropPropsRequest` primitive contains the Group-ID.

Information Element	Req	Type	Description
Message-Type	M	GetGroupPropsRequest	Message identifier
Meta-Information	M	Structure of Meta-Information	The meta-information (see 8.1).
Group-ID	M	String	Identifies the group

Table 129. Information elements in GetGroupPropsRequest Primitive

16.1.15 The "GetGroupPropsResponse" Primitive

The `GetGroupPropsResponse` primitive allows the provider server to return the result with a list of group properties and its own properties of the specified group.

Information Element	Req	Type	Description
Message-Type	M	GetGroupPropsResponse	Message identifier
Status-Info	M	Structure of Status-Primitive	Status information (see 8.2).

Group-Prop-List	M	Structure	The list of group properties.
Own-Prop-List	M	Structure	The list of the user's properties in that group.

Table 130. Information elements in GetGroupPropsResponse Primitive

16.1.16 The "SetGroupPropsRequest" Primitive

The `SetGroupPropsRequest` primitive allows the user with sufficient access rights in the requestor server to update the properties of a group, and/or its own properties in that particular group. The `SetGroupPropsRequest` primitive contains the Group-ID, the new properties of the group and/or the new user properties.

Information Element	Req	Type	Description
Message-Type	M	SetGroupPropsRequest	Message identifier
Meta-Information	M	Structure of Meta-Information	The meta-information (see 8.1).
Group-ID	M	String	Identifies the group
Group-Prop-List	O	Structure	The list of group properties.
Own-Prop-List	O	Structure	The list of the user's properties in that group.

Table 131. Information elements in SetGroupPropsRequest Primitive

16.1.17 The "RejectListRequest" Primitive

The `RejectListRequest` primitive allows the user with sufficient access rights in the requestor server to retrieve / update the reject list of a group. Users on the reject list cannot join the group.

Information Element	Req	Type	Description
Message-Type	M	RejectListRequest	Message identifier
Meta-Information	M	Structure of Meta-Information	The meta-information (see 8.1).
Group-ID	M	String	Identifies the group
Add-User-ID-List	O	Structure	The list of users to be added to the reject list
Remove-User-ID-List	O	Structure	The list of users to be removed from the reject list.

Table 132. Information elements in RejectListRequest Primitive

16.1.18 The "RejectListResponse" Primitive

The `RejectListResponse` primitive allows the provider server to return the reject list of the group.

Information Element	Req	Type	Description
Message-Type	M	RejectListResponse	Message identifier
Status-Info	M	Structure of Status-Primitive	Status information (see 8.2).

Reject-User-ID-List	O	Structure	A list of users in the reject list.

Table 133. Information elements in RejectListResponse Primitive

16.1.19 The "SubscribeGroupChangeRequest" Primitive

The `SubscribeGroupChangeRequest` primitive allows the user in the requestor server to subscribe to a group change notice whenever another user leaves or joins the group, or the group properties have been changed.

Information Element	Req	Type	Description
Message-Type	M	SubscribeGroupChangeRequest	Message identifier
Meta-Information	M	Structure of Meta-Information	The meta-information (see 8.1).
Group-ID	M	String	Identifies the group

Table 134. Information elements in SubscribeGroupChangeRequest Primitive

16.1.20 The "UnsubscribeGroupChangeRequest" Primitive

The `UnsubscribeGroupChangeRequest` primitive is used to cancel the current subscription.

Information Element	Req	Type	Description
Message-Type	M	UnsubscribeGroupChangeRequest	Message identifier
Meta-Information	M	Structure of Meta-Information	The meta-information (see 8.1).
Group-ID	M	String	Identifies the group

Table 135. Information elements in UnsubscribeGroupChangeRequest Primitive

16.1.21 The "GetGroupSubStatusRequest" Primitive

The `GetGroupSubStatusRequest` primitive allows the user in the requestor server to retrieve its subscription status to the group change notice. The `GetGroupSubStatusRequest` primitive contains the Group-ID.

Information Element	Req	Type	Description
Message-Type	M	GetGroupSubStatusRequest	Message identifier
Meta-Information	M	Structure of Meta-Information	The meta-information (see 8.1).
Group-ID	M	String	Identifies the group

Table 136. Information elements in GetGroupSubStatusRequest Primitive

16.1.22 The "GetGroupSubStatusResponse" Primitive

The `GetGroupSubStatusResponse` primitive allows the provider server to return the result with its current subscription status to a group change notice.

Information Element	Req	Type	Description
Message-Type	M	GetGroupSubStatusResponse	Message identifier

Status-Info	M	Structure of Status-Primitive	Status information (see 8.2).
Group-ID	M	String	Identifies the group
Subscription-Status	M	'S' | 'U'	Indicates the subscription status – subscribed ('S') or not ('U').

Table 137. Information elements in GetGroupSubStatusResponse Primitive

16.1.23 The "GroupChangeNotice" Primitive

The `GroupChangeNotice` primitive allows the provider server to send notifications to the subscribed users whenever users leave or join the group, or the group properties have been changed.

Information Element	Req	Type	Description
Message-Type	M	GroupChangeNotice	Message identifier
Meta-Information	M	Structure of Meta-Information	The meta-information (see 8.1).
Subscribing-User-ID-List	M	Structure	Identifies the users who subscribed to the group change.
Group-ID	M	String	Identification of the group.
Joined-User-Screen-Name-List	O	Structure	A list of users that have joined the group since last notification. The users are identified by their screen names
Left-User-Screen-Name-List	O	Structure	A list of users that have left the group since last notification. The users are identified by their screen names
Group-Prop-List	O	Structure	The new properties of the group.
Own-Props	O	Structure	The new properties of the user in the group.

Table 138. Information elements in GroupChangeNotice Primitive

16.2 Transactions

16.2.1 The "CreateGroup" Transaction

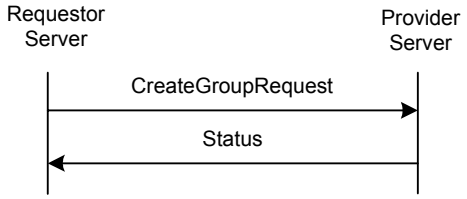

Figure 60. The "CreateGroup" Transaction

A user may create its own private group at any suitable time. The purpose of "**CreateGroup**" transaction is to allow the user in the requestor server to create the user's own private group.

The requestor server sends a `CreateGroupRequest` request to the provider server with the specified properties. The provider server returns a `Status` response.

This transaction belongs to the complementary service.

Primitive	Direction
CreateGroupRequest	Requestor Server → Provider Server
Status	Requestor Server ← Provider Server

Table 139. Primitive Directions for CreateGroup Transaction

16.2.2 The "DeleteGroup" Transaction

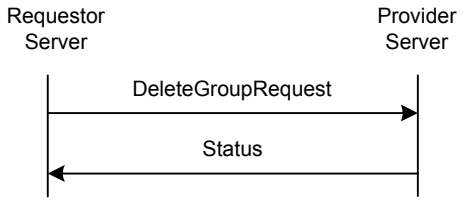

Figure 61. The "DeleteGroup" Transaction

A user with sufficient access rights may delete a private user group at any suitable time.

The requestor server sends a `DeleteGroupRequest` request to the provider server with the Group-ID. The provider server removes all currently joined users from the group (ServerInitiatedLeaveGroup transaction), deletes the specified group, and responds with a `Status` message.

This transaction belongs to the complementary service.

Primitive	Direction
DeleteGroupRequest	Requestor Server → Provider Server
Status	Requestor Server ← Provider Server

Table 140. Primitive Directions for DeleteGroup Transaction

16.2.3 The "JoinGroup" Transaction

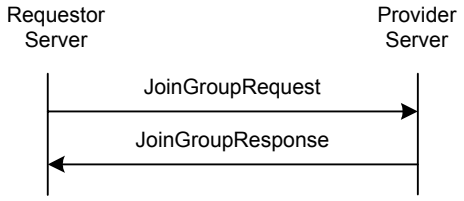

Figure 62. The "JoinGroup" Transaction

A user may join a discussion group at any suitable time.

The requestor server sends a `JoinGroupRequest` request to the provider server with the Group-ID, its screen name shown during the discussion, and the joined users' list request. The provider server returns a `JoinGroupResponse` response including the processing result with the list of currently joined users (if requested), and optionally a welcome note.

After a user successfully joins the group, the user may receive / send messages from / to the particular group.

Primitive	Direction
JoinGroupRequest	Requestor Server → Provider Server
JoinGroupResponse	Requestor Server ← Provider Server

Table 141. Primitive Directions for JoinGroup Transaction

16.2.4 The "LeaveGroup" Transaction

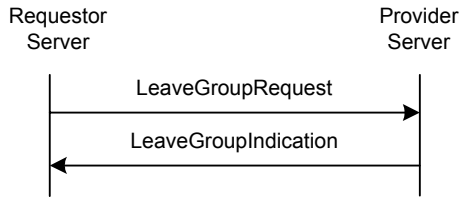

Figure 63. The "LeaveGroup" Transaction

A user may leave a discussion group at any suitable time.

The requestor server sends a `LeaveGroupRequest` request to the provider server with the Group-ID. The provider server returns a `LeaveGroupIndication` response.

Primitive	Direction
LeaveGroupRequest	Requestor Server → Provider Server
LeaveGroupIndication	Requestor Server ← Provider Server

Table 142. Primitive Directions for LeaveGroup Transaction

16.2.5 The "ServerInitiatedLeaveGroup" Transaction

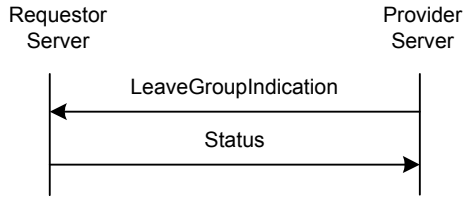

Figure 64. The "ServerInitiatedLeaveGroup" Transaction

A server may initiate a group leaving due to user kickout, group deletion etc.

The provider server sends a `LeaveGroupIndication` request to the requestor server.

Primitive	Direction
LeaveGroupIndication	Requestor Server ← Provider Server

Table 143. Primitive Directions for ServerInitiatedLeaveGroup Transaction

16.2.6 The "GetJoinedMember" Transaction

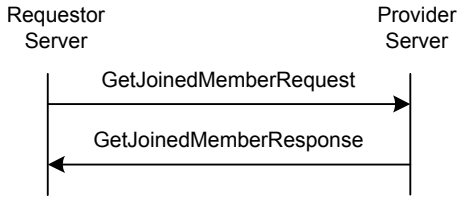

Figure 65. The "GetJoinedMember" Transaction

This transaction belongs to the complementary service.

Primitive	Direction
GetJoinedMemberRequest	Requestor Server → Provider Server
GetJoinedMemberResponse	Requestor Server ← Provider Server

Table 144. Primitive Directions for GetJoinedMember Transaction

16.2.7 The "GetGroupMember" Transaction

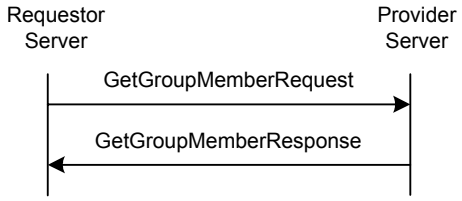

Figure 66. The "GetGroupMember" Transaction

A user with sufficient access rights may retrieve the member list of a group.

The requestor server sends a `GetGroupMemberRequest` request to the provider server with the Group-ID. The provider server returns a `GetGroupMemberResponse` response with the list of all group members.

This transaction belongs to the complementary service.

Primitive	Direction
GetGroupMemberRequest	Requestor Server → Provider Server
GetGroupMemberResponse	Requestor Server ← Provider Server

Table 145. Primitive Directions for GetGroupMember Transaction

16.2.8 The "AddGroupMember" Transaction

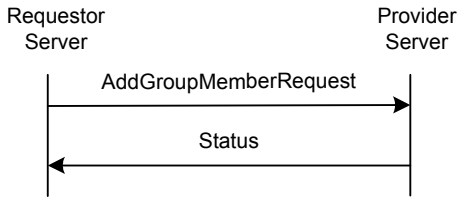

Figure 67. The "AddGroupMember" Transaction

A user with sufficient access rights may add user(s) to the member list of a group.

The requestor server sends a `AddGroupMemberRequest` request to the provider server with the Group-ID and the list(s) of users to be added. The provider server returns a `Status` response.

This transaction belongs to the complementary service.

Primitive	Direction
AddGroupMemberRequest	Requestor Server → Provider Server
Status	Requestor Server ← Provider Server

Table 146. Primitive Directions for AddGroupMember Transaction

16.2.9 The "RemoveGroupMember" Transaction

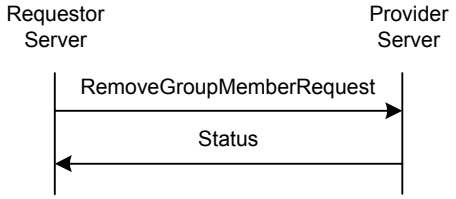

Figure 68. The "RemoveGroupMember" Transaction

A user with sufficient access rights may remove user(s) from the member list of a group.

The requestor server sends a `RemoveGroupMemberRequest` request to the provider server with the Group-ID and the list(s) of users to be removed. The provider server returns a `Status` response.

This transaction belongs to the complementary service.

Primitive	Direction
RemoveGroupMember Request	Requestor Server → Provider Server
Status	Requestor Server ← Provider Server

Table 147. Primitive Directions for RemoveGroupMember Transaction

16.2.10 The "MemberAccess" Transaction

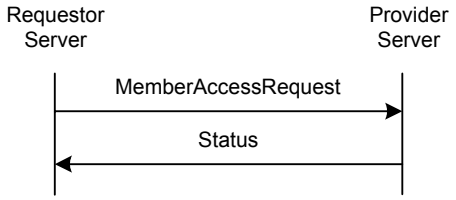

Figure 69. The "MemberAccess" Transaction

This transaction belongs to the complementary service.

Primitive	Direction
MemberAccessRequest	Requestor Server → Provider Server
Status	Requestor Server ← Provider Server

Table 148. Primitive Directions for MemberAccess Transaction

16.2.11 The "GetGroupProps" Transaction

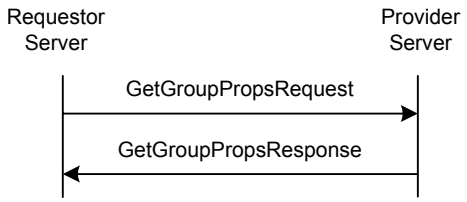

Figure 70. The "GetGroupProps" Transaction

A user with sufficient access rights may retrieve the properties of a group, and it's the user's own properties in that particular group.

The requestor server sends a `GetGroupPropsRequest` request to the provider server with the Group-ID. The provider server returns a `GetGroupPropsResponse` response with the list of group properties and the user's own properties for the specified group.

Primitive	Direction
GetGroupPropsRequest	Requestor Server → Provider Server
GetGroupPropsResponse	Requestor Server ← Provider Server

Table 149. Primitive Directions for GetGroupProps Transaction

16.2.12 The "SetGroupProps" Transaction

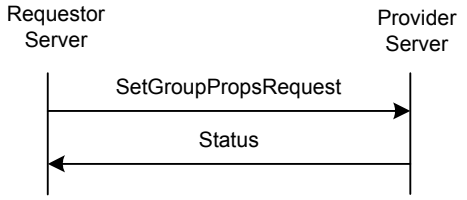

Figure 71. The "SetGroupProps" Transaction

A user with sufficient access rights may update the properties of a group, and/or it's the user's own properties in that particular group.

The requestor server sends a `SetGroupPropsRequest` request to the provider server with the Group-ID, the new properties of the group and/or the new user properties. The provider server returns a `Status` response.

Primitive	Direction
SetGroupPropsRequest	Requestor Server → Provider Server
Status	Requestor Server ← Provider Server

Table 150. Primitive Directions for SetGroupProps Transaction

16.2.13 The "RejectList" Transaction

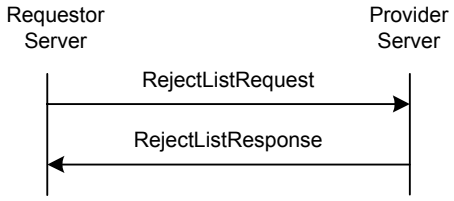

Figure 72. The "RejectList" Transaction

This transaction belongs to the complementary service.

Primitive	Direction
RejectListRequest	Requestor Server → Provider Server
RejectListResponse	Requestor Server ← Provider Server

Table 151. Primitive Directions for RejectList Transaction

16.2.14 The "SubscribeGroupChange" Transaction

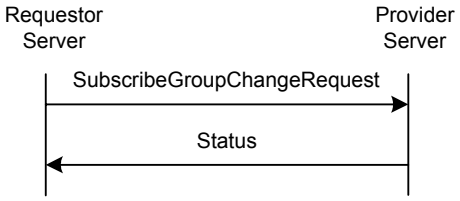

Figure 73. The "SubscribeGroupChange" Transaction

A user may subscribe to a group change notice whenever another user leaves or joins the group, or the group properties have been changed.

The requestor server sends a `SubscribeGroupChangeRequest` request to the provider server with the Group-ID and an optional subscription expiration time. The provider server returns a `Status` response.

Primitive	Direction
SubscribeGroupChange Request	Requestor Server → Provider Server
Status	Requestor Server ← Provider Server

Table 152. Primitive Directions for SubscribeGroupChange Transaction

16.2.15 The "UnsubscribeGroupChange" Transaction

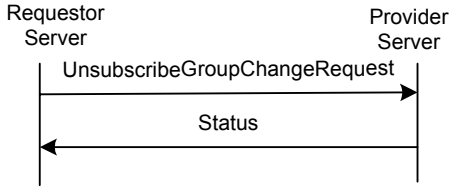

Figure 74. The "UnsubscribeGroupChange" Transaction

A user may cancel the subscription to the group change notice.

The requestor server sends a `UnsubscribeGroupChangeRequest` request to the provider server with the Group-ID. The provider server returns a `Status` response.

Primitive	Direction
UnsubscribeGroupChange Request	Requestor Server → Provider Server
Status	Requestor Server ← Provider Server

Table 153. Primitive Directions for UnsubscribeGroupChange Transaction

16.2.16 The "GetGroupSubStatus" Transaction

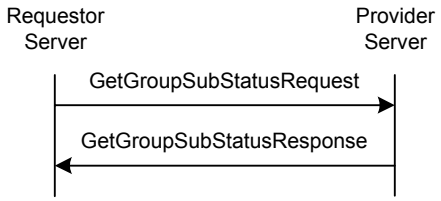

Figure 75. The "GetGroupSubStatus" Transaction

A user may retrieve its subscription status to a group change notice.

The requestor server sends a `GetGroupSubStatusRequest` request to the provider server with the Group-ID. The provider server returns a `GetGroupSubStatusResponse` response with the user's current subscription status to a group change notice.

Primitive	Direction
GetGroupSubStatusRequest	Requestor Server → Provider Server
GetGroupSubStatus Response	Requestor Server ← Provider Server

Table 154. Primitive Directions for GetGroupSubStatus Transaction

16.2.17 The "NotifyGroupChange" Transaction

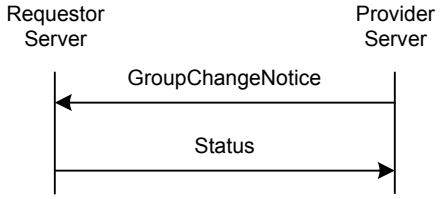

Figure 76. The "NotifyGroupChange" Transaction

The server may send group change notification(s) to the subscribed users whenever a user leaves or joins the group, or the group properties have been changed.

The provider server sends a `GroupChangeNotice` request to the requestor server with a list of recently joined or left users, or the new properties of the group.

Primitive	Direction
GroupChangeNotice	Requestor Server ← Provider Server
Status	Requestor Server → Provider Server

Table 155. Primitive Directions for NotifyGroupChange Transaction

16.3 Status Code

16.3.1 "CreateGroup" Transaction

- Group already exists (801)
- Invalid group attribute(s) (806)
- The maximum number of groups has been reached (user limit) (814)
- The maximum number of groups has been reached for the server (815)
- Cannot have searchable group without name or topic. (822)

16.3.2 "DeleteGroup" Transaction

- Group does not exist (800)
- Group is public (804)
- Insufficient group privileges (816)

16.3.3 "JoinGroup" Transaction

- Group does not exist (800)
- Invalid/unsupported group properties (806)
- User already joined (807)
- Cannot join: "rejected"(809)
- Cannot join with the specified screen name; it is already in use (811)
- Insufficient group privileges (816)
- The maximum number of allowed users has been reached (817)

16.3.4 "LeaveGroup" Transaction

- Group was not joined before transaction (808)

16.3.5 Group Membership Transactions

- Unknown user (531)
- Group does not exist (800)
- Insufficient group privileges (816)
- Group was not joined before transaction. (808)

16.3.6 Group Properties Transactions

- Group does not exist (800).
- Invalid group attribute(s) (806).

- Insufficient group privileges (816).
- Cannot have searchable group without name or topic. (822)

16.3.7 “RejectList” Transaction

- User unknown (531).
- Group does not exist (800).
- Insufficient group privileges (816).

16.3.8 Group Change Transactions

- Group does not exist (800)
- Group was not joined before transaction. (808)

16.3.9 “GetJoinedMember” Transaction

- Group does not exist (800).

17.Status Codes and Descriptions

SSP uses the concept and paradigm of HTTP/1.1 response to define the status code. However, there is no logical or semantic relationship between the status codes in SSP and the status codes in HTTP. The following sections define the general categories as well as each status code.

17.1 1xx – Informational

The client or server MUST be prepared to accept one or more 1xx status codes prior to a regular response even if the client does not expect a 100 "Continue" status code. A client or server agent SHALL ignore unexpected 1xx status code. This category of the status codes does not complete a transaction.

17.1.1 100 – Continue

The client SHOULD continue with its request. The server has accepted the request for processing, but the processing has not been completed. The request might or might not eventually be successfully completed. The server MUST send a final response again upon completing the request. The "100" response is used when time of completion will be too long, possibly causing the server and client connection to break.

17.1.2 101 – Queued

The client SHOULD continue with its request. The server has accepted the request, but does not have resources to start processing. The request might or might not eventually be successfully completed. The server MUST send a final response again upon completing the request.

17.1.3 102 – Started

The client SHOULD continue with its request. The server has accepted the request for processing. The "102" response is used when server needs to start additional transactions in order to process the request. The server MUST send a final response again upon completing the request.

17.1.4 104 – Server Queued

The client MAY continue with its next requests. The server has accepted the request, but does not have resources to start processing. This status is used to indicate the overload of the server and therefore it is expected, that the client will (re)direct the next requests to other possible connections between the servers. The request processing will take place and the server MUST send a final response again upon completing the request.

17.2 2xx – Successful

The 2xx class of status codes indicates that the client's request was successfully received, understood and accepted.

17.2.1 200 – Successful

This is used to indicate that the request succeeded.

17.2.2 201 – Partially Successful

This is used to indicate that the request was successfully completed, but some parts were not completed due to certain errors. The details of the error case(s) are indicated in the response.

17.2.3 202 – Accepted

This is used to indicate that server accepted the request, but not able to receive acknowledgment about delivery to client device. The request might or might not eventually be acted upon. There is no facility for re-sending a status code from an asynchronous operation such as this.

17.3 4xx – Client Error

The 4xx class of status codes is intended for cases in which the client seems to have erred. The server SHOULD include the explanation of the error situation including whether it is a temporary or permanent condition. The user agents should be able to display the error description to the user.

17.3.1 400 – Bad Request

The server could not understand the request due to the malformed syntax. The client SHALL NOT repeat the request without modification.

17.3.2 401 – Unauthorized

When an authorization request is expected, the presence server will respond with this status code. Properties will contain details of available authorization schemes.

17.3.3 402 – Bad Parameter

The server cannot understand one of the parameters in the request. The client SHALL NOT repeat the request without modification.

17.3.4 403 – Forbidden

The server understood the request, but the principal settings denied access to some of the presence, contact information, or group. Authorization will not help and the request SHOULD NOT be repeated. This type of response is also returned if user not logged into the network.

17.3.5 404 - Not Found

The server cannot find anything matching the request. No indication is given of whether the condition is temporary or permanent.

17.3.6 405 – Service Not Supported

The server does not support the service method in the request.

17.3.7 410 – Unable to Delivery

The server cannot deliver the request. The requested resource is no longer available at the server and no forwarding address is known.

17.3.8 415 – Unsupported Media Type

The server cannot deliver the request, because the client cannot support the format of the entity that it requested.

17.3.9 420 – Invalid Transaction-ID

The server encountered an invalid Transaction-ID.

17.3.10 422 – User-ID and Client-ID Does Not Match

The User-ID and the Client-ID do not match in the request.

17.3.11 423 – Invalid Invitation-ID

The server encountered an invalid invitation ID.

17.3.12 424 – Invalid Search-ID

The server encountered an invalid search ID.

17.3.13 425 – Invalid Search-Index

The server encountered an invalid search index.

17.3.14 426 – Invalid Message-ID

The server encountered an invalid Message-ID.

17.3.15 431 – Unauthorized Group Membership

The user agent is not an authorized member of the group.

17.4 5xx – Server Error

The 5xx class of status codes is intended for cases in which the server is aware that it has erred or is incapable of performing the request.

17.4.1 500 – Internal Server Error

The provider server encountered an unexpected condition that prevented it from fulfilling the request.

17.4.2 501 – Not Implemented

The server does not support the functionality required to fulfill the request. This is the appropriate response when the server does not recognize the request method, and it is not capable of supporting it for any resources.

17.4.3 503 – Service Unavailable

The server is currently unable to handle the request due to a temporally overloading of the server.

17.4.4 504 – Invalid Timeout

The provider server has not returned the response within the repeat time.

17.4.5 505 – Version Not Supported

The server does not support, or refuses to support, the request version that was used. The response should contain the preferred supported version.

17.4.6 506 – Service Not Agreed

The service request refers to a service that does not correspond to the service agreement between the service requestor and provider server. The requestor server SHALL NOT repeat the request without a new service negotiation.

17.4.7 507 – Message Queue is Full

The server cannot fulfill the request because its message queue is full. The client MAY repeat the request.

17.4.8 516 – Domain Not Supported

The server does not support forwarding to different a domain space.

17.4.9 521 – Unresponded Presence Request

The presence information provider does not respond to the presence service specified in the request.

17.4.10 522 – Unresponded Group Request

The group service provider does not respond to the requested group transaction.

17.4.11 531 – Unknown User

The specified user is unknown / User-ID is invalid.

17.4.12 532 –Recipient Blocked the Sender

The recipient of the message or invitation blocked the sender.

17.4.13 533 – Message Recipient Not Logged in

The recipient of the message is not logged in.

17.4.14 534 – Message Recipient Unauthorized

The recipient of the message is not authorized.

17.4.15 535 – Search Timed Out

The server has invalidated the requested search-request.

17.4.16 536 – Too many hits.

The query returned too many hits. The client needs to narrow the query.

17.4.17 537 – Too broad search criteria

The query cannot be processed since it is too broad.

17.5 6xx – Session

The 6xx class status code indicates the session-related status.

17.5.1 600 – Session Expired

The server connection was disconnected because the time-to-live parameter of provider session has expired.

17.5.2 601 – Forced Logout

The provider server has disconnected the requestor server.

17.5.3 604 – Invalid Session / Not Logged In

There is no such user session. (Previously not logged in, disconnected, or logged out.)

17.5.4 606 – Invalid Service-ID

Unknown Service-ID.

17.5.5 607 – Redirection Refused

The redirected connection is refused.

17.5.6 608 – Invalid Password

The password provided by the requestor server was incorrect; it does not match with the given Service-ID. The requestor SHALL NOT repeat the request without modification.

17.5.7 609 – Connection Expired

The connection was disconnected because the time-to-live parameter has expired. This is NOT the last active connection pair.

17.5.8 610 – Server Search Limit is Exceeded

The search limit exceeds the server limit.

17.5.9 620 – Invalid Server Session

There is no such session. (Previously not logged in, disconnected, or logged out.) If only the session-ID is invalid in the Meta-information, this error indication should be used instead of Unknown transaction.

17.6 7xx – Presence and contact list

The 7xx class indicates the presence and contact list related status codes.

17.6.1 700 – Contact List Does Not Exist

The contact list specified in the request does not exist.

17.6.2 701 – Contact List Already Exists

The contact list specified in the request already exists.

17.6.3 702 – Invalid or Unsupported User Properties

The user properties specified in the request are invalid or not supported.

17.6.4 750 – Invalid or Unsupported Presence Attributes

The presence attributes specified in the request are invalid or not supported.

17.6.5 751 – Invalid or Unsupported Presence Value

The presence value(s) specified in the request are invalid or not supported. The client SHOULD NOT repeat the request without modification.

17.6.6 752 – Invalid or Unsupported Contact List Property

One or more contact list properties specified in the request are invalid or not supported. The client SHOULD NOT repeat the request without modification.

17.6.7 760 – Automatic Subscription / Unsubscription is not supported

The server does not support the automatic subscription when adding a user to the contact list, and does not support the automatic unsubscription when deleting the contact list or removing a user from the contact list.

17.7 8xx – Groups

The 8xx class indicates the group-related status codes.

17.7.1 800 – Group Does Not Exist

The group specified in the request does not exist.

17.7.2 801 – Group Already Exists

The group specified in the request already exists.

17.7.3 802 – Group is Open

The group specified in the request is an open group.

17.7.4 803 – Group is Closed

The group specified in the request is a closed group.

17.7.5 804 – Group is Public

The group specified in the request is public.

17.7.6 805 – Group Private

The group specified in the request is private.

17.7.7 806 – Invalid / Unsupported Group Properties

The group properties specified in the request are invalid or not supported.

17.7.8 807 – Group is Already Joined

The group specified in the request is already joined. If the server does not allow the same user to join a group more than once, this error code is used to indicate that the user is already joined to the particular group.

17.7.9 808 – Group is Not Joined

The request cannot be processed, because it requires the user to be joined to the group.

17.7.10 809 – Rejected

The user has been rejected from the particular group. He/she is forced to leave the group and cannot join.

17.7.11 810 – Not a Group Member

The request cannot be processed because the user is not a member of the specified closed group.

17.7.12 811 – Screen Name Already in Use

The screen name specified in the request is already in use. If the server does not allow the same screen name to be used in a group more than once then this error code is used to indicate that the screen name is already in use. The requesting user may try to change his/her screen name and repeat the transaction.

17.7.13 812 – Private Messaging is Disabled for Group

The client requested private message delivery, but the private messaging is disabled in the particular group.

17.7.14 813 – Private Messaging is Disabled for User

The client requested private message delivery, but the private messaging is disabled for the particular user.

17.7.15 814 – The Maximum Number of Groups Has Been Reached for the User

The server limits the maximum number of groups per user. The limit has been reached; additional groups cannot be created. The client SHOULD NOT repeat the request until a group that belongs to the particular user has been deleted.

17.7.16 815 – The Maximum Number of Groups Has Been Reached for the Server

The maximum number of groups is limited on the server. The server limit has been reached; additional groups cannot be created. The client MAY repeat the request.

17.7.17 816 – Insufficient Group Privileges

The user does not have sufficient privileges in the particular group to perform the requested operation. The client SHOULD NOT repeat the request until the user has been authorized properly.

17.7.18 817 – The Maximum Number of Joined Users Has Been Reached

The maximum number of joined users has been reached in the requested group. The client MAY repeat the request.

17.7.19 821 – History is Not Supported

The server does not support group message history caching.

17.7.20 822 - Cannot have searchable group without name or topic.

The server cannot perform group search without group name or group topic. Either group name or group topic or both must be non-empty to support group search.

17.8 9xx – General errors

The 9xx class indicates status codes too general to fit into other classes.

17.8.1 900 – Multiple errors

No part of the transaction was successfully processed for several reasons, thus not only one other status code can indicate the errors. The details of the error cases are indicated in the response.

17.8.2 901 – General Address Error

The general address is not supported. No specific error is given due to security or privacy reason.

18.Static Conformance Requirements

The static conformance requirements for this specification is specified in [CSP SCR] and [SSP SCR].

Appendix A. Change History (Informative)

A.1 Approved Version History

Reference	Date	Description
OMA-WV-SSP -V1_1	01 Oct 2002	Version 1.1

A.2 Candidate Version 1.2 History

Document Identifier	Date	Sections	Description
Candidate Versions OMA-IMPS-WV-SSP -V1_2	21 Feb 2003	n/a	Status changed to Candidate by TP TP ref # OMA-TP-2003-0109-IMPS-V1_2-Candidate-Package
	07 Mar 2003	n/a	Applied the 2004 specification template.
	24 Apr 2004	6.3.1, 9.2.1, 16.1.15, 6.3.8	The contents of these CRs were included: OMA-IMPS-2003-0059-Motorola_V1_2_CRs OMA-IMPS-2003-0061-Motorola_V1_2_SSP_CRs
	27 Apr 2004	15.3.2, 8.4	The contents of these CRs were included: OMA-IM-2004-0010R01-SSPSEM OMA-IM-2004-0054-SSPGenErrHand
	22 May 2004	2	Corrected revision date and references to other IMPS documents