Server-Server Protocol Transport Binding

Candidate Version 1.3 – 11 Oct 2005

Open Mobile Alliance™

OMA-TS-IMPS-SSP_Transport-V1_3-20051011-C

Contents

1. SCOPE 4
2. REFERENCES 5
2.1 NORMATIVE REFERENCES 5
2.2 INFORMATIVE REFERENCES 5
3. TERMINOLOGY AND CONVENTIONS 6
3.1 CONVENTIONS 6
3.2 DEFINITIONS 6
3.3 ABBREVIATIONS 6
4. INTRODUCTION 7
5. THE HTTP / HTTPS OVER TCP BINDING 8
5.1 CONNECTION PAIR 8
5.2 CONNECTION PAIR REUSE 9
5.3 MULTIPLE CONNECTION PAIRS 10
5.4 SSP MESSAGE CONTENT TYPE 10
5.5 HTTP / HTTPS REDIRECTION 10
5.6 HEADER EXTENSIONS FOR HTTP / HTTPS BINDING 10
APPENDIX A. CHANGE HISTORY (INFORMATIVE) 12
A.1 APPROVED VERSION HISTORY 12
A.2 DRAFT/CANDIDATE VERSION 1.3 HISTORY 12
APPENDIX B. STATIC CONFORMANCE REQUIREMENTS (NORMATIVE) 13

Figures

Figure 1: HTTP / HTTPS Binding for One Session Provisioned by Server B 8
Figure 2: HTTP / HTTPS Binding for the Other Session Provisioned by Server A 9

1. Scope

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

- Presence
- Instant Messaging
- Groups
- Shared Content

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

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

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

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

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

2. References

2.1 Normative References

[IOPPROC] "OMA Interoperability Policy and Process", Version 1.1, Open Mobile Alliance™, OMA-IOP-Process-V1_1, http://www.openmobilealliance.org/

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

[RFC2616] "Hypertext Transfer Protocol – HTTP/1.1", Fielding R.; Gettys J.; Mogul J.; Frystyk H.; Masinter L.; Leach P.; Berners-Lee T., June 1999. URL:http://www.ietf.org/rfc/rfc2616.txt

2.2 Informative References

[Arch] "IMPS Architecture Version 1.3", OMA-AD-IMPS-V1_3, Open Mobile Alliance™. http://www.openmobilealliance.org/

[CSP] "Client-Server Protocol Session and Transactions Version 1.3", OMA-TS-IMPS-CSP-V1_3, Open Mobile Alliance™. http://www.openmobilealliance.org/

[CSP DTD] "Client-Server Protocol XML Syntax Version 1.3", OMA-TS-IMPS-CSP-XMLS-V1_3, Open Mobile Alliance™. http://www.openmobilealliance.org/

[CSP Trans] "Client-Server Protocol Transport Bindings Version 1.3", OMA-TS-IMPS-CSP-Transport-V1_3, Open Mobile Alliance™. http://www.openmobilealliance.org/

[CSP DataType] "Client-Server Protocol Data Types Version 1.3", OMA-TS-IMPS-CSP-Data_Types-V1_3, Open Mobile Alliance™. http://www.openmobilealliance.org/

[CSP SMS] "Client-Server Protocol Plain Text Syntax Version 1.3", OMA-TS-IMPS-CSP-PTS-V1_3, Open Mobile Alliance™. http://www.openmobilealliance.org/

[CSP WBXML] "Client-Server Protocol Binary XML Definition and Examples Version 1.3", OMA-TS-IMPS-CSP-_WBXML-V1_3, Open Mobile Alliance™. http://www.openmobilealliance.org/

[PA] "Presence Attributes Version 1.3", OMA-TS-IMPS-PA-V1_3, Open Mobile Alliance™. http://www.openmobilealliance.org/

[PA DTD] "Presence Attribute XML Syntax Version 1.3", OMA-TS-IMPS-PA_XMLS-V1_3, Open Mobile Alliance™. http://www.openmobilealliance.org/

[SSP] "Server-Server Protocol Semantics Version 1.3", OMA-TS-IMPS-SSP-V1_3, Open Mobile Alliance™. http://www.openmobilealliance.org/

[SSP Syntax] "Server-Server Protocol XML Syntax Version 1.3", OMA-TS-IMPS-SSP_XMLS-V1_3, Open Mobile Alliance™. http://www.openmobilealliance.org/

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

None.

3.3 Abbreviations

CSP	Client-Server Protocol
IMPS	Instant Messaging and Presence Service
OMA	Open Mobile Alliance
SSP	Server-Server Protocol
WV	Wireless Village

4. Introduction

The SSP messages are carried and transmitted by the reliable HTTP or HTTPS over TCP transport protocol. The physical connections carry the service requests of the Requestor Server and the notification requests of the Provider Server.

The SSP transactions are independent of the underlying transport protocol transactions, i.e., one SSP transaction may be carried by two transport protocol transactions.

The SSP transaction identifier MUST always be generated by the initiator of the transaction request. The SSP response MUST include the same transaction identifier, which was transmitted in the request. The SSP transaction request and response MUST carry the identifier of the service provisioning session.

5. The HTTP / HTTPS over TCP Binding

5.1 Connection Pair

The HTTP / HTTPS protocol is an asymmetrical protocol, therefore two physical TCP connections are needed for the HTTP / HTTPS binding. One TCP connection is originated as the HTTP / HTTPS client from the Requestor Server to the Provider Server, i.e., the physical connection 1, and similarly another TCP connection is originated as an HTTP / HTTPS client from the Provider Server to the Requestor Server, i.e., the physical connection 2. HTTP v1.1 is required [RFC2616].

The physical connection 1 shall carry the service requests from the Requestor Server to the Provider Server and the physical connection 2 the notification requests from the Provider Server to the Requestor Server.

The HTTP / HTTPS transport for SSP REQUIRES persistent TCP connection between the servers. HTTP / HTTPS requests and responses are pipelined on the TCP connection. Pipelining allows a HTTP / HTTPS client to make multiple requests without waiting for each response, but the HTTP / HTTPS server must send its responses to those requests in the same order that the requests were received.

The pipelining behavior of the persistent TCP connection MAY decrease the service provisioning throughput, because one request whose response needs more processing time MAY block all the other ready responses belonging to later requests. For this the reason the SSP transaction is separated from the HTTP / HTTPS transaction on the manner shown on Figure 1.

The SSP transaction request and the reply are delivered only by HTTP / HTTPS POST requests. The SSP request is carried in the HTTP / HTTPS body. The HTTP /HTTPS POST reply is a dummy reply, i.e., the body is empty (status code= OK).

The SSP transaction request initiated by the Requestor Server is transmitted on the physical connection 1, and the response of the same SSP transaction is delivered on the physical connection 2. The transaction identifier associates the two transaction halves.

Similarly the SSP notification transaction request initiated by the Provider Server is transmitted on the physical connection 2, and the response of the same SSP transaction is delivered on the physical connection 1.

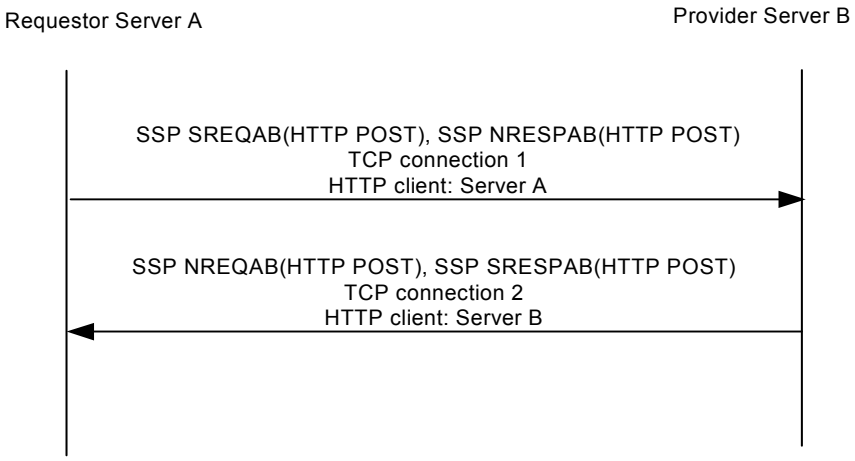

Figure 1: HTTP / HTTPS Binding for One Session Provisioned by Server B

In this example server A is the Requestor Server and server B is the Provider Server.

SREQAB: service request from A to service provider B

NRESPAB: notification response from server A to service provider B

NREQAB: notification request from B to service requester A

SRESPAB: service response from B to service requester A

In this example server A is the Provider Server and server B is the Requestor Server as shown on Figure 2.

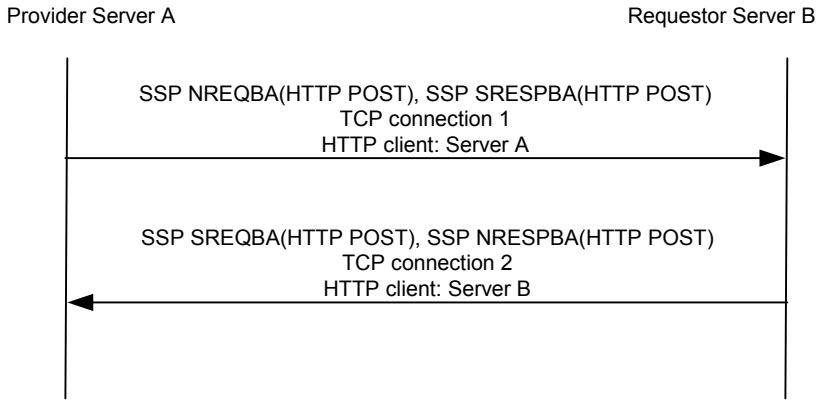

Figure 2: HTTP / HTTPS Binding for the Other Session Provisioned by Server A

where:

SREQBA: service request from B to service provider A

NRESPBA: notification response from server B to service provider A

NREQBA: notification request from A to service requester B

SRESPBA: service response from A to service requester B

5.2 Connection Pair Reuse

If the connection pair is (re)used by the two sessions, the physical connection 1 MUST carry:

for session 1

the SSP service transaction requests from Requestor Server A to Provider Server B

the SSP notification responses from Requestor Server A to Provider Server B

for session 2

the SSP service transaction response from Provider Server A to Requestor Server B

the SSP notification request from Provider Server A to Requestor Server B

and similarly the physical connection 2 MUST carry:

for session 1

the SSP service transaction response from Provider Server B to Requestor Server A

the SSP notification request from Provider Server B to Requestor Server A

for session 2

the SSP service transaction request from Requestor Server B to Provider Server A

the SSP notification responses from Requestor Server B to Provider Server A

5.3 Multiple Connection Pairs

Servers MAY open additional connection pairs belonging to the same session pair if the SSP redirection is allowed.

5.4 SSP Message Content Type

The SSP content type is registered with IANA. The content type of the SSP message is:

application/vnd.wv.ssp+xml

Servers MUST support the SSP Message content type.

Servers that provide communication means for servers that are using earlier version(s) of the IMPS specification MUST apply the appropriate SSP Message content type before sending.

5.5 HTTP / HTTPS Redirection

The IMPS domain MUST support standard HTTP / HTTPS redirection codes [RFC2616] and associated information headers. HTTP / HTTPS redirection allows IMPS server to redirect to other servers based on existing load balancer.

HTTP / HTTPS redirection MUST only be allowed in Step 1 and / or Step 3 of the connection establishment, i.e., the first SendSecretToken primitive after the TCP connection is set up.

5.6 Header Extensions for HTTP / HTTPS Binding

The following two headers are extensions for faster dispatching of the SSP messages to spare the XML document parsing.

This header extension MUST be used to carry the transaction identifier in all HTTP / HTTPS POST requests:

```
header       =  x-wv-transactionid ":"  header-value  CRLF
header-value  =  1*alphanum
alphanum = alpha | digit | "_"
```

This header extension MUST be used to carry the session identifier in all HTTP / HTTPS POST requests if the session is established:

```
header       =  x-wv-sessionid ":"  header-value  CRLF
header-value  =  1*alphanum
alphanum = alpha | digit | "_"
alpha    = lowalpha | upalpha
lowalpha = "a" | "b" | "c" | "d" | "e" | "f" | "g" | "h" | "i" |
           "j" | "k" | "l" | "m" | "n" | "o" | "p" | "q" | "r" |
           "s" | "t" | "u" | "v" | "w" | "x" | "y" | "z"
upalpha  = "A" | "B" | "C" | "D" | "E" | "F" | "G" | "H" | "I" |
           "J" | "K" | "L" | "M" | "N" | "O" | "P" | "Q" | "R" |
           "S" | "T" | "U" | "V" | "W" | "X" | "Y" | "Z"
digit    = "0" | "1" | "2" | "3" | "4" | "5" | "6" | "7" |
           "8" | "9"
```

The character "*" preceding an element indicates repetition. The full form is "<n>*element" indicating at least <n> occurrences of the element; "1*element" REQUIRES at least one.

Elements separated by a bar ("|") are alternatives, *e.g.*, "yes | no" will accept yes or no.

Elements separated by a bar ("|") are alternatives, *e.g.*, "yes | no" will accept yes or no.

Appendix A. Change History (Informative)

A.1 Approved Version History

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

A.2 Draft/Candidate Version 1.3 History

Document Identifier	Date	Sections	Description
Draft Versions OMA-IMPS-WV-SSP_Transport-V1_3	09 Jan 2005	2, 5, 6	OMA-IMPS-WV-SSP_Transport-V1_2-20041217-C used as baseline Removed reference to SCR documents Updated references to 1.3 specifications Added SCR table (empty content)
	31 Jan 2005		SCR Restructuring
	31 Mar 2005		Updated with approved CRs: OMA-IM-2005-0089-Editorial-changes-SSP-Trans-and-XML-IMPS-1.3
	25 Apr 2005		Updated with following approved CRs:
Draft Versions OMA-TS-IMPS-SSP_Transport-V1_3	28 Jul 2005		Fixed copyright date on cover page. Changed Open Mobile Alliance to Open Mobile Alliance™ Following agreed CRs have been included: - OMA-IM-2005-0366-IMPS13-ArchRef-SSP_Trans - OMA-IM-2005-0374R01-IMPS-13-CONRR-Correction-SSP-Trans - OMA-IM-2005-0458R01-SSP-Registered-Identifiers
	8 Aug 2005		Following agreed CRs have been included: - OMA-IM-2005-0566-IMPS-1_3-SSP-Transport-Remove-CLP - OMA-IM-2005-0589-IMPS-1_3-SSP-Transport-scr update
	9 Aug 2005		Editorial changes
	26 Aug 2005		Editorial update: change the references to OMA documents. See mail Peter Arnby
Candidate Versions OMA-TS-IMPS-SSP_Transport-V1_3	11 Oct 2005		Status changed to Candidate by TP TP ref # OMA-TP-2005-0279R01-IMPS-V1_3-for-Candidate-approval

Appendix B. Static Conformance Requirements (Normative)

The notation used in this appendix is specified in [IOPPROC].

Item	Function	Reference	Status	Requirement
IMPS-SSP-Transport-S-001	Support HTTP or HTTPS	Section 5	M	IMPS-SSP-Transport-S-002 OR IMPS-SSP-Transport-S-003
IMPS-SSP-Transport-S-002	Support HTTP	Section 5	O	
IMPS-SSP-Transport-S-003	Support HTTPS	Section 5	O	
IMPS-SSP-Transport-S-004	Transaction identifier is generated by initiator of the transaction request	Section 5.6	M	
IMPS-SSP-Transport-S-005	Response includes same transaction identifier as request	Section 5.6	M	
IMPS-SSP-Transport-S-006	Request and response carry the identifier of the service provisioning session	Section 5.6	M	
IMPS-SSP-Transport-S-007	Support SSP Connection Pair	Section 5.1	M	
IMPS-SSP-Transport-S-008	Support SSP Connection Pair Reuse	Section 5.2	O	
IMPS-SSP-Transport-S-009	Support Multiple Connection Pairs	Section 5.3	O	
IMPS-SSP-Transport-S-010	Support the SSP content type	Section 5.4	M	
IMPS-SSP-Transport-S-011	Support HTTP redirection	Section 5.5	M	
IMPS-SSP-Transport-S-012	Support Header extension for HTTP(S) binding	Section 5.6	M	