



WV-054 SSP – Transport Binding

Approved Version 1.2 – 25 Jan 2005

Open Mobile Alliance
OMA-IMPS-WV-SSP-Transport-V1_2-20050125-A

Continues the Technical Activities
Originated in the Wireless Village Initiative



Use of this document is subject to all of the terms and conditions of the Use Agreement located at <http://www.openmobilealliance.org/UseAgreement.html>.

Unless this document is clearly designated as an approved specification, this document is a work in process, is not an approved Open Mobile Alliance™ specification, and is subject to revision or removal without notice.

You may use this document or any part of the document for internal or educational purposes only, provided you do not modify, edit or take out of context the information in this document in any manner. Information contained in this document may be used, at your sole risk, for any purposes. You may not use this document in any other manner without the prior written permission of the Open Mobile Alliance. The Open Mobile Alliance authorizes you to copy this document, provided that you retain all copyright and other proprietary notices contained in the original materials on any copies of the materials and that you comply strictly with these terms. This copyright permission does not constitute an endorsement of the products or services. The Open Mobile Alliance assumes no responsibility for errors or omissions in this document.

Each Open Mobile Alliance member has agreed to use reasonable endeavors to inform the Open Mobile Alliance in a timely manner of Essential IPR as it becomes aware that the Essential IPR is related to the prepared or published specification. However, the members do not have an obligation to conduct IPR searches. The declared Essential IPR is publicly available to members and non-members of the Open Mobile Alliance and may be found on the “OMA IPR Declarations” list at <http://www.openmobilealliance.org/ipr.html>. The Open Mobile Alliance has not conducted an independent IPR review of this document and the information contained herein, and makes no representations or warranties regarding third party IPR, including without limitation patents, copyrights or trade secret rights. This document may contain inventions for which you must obtain licenses from third parties before making, using or selling the inventions. Defined terms above are set forth in the schedule to the Open Mobile Alliance Application Form.

NO REPRESENTATIONS OR WARRANTIES (WHETHER EXPRESS OR IMPLIED) ARE MADE BY THE OPEN MOBILE ALLIANCE OR ANY OPEN MOBILE ALLIANCE MEMBER OR ITS AFFILIATES REGARDING ANY OF THE IPR'S REPRESENTED ON THE “OMA IPR DECLARATIONS” LIST, INCLUDING, BUT NOT LIMITED TO THE ACCURACY, COMPLETENESS, VALIDITY OR RELEVANCE OF THE INFORMATION OR WHETHER OR NOT SUCH RIGHTS ARE ESSENTIAL OR NON-ESSENTIAL.

THE OPEN MOBILE ALLIANCE IS NOT LIABLE FOR AND HEREBY DISCLAIMS ANY DIRECT, INDIRECT, PUNITIVE, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR EXEMPLARY DAMAGES ARISING OUT OF OR IN CONNECTION WITH THE USE OF DOCUMENTS AND THE INFORMATION CONTAINED IN THE DOCUMENTS.

© 2005 Open Mobile Alliance Ltd. All Rights Reserved.

Used with the permission of the Open Mobile Alliance Ltd. under the terms set forth above.

Contents

1. SCOPE	4
2. REFERENCES	5
2.1 NORMATIVE REFERENCES.....	5
2.2 INFORMATIVE REFERENCES.....	5
3. TERMINOLOGY AND CONVENTIONS	7
3.1 CONVENTIONS.....	7
3.2 DEFINITIONS.....	7
3.3 ABBREVIATIONS	7
4. INTRODUCTION	8
5. THE HTTP / HTTPS OVER TCP BINDING	9
5.1 CONNECTION PAIR.....	9
5.2 CONNECTION PAIR REUSE.....	10
5.3 MULTIPLE CONNECTION PAIRS.....	11
5.4 SSP MESSAGE CONTENT TYPE	11
5.5 HTTP / HTTPS REDIRECTION.....	11
5.6 HEADER EXTENSIONS FOR HTTP / HTTPS BINDING	11
6. STATIC CONFORMANCE REQUIREMENTS.....	12
APPENDIX A. CHANGE HISTORY (INFORMATIVE).....	13
A.1 APPROVED VERSION HISTORY	13

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

- [IOPPROC] "OMA Interoperability Policy and Process", Version 1.1, Open Mobile Alliance™, OMA-IOP-Process-V1_1, <http://www.openmobilealliance.org/>
- [CSP SCR] "WV-048 Client-Server Protocol Static Conformance Requirement Version 1.2". Open Mobile Alliance. <http://www.openmobilealliance.org/>
- [RFC0793] "Transmission Control Protocol", Jon Postel, September 1981. URL:<http://www.ietf.org/rfc/rfc793.txt>
- [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>
- [SSP SCR] "WV-055 SSP – Server-Server Protocol Static Conformance Requirement Version 1.2". Open Mobile Alliance. <http://www.openmobilealliance.org/>

2.2 Informative References

- [Arch] "WV-040 System Architecture Model Version 1.2". Open Mobile Alliance. <http://www.openmobilealliance.org/>
- [FeaFun] "WV-041 Features and Functions Version 1.2". Open Mobile Alliance. <http://www.openmobilealliance.org/>
- [CSP] "WV-042 Client-Server Protocol Session and Transactions Version 1.2". Open Mobile Alliance. <http://www.openmobilealliance.org/>
- [CSP DTD] "WV-043 Client-Server Protocol DTD and Examples Version 1.2". Open Mobile Alliance. <http://www.openmobilealliance.org/>
- [CSP Trans] "WV-044 Client-Server Protocol Transport Bindings Version 1.2". Open Mobile Alliance. <http://www.openmobilealliance.org/>
- [CSP DataType] "WV-045 Client-Server Protocol Data Types Version 1.2". Open Mobile Alliance. <http://www.openmobilealliance.org/>
- [CSP SMS] "WV-046 Client-Server Protocol SMS Binding Version 1.2". Open Mobile Alliance. <http://www.openmobilealliance.org/>
- [CSP WBXML] "WV-047 Client-Server Protocol Binary Definition and Examples Version 1.2". Open Mobile Alliance. <http://www.openmobilealliance.org/>
- [CSP SCR] "WV-048 Client-Server Protocol Static Conformance Requirement Version 1.2". Open Mobile Alliance. <http://www.openmobilealliance.org/>
- [PA] "WV-049 Presence Attributes Version 1.2". Open Mobile Alliance. <http://www.openmobilealliance.org/>
- [PA DTD] "WV-050 Presence Attribute DTD and Examples Version 1.2". Open Mobile Alliance. <http://www.openmobilealliance.org/>
- [CLP] "WV-051 Command Line Protocol Version 1.2". Open Mobile Alliance. <http://www.openmobilealliance.org/>
- [SSP] "WV-052 SSP - Server-Server Protocol Semantics Document Version 1.2". Open Mobile Alliance. <http://www.openmobilealliance.org/>
- [SSP Syntax] "WV-053 Server-Server Protocol XML Syntax Document Version 1.2". Open Mobile Alliance. <http://www.openmobilealliance.org/>

- [SSP Trans] "WV-054 SSP - Transport Binding Version 1.2". Open Mobile Alliance.
<http://www.openmobilealliance.org/>
- [SSP SCR] "WV-055 SSP – Server-Server Protocol Static Conformance Requirement Version 1.2". Open Mobile Alliance. <http://www.openmobilealliance.org/>
- [WAPARCH] "WAP Architecture, Version 12-July-2001". Open Mobile Alliance™. WAP-210-WAPArch.
<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

None

4. Introduction

The SSP messages are carried and transmitted by the reliable HTTP / 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 is always 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 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.

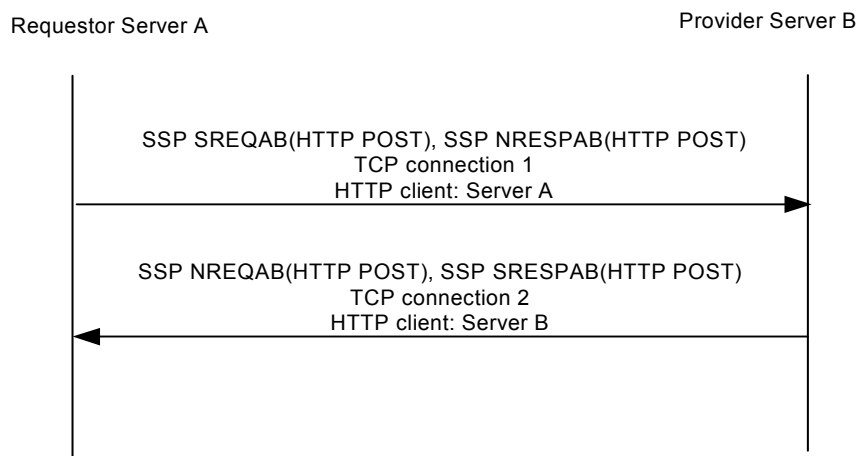


Figure 1. HTTP / HTTPS Binding for One Session Provisioned by Server B

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.

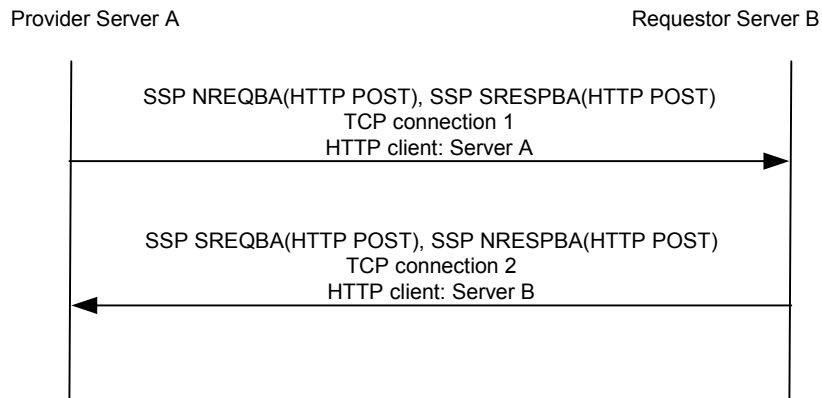


Figure 2. **HTTP / HTTPS Binding for the Other Session Provisioned by Server A**

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 carries:

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 carries:

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 content type of the SSP message is:

```
Content-Type:          application/vnd.wv.ssp.xml
```

5.5 HTTP / HTTPS Redirection

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

HTTP / HTTPS redirection is only 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.

6. 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_Transport-V1_1-20021001-A	01 Oct 2002	Version 1.1
OMA-IMPS-WV-SSP-Transport-V1_2-20050125-A	25 Jan 2005	Version 1.2 Ref TP Doc# OMA-TP-2004-0457-IMPS-V1_2-for-final-approval