



# **Device Management Push Binding**

Candidate Version 1.3 – 07 Dec 2010

---

**Open Mobile Alliance**

OMA-TS-DM\_PushBinding-V1\_3-20101207-C

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.

© 2010 Open Mobile Alliance Ltd. All Rights Reserved.

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

# Contents

<b>1. SCOPE</b> .....	<b>4</b>
<b>2. REFERENCES</b> .....	<b>5</b>
<b>2.1 NORMATIVE REFERENCES</b> .....	<b>5</b>
<b>2.2 INFORMATIVE REFERENCES</b> .....	<b>5</b>
<b>3. TERMINOLOGY AND CONVENTIONS</b> .....	<b>6</b>
<b>3.1 CONVENTIONS</b> .....	<b>6</b>
<b>3.2 DEFINITIONS</b> .....	<b>6</b>
<b>3.3 ABBREVIATIONS</b> .....	<b>6</b>
<b>4. INTRODUCTION</b> .....	<b>7</b>
<b>5. PUSH BINDINGS</b> .....	<b>8</b>
<b>5.1 PUSH OTA PROTOCOL OVER WSP</b> .....	<b>8</b>
5.1.1 Non-secure Push OTA Protocol over WSP .....	8
5.1.2 Secure Push OTA Protocol over WSP .....	8
5.1.3 Using non-WSP Push capable devices.....	8
<b>5.2 PUSH OTA PROTOCOL OVER SIP</b> .....	<b>8</b>
<b>5.3 PUSH OTA PROTOCOL OVER HTTP</b> .....	<b>9</b>
<b>5.4 PUSH OVER OBEX</b> .....	<b>9</b>
<b>APPENDIX A. CHANGE HISTORY (INFORMATIVE)</b> .....	<b>10</b>
<b>A.1 APPROVED VERSION HISTORY</b> .....	<b>10</b>
<b>A.2 DRAFT/CANDIDATE VERSION 1.3 HISTORY</b> .....	<b>10</b>
<b>APPENDIX B. STATIC CONFORMANCE REQUIREMENTS (NORMATIVE)</b> .....	<b>11</b>
<b>B.1 CLIENT FEATURES</b> .....	<b>11</b>
<b>B.2 SERVER FEATURES</b> .....	<b>11</b>

# 1. Scope

This document describes the Push Binding for carrying DM Messages based on DM representation **Error! Reference source not found.** DM Notification information can be found in the DM Notification document [DMNOTI].

## 2. References

### 2.1 Normative References

- [DMHTTP] “OMA Device Management HTTP Binding”, Open Mobile Alliance™, OMA-TS-DM\_HTTPBinding-V1\_3, [URL:http://www.openmobilealliance.org/](http://www.openmobilealliance.org/)
- [DMNOTI] “OMA Device Management Notification”, Open Mobile Alliance™, OMA-TS-DM\_Notification-V1\_3, [URL:http://www.openmobilealliance.org/](http://www.openmobilealliance.org/)
- [DMOBEX] “OMA Device Management OBEX Binding”, Open Mobile Alliance™, OMA-TS-DM\_OBEXBinding-V1\_3, [URL:http://www.openmobilealliance.org/](http://www.openmobilealliance.org/)
- [IOPPROC] “OMA Interoperability Policy and Process”, Version 1.1, Open Mobile Alliance™, OMA-IOP-Process-V1\_1, [URL:http://www.openmobilealliance.org/](http://www.openmobilealliance.org/)
- [OMAPush] “OMA Push Enabler”, Open Mobile Alliance™, OMA-ERELED-Push-V2\_3, [URL:http://www.openmobilealliance.org/](http://www.openmobilealliance.org/)
- [OMNAWSP] “OMNA WSP Content Type Numbers”, Open Mobile Alliance™, [URL:http://www.openmobilealliance.org/Tech/omna/omna-wsp-content-type.aspx](http://www.openmobilealliance.org/Tech/omna/omna-wsp-content-type.aspx)
- [PushOTA] “Push Over The Air”, Open Mobile Alliance™, OMA\_TS-PushOTA-V2\_3, [URL:http://www.openmobilealliance.org](http://www.openmobilealliance.org/)
- [RFC2119] “Key words for use in RFCs to Indicate Requirement Levels”, S. Bradner, March 1997, [URL:http://www.ietf.org/rfc/rfc2119.txt](http://www.ietf.org/rfc/rfc2119.txt)
- [RFC5627] “Obtaining and Using Globally Routable User Agent URIs (GRUUs) in the Session Initiation Protocol (SIP)”, [URL:http://tools.ietf.org/html/rfc5627](http://tools.ietf.org/html/rfc5627)

### 2.2 Informative References

## 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.

Any reference to components of the SyncML DTD or XML snippets is specified in this typeface.

### 3.2 Definitions

**Connection** A transport layer virtual circuit established between two programs for the purpose of communication.

### 3.3 Abbreviations

<b>HTTP</b>	Hypertext Transfer Protocol
<b>OMA</b>	Open Mobile Alliance
<del><b>SSL</b></del>	<del>Secure Socket Layer</del>
<del><b>TLS</b></del>	<del>Transport Layer Security</del>
<b>WAP</b>	Wireless Application Protocol
<b>WBXML</b>	WAP Binary XML Content Format
<b>WDP</b>	Wireless Datagram Protocol
<b>WSP</b>	Wireless Session Protocol
<b>XML</b>	Extensible Markup Language

## 4. Introduction

This document defines the binding requirements for pushing DM Messages via the OMA Push enabler [OMAPUSH]. OMA Push allows for several transports and this binding provides additional settings. Push will only be used for single DM Messages such as Bootstrap or Sessionless. Normally, the originator of the DM Message is called the Push Server, and the recipient of the DM Message is called the Push Client.

A Push Message consists of a header section and a body section. The header section is transport dependent, but will identify the version of the DM Message being pushed.

DM Clients MAY support this binding.

## 5. Push Bindings

The following sections define the requirements for the Push Binding of DM Messages. The DM Client MUST support at least one of these push methods if it supports this binding. Other push protocols MAY be used but are not defined in this binding.

### 5.1 Push OTA Protocol over WSP

#### 5.1.1 Non-secure Push OTA Protocol over WSP

A DM Message MAY be non-securely pushed to the DM Client using the Push OTA Protocol over WSP (OTA-WSP) [PushOTA] with the following additional rules:

- The DM Message MUST be sent using the non-secure connectionless push.
- The application-id code 0x07 MUST be used.
- The Content-Type code 0x42 (WBXML) or 0x43 (XML) MUST be used. Note that these values are defined on the OMNA page [OMNAWSP].

#### 5.1.2 Secure Push OTA Protocol over WSP

A DM Message MAY be securely pushed to the DM Client using the Push OTA Protocol over WSP (OTA-WSP) [PushOTA] with the following additional rules:

- The DM Message MUST be sent using the secure connectionless push.
- The application-id code 0x07 MUST be used.
- The Content-Type code 0x42 (WBXML) or 0x43 (XML) MUST be used. Note that these values are defined on the OMNA page [OMNAWSP].

#### 5.1.3 Using non-WSP Push capable devices

If the receiver is not a WAP device, it is very unlikely that any other application would be active on the same port, which has been publicly registered with IANA. The decoding of the message headers is very straightforward even if the device lacks a full WAP stack and therefore the device MUST examine if the message has been sent to the default WAP push port (2948) and if the application-id and the MIME type are ones assigned to the OMA DM Message. If all these conditions are satisfied then the message MUST be routed to the OMA Device Management application.

### 5.2 Push OTA Protocol over SIP

A DM Message MAY be pushed to the DM Client using the Push OTA Protocol over SIP (OTA-SIP) [PushOTA] with the following additional rules:

- The DM Client MUST register with the SIP/IP Core as soon as practical.
- If GRUU [RFC5627] is supported on the device, then it MUST be used in the registration process.
- The Content-Type MUST be *'application/vnd.syncml.dm+xml'* or *'application/vnd.syncml.dm+wbxml'*.
- "syncml.dm" SHALL be used for "g.oma.eventappid" media feature tag.
- "SIP MESSAGE method (Pager-Mode)" SHALL be used to deliver the DM Message.



## 5.3 Push OTA Protocol over HTTP

A DM Message MAY be pushed to the DM Client using the Push OTA Protocol over HTTP (OTA-HTTP) [PushOTA] with the following additional rules:

- The Content-Type MUST be '*application/vnd.syncml.dm+xml*' or '*application/vnd.syncml.dm+wbxml*'.
- The connection MUST use the same security methods as in the DM HTTP Binding [DMHTTP].

## 5.4 Push over OBEX

A DM Message MAY be pushed to the DM Client over OBEX protocol by using the PUT command of the OBEX protocol. This happens in the same way as sending the DM Notification over OBEX to a DM client [DMNOTI], [DMOBEX].

- The connection MUST use the same security methods as in the DM OBEX Binding [DMOBEX].

## Appendix A. Change History

(Informative)

### A.1 Approved Version History

Reference	Date	Description
N/A	N/A	No prior 1.3 version

### A.2 Draft/Candidate Version 1.3 History

Document Identifier	Date	Sections	Description
Draft Version OMA-TS-DM_PushBinding-V1_3	26 Aug 2010	All	Baseline as agreed in “OMA-DM-DM13-2010-0088R05- INP_Push_Binding”
Candidate Version OMA-TS-DM_PushBinding-V1_3	07 Dec 2010	N/A	Status changed to Candidate by TP Ref #OMA-TP-2010-0502- INP_DM_V1_3_ERP_and_ETR_for_Candidate_re_approval

## Appendix B. Static Conformance Requirements (Normative)

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

### B.1 Client Features

Item	Function	Ref.	Status	Requirement
DM-PUSH-C-001	Support for Push Client	4, 5	O	DM-PUSH-C-002 OR DM-PUSH-C-003 OR DM-PUSH-C-004 OR DM-PUSH-C-005 OR DM-PUSH-C-006
DM-PUSH-C-002	Support for Non-secure Push Protocol over WSP	5.1	O	
DM-PUSH-C-003	Support for Secure Push Protocol over WSP	5.1	O	
DM-PUSH-C-004	Support for Push Protocol over SIP	5.2	O	
DM-PUSH-C-005	Support for Push Protocol over HTTP	5.3	O	DM-PUSH-C-007
DM-PUSH-C-006	Support for Push Over OBEX	5.4	O	DM-PUSH-C-008
DM-PUSH-C-007	Support for HTTP security	5.3	O	
DM-PUSH-C-008	Support for OBEX security	5.4	O	

### B.2 Server Features

Item	Function	Ref.	Status	Requirement
DM-PUSH-S-001	Support for Push Server	4,5	O	DM-PUSH-S-002 OR DM-PUSH-S-003 OR DM-PUSH-S-004 OR DM-PUSH-S-005 OR DM-PUSH-S-006
DM-PUSH-S-002	Support for Non-secure Push Protocol over WSP	5.1	O	
DM-PUSH-S-003	Support for Secure Push Protocol over WSP	5.1	O	
DM-PUSH-S-004	Support for Push Protocol over SIP	5.2	O	
DM-PUSH-S-005	Support for Push Protocol over HTTP	5.3	O	DM-PUSH-S-007
DM-PUSH-S-006	Support for Push Over OBEX	5.4	O	DM-PUSH-S-008
DM-PUSH-S-007	Support for HTTP security	5.3	O	
DM-PUSH-S-008	Support for OBEX security	5.4	O	