



OMA Push Management Object

Approved Version 1.0 – 09 Aug 2011

Open Mobile Alliance
OMA-TS-Push_MO-V1_0-20110809-A

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.

© 2011 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.....	6
3.1 CONVENTIONS	6
3.2 DEFINITIONS.....	6
3.3 ABBREVIATIONS	6
4. INTRODUCTION	7
5. PUSH MANAGEMENT OBJECT.....	8
5.1 MANAGEMENT OBJECT PARAMETERS	8
APPENDIX A. CHANGE HISTORY (INFORMATIVE).....	12
A.1 APPROVED VERSION HISTORY	12

Figures

Figure 1.....	8
---------------	---

1. Scope

This document defines the OMA Push Management Object that manages the push whitelist.

2. References

2.1 Normative References

- [PUSH] "OMA Push Over The Air, Version 2.2 ". Open Mobile Alliance™
OMA-TS-PushOTA-V2_2. [URL:http://www.openmobilealliance.org](http://www.openmobilealliance.org)
- [DMSTDOBJ] "OMA Device Management Standardized Objects, Version 1.2". Open Mobile Alliance™
OMA-TS-DM-StdObj-V1_2. [URL:http://www.openmobilealliance.org](http://www.openmobilealliance.org)
- [DM-TND-V1-2] "OMA Device Management Tree and Description, Version 1.2". Open Mobile Alliance™
OMA-TS-DM_TND-V1_2 [URL:http://www.openmobilealliance.org](http://www.openmobilealliance.org)
- [DMBOOT] "OMA Device Management Bootstrap, Version 1.2". Open Mobile Alliance™. OMA-TS-DM_Bootstrap-V1_2. [URL:http://www.openmobilealliance.org](http://www.openmobilealliance.org)
- [DMTNDS] "OMA Device Management Tree and Description Serialization Specification, Version 1.2". Open Mobile Alliance. OMA-TS-DM_TNDS-V1_2. [URL:http://www.openmobilealliance.org](http://www.openmobilealliance.org)
- [RFC1918] *Address Allocation for Private Internets*
<http://www.rfc-editor.org/rfc/rfc1918.txt>
- [RFC791] *RFC 791, Internet Protocol,*
DARPA, 1981, URL:<http://www.ietf.org/rfc/rfc791.txt>
- [RFC3513] *RFC 3513, Internet Protocol Version 6 (IPv6) Addressing Architecture,* §§2.2, 2.3
The Internet Society, 2003, URL:<http://www.ietf.org/rfc/rfc3513.txt>
- [RFC2373] *IP Version 6 Addressing Architecture*
<http://www.ietf.org/rfc/rfc2373.txt>
- [RFC3986] URI Generic Syntax
<http://rfc.net/rfc3986.html>
- [GENFORM] "WAP General Formats Document", WAP Forum_, WAP-188-WAPGenFormats, URL:
<http://www.openmobilealliance.org/>

2.2 Informative References

- [PUSHMO-DDF] "Push Management Object Device Description Framework", URL:
<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

See the DM Tree and Description [DM-TND-V1-2] document for definitions of terms related to the management tree.

3.3 Abbreviations

OMA	Open Mobile Alliance
MO	Management Object
SMSC	Short Message Service Centre
PPG	Push Proxy Gateway

4. Introduction

DM group has defined Management Objects where parameters can be easily managed and used by applications. This document describes the OMA Push Management Object syntax that manages the push whitelists.

5. Push Management Object

Push Management Object (MO) is an object for OMA BAC Push that restricts the accepted push messages depending on the originating PPG address or the originating SMSC address. The MO can be initially provisioned and is used for continuous provisioning to update service configurations.

If the Push MO is provisioned together with other management object(s) during bootstrap then [DMTND5] and [DMBOOT] MUST be used.

The OMA BAC Push Management Object consists of relevant parameters required by the PUSH enabler. It is compatible with OMA Device Management protocol specifications, version 1.2, and is defined using the OMA DM Device Description Framework as described in [DM-TND-V1-2] and [DMSTDOBJ].

The Management Object Identifier is: urn:oma:mo:oma-push:1.0

Protocol compatibility: This MO is compatible with OMA DM 1.2.

The following figure shows the nodes and leaf objects for the OMA_PUSH Management Object.

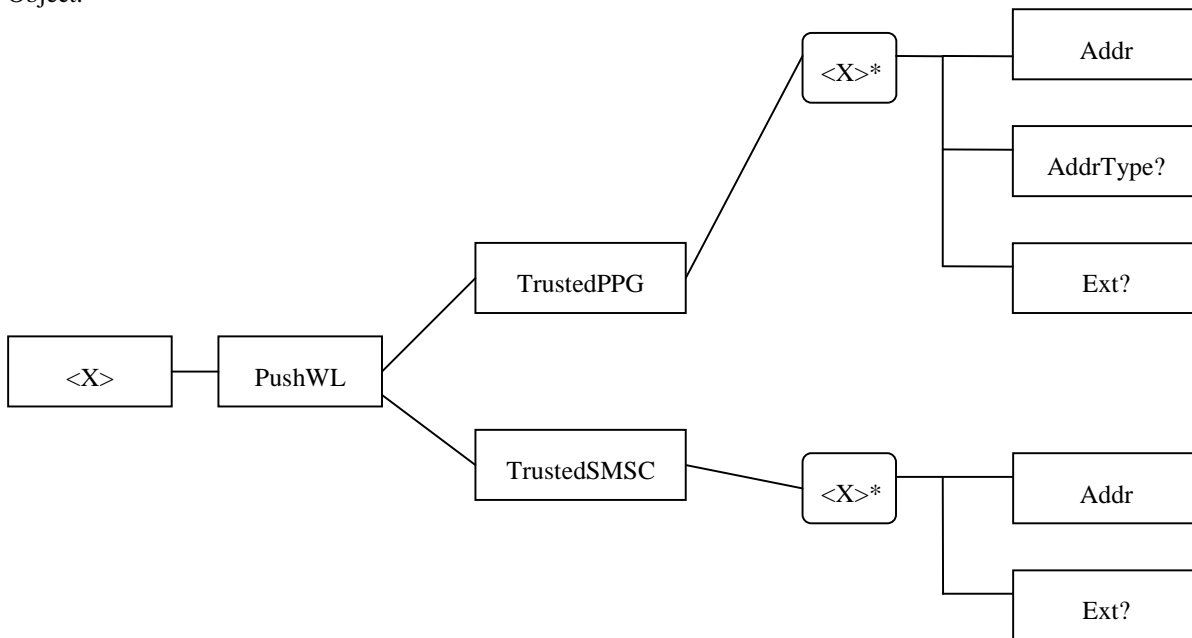


Figure 1

5.1 Management Object parameters

This section describes the parameters for the OMA BAC PUSH Management Object. The procedure to validate whether the Push PDU originates from a trusted source or not is defined in [PUSH].

Node: /<X>

This interior node acts as a placeholder for one or more accounts for a fixed node. It specifies the object root of a BAC PUSH management object. The purpose of this interior node is to group together the parameters of a single

BAC PUSH object. The ancestor elements of this node define the position in the management tree of the BAC PUSH object. But the structure of the DM tree and hence positions in the tree of management objects is out of scope of this specification.

Status: Required
Occurrence: OneOrMore
Format: Node
Access Types: Get
Values: N/A

/<X>/PushWL

The PushWL interior node is used to hold a list of PPG Addresses and/or a list of SMSCAddresses.

Status: Required
Occurrence: One
Format: Node
Access Type: Get
Value: N/A

/<X>/PushWL/TrustedPPG

The TrustedPPG interior node is used to list the PPG addresses from which push message is trusted. It makes it possible to specify a plurality of addresses.

Status: Required
Occurrence: One
Format: Node
Access Type: Get
Value: N/A

/<X>/PushWL/TrustedSMSC

The TrustedSMSC interior node is used to list the SMSC addresses from which push message content is trusted. It makes it possible to specify a plurality of addresses.

Status: Required
Occurrence: One
Format: Node
Access Type: Get
Value: N/A

/<X>/PushWL/TrustedPPG /<X>*

This node contains the instances of authorized Push Proxy Gateway addresses.

Status: Required
Occurrence: ZeroOrMore
Format: Node
Access Type: Get
Value: N/A

/<X>/PushWL/TrustedSMSC /<X>*

This node contains the instances of authorized SMSC addresses.

Status: Required
Occurrence: ZeroOrMore
Format: Node
Access Type: Get
Value: N/A

/<X>/PushWL/TrustedPPG /<X>/Addr

The Addr node holds addresses of different types, for example, an IP address or an URI. The type of address in the

field can be determined on the AddrType node.

Status: Required
 Occurrence: One
 Format: Chr
 Access Type: Get
 Value: N/A

/<X>/PushWL/TrustedPPG/<X>+/AddrType?

This leaf node specifies the type of NAP address supplied as the **Addr** leaf node value. If this node is omitted, the type of the Addr node value MUST be IPv4.

AddrType	Value of Addr node
IPv4	An IPv4 address [RFC791] represented in string form dotted-decimal CIDR notation Subnetwork addressing using the CIDR notation is allowed (e.g. 12.11.10.9/15) [RFC1918] IPV4 is the default value of the AddrType node
IPv6	An IPv6 address represented in string form as in [RFC3513] Subnetwork addressing using the CIDR notation is allowed [RFC2373]
URI	URI formed as in [RFC3986]
E164	A phone number according to the E164 scheme [GENFORM]

Status: Optional
 Occurrence: ZeroOrOne
 Format: Chr
 Access Type: Get
 Value: IPv4

/<X>/PushWL/TrustedPPG /<X>+/Ext?

The Ext is an interior node where the vendor-specific information about the OMA_BAC-PUSH MO is placed (“vendor” means application vendor, device vendor etc.). Usually the vendor extension is identified by a vendor-specific name under the ext node. The tree structure under the vendor identified is not defined and can therefore include a non-standardized sub-tree.

Status: Optional
 Occurrence: ZeroOrOne
 Format: node
 Access Types: Get
 Values: N/A

/<X>/PushWL/TrustedSMSC/<X>+/Addr

The Addr node holds the trusted SMSC E164 address.

Status: Required
 Occurrence: One
 Format: Chr
 Access Type: Get
 Value: N/A

/<X>/PushWL/TrustedSMSC/<X>+/Ext?

The Ext is an interior node where the vendor-specific information about the OMA_BAC-PUSH MO is placed (“vendor” means application vendor, device vendor etc.). Usually the vendor extension is identified by a vendor-specific name under the ext node. The tree structure under the vendor identified is not defined and can therefore include a non-standardized sub-tree.

Status: Optional
 Occurrence: ZeroOrOne
 Format: node

Access Types: Get
Values: N/A

The complete Device Description Framework of this Push management object can be found in [PUSHMO-DDF].

Appendix A. Change History (Informative)

A.1 Approved Version History

Reference	Date	Description
Approved Version: OMA-TS-Push_MO-V1_0-20110809-A	09 Aug 2011	Status changed to Candidate by TP: OMA-TP-2011-0282-INP_Push_V2_2_ERP_for_Final_Approval