# GwMO Requirements

Candidate Version 1.0 – 31 Aug 2010

**Open Mobile Alliance**

OMA-RD-GwMO-V1_0-2010831-C

Each Open Mobile Alliance member has agreed to use reasonable endeavours 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.

# Contents

# Tables

# 1. Scope (Informative)

This document lists the requirements for the OMA DM Gateway Management Object enabler. It mainly focuses on requirements to enable a DM Server to manage devices that are not directly accessible to the OMA-DM Server e.g. because the devices are deployed behind a firewall or because the devices do not support the OMA-DM protocol. This document also provides requirements for management of devices in a Machine to Machine (M2M) ecosystem (e.g. fanning out DM commands from a DM Server to multiple end devices and aggregating responses from multiple end devices so that a consolidated response is sent back to the DM Server).

The following issues are outside the scope of this document:

- Device discovery mechanisms
- Management protocol adaptation rules

# 2. References

## 2.1 Normative References

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

## 2.2 Informative References

**[DMDICT]** " OMA Device Management Dictionary", Draft Version 1.0, , Open Mobile Alliance™, URL:http://www.openmobilealliance.org/

**[OMADICT]** “Dictionary for OMA Specifications”, Version x.y, Open Mobile Alliance™, OMA-ORG-Dictionary-Vx_y, 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

Kindly consult [DMDICT] and [OMADICT] for all definitions used in this document.

## 3.3 Abbreviations

| | |
|---|---|
| **DM** | Device Management |
| **GwMO** | Gateway Management Object |
| **OMA** | Open Mobile Alliance |

# 4. Introduction (Informative)

The OMA DM protocol is used for the remote management of devices. In many instances, the OMA-DM Server and the OMA-DM Client communicate with each other directly. However, direct communication between the DM Server and the DM Client is not always possible, nor desirable, due to inaccessibility of devices behind a firewall or devices supporting a management protocol other than OMA-DM. This document provides the requirements for OMA DM to manage devices indirectly i.e. through a gateway. This gateway is managed by an OMA DM server, and in turn, the gateway manages other devices under it.

# 5. Gateway Management Object release description (Informative)

The GwMO Enabler SHALL be compatible with DM 1.3 and later versions of the OMA-DM protocol.

## 5.1 Modes of Operation

The GwMO enabler defines the following operation modes:

- **Transparent Mode**: The DM Gateway maintains a mapping between the local/private and global/public identity of the device to assist the DM server in sending a notification to the DM client deployed behind the DM Gateway.
- **Proxy Mode**: The DM Gateway manages devices on behalf of the OMA-DM Server over DM protocol.
- **Adaptation Mode**: The DM Gateway manages non-OMA-DM devices on behalf of the OMA-DM Server over a device supported protocol.

# 6. Requirements (Normative)

## 6.1 High-Level Functional Requirements

| Label | Description | Release |
|---|---|---|
| GwMO-HLF-001 | The GwMO enabler SHALL support a mechanism to allow DM sessions against a device placed behind a firewall or NAT (“Network Address Translator”). | 1.0 |
| GwMO-HLF-002 | The GwMO enabler SHALL specify a mechanism to allow continuous management of devices, even if the devices are moved across networks. | 1.0 |
| GwMO-HLF-003 | The GwMO enabler SHALL support adding a new Device, so that the Device can be managed through the Gateway. | 1.0 |

**Table 1: High-Level Functional Requirements**

### 6.1.1 Security

#### 6.1.1.1 Authentication

| Label | Description | Release |
|---|---|---|
| GwMO-SECACATE-001 | The GwMO enabler SHALL conform to the authentication requirements of OMA-DM. | 1.0 |
| GwMO-SECACATE-002 | The GwMO enabler SHALL provide a mechanism to have a single authentication for a group of devices under the DM Gateway. | 1.0 |

**Table 2: High-Level Functional Requirements – Authentication Items**

#### 6.1.1.2 Authorization

| Label | Description | Release |
|---|---|---|
| GwMO-SECARIZE-001 | The GwMO enabler SHALL conform to the authorization requirements of OMA-DM. | 1.0 |

**Table 3: High-Level Functional Requirements – Authorization Items**

#### 6.1.1.3 Data Integrity

| Label | Description | Release |
|---|---|---|
| GwMO-SECDI-001 | The GwMO enabler SHALL conform to the data integrity requirements of OMA-DM. | 1.0 |

**Table 4: High-Level Functional Requirements – Data Integrity Items**

#### 6.1.1.4 Confidentiality

| Label | Description | Release |
|---|---|---|
| DM-SECCONF-001 | The GwMO enabler SHALL conform to the confidentiality requirements of OMA-DM. | 1.0 |

**Table 5: High-Level Functional Requirements – Confidentiality Items**

### 6.1.2 Charging Events

N/A

### 6.1.3 Administration and Configuration

| Label | Description | Release |
|---|---|---|
| GwMO-ADM-001 | The GwMO enabler SHALL support the management of the DM Gateway and associated functionalities (e.g. NAT, firewall, router). | 1.0 |

**Table 6: High-Level Functional Requirements – Administration and Configuration Items**

### 6.1.4 Usability

N/A

### 6.1.5 Interoperability

| Label | Description | Release |
|---|---|---|
| GwMO-IOP-001 | The GwMO enabler SHALL allow a device with a non OMA-DM Client to be managed by an OMA-DM Server, via a DM Gateway operating in the Protocol Adaptation mode. | 1.0 |

**Table 7: High-Level Functional Requirements – Interoperability Items**

### 6.1.6 Privacy

N/A

## 6.2 Overall System Requirements

N/A

## 6.3 Modes of Operation

| Label | Description | Release |
|---|---|---|
| GwMO-MOO-001 | The GwMO enabler SHALL provide a mechanism to allow a DM Gateway to choose which operation modes (Transparent mode, Proxy mode or Adaptation mode) should be used. | 1.0 |

**Table 8: Operation Modes Requirements**

### 6.3.1 Transparent Mode

| Label | Description | Release |
|---|---|---|
| GwMO-TMode-001 | The GwMO enabler SHALL enable a DM Server to send a notification to a DM Client that is running on a device that does not have a publicly routable address. | 1.0 |

**Table 9: Transparent Mode Requirements**

### 6.3.2 Proxy Mode

| Label | Description | Release |
|---|---|---|
| GwMO-PMode-001 | The GwMO enabler SHALL support a proxy mechanism between DM Server and DM Client that is running on a device which is behind the DM Gateway. | 1.0 |
| GwMO-PMode-002 | The GwMO enabler SHALL allow a DM Gateway, operating in the Proxy Mode, to bootstrap a DM Client running on the end Device. | 1.0 |
| GwMO-PMode-003 | The GwMO enabler SHALL support a mechanism to enable remote management of an end device that is not bootstrapped with any external DM Server. | 1.0 |

**Table 10: Proxy Mode Requirements**

### 6.3.3 Protocol Adaptation Mode

| Label | Description | Release |
|---|---|---|
| GwMO-AMode-001 | The GwMO enabler SHALL support the ability to manage devices that support management protocols other than OMA-DM. | 1.0 |

**Table 11: Protocol Adaptation Mode Requirements**

## 6.4 Device Inventory

| Label | Description | Release |
|---|---|---|
| GwMO-DI-001 | The GwMO enabler SHALL support querying of a DM Gateway to obtain specified information of a device that is deployed behind a DM Gateway. | 1.0 |
| GwMO-DI-002 | The GwMO enabler SHALL support querying of a DM Gateway to obtain summarized information pertaining to all the devices that are deployed behind the Gateway. | 1.0 |
| GwMO-DI-003 | The GwMO enabler SHALL support the ability to show the status, attached or detached, of the registered device behind a DM Gateway. | 1.0 |
| GwMO-DI-004 | The GwMO enabler SHALL support the ability to inform the DM Server about the newly registered devices behind a DM Gateway. | 1.0 |
| GwMO-DI-005 | The GwMO enabler SHALL allow the DM Server to configure whether it will be informed for newly registered devices behind a DM Gateway. | 1.0 |

**Table 12: Device Inventory Requirements**

## 6.5 Command Fan-out and Response Aggregation

| Label | Description | Release |
|---|---|---|
| GwMO-FORA-001 | The GwMO enabler SHALL support the ability to fan-out DM commands from a DM Server to a desired set of end Devices behind the Gateway. | 1.0 |
| GwMO-FORA-002 | The GwMO enabler SHALL support the ability to aggregate responses from multiple end Devices and send a consolidated response back to the DM Server. | 1.0 |

**Table 13: Command Fan-out and Response Aggregation Requirements**

## 6.6 Device Configuration and Image Storage

| Label | Description | Release |
|---|---|---|
| GwMO-DCIS-001 | The GwMO enabler SHALL support the ability to store data from the DM Server on the DM Gateway, e.g. Delivery Package for SCOMO, for local retrieval by devices behind this DM Gateway. | 1.0 |
| GwMO-DCIS-002 | The GwMO enabler SHALL provide an optimized and configurable mechanism to store data on a DM Gateway, e.g., Delivery Package for SCOMO, if the data are the same for multiple devices behind the DM Gateway. | 1.0 |
| GwMO-DCIS-003 | The GwMO enabler SHALL allow the DM Server to configure whether the data, e.g. Delivery Package for SCOMO can be stored on a DM Gateway for local retrieval by devices behind it. | 1.0 |

**Table 14: Device Configuration and Image Storage Requirements**

# 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 GwMO 1.0 History

| Document Identifier | Date | Sections | Description |
|---|---|---|---|
| Draft Versions<br>OMA-RD-GwMO-V1_0 | 30 Apr 2010 | All | Baseline document as agreed in "OMA-DM-GwMO-2010-0002-INP_Baseline_RD":<br>Imported the gateway requirements that were deleted from OMA-RD-DM-V2_0-20100124-D<br>Added some requirements based on OMA-DM-GwMO-2010-0001R01-INP_Use_Case_Discussion |
| | 03 May 2010 | All | Clerical change from "TS" to "document" in section 4<br>Re-numbering of tables in the whole document. |
| | 25 May 2010 | 4, 6.1, Appendix B | Incorporated Agreed CR "OMA-DM-GwMO-2010-0005R01-CR_Additional_Requirements_for_GwMO" |
| | 30 Jun 2010 | All | Incorporated the following Agreed CRs:<br>OMA-DM-GwMO-2010-0006R03-CR_Adding_New_Requirements<br>OMA-DM-GwMO-2010-0007-CR_RD_Aggregation_Revised<br>OMA-DM-GwMO-2010-0010R01-CR_Reqs_related_to_M2M<br>OMA-DM-GwMO-2010-0012R01-CR_Clarification_Changes<br>OMA-DM-GwMO-2010-0014R01-CR_Clarification_Changes__GwMO_HLF_007 |
| | 13 Jul 2010 | All | Incorporated the following Agreed CRs:<br>OMA-DM-GwMO-2010-0020R01-CR_GwMO_RD_Restructuring<br>OMA-DM-GwMO-2010-0021R01-CR_RD_Appendix_Update |
| Candidate Version<br>OMA-RD-GwMO-V1_0 | 31 Aug 2010 | N/A | Status changed to Candidate by TP<br>TP ref # OMA-TP-2010-0380-INP_GwMO_V1_0_RD_for_Candidate_approval |

# Appendix B. Use Cases (Informative)

As part of the use case analysis, the DM WG prioritized the use cases for GwMO. The high priority use cases for GwMO are listed in the following sub-sections. It needs to be noted that not all the requirements in this RD have accompanying use cases.

## B.1 Server initiated session, with DM Gateway operating in Transparent Mode

John Doe has a device that sits behind a residential gateway that provides the DM Gateway functionality. The DM Gateway is operating in the Transparent Mode. A DM Server needs to perform a management action on John Doe's device. The DM Server knows beforehand that John Doe's device is sitting behind the DM Gateway. In order to trigger the device to initiate a session, the DM Server initiates a management session with the DM Gateway and obtains the publicly routable address for John Doe's device. The DM Server then uses this address to push Package 0 to John Doe's device, using OMA-Push. John Doe's device validates the notification message (checking that the digest is valid, the Server has been previously bootstrapped etc.) and establishes a management session with the DM Server.

## B.2 Server initiated session, with DM Gateway operating in Proxy Mode

Ronnie Arbuckle has a device that sits behind a residential gateway, which provides the DM Gateway functionality. The DM Gateway is operating in the Proxy Mode. A DM Server needs to perform a management action on Ronnie Arbuckle's device. The DM Server knows beforehand that Ronnie Arbuckle's device is sitting behind the DM Gateway. In order to trigger the device to initiate a session, the DM Server sends the DM notification to the DM Gateway. The notification message contains the address of the target device. The DM Gateway validates the notification message (checking that the digest is valid, the Server has been previously bootstrapped etc.) and resolves the target device address. It then forwards the notification message to Ronnie Arbuckle's device.

Ronnie Arbuckle's device also validates the notification message before establishing a management session with the DM Gateway. The DM Gateway manages Ronnie Arbuckle's device on behalf of the DM Server. The DM Gateway plays the role of the DM Server for Ronnie Arbuckle's device and the role of the DM Client for the DM Server.

## B.3 Nomadic device address change

Hans Mustermann owns a device that he plugs into different networks at different times (home, office, friend's house etc.). The device is configured in such a way that whenever the address of the device changes, the designated DM Servers receive an alert that contains the updated address, except in the case where the change in address is from one private address to another.

## B.4 LAN device inventory query

All OMA-DM enabled devices in the XYZ Corporation sit behind a DM Gateway. The DM Server queries the DM Gateway for summarized information pertaining to all the devices that are deployed behind the Gateway. The DM Gateway provides this information to the DM Server.

## B.5 Adding a new Device

Vincent purchases a new device for his home. The device is added to his home network, which is behind a residential gateway that provides the DM Gateway functionality. He needs to setup some services in his device. This requires, for example, an external DM server to perform DM account creation / management actions to setup the desired services in the device. But the DM Gateway has no apriori knowledge of the new device. The DM Gateway is provided necessary information about the new device. This will enable the DM Server to perform management actions on the device through the DM Gateway.

## B.6 Aggregation function at the DM Gateway

The Super Duper electronic security company has installed many electronic surveillance devices throughout a high-rise building. The building is serviced by a DM Gateway, and the surveillance devices are deployed behind the Gateway. The company wants to run a diagnostic test on all the devices in the building. A DM request for this purpose is sent from a DM Server to the DM Gateway. The DM Gateway fans out the request to all the surveillance devices (perhaps in a staggered manner, in order to avoid jeopardizing the security of the entire building: however, this is completely transparent to the DM Server). Each device processes the request and sends the result to the DM Gateway. The DM Gateway collects the results and sends the aggregated response to the DM Server.