GwMO Requirements

Approved Version 1.0 – 18 Jun 2013

Open Mobile Alliance

OMA-RD-GwMO-V1_0-20130618-A

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 OMADM Server (for example, 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 (for example, 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

[DMDICT] "OMA Device Management Dictionary, Version 1.0". Open Mobile Alliance™. OMA-SUP-DM_Dictionary-v1_0. URL: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

2.2 Informative References

None.

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] for all definitions used in this document.

3.3 Abbreviations

Kindly consult [DMDICT] for all abbreviations used in this document.

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 (that is, through a gateway). This gateway is managed by an OMA DM Server; 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 DM Gateway has the following operation modes:

- **Transparent Mode**: The DM Gateway assists the DM Server in sending a DM Notification to the End Device(s) behind the DM Gateway. In this mode, the DM Gateway forwards the DM Notification to the End Device(s). The DM Gateway does not participate in the management session that gets established between the DM Server and the End Device after the delivery of the DM Notification to the End Device(s).
- **Proxy Mode**: The DM Gateway manages End Device(s) behind the DM Gateway on behalf of the DM Server over DM protocol. Two related DM sessions are established: one is between the DM Server and the DM Gateway; the other is between the DM Gateway and the End Device(s).
- **Adaptation Mode**: The DM Gateway manages End Device(s) behind the DM Gateway on behalf of the OMA DM Server over a non-OMA DM protocol.

The DM Gateway can operate in different modes for different devices simultaneously.

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
GwMO-HLF-004	The GwMO enabler SHALL support a mechanism to allow management of one or more End Devices via a shared DM Account.	1.0
GwMO-HLF-005	The GwMO enabler SHALL allow a DM Gateway to bootstrap the End Device to the DM Gateway.	1.0
GwMO-HLF-006	The GwMO enabler SHALL allow a DM Gateway to bootstrap the End Device to the DM Server.	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 from a DM Server.	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 the DM Server and the DM Client that is running on a device that 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.	Deleted

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 of 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 of newly registered devices behind a DM Gateway.	1.0

Table 12: Device Inventory Requirements

6.5 Device Group

Label	Description	Release
GwMO-Group-001	The GwMO enabler SHALL allow the DM Server to manage device groups on the DM Gateway.	1.0

Table 13: Device Group Requirements

6.6 Command Fanout and Response Aggregation

Label	Description	Release
GwMO-FORA-001	The GwMO enabler SHALL support the ability to fanout 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 14: Command Fanout and Response Aggregation Requirements

6.7 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 (for example 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 (for example, 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 (for example, Delivery Package for SCOMO) can be stored on a DM Gateway for local retrieval by devices behind it.	1.0

Table 15: Device Configuration and Image Storage Requirements

Appendix A. Change History (Informative)

A.1 Approved Version History

Reference	Date	Description
OMA-RD-GwMO-V1_0-20130618-A	18 Jun 2013	Status changed to Approved by TP TP Ref # OMA-TP-2013-0200-INP_GwMO_V1_0_ERP_for_Final_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 of the requirements in this RD have accompanying use cases.

B.1 Server Initiated Session with the End Device Bypassing the DM Gateway

John Doe has a device that sits behind a residential gateway that provides the DM Gateway functionality. The device has a publicly routable address. 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. 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 directly 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 directly with the DM Server.

B.2 Server Initiated Session with DM Gateway Operating in Transparent Mode

Fred Bloggs has a device that sits behind a residential gateway that provides the DM Gateway functionality. The device does not have a publicly routable address. The DM Gateway is operating in the Transparent Mode. A DM Server needs to perform a management action on Fred's device. The DM Server knows beforehand that Fred's device is sitting behind the DM Gateway. To trigger Fred's device to initiate a session, the DM Server sends a specially formatted DM Notification message to the DM Gateway. The message contains a special header that indicates Fred's device is the target. The DM Gateway validates the notification message (checking that the digest is valid, the Server has been previously bootstrapped, etc.) and forwards the notification message to Fred's device. In turn, Fred's device performs its own validation of the notification message prior to establishing a management session with the DM Server.

B.3 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's device. The DM Server knows beforehand that Ronnie's device is sitting behind the DM Gateway. The DM Server sets up a session with the DM Gateway; within the context of that session, the DM Server sends the DM commands for execution by Ronnie's device to the DM Gateway. The DM Gateway sets up a session with Ronnie's device and forwards the DM commands to Ronnie's device. The DM Gateway receives the response from Ronnie's device, which is stored in the DM Gateway for retrieval by the DM Server. In this case, the DM Gateway plays the role of the DM Server for Ronnie's device and the role of the DM Client for the DM Server.

B.4 Continued Management of Nomadic Devices

Hans Mustermann owns a device that he plugs into different networks at different times (home, office, friend's house, etc.). Even after the device has moved to a different location, a previously bootstrapped DM Server can continue managing the device via its local DM Gateway.

B.5 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 of the devices that are deployed behind the Gateway. The DM Gateway provides this information to the DM Server.

B.6 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 set up some services in his device. This requires, for example, an external DM Server to perform DM account creation /management actions to set up the desired services in the device. But the DM Gateway has no prior knowledge of the new device. The DM Gateway is provided necessary information about the new device, including the security credentials to use. After the DM Gateway discovers the device, the DM Server is able to perform management actions on the device through the DM Gateway.

B.7 Command Fanout and Response 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 of 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 of the surveillance devices. Each device processes the request and sends the result to the DM Gateway. The DM Gateway collects the results and makes the aggregated response available to the DM Server.DM Gateway Needs to be Bootstrapped by the DM Server.

Device ‘A’ is bootstrapped to DM Gateway ‘DMG1’ and ‘DMG1’ has been bootstrapped to DM Server ’DMS1’. Now Device ‘A’ is relocated to a new environment where it can be bootstrapped to ’DMG2’; however, ‘DMG2’ has not been bootstrapped by ’DMS1’. In this scenario, new DM Gateway ‘DMG2’ needs to find a way to be bootstrapped by the DM Server ‘DMS1’ so that ‘DMS1’ can continue to manage Device ‘A’.

B.8 Image Distribution with the DM Gateway

Chagall has a couple of devices that need to be updated since they have the old version of software installed. The DM Server delivers the updated image required for the software update to the local DM Gateway. After obtaining the URI of the image stored at the DM Gateway, the DM Server asks the DM Gateway to initiate a fanout operation, which contains the obtained URI to update the software. The fanout operation efficiently updates Chagall’s devices since each device downloads the image from the local DM Gateway.

B.9 Inventory Update Alert

Vincent purchases an office gateway with integrated firewall functionality for his company’s office from the operator Pavan. The office gateway has already been factory bootstrapped to Pavan’s DM Server. Once Vincent installs and does the required initial configuration on the office gateway, it establishes a DM session with Pavan’s DM Server. A few weeks later, Vincent purchases a new device from Pavan for his office. In Vincent’s office, all devices are deployed behind a firewall and are assigned a private IP address. The device is added to Vincent’s office network. The device discovers the office gateway and establishes a DM session with it. The gateway sees that this is a new device (that is, not previously connected). Thereafter, the office gateway sends an inventory update alert to Pavan’s DM Server to announce that a new device has been added to the network and can now be managed via the office gateway.

B.10 DM Gateway Operating in Adaptation Mode for End Devices

B.10.1 Short Description

Joe purchases a device for his home use. The device is added to his home network, which is behind a gateway that provides the DM Gateway functionality. While all Joe’s existing devices on the home network support OMA DM, Joe’s new device only supports non-OMA DM protocol. Since the home gateway that provides the DM gateway functionality also supports non-OMA DM protocol on Joe’s new device, Joe’s current service provider can manage and provision Joe’s new device along with his existing home devices through the OMA DM Server available in the Service Provider’s network without additional installations or support.