OMA Device Management Sessionless Command Message

Approved Version 1.3 – 24 May 2016

Open Mobile Alliance

OMA-TS-DM_Sessionless-V1_3-20160524-A

Contents

Figures

1. Scope

This document defines how an OMA DM message may be sent to a DM Client for continuous management in a sessionless manner.

2. References

2.1 Normative References

[ConnMO] "Connectivity Management Objects, Version 1.0", Open Mobile Alliance™, OMA-DDS-DM_ConnMO-V1_0, URL:http://www.openmobilealliance.org

[DMBootstrap] "OMA Device Management Bootstrap, Version 1.3". Open Mobile Alliance™. OMA-TS-DM_Bootstrap-V1_3. URL:http://www.openmobilealliance.org

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

[DMPRO] "OMA Device Management Protocol, Version 1.3". Open Mobile Alliance™. OMA-TS-DM_Protocol-V1_3. URL:http://www.openmobilealliance.org/

[DMSecurity] "OMA Device Management Security, Version 1.3". Open Mobile Alliance™. OMA-TS-DM_Security-V1_3. URL:http://www.openmobilealliance.org

[DMSTDOBJ] "OMA Device Management Standardized Objects, Version 1.3". Open Mobile Alliance™. OMA-TS-DM_StdObj-V1_3. URL:http://www.openmobilealliance.org

[DMTND] "OMA Device Management Tree and Description, Version 1.3". Open Mobile Alliance™. OMA-TS-DM_TND-V1_3. URL:http://www.openmobilealliance.org

[DMTNDS] "OMA Device Management Tree and Description Serialization, Version 1.3". Open Mobile Alliance™. OMA-TS-DM_TNDS-V1_3. URL:http://www.openmobilealliance.org

[META] "OMA Device Management Meta Information", Open Mobile Alliance™, OMA-TS-DM_DM_MetaInfo-V1_3, 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

[SCRRULES] "SCR Rules and Procedures", Open Mobile Alliance™, OMA-ORG-SCR_Rules_and_Procedures, URL:http://www.openmobilealliance.org/

[WBXML1.1] "WAP Binary XML Content Format Specification", WAP Forum™. SPEC-WBXML-19990616.pdf. URL:http://www.openmobilealliance.org

[WBXML1.2] "WAP Binary XML Content Format Specification", WAP Forum™. WAP-154-WBXML. URL:http://www.openmobilealliance.org

[WBXML1.3] "WAP Binary XML Content Format Specification", WAP Forum™. WAP-192-WBXML. URL:http://www.openmobilealliance.org

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

Other OMA DM specifications define how a DM Client is bootstrapped, or how a DM management session is established and maintained. This specification defines the Sessionless Command Message and Sessionless Process which is an alternative to session-based DM mechanism. Sessionless Process can be performed by sending a Sessionless Command Message to a DM Client using a push technology.

5. Sessionless Management

5.1 Sessionless Management Scenario

OMA DM devices need to be able to function in diverse network environments and use a large set of protocols. This makes it hard to find a 'one size fits all' solution to the sessionless management problem. This section illustrates the requirements and processes for Sessionless Process.

5.1.1 Requirements

An OMA DM solution capable of continuous management outside a normal DM session needs to address these requirements:

- Re-use technology (WAP Push, SIP Push, HTTP Push, OMA BCAST, etc),
- Highly interoperable,
- Secure (signed and authenticated),
- Transport encoding is [WBXML1.1], or [WBXML1.2], or [WBXML1.3],
- Previously bootstrapped DM Client.

5.1.2 Solutions

This document defines how to perform the Sessionless Process. A DM Server sends out a Sessionless Command Message via some push mechanisms or broadcast mechanisms as specified in section 5.3.

Regardless of how the device has been configured, the DM Server is now in a position where it can send out a Sessionless Command Message. This Sessionless Command Message contains management commands to the device as defined in section 5.2.

It is critical that DM Clients accept Sessionless Management messages only from DM Servers that have a corresponding DMAcc on the device. Furthermore, each Sessionless Command Message MUST be signed. The DM Client MUST authenticate every Sessionless Command Message.

Figure 1 gives an overview of this scenario.

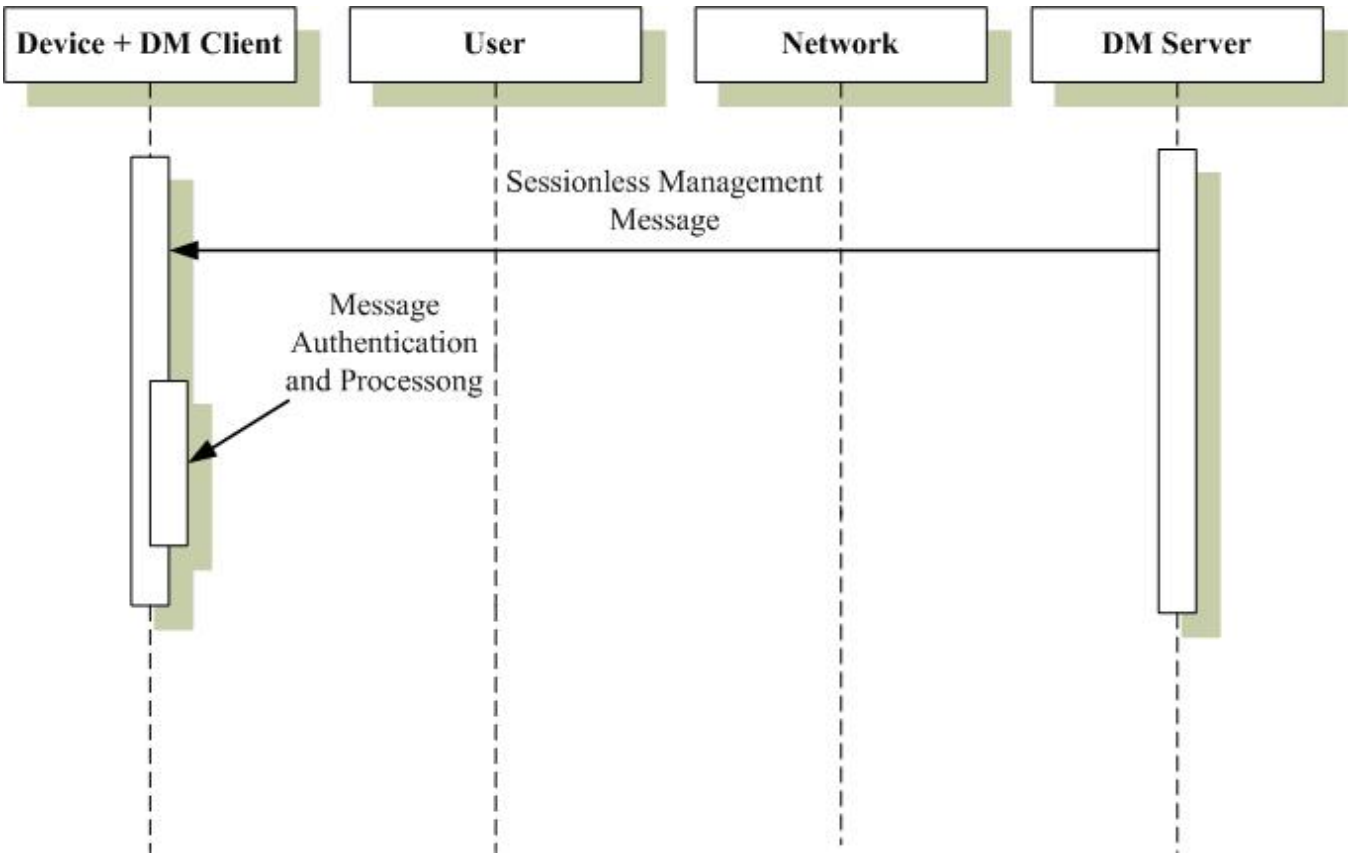

Figure 1: Sessionless Management

5.2 Sessionless Command Message Content

Sessionless Command Message is a standalone DM Message sent from a DM Server to a DM Client, outside a Management Session. The content of a Sessionless Command Message is an OMA DM message. However, this message is a special package in many ways since it is not part of an ongoing OMA DM session but rather a one-time message. Hence, many of the elements needed to manage the session are superfluous in this context, but they must still be included so that the message can be processed by the normal DM client.

In terms of structure and method of delivery to the DM Client, the Sessionless DM Message is somewhat similar to the DM Bootstrap message [DMBootstrap], although the two are used for completely different purposes. It is, however, quite easy to distinguish between these two types of messages. A DM Bootstrap message contains TNDS data pertaining to a DMAcc Management Object whereas a Sessionless DM Message does not.

This is the list of requirements for Sessionless Command Message.

- Within the SyncHdr element:
  - The value of the VerDTD element MUST be '1.2'.
  - The value of the VerProto element MUST be ‘DM/1.3’.
  - SessionID MAY be ignored by the DM Client.
  - MsgID MAY be ignored by the DM Client.
  - The Target element MUST be used to identify the target device.
  - The Source element MUST match the value of the ServerID node in one of the previously bootstrapped DMAcc MO instances.

- Cred element MUST be used to include DM Server's authentication information according to the rules described in Section 5.4.

- Within the SyncBody:
  - CmdID is REQUIRED.
  - Source MUST be used if URI is needed to further address the source dataset.
  - Target MUST be used if URI is needed to further address the target dataset.
  - The Data element inside Item is used to include the data itself unless the command does not require a Data element.
  - The Meta element inside an operation or inside an Item MUST be used when the Type or Format are not the default values [META].
- The Final element MUST be used in the SyncBody for the message.
- The GET command MUST NOT be included.

The Sessionless Command Messages MUST be [WBXML1.1], or [WBXML1.2], or [WBXML1.3] encoded. The DM servers MUST NOT expect any response to a Sessionless Command Message.

A DM Client MUST support WBXML encoded TNDS objects and normal TNDS objects [DMTNDS] and MUST support the Inbox.

5.3 Sessionless Command Message Size Restriction

The Bootstrap Message MUST NOT exceed the maximum message size, as specified by the *MaxMsgSize* [META] meta information element. In other words, the entire Bootstrap Message MUST fit entirely within one DM message and it MUST NOT use the Large Object [DMPRO] feature.

5.4 Transport

The Sessionless Command Message can be delivered over different transports as shown below:

- WAP Push
- SIP Push
- HTTP Push
- OMA BCAST

Other transport MAY also be used to send the Sessionless Command Message to the DM Client.

The Sessionless Command Message MUST be sent to the DM Client via secure transport. Transport neutral security MAY also be applied to the Sessionless Command Message.

See the security document for further information [DMSecurity].

5.5 Authentication and Management Object Access Rights

When the transport to send the Sessionless Command Message is unable to provide authentication and integrity, HMAC-SHA256 authentication mechanism, which is defined in [DMSecurity], MUST be used as transport neutral integrity.When a Sessionless Command Message adds new TNDS objects [DMTNDS] - any ACL values that are to be set for these objects MUST be included in the TNDS data as ACL property data for the applicable nodes.

5.6 Processing of the Sessionless Command Message

The DM Client MUST have previously bootstrapped with the DMAcc [DMSTDOBJ] for the DM Server sending the Sessionless Command Message.

A Sessionless Command Message is processed just like a normal DM message, except:

- The DM Client MUST NOT send response message to the DM Server; (Note that this does not preclude the device from initiating a new DM session as a consequence of the Sessionless Command Message if supported by the relevant Management Object specifications);
- The ServerID in the SyncHdr/Source/LocURI MUST match a ServerID in only one of the DMAcc in the DM Tree;
- The DM Client MUST authenticate the Sessionless Command Message based on the authentication information in the matching DMAcc;
- The DM Client MUST use the ServerID from the matching DMAcc for all ACL decisions for the Sessionless Command Message;
- The DM Client MUST reject the Sessionless Command Message if there is no matching DMAcc for this ServerID.
- The DM Client MUST reject the Sessionless Command Message if there is transport neutral security and it fails.

The DM Client MAY rename a new Management Object if it is delivered within a Sessionless Command Message. In the case of the Connectivity or Proxy Management Object [ConnMO] the DM Client SHOULD also rename the values of the corresponding connectivity references to the new name for all MO's encoded within the same TNDS object.

When a TNDS object contains a MO where connectivity references are linked to a Connectivity or Proxy MO that also are included in the same TNDS object, then the values of those connectivity references MAY contain a URI that starts with "./Inbox". In that case the URI MUST have the value of "./Inbox/" plus the URI of that Connectivity or Proxy MO's location in the same TNDS object.

If a DM Client encounters an item with a URI of the EXT sub-tree that it is not prepared to handle, the DM Client MAY ignore that item so that the overall message may succeed.

If the Sessionless Command Message contains a MO that the DM Client does not support, the DM Client MAY ignore this MO, so that the overall message may succeed.

If the Sessionless Command Message contains multiple versions of a MO, the DM Client SHOULD use the latest version of that MO that it supports and ignore the other versions so that the overall message may succeed.

6. Sessionless Command Message Usage

There are two major usages for Sessionless Command Message:

- Adding new Management Objects into the management tree;
- Managing exiting Management Objects using Add, Replace, Delete and Exec commands.

Sessionless Command Message MUST NOT be used to provision the DM Account MO to the devices. The bootstrap mechanism defined in DM Bootstrap [DMBootstrap] is used for provisioning DM Account MO to the devices.

6.1 Add New MO using Sessionless Command Message

There are two ways to provision the new Management Object into the devices as shown below.

6.1.1 Inbox + TNDS

The new Management Object can be transformed into xml or wbxml file using the TNDS mechanism specified in [DMTNDS]. In case the DM Server wants the DM Client to choose where to create a management object in the management tree, the DM Server can send the TNDS encoded Management Object to the device with the URI "./Inbox" as defined in [DMSTDOBJ]. The DM Client MUST add this Management Object into the DM tree using a location of DM Client's choice.

It is not possible to add new Management Object node by node against the URI "./Inbox" since no child nodes are allowed for "./Inbox" and Inbox mechanism has to be used together with TNDS mechanism.

6.1.2 Absolute URI or Relative URI

In case the DM Server knows exactly where the new Management Object is located, the DM Server can send the TNDS encoded Management Object to the device using one Add command with the absolute URI or relative URI [DMPRO]. Alternatively the DM Server can send the new Management using multiple Add commands without TNDS encoding.

6.2 Managing existing MO using Sessionless Command Message

Since no child nodes are allowed for "./Inbox" and only Add command is allowed to be used on "./Inbox" mechanism as described in [DMSTDOBJ], it is not possible to send Sessionless Command Message using "./Inbox" as the target URI for managing existing MOs. In order to manage existing MOs using Sessionless Command Message, the DM Server MUST either knows absolute URI or relative URI [DMPRO] of each node to be manipulated in advance or use the Virtual URI mechanism defined in section 7.2 of [DMTND].

6.2.1 Absolute URI or Relative URI

In order to manage existing MOs using Sessionless Command Message, if the DM Server knows in advance the exact location of nodes to be manipulated, nodes' Absolute URI or relative URI [DMPRO] can be included in Add, Replace, Delete or Exec commands.

6.2.2 Virtual URI

If the DM Server does not know the exact location of nodes to be manipulated, Virtual URI mechanism can be used with Add, Replace, Delete or Exec commands as specified in the Section 7.2 of [DMTND]. The DM Client and the DM Server MUST support Virtual URI mechanism if Sessionless Command Message is supported.

Appendix A. Change History (Informative)

A.1 Approved Version History

Reference	Date	Description
OMA-TS-DM_Sessionless-V1_3-20160524-A	24 May 2016	Status changed to Approved by TP TP Ref # OMA-TP-2016-0041R01-INP_DM_V1_3_ERP_for_final_Approval

Appendix B. Static Conformance Requirements (Normative)

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

B.1 SCR for DM Client

Item	Function	Reference	Requirement
DM-SM-C-001-M	Support for OMA Sessionless Management	Section 5.2	
DM-SM-C-002-M	Support for embedded WBXML encoded TNDS objects and normal TNDS objects.	Section 5.2	
DM-SM-C-003-M	Support for Inbox.	Section 5.2	
DM-SM-C-004-M	ServerID in SyncHdr/Source/LocURI must match the ServerID in only one DMAcc	Section 5.6	
DM-SM-C-005-M	ServerID in SyncHdr/Source/LocURI is used for all ACL calculations	Section 5.6	
DM-SM-C-006-M	Support for Virtual URI Addressing Mechanism	Section 6.2	
DM-SM-C-007-M	Not send response message to Sessionless Command Message	Section 5.2	

B.2 SCR for DM Server

Item	Function	Reference	Requirement
DM-SM-S-001-M	Support for OMA Sessionless Management	Section 5.2	
DM-SM-S-002-M	Encode DM message into WBXML if DM Message.	Section 5.2	
DM-SM-S-003-M	Write ServerID in SyncHdr/Source/LocURI	Section 5.2	
DM-SM-S-004-M	Transport specific security is employed	Section 5.4	
DM-SM-S-005-M	ACL properties for new objects are included with TNDS data.	Section 5.5	
DM-SM-S-006-M	Support for Virtual URI Addressing Mechanism	Section 6.2	
DM-SM-S-007-M	Cred in SyncHdr is used to include DM Server's authentication information	Section 5.2	
DM-SM-S-008-M	Not include Get command within Sessionless Command Message	Section 5.2	