



# Device Management Connectivity Management Object Requirements

Approved Version 1.0 – 06 Dec 2005

---

**Open Mobile Alliance**  
OMA-RD-ConnMO-V1\_0-20051206-A.doc

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 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.

© 2005 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 (INFORMATIVE) .....	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 (INFORMATIVE).....	7
5. USE CASES (INFORMATIVE).....	8
5.1 USE CASE—CONFIGURATION AND MAINTENANCE OF STANDARD DATA CONNECTIVITY PARAMETERS.....	8
5.1.1 Short Description .....	8
5.1.2 Actors.....	8
5.1.3 Pre-conditions .....	8
5.1.4 Post-conditions.....	8
5.1.5 Normal Flow.....	8
5.1.6 Alternative Flow .....	9
5.1.7 Operational and Quality of Experience Requirements.....	9
6. REQUIREMENTS (NORMATIVE).....	10
6.1 HIGH-LEVEL FUNCTIONAL REQUIREMENTS .....	10
6.1.1 Security .....	10
6.1.2 Charging.....	10
6.1.3 Administration and Configuration .....	10
6.1.4 Usability.....	10
6.1.5 Interoperability.....	10
6.1.6 Privacy .....	10
6.2 OVERALL SYSTEM REQUIREMENTS .....	11
APPENDIX A. CHANGE HISTORY (INFORMATIVE).....	12
A.1 APPROVED VERSION HISTORY .....	12

## Tables

Table 1: High-Level Functional Requirements .....	10
Table 2: Overall System Requirements .....	11

# 1. Scope (Informative)

A number of Device Management specifications have been defined within OMA. See [DMBOOT], [DMDDFDTD], [DMNOTI], [DMPRO], [DMREPU], [DMRD], [DMSEC], [DMSTDOBJ], [DMTND], and [DMTNDS]. These specifications, in its entirety referred to as OMA DM v1.2 specifications in [ERELDDM], define protocol and mechanism to be used between a management server and a mobile device, data model made available for remote manipulation of a mobile device, security and policy to control the access to a particular resource in the mobile device.

This document defines the requirements for Device Management Connectivity Management Object, which is based on OMA DM v1.1.2 specifications and makes use of the functionalities provided by OMA DM v1.1.2 specifications to define standardized Management Object for connectivity parameter settings.

## 2. References

### 2.1 Normative References

- [OMA-DM] *OMA Device Management, Version 1.1.2*, Open Mobile Alliance™,  
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

- [ARCH-PRINC] *OMA Architecture Principles V1.2*, OMA-ArchitecturePrinciples-V1\_2,  
Open Mobile Alliance™, 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

**Management Object** A schema for configuration settings that an OMA DM client exposes to OMA DM servers for management operations defined in the OMA DM Enabler [OMA-DM]

**Device Management Authority** Any legal entity authorized, either directly or through delegation, to perform management operations on a terminal using the OMA Device Management protocol through a set of management objects.

### 3.3 Abbreviations

<b>OMA</b>	Open Mobile Alliance
<b>DM</b>	Device Management
<b>MO</b>	Management Object

## 4. Introduction

**(Informative)**

This document defines requirements for a set of managed objects which offer a standardized way to represent data network connectivity settings in a Devices's OMA Device Management tree.

While these objects are optional for any OMA DM implementation, their widespread use will simplify the management of basic connectivity parameters in OMA DM enabled Devices.

## 5. Use Cases (Informative)

### 5.1 Use Case—Configuration and Maintenance of Standard Data Connectivity parameters

#### 5.1.1 Short Description

Operator A has provisioned end-user devices with connectivity information, but wishes to subsequently manage these settings (e.g. modify, add or delete) via the OMA Device Management protocol. The operator wishes to do this in a standardised manner in order to consistently manage different devices from different vendors and distinguish vendor-specific extensions.

#### 5.1.2 Actors

- **User**
- **Device**
- **Device Management Server**
- **Device Management Authority**

##### 5.1.2.1 Actor Specific Issues

- **User:** User-specific preferences are not altered.
- **Device Management Authority:** The Device Management Authority is authorised to provision the configuration data and settings in the Device

##### 5.1.2.2 Actor Specific Benefits

- **User:** User is able to access network data services.
- **Device Management Authority:** The Device Management Authority is able to reliably and efficiently manage device connectivity settings, allowing them to adapt to changing network service needs.

#### 5.1.3 Pre-conditions

- Device is in a state where it's not able to connect to one or more network data services.
- Device is capable of connecting to the Device Management Server.

#### 5.1.4 Post-conditions

Device is configured with effective data network access parameters required to access the network data services.

#### 5.1.5 Normal Flow

1. Device Management Authority issues a request to the Device Management Server to provision or manage data connectivity parameters in one or more devices.
2. The Device Management Server sends a Server Initiated Notification to Device.
3. Device Management Client establishes a session with the Device Management Server.
4. Device Management Server queries Device for current settings (including any device-specific extensions) and sends DM Protocol commands to adjust the Device configuration to conform to requirements established by the Device Management Authority.
5. Device Management Client and Device Management Server end their management session.



6. Device is able to access network data services using the configured connectivity parameters.

### 5.1.6 Alternative Flow

N/A

### 5.1.7 Operational and Quality of Experience Requirements

N/A

## 6. Requirements

(Normative)

### 6.1 High-Level Functional Requirements

Label	Description	Enabler Release
HFR-01	The Connectivity MO enabler MUST enable DM server to add and maintain network access point parameters	1.0
HFR-02	The Connectivity MO enabler MUST enable DM server to add and maintain proxy parameters	1.0
HFR-03	The Connectivity MO enabler MUST support configuring a network access point for WAP Proxy	1.0
HFR-04	The Connectivity MO enabler SHOULD support configuring other network access proxy types	1.0
HFR-05	The Connectivity MO enabler MUST support configuring 3GPP Circuit Switched Data Bearer parameters	1.0
HFR-06	The Connectivity MO enabler MUST support configuring 3GPP Packet Switch Data Bearer parameters	1.0
HFR-07	The Connectivity MO enabler MUST support configuring 3GPP2 CDMA Data Bearer parameters	1.0
HFR-08	The Connectivity MO enabler MUST support configuring Wireless Local Area Network (WLAN) Data Bearer parameters	1.0

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

#### 6.1.1 Security

No additional security requirements beyond the ones defined in [OMA-DM].

#### 6.1.2 Charging

No additional charging requirements beyond the ones defined in [OMA-DM].

#### 6.1.3 Administration and Configuration

The purpose of the document is administration and configuration of connectivity management. No additional requirements beyond defined in [OMA-DM].

#### 6.1.4 Usability

No additional usability requirements beyond the ones defined in [OMA-DM].

#### 6.1.5 Interoperability

No additional interoperability requirements beyond the ones defined in [OMA-DM].

#### 6.1.6 Privacy

No additional privacy requirements beyond the ones defined in [OMA-DM].

## 6.2 Overall System Requirements

Label	Description	Enabler Release
OSR-01	The Connectivity MO enabler MUST specify interfaces that are access technology neutral	All
OSR-02	The Connectivity MO enabler MUST be specified in a way that bearer dependant parts can be specified independently of bearer neutral part.	All
OSR-03	The Connectivity MO enabler MUST be specified in a way that allows vendor specific extensions	All
OSR-04	The Connectivity MO enabler SHOULD NOT rely on OMA DM features released after Approval of the DM 1.1.2 release of [OMA-DM].	All
OSR-05	The Connectivity MO enabler MUST be specified in a way that it is possible to add new bearer specific parts without revising existing bearer specific parts	All

**Table 2: Overall System Requirements**

## Appendix A. Change History

(Informative)

### A.1 Approved Version History

Reference	Date	Description
OMA-RD-ConnMO-V1_0	06 Dec 2005	TP Approval: OMA-TP-2005-0368-ConnMO-RD-For-ReviewAndApproval