DM DiagMon Architecture

Candidate Version 1.0 – 14 Apr 2009

Open Mobile Alliance

OMA-AD-DM-DiagMon-V1_0-20090414-C

Contents

1. Scope (Informative)

OMA has defined enabler releases in the Device Management space. One such enabler is referred to as OMA DM v1.2 specifications in [DMPRO], which defines protocols and mechanisms to be used between a Device Management Server and a mobile device, as well as the data model made available for remote diagnostics and monitoring of a mobile device.

This document describes the architecture of the DM Diagnostics and Monitoring Enabler. The architecture is based on the requirements and the use cases included in [DMDIAGMON-RD], and described at high level as believed to be significant from the architectural point of view. The dependency that Diagnostics and Monitoring Enabler has upon other DM Enablers is also addressed.

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

[DMDIAGMON-RD] OMA Device Management Diagnostics and Monitoring Requirements, Open Mobile Alliance™, OMA-RD-DiagMon-V1_0, URL:http://www.openmobilealliance.org/

[DMTND] "OMA Device Management Tree and Description, Version 1.2". Open Mobile Alliance™. OMA-TS-DM_TND-V1_2. URL: http://www.openmobilealliance.org

2.2 Informative References

[DMPRO] "OMA Device Management Protocol", Version 1.2, Open Mobile Alliance, OMA-TS-DM_Protocol-V1_2, URL: http://www.openmobilealliance.org/

[DMSEC] "OMA Device Management Security, Version 1.2". Open Mobile Alliance™. OMA-TS-DM_Security-V1_2. URL: http://www.openmobilealliance.org

[OMADICT] "Dictionary for OMA Specifications", Version 2.6, Open Mobile Alliance™, OMA-ORG-Dictionary-V2_7, 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

Device	Equipment which is normally used by users for communications and related activities. The definition can be extended to cover remote monitoring applications where there is no user present, but the communications to and from the remote monitor use the same communications channels as when used by users [OMADICT].
Device Management Authority	An entity that has the right to perform a specific Device Management function on a Device or manipulate a given data element or parameter. For example, the Network Operator, handset manufacturer, enterprise, or Device owner may be the authority or share authority for managing the Device. One Management Authority may own all Device resources or may share or delegate all or parts of these with/to other Management Authorities
DM Client	A component defined in [DMTND] as a software component in a managed device that correctly interprets OMA DM commands, executes appropriate actions in the device and sends back relevant responses to the issuing management server.
DM Server	A component defined in [DMTND] as a network based entity that issues OMA DM commands to devices and correctly interprets responses sent from the devices.
Management Object	A data model for information which is a logical part of the interfaces exposed by device for management purpose.
Network Operator	The entity providing network connectivity for a Device [OMADICT].

3.3 Abbreviations

DiagMon	Diagnostics and Monitoring
DM	Device Management
DMS	Device Management Server
MO	Management Object
OMA	Open Mobile Alliance

4. Introduction (Informative)

The primary objective for Device Management protocols and mechanisms are to manage distributed, mobile wireless devices, in order to optimize a subscriber's experience and reduce network operating costs. This enabler will introduce Device Management (DM) remote device diagnostics and network monitoring functionality that achieves some of these objectives.

The overall goal of DM diagnostics and monitoring is to enable management authorities to proactively detect and repair troubles even before the users are impacted, or to determine actual or potential problems with a device when an opportunity presents itself. A device management authority (DMA) is an entity that has the right to perform a specific DM function on a device or manipulate a given data element or parameter. For example, the network operator, handset manufacturer, enterprise, or device owner may be the authority or share authority for managing the device.

Further, the technology must also enable management authorities to remotely interrogate the device for trouble isolation. Based on this, the Diagnostics and monitoring enabler must address the following areas:

1) Diagnostics Policies Management: Support for specification and enforcement of policies related to the management of diagnostics features and data.

2) Fault Reporting: Enable the device to report faults to the network as the trouble is detected at the device.

3) Performance Monitoring: Enable the device to measure, collect and report key performance indicators (KPIs) data as seen by the device such as on a periodic basis.

4) Device Interrogation: Enable the network to query the device for additional diagnostics data in response to a fault

5) Remote Diagnostics Procedure Invocation: Enable management authorities to invoke specific diagnostics procedures embedded in the device to perform routine maintenance and diagnostics.

6) Remote Device Repairing: Enable management authorities to invoke specific repairing procedures based on the results of diagnosis procedures.

The DM Diagnostics and Monitoring Enabler leverages the functionality of the existing DM Enablers, in particular the OMA DM Enabler [DMPRO], to transport Diagnostics and Monitoring data and messages between the DM client and the DM server.

4.1 Planned Phases

At the moment of writing, there is no future planned phase additional to the descrbed architecture in this document.

4.2 Security Considerations

The management objects defined in this enabler are dependent on the security mechanisms and protections provided by the DM enabler. No new security issues are introduced by these management objects. Readers are encouraged to review the DM enabler security specification [DMSEC] for more information regarding these mechanisms.

4.3 Use Cases and Requirements

Current use cases for DM Diagnostics and Monitoring can be found at [DMDIAGMON-RD]. No additional use cases are planned.

Current requirements for DM Diagnostics and Monitoring can be found at [DMDIAGMON-RD]. No extra Diagnostics and Monitoring requirements are planned.

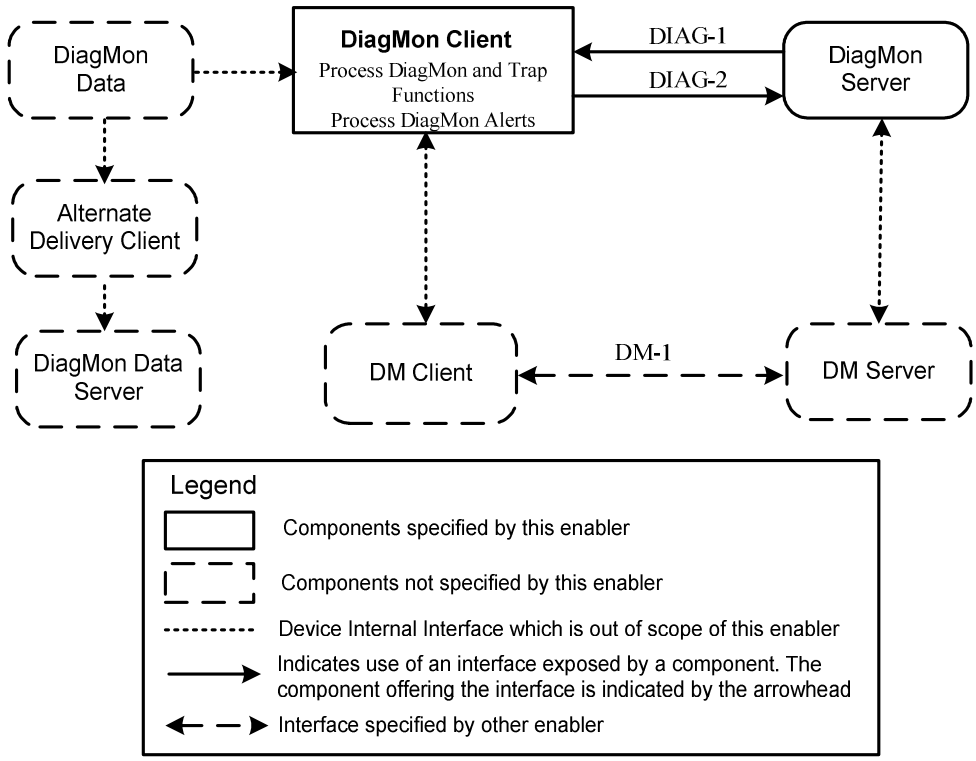
5. Architectural Model

5.1 Dependencies

OMA Device Management [DMPRO] Enabler

The DM Diagnostics and Monitoring Enabler is dependant upon the OMA Device Management Enabler [DMPRO]. The version of OMA Device Management Enabler referenced in the described architecture is V1.2 Enabler release or higher. It is also known as OMA DM Base Protocol. The DM DiagMon Enabler relies on the OMA Device Management Enabler for the execution of diagnostics and monitoring management tasks and the transports for the DiagMon Messages between DM Client and Server.

5.2 DiagMon Architecture Diagram



5.3 DiagMon Functional Components and Interfaces

5.3.1 Functional Components

5.3.1.1 DiagMon Client

The DiagMon client function is responsible for the Diagnostics and Monitoring activities. The DiagMon client processes and consumes the Diagnostic and Monitoring component (e.g. commands, alerts, packages) delivered to the device by the OMA DM client.

The DiagMon client also communicates a success or failure result to the DM client at the termination of the Diagnostics and Monitoring activity, for communication back to the DM server.

5.3.1.2 DM Client

The DM client makes it possible for the DM Server to manage the device using the DM protocol. For Diagnostics and Monitoring activities, the DM server and the DM client interact over the DIAG-1 interface as well.

5.3.1.3 Device Management System

The Device Management system for Diagnostics and Monitoring is comprised of a Device Management server, DiagMon server and potentially other external management systems. The DM server component supports device discovery, determination of an appropriate Diagnostics and Monitoring component and its delivery to the device over various bearer technologies, represented by the DM-1 interface. It also receives a notification from the DM Client for success or failure of a diagnostics event or diagnostics or monitoring data, invoked over the DIAG-1 interface

5.3.1.4 DiagMon Data

The specific diagnostics and monitoring data and associated components are outside the scope of this enabler. This includes such entities as call and data loggers, and other associated management objects such as Key Performance Indicators or Scheduling. The DiagMon Data may be sent via an alternate delivery protocol to a data server for e.g. processing. However when necessary, the DiagMon alerts are sent over the DIAG-2 interface.

5.3.1.5 Alternate Delivery Client

The alternate delivery client component is an optional feature of the device that makes it possible to update a data server using the alternate delivery protocol. The interaction of the DiagMon agent with the Alternate Delivery Client is out of scope.

5.3.2 Interfaces

5.3.2.1 DIAG-1 Interface

The DIAG-1 interface is exposed by the DiagMon Client, which allows other components, such as DiagMon Server, to perform Diagnostics and Monitoring Operations. Through this interface the DiagMon Server can enable and disable diagnostics and/or trap functions on the device. The DiagMon functions will be conveyed by DM messages via the underlying DM-1 interface.

The interface DIAG-1 describes interactions between the Device Management System or server and the device (e.g. DM Client) in setting up the DM sessions, delivering diagnostics and monitoring packages, and communicating results for the DiagMon activities invoked.

5.3.2.2 DIAG-2 Interface

The DIAG-2 interface is exposed by the DiagMon Server, which allows other components, such as DiagMon Client, to send DiagMon Alerts. Through this interface the DiagMon Server can receive results for the DiagMon activities invoked on the device. The DiagMon Alerts will be conveyed by DM messages through underlying DM-1 interface, or an alternate delivery mechanism..

5.3.2.3 DM-1 Interface

This interface describes the client-server protocol and is out of scope for the Diagnostics and Monitoring enabler as it is defined by DM 1.2 enabler release [DMPRO]. However, the DM-1 interface is leveraged in Diagnostics and Monitoring activities.

5.4 Flows

5.4.1 Diagnostics Fault Detection, Querying and Reporting

This flow describes the interaction between DM client and the DM server over the OMA-DM protocols to the device in a typical remote diagnostics session.

5.4.1.1 Normal Flow

1. End user calls customer care .
2. Management Authority (customer care /DM Server) sends a query to Device for configuration or other reporting information
3. The device then gathers performance and QoS related information.
4. Device reports its configuration information and/or performance data to the customer care/DM server

5.4.1.2 Alternative Flow – Preconfigured DiagMon Operations

The device triggers a DM session based on certain predetermined collection and reporting criteria as determined by a management object

5.4.1.3 Alternative Flow – Automatic Reporting

1. A device is used to access a service, an unknown error occurs;
2. Device collects the fault information, such as memory dump, error code, application type, vendor etc.
3. Device transfers this information to the Management Authority.
4. Management Authority analyzes the fault information.

5. The Management Authority confirms the fault, identifies a, solution, if available, and provides the solution (executes management operations as necessary).

5.4.2 Network Monitoring

This flow describes the interaction between DM client and the DM server over the OMA-DM protocols to the device in a typical remote diagnostics session.

5.4.2.1 Normal Flow

1. DMS configures device with policy(s) for recording information and reporting information
2. The device starts recording performance information per policy
3. According to reporting policy, the device initiates contact with DM Server.
4. Device reports its performance data (and device information) per policy
5. DMS closes the session or requests additional details based on contents of the reports
6. Device sends acknowledgement to the DM server

5.4.3 Trap Flows

The flow described in this section shows how the Management Authority can receive notifications about the Events on which they registered, and how the captured Events are used as a trigger for other management operations.

5.4.3.1 Trap Notification Flow

This flow shows a sequence of the steps taken until the Management Authority is able to receive the notifications about the Events and the associated information.

1. A Management Authority gets information about a list of the available Events that can be captured and reported.
2. The Management Authority registers on one of those Events.
3. The Event occurs and it is captured.
4. The DiagMon Client gets indication about the occurrence of the Event and the associated information.
5. The DiagMon Client sends a notification message requests the DM Client to send a notification message to the management authority.
6. DM Client sends a notification message.

Note: It is possible that multiple Management Authorities may register on any Events at the same time.

5.4.3.2 Trap Notification Flow (Inward)

This flow describes a sequence of the steps taken from scheduling the management operation to the execution of it at the occurrence of an Event (Trap).

1. A Management Authority gets information about a list of the available Events (Traps).

2. The Management Authority creates and installs a Schedule that is based on one of the Events (Traps) as a trigger.
3. The Event (Trap) occurs.
4. The DiagMon Agent captures the Event (Trap) and provides a trigger (or inward notification) to the DM Scheduling Agent.
5. The DM Scheduling Agent executes the management operation included in the Schedule.

Note: It is possible that multiple Management Authorities may create the different Schedules that are based on the same Events (Traps).

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 1.0 History

Document Identifier	Date	Sections	Description
Draft Versions: OMA-AD-DM-DiagMon-V1_0	07 Dec 2005	All	Initial Draft Version
	03 Mar 2006	5	Added Architecture Diagram
	29 Mar 2006	5.4	Added Flow Section
	22 Jun 2006		Updated Flow sections
	27 Feb 2007		Accomodated CRs 2007-001R03 & 2007-002R02
	01 May 2007		Accomodated CRs 2007-016R01 & 2007-017
	11 Jun 2007	5	Accomodated CR 2007-023
	19 Jun 2007	5	Accomodated CR 2007-028
	30 Aug 2007	All	Accomodated CRs 2007-31R01, 34, 35, 36R01, 38, 40
	02 Oct 2007	All	Accomodated ADRR 16, 34, 39 and CRs 2007-41, 42, 43
	11 Oct 2007	All	Accomodated CR 38 – missed ones during 30 August chnages
	25 Jun 2008	All	Accomodated CR 12R02
	03 Dec 2008	All	Editorial clean up prior to consistency review
Candidate Versions: OMA-AD-DM-DiagMon-V1_0	14 Apr 2009	n/a	Status changed by TP OMA-TP-2009-0138-INP_DiagMon_V1_0_ERP_for_Candidate_Approval