DM Diagnostics and Monitoring Requirements

Approved Version 1.0 – 20 Dec 2011

Open Mobile Alliance

OMA-RD-DiagMon-V1_0-20111220-A

Contents

1. SCOPE (INFORMATIVE) 5
2. REFERENCES 6
   2.1 NORMATIVE REFERENCES 6
   2.2 INFORMATIVE REFERENCES 6
3. TERMINOLOGY AND CONVENTIONS 7
   3.1 CONVENTIONS 7
   3.2 DEFINITIONS 8
   3.3 ABBREVIATIONS 9
4. INTRODUCTION (INFORMATIVE) 11
5. USE CASES (INFORMATIVE) 12
   5.1 FAULT DETECTION, QUERY AND REPORTING 12
      5.1.1 Short Description 12
      5.1.2 Actors 13
      5.1.3 Pre-conditions 13
      5.1.4 Post-conditions 13
      5.1.5 Normal Flow 13
      5.1.6 Alternative Flow 14
      5.1.7 Operational and Quality of Experience Requirements 14
   5.2 DEVICE-AIDED NETWORK PERFORMANCE MONITORING 14
      5.2.1 Actors 15
      5.2.2 Pre-conditions 15
      5.2.3 Post-conditions 16
      5.2.4 Normal Flow 16
   5.3 FAULT DETECTION, AUTOMATICALLY REPORTING 16
      5.3.1 Short Description 16
      5.3.2 Actors 16
      5.3.3 Pre-conditions 17
      5.3.4 Post-conditions 17
      5.3.5 Normal Flow 17
      5.3.6 Alternative Flow 17
   5.4 DEVICE EVENTS MONITORING 17
      5.4.1 Short Description 17
      5.4.2 Actors 17
      5.4.3 Pre-conditions 18
      5.4.4 Post-conditions 18
      5.4.5 Normal Flow 18
6. REQUIREMENTS (NORMATIVE) 19
   6.1 HIGH-LEVEL FUNCTIONAL REQUIREMENTS 19
      6.1.1 Security 20
      6.1.2 Charging 20
      6.1.3 Administration and Configuration 20
      6.1.4 Usability 20
      6.1.5 Interoperability 20
      6.1.6 Privacy 21
   6.2 OVERALL SYSTEM REQUIREMENTS 22

APPENDIX A. CHANGE HISTORY (INFORMATIVE) 23
   A.1 APPROVED VERSION HISTORY 23

Tables

Table 1: High-Level Functional Requirements **19**

Table 2: High-Level Functional Requirements – Security Items **20**

Table 3: High-Level Functional Requirements – Charging Items **20**

Table 4: High-Level Functional Requirements – Administration and Configuration Items **20**

Table 5: High-Level Functional Requirements – Usability Items **20**

Table 6: High-Level Functional Requirements – Interoperability Items **21**

Table 7: High-Level Functional Requirements – Privacy Items **21**

Table 8: High-Level System Requirements **22**

1. Scope (Informative)

OMA has defined an enabler releases in the Device Management space. One such enabler is referred to as OMA DM v1.2 specifications in [ERELDDM], that defines protocols and mechanisms to be used between a Device 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 Diagnostics and Monitoring functionality, which builds on OMA DM v1.2 specifications and makes use of the functionalities provided by OMA DM v1.2 specifications to define special capabilities of processing management actions and/or other types of actions for remote diagnostics of mobile device issues and monitoring mobile devices.

2. References

2.1 Normative References

[ERELDDM] "Enabler Release Definition for OMA Device Management Specifications, version 1.2". Open Mobile Alliance™. OMA-ERELD-DM-V1_2.
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

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

Content Provider An entity that provides data which forms the basis of a service.

Customer-Care A service or system accessible by a management authority to manage the device associated with the subscriber, including changing configurations, adding applications, diagnosing problems with the device, etc. wherein the service employs a device management system to access the device.

Device In this context, a Device is a voice and/or data terminal that uses a Wireless Bearer for data transfer. Device types may include (but are not limited to): mobile phones (GSM, CDMA, 3GSM, etc.), data-only terminals, PDAs, laptop computers, PCMCIA cards for data communication, unattended data-only Devices (e.g., vending machines), and smart cards if associated with these Devices. If within a particular context an associated smart card should not be regarded as part of a Device this is marked explicitly.

Device Management Management of the Device configuration and other managed objects of Devices from the point of view of the various Management Authorities. Device Management includes:

- Setting initial configuration information in Devices
- Subsequent updates of persistent information in Devices
- Retrieval of management information from Devices
- Processing events and alarms generated by Devices

DM scheduling Device Management Scheduling specifications provide special capabilities of processing management actions and/or other types of actions in given times and conditions according to the schedule set by the management authority in advance.

Device Management System A background system capable to interact with a (set of) Device(s) for the purpose of Device Management.

Device Profile A set of management objects that provide information about the device. It contains some static and dynamic device specific data. For example, DevInfo and DevDetail together can provide some information about the device.

Device Query The process of polling a mobile Device for a specific piece of information.

Device Reporting The process whereby a Device sends specific information to a management server in the network. This can occur as a response to a Device Query (pull) or it can occur autonomously in response to a state change in the Device (push). The information that is sent may either be parameters stored in data fields in the Device, information about the configuration of the Device, information about the capabilities of the Device, or data that has been collected, stored, and assembled for later forwarding (e.g., performance metrics).

Diagnostics and Monitoring System A system that is associated with the Device Management System and is also under the administration of a management authority. It employs the standard Device Management System interaction with a (set of) device(s). The Diagnostics and Monitoring System provides enhancements to the Device Management System to support Diagnostics and Monitoring.

Enterprise A business with deployment and Management Authority for WLAN Bearers, Local Wired Bearers, computers, Devices, software, and employees.

Local Wired Bearers Serial, USB, Ethernet

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

Network Bearers Wireless Bearer and Local Wired Bearers

Network Operator An entity that is licensed and allocated frequency to operate a public mobile wireless telecommunications network for the purpose of providing publicly available commercial services.

Parameters	In this context, parameters are service-related data elements that are stored in the Device and can be manipulated (i.e., changed, added, or deleted) over Network Bearers. For example, system parameters can be used to establish or maintain a bearer session, and application parameters can be used to specify the profile of a particular service, or some parameters may be related with performance characteristics.
PC Agent	Application running on a PC or PC-like device in User's proximity, not the Device itself, that facilitates Device Management functionality, and which MAY involve a logical association with a DMS.
Policy	The set of Service configuration settings and installed applications which are mandated by the Management Authority or subscriber.
Provisioning Mechanisms	Network bearers, smart card, and Media card
Radio Software	The software within a Device that is coupled with the radio hardware to derive the overall "radio" functionality. Radio software is not to be confused with User applications and content, but has certain commonality for functional requirements for device management.
Self-Care	A service or system accessible by a subscriber to manage the device associated with the subscriber, including changing configurations, adding applications, diagnosing problems with the device, etc. wherein the service employs a device management system to access the device.
Service Provider	An entity that provides and administers a service to a Subscriber and/or User. The Network Operator is often a Service Provider.
Service Level Tracing	Service Level Tracing (SLT) is the ability to capture and log all relevant information at each enabler component within a service chain, associated with a specific service that is initiated either by an end user or a component.
Subscriber	The individual or organisation that is paying for service.
Subscriber Profile	A set of management objects that provide subscriber-specific data.
Trap	A mechanism employed by a management authority to enable the Device to capture and report events and other relevant information generated from various components of the Device, such as a protocol stack, device drivers, or applications.
User	The individual who is in possession of and operates the Device.
Wireless Bearer	WAN Network Bearers (e.g. GPRS, GSM Data, CDMA), WLAN Bearers (802.1x), Local Wireless Network Bearers (e.g. Bluetooth, IrDA)

3.3 Abbreviations

CC	Customer Care
CDMA	Code Division Multiple Access
DM	Device Management
DMS	Device Management Server
E2E	End-to-End
EDGE	Enhanced Data GSM Environment
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
HW	Hardware
IrDA	Infrared Data Association

KPI	Key Performance Indicator
MMS	Multimedia Messaging Service
MO	Management Object
OMA	Open Mobile Alliance
PoC	Push-to-Talk over Cellular
QoS	Quality of Service
RF	Radio Frequency
SMS	Short Message Service
USB	Universal Serial Bus
WAN	Wide Area Network
WAP	Wireless Access Protocol
WLAN	Wireless Local Area Network

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) Diagnostics and device monitoring functionality that achieves some of these objectives.

The overall goal of DM Device 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 management authority 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.

Use-cases specific to customer care will be addressed. Such use cases for example involve DM clients or servers selectively setting traps, collecting performance data, such as, call setup failures, call release causes such as RF loss, QoS attributes (low throughput, high erasure rate, high delay), and creating schedules to manage different tasks at the device and allow the possibility of subsequently resolving these issues. These operations are completed with or without a customer care representative. Reporting of configuration or performance data by a device may be scheduled based on a set of local DM client conditions or based on some event on the device. The local conditions on the device or policies governed by DM server may effect if the reports are collected real-time or cached for later reporting. This information can be configured to be collected at varying sampling rates and time periods.

5. Use Cases (Informative)

The following four basic diagnostics and monitoring use case categories can be considered:

1. Device diagnostics – fault detection, query and reporting, targeted collection
2. Device aided Network performance monitoring - passive bulk collection
3. Fault Detection, Automated reporting
4. Device Events Monitoring

Moreover, the goal of OMA DM Device Diagnostics and Monitoring is to enable operators 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. Thus, there are variations within the basic flows depending on the use case.

One means to meet this goal for the three use cases defined above is to use policy-based triggers which would enable the automatic or periodic reporting of faults, key performance indicators, and specific diagnostics procedures.

Finally, requirements on the amount of data to be reported (therefore sessions and corresponding air time) from a request by a given specific user complaint versus an automated mass and/or statistical data gathering from thousands of devices needs to be devised.

The status of the device or a service is composed of several attributes which can be classified as static, semi-static or dynamic. In the process of the retrieval of corresponding information from the device, the amount of messages and "traffic" is highly correlated to the above mentioned attributes. Definitely, the retrieval of the dynamic attributes would be needed more frequently than static ones. For example information as HW (static) would vary much less in time compared to settings (semi-static) which themselves would vary to lesser extent than device call summary (Voice, Data, Video, PoC) related to key performance indicators such as statistics of ineffective access and related root causes.

Therefore, high level requirements for the above use cases need to be devised in order to allow flexibility, minimize reporting traffic and processing/power consumption via the trap/policies management:

- Information model and corresponding objects needed

- Mechanisms of retrieval within OMA-DM framework

- Trap/policies for dynamic attributes recording

- Trap/policies for reporting/retrieval of data

- Relevant interfaces requirements between a DMS and operator customer care systems

5.1 Fault Detection, Query and Reporting

5.1.1 Short Description

A Subscriber calls the operator's customer care facility or corporate help desk complaining that their Device is reporting an error, or a service is failing to work. The corporate help desk or operator's Customer care server Help Desk agent can query the Device to determine key information

- Device profile / information
- Subscription information
- Settings information

- Applications information

Based upon this information, the Help Desk agent may be able to determine the cause of the issue, and take Device Management actions that resolve it.

5.1.2 Actors

- Subscriber (User or Corporate Customer): A Corporate Customer may be able to specify aspects of the configuration and issue resolution procedures for its Devices.
- Device: The Device protects its configuration from unauthorized access.
- Management Authority: The Management Authority can access the Device configuration, and change it.

5.1.2.1 Actor Specific Issues

N/A

5.1.2.2 Actor Specific Benefits

- Subscriber (User or Corporate Customer): Reduction in timing to resolve device faults or service issues.
- Device: The device and associated services operate properly.
- Management Authority: Reduction in customer service costs.

5.1.3 Pre-conditions

- Device supports Device Management queries and actions from the management server.
- The Network Operator has a Device Management server supporting Device Management queries and actions.

5.1.4 Post-conditions

N/A

5.1.5 Normal Flow

1. 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. Customer Care sends request to User for authorization to download application to Device
6. User grants authorisation
7. Customer Care downloads application to device, installs and executes it
8. Device sends acknowledgement to Customer Care/DM server

5.1.6 Alternative Flow

A Subscriber calls the operator's customer care facility or corporate help desk complaining that their data services (GPRS, EDGE, etc.) in the Device is not accessible. The Customer care (CC) requests the device to communicate configuration using any available means. The device, specifically a diagnostic client in the device, receives the request, identifies an available communication means (one that is working), collects the configuration (and other information) requested, and communicates it to the Customer Care server. For example, if the GPRS service is not configured properly, and is therefore not available, the device employs the SMS service to send configuration information to the customer care server.

The device may employs one of the following communication means to send configuration data back to the Customer care for analysis:

- GPRS
- 802.11 b/g
- SMS

Based upon this configuration received, the CC agent may be able to determine the cause of the problem, and take Device Management actions that resolve it such as updating the radio software by leveraging an alternate communication means available, per the flow below:

1. User calls Customer Care with a problem regarding main/ primary data service
2. Customer Care sends a query to Device for retrieving and returning configuration or other reporting information using ANY communication means possible
3. The device identifies at least one available communication means and selects one for communicating requested configuration.
4. Device reports its configuration information to the Customer Care server using the available / selected communication means.
5. Customer Care sends request to Device to alter configuration (as necessary)
6. Device updates configuration
7. Customer Care receives acknowledgement from device on successful update
8. Customer Care Representative confirms success to the user

5.1.7 Operational and Quality of Experience Requirements

None.

5.2 Device-aided Network Performance Monitoring

Network performance monitoring is used to perform bulk or system wide data collection. This information may be subsequently leveraged to build coverage maps, traffic distribution, service quality statistics and/or maps as well as update device or network parameters.

Within the area of Performance monitoring, device-aided network monitoring use case addresses overall user experience from a system/network perspective.

The device management server selectively sets the policy for collecting performance data. Specifically this can include call setup failures, call release causes such as RF loss indication of forward or reverse link, QoS attributes at high/low gage levels (low throughput, high erasure rate, high delay), mobility handoff threshold gauge level, RF conditions such as sudden loss of RF signal or service or time. These operations are completed without a customer care agent.

Performance information can be configured to be collected at varying sampling rates and time periods, i.e. 1 sample per second, over the last 10 seconds, 30 seconds. The collection information can be subscribed to on a per network element basis such as base station or carrier in order to keep balance data collection requirements with monitoring or optimization functions.

Reporting of configuration or performance data may be constrained by the device based on a set of local device conditions such as battery level, system loading level, predetermined reporting time, or based on some other event on the device. The local conditions on the device or policies governed by DM server may effect if the reports are collected real-time or cached for later reporting

Following subscriber activation of a device on an operator's network wherein during the initial registration / activation process, the device is optionally configured with policies to record or retain performance information and to report this information.

The information requested during network monitoring mode may consist of the following:

- Call statistics information
- Call detail information
- RF environment information

5.2.1 Actors

- Device.
- Management Authority.

5.2.1.1 Actor Specific Issues

N/A

5.2.1.2 Actor Specific Benefits

- Device: Improved user experience
- Management Authority: This network performance monitoring may be leveraged to build coverage maps, traffic distribution, service quality statistics and/or maps as well as update device or network parameters. Bulk collection allows for proactive recognition of poor service level conditions.

5.2.2 Pre-conditions

- Device supports Device Management queries and actions from the management server.
- The Network Operator has a Device Management server supporting Device Management policy configuration control and report collection.

5.2.3 Post-conditions

The DM server may be configured to share the information with post processing or operations for additional analysis.

5.2.4 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

5.3 Fault Detection, Automatically Reporting

5.3.1 Short Description

Subscriber is playing some services. During the process, one error occurs.

When this fault occurs, Device would collect some error information and report it to the Management Authority automatically. The error information would be analysed, and forward to the external corresponding system if needed. Based upon this information, a solution can be worked out and some Device Management actions can be performed to resolve the problem. This mechanism will be much helpful for operator/vendor to enhance customer's experience

5.3.2 Actors

- **Management Authority:** Perform management authority to configure service.
- **Device**: The Device can send necessary information to Management Authority
- **External System:** When receiving a request from the Management Authority, External system works out corresponding solutions and then feedbacks.

5.3.2.1 Actor Specific Issues

- **Device**: Device can support fault auto report mechanism.
- **Management Authority**: Receiving the fault information reported from the device.
- **External System**: as 3rd party vendor, it can work out the corresponding solution.

5.3.2.2 Actor Specific Benefits

- **Device**: Since the fault can be detected and reported as soon as possible, the solution can be worked out. Device gets faults fixed automatically.
- **Management Authority**: Help the operator provide solutions to the device and increase revenue from providing robust service.
- **External System**: Improve the maturity of the service.

5.3.3 Pre-conditions

- The Device is proper configured.
- Management authority should configure the Device to report the failure back.
- Device can access the Management Authority by an available communication means employing appropriate authentication
- Management Authority can access external systems, if necessary, to transfer corresponding information.

5.3.4 Post-conditions

- DM server can collect the fault report which includes required information for error diagnostic. Operator or device manufacturer can have additional information to work out corresponding solution for the fault.

5.3.5 Normal Flow

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).

5.3.6 Alternative Flow

If Management Authority cannot resolve the problem, the fault information is transferred to an External System, such as device vendor/software provider, or other related 3rd party to work out one solution. And the solution is transferred back to Management Authority.

5.4 Device Events Monitoring

5.4.1 Short Description

The Device events requested for monitoring may include:

- User changing service parameters on the device
- User updating firmware/software manually without interaction with Management Authority
- Device changes some settings indicated by installed applications
- Application usage statistics such as, start & stop time.

These events occurring in device can be monitored by the monitoring task which Management Authority has sent to the Device beforehand. When these events occur, the Device records and subsequently reports the events to the Management Authority. The Management Authority can analyse the event information and determine whether or not to initiate a management session with the Device to do some operations.

5.4.2 Actors

- User.

- Device.
- Management Authority.

5.4.2.1 Actor Specific Issues

- User: User would like to be able to do some offline operations to his device safely.
- Device:
- Management Authority: The Management Authority is likely to be informed of the events that occurred in the device.

5.4.2.2 Actor Specific Benefits

- User: improved user experience.
- Device: Device reporting events avoids errors in application configurations and settings.
- Management Authority: Monitoring facilitates service providing.

5.4.3 Pre-conditions

- Device has been properly configured and is capable of interacting with the Management Authority.
- Device is capable of receiving and executing a monitoring task.

5.4.4 Post-conditions

The Management Authority discovers the device events and may take further management operations.

5.4.5 Normal Flow

1. Management Authority sends a request to the User for authorisation to install the monitoring task to the Device.
2. User grants authorisation.
3. Management Authority installs the monitoring task configured with recording and reporting conditions to the Device.
4. User does some offline operations to his device or applications change something in the device.
5. Device discovers the events according to configured recording condition.
6. Device reports the events to the Management Authority according to configured reporting condition.

6. Requirements (Normative)

6.1 High-Level Functional Requirements

Label	Description	Enabler Release
DIAG-GEN-1	Diagnostics information SHOULD be collected from a device as defined by DM managed objects.	DiagMon Version 1.0
DIAG-GEN-2	Network monitoring information SHOULD be collected from a device as defined by DM managed objects.	DiagMon Version 1.0
DIAG-GEN-3	Diagnostics and Monitoring information from a device SHOULD be collected per the policies set by management authority.	DiagMon Version 1.0
DIAG-GEN-4	Diagnostics and Monitoring Enabler SHALL support a mechanism to allow the collection, logging, storage or Reporting Diagnosis and Monitoring information based on time or events.	DiagMon Version 1.0
DIAG-GEN-5	The Diagnostics and Monitoring enabler SHOULD support Diagnosis and Monitoring of information coming from various types of measurements done by the device.	DiagMon Version 1.0
DIAG-GEN-6	It SHALL be possible for the device to log or store the Diagnostics and Monitoring events and associated information on the Device for later reporting or fetch for the DM Server.	DiagMon Version 1.0
DIAG-GEN-7	The Diagnostics and Monitoring Enabler MUST support a mechanism that selectively detects changes to client configuration parameters.	DiagMon Version 1.0
DIAG-GEN-8	The device SHALL provide a means to notify the Diagnostics and Monitoring management authority of changes to client configuration parameters.	DiagMon Version 1.0
DIAG-GEN-9	The device SHALL provide a means to notify the Diagnostics and Monitoring management authority of faults.	DiagMon Version 1.0
DIAG-GEN-10	A management authority SHOULD have a means to query and set parameters for dynamic attributes of the device, e.g. battery level, available resources, via managed objects.	DiagMon Version 1.0
DIAG-GEN-11	Diagnostics and Monitoring Enabler MAY report Trap events to other DM components, such as DM Scheduling	DiagMon Version 1.0
DIAG-GEN-12	The Diagnostic and Monitoring System SHOULD support a mechanism to invoke specific diagnostics procedures remotely.	DiagMon Version 1.0
DIAG-GEN-13	The device SHOULD provide a means to notify the Diagnostics and Monitoring management authority of firmware offline update, software offline installation, update and removal.	DiagMon Version 1.0
DIAG-GEN-14	Diagnostic and Monitoring Enabler SHALL support a mechanism that provides an error-reporting capability.	DiagMon Version 1.0
DIAG-GEN-15	Diagnostic and Monitoring Enabler SHALL support a mechanism that enables Service Level Tracing operations (e.g. activate and deactivate traces on devices, relay to the device Service Tracing Tasks, expose and retrieval of all captured Service Level Trace information) as defined by DM managed objects.	DiagMon Version 1.0
DIAG-GEN-16	Diagnostic and Monitoring Enabler SHALL support a mechanism that allows the Device to notify the Diagnostics and Monitoring Management Authority that an event has occurred, e.g. notify Diagnostics and Monitoring Management Authority that collected traced data is ready to be retrieved or that a Trap event has occurred.	DiagMon Version 1.0
DIAG-GEN-17	Diagnostics and Monitoring information from a device SHOULD be reported per the policies set by management authority.	DiagMon Version 1.0

Table 1: High-Level Functional Requirements

6.1.1 Security

Label	Description	Enabler Release
DIAG-SEC-1	The non-repudiation of a diagnostics and monitoring session MUST be ensured.	DiagMon Version 1.0
DIAG-SEC-2	Diagnostic and Monitoring Enabler SHALL support a mechanism to protect diagnostic and monitoring data stored on the device by authenticating and authorising the Management Authority.	DiagMon Version 1.0

Table 2: High-Level Functional Requirements – Security Items

6.1.2 Charging

Label	Description	Enabler Release
N/A	N/A	N/A

Table 3: High-Level Functional Requirements – Charging Items

6.1.3 Administration and Configuration

Label	Description	Enabler Release
DIAG-ADMIN-1	Confirmation request messages SHALL be uniquely identified and contain at least the subscriber id, data or data summary, and date/time.	DiagMon Version 1.0
DIAG-ADMIN-2	Result messages SHALL be uniquely identified and correlated to the request.	DiagMon Version 1.0

Table 4: High-Level Functional Requirements – Administration and Configuration Items

6.1.4 Usability

Label	Description	Enabler Release
DIAG-USE-1	The end user MAY initiate a self-care activity for diagnosing a problem for devices enabled with self-care capabilities.	DiagMon Version 1.0
DIAG-USE-2	The end user MAY be made aware that a diagnostics or monitoring activity is commencing.	DiagMon Version 1.0
DIAG-USE-3	Network monitoring data logging or reporting MAY be transparent to the end user.	DiagMon Version 1.0
DIAG-USE-4	The end user MAY be informed that a session with a management authority is taking place prior to or after introducing client configuration changes.	DiagMon Version 1.0
DIAG-USE-5	If there is an interruption in a diagnostics and monitoring operation, the operation SHALL be resumed at the next practical opportunity.	DiagMon Version 1.0
DIAG-USE-6	The user SHOULD be asked for confirmation to proceed before diagnostic and monitoring tasks are implemented on the device.	DiagMon Version 1.0
DIAG-USE-7	Diagnostics and Monitoring enabler SHALL allow Diagnostics and Monitoring operations on the device based on a single user confirmation and/or single Diagnostics and Monitoring Management Authority confirmation.	DiagMon Version 1.0

Table 5: High-Level Functional Requirements – Usability Items

6.1.5 Interoperability

Label	Description	Enabler Release
DIAG-IOP-1	The Diagnostics and Monitoring system MAY be interfaced with external systems, e.g. a Customer Care application, SLT, or other management authorities via a standard interface.	WSI 1.0

Table 6: High-Level Functional Requirements – Interoperability Items

6.1.6 Privacy

Label	Description	Enabler Release
DIAG-PRIVACY-1	All data communication between the Device Management Server and a Device, that is personal to the user or confidential to the owner of the information (e.g. some network operator settings) MUST be confidentiality protected.	DiagMon Version 1.0
DIAG-PRIVACY-2	All Diagnostics data communication between Device Management Servers MUST be confidentiality protected.	DiagMon Version 1.0
DIAG-PRIVACY-3	The DiagMon enabler SHALL NOT hinder the User's control over collection, use and distribution of their personal information	DiagMon Version 1.0
DIAG-PRIVACY-4	Diagnostics and Monitoring enabler SHALL support a mechanism to inform the user about implications of installing diagnostic and monitoring MOs on the device.	DiagMon Version 1.0

Table 7: High-Level Functional Requirements – Privacy Items

6.2 Overall System Requirements

Label	Description	Enabler Release
DIAG-SYS-1	Discovery of the device by the DMS MUST be supported by the Diagnostics and Monitoring System.	DiagMon Version 1.0
DIAG-SYS-2	The Device SHALL be able to communicate all of its relevant properties (e.g., manufacturer, model, firmware, etc.) to the Diagnostics and Monitoring System on request.	DiagMon Version 1.0
DIAG-SYS-3	The Device SHALL be able to communicate its capabilities and configuration (e.g., WAP/MMS settings, installed software applications, etc.) to the Diagnostics and Monitoring System on request.	DiagMon Version 1.0
DIAG-SYS-4	The Device SHALL be capable of autonomously (i.e., without User interaction) accepting and storing downloaded Diagnostics and Monitoring Management Objects (e.g., parameters, software, etc.) after the one time initial trust relationship configuration (bootstrap) with the Diagnostics and Monitoring System is performed.	DiagMon Version 1.0
DIAG-SYS-5	The DM tree containing DM Diagnostics and Monitoring objects on the Device SHALL be capable of being modified (i.e., nodes or data fields added or deleted), read from, and/or written to.	DiagMon Version 1.0
DIAG-SYS-6	The Device SHALL be capable of receiving and displaying a command from the Diagnostics and Monitoring System to request User confirmation for a diagnostics and monitoring management action.	DiagMon Version 1.0
DIAG-SYS-7	The Device SHALL be capable of accepting User input regarding confirmation of a proposed DiagMon management action, and sending the result of that confirmation to the Diagnostics and Monitoring System.	DiagMon Version 1.0
DIAG-SYS-8	The Device SHALL be able to acknowledge the receipt and installation of DiagMon data downloaded from the Diagnostics and Monitoring System.	DiagMon Version 1.0
DIAG-SYS-9	In the event the device is resource constrained, it SHOULD be possible to prioritize events and actions associated with DM Diagnostics and Monitoring.	DiagMon Version 1.0
DIAG-SYS-10	The Diagnostics and Monitoring System SHALL be capable of querying Devices for information about Device properties, configuration, and capabilities.	DiagMon Version 1.0
DIAG-SYS-11	The Diagnostics and Monitoring System SHALL be capable of manipulating a Device's Diagnostics and Monitoring Management Object.	DiagMon Version 1.0
DIAG-SYS-12	The Device SHALL acknowledge a DM Diagnostics and Monitoring operation indication of success/failure to the Diagnostics and Monitoring System.	DiagMon Version 1.0
DIAG-SYS-13	The Diagnostics and Monitoring System SHALL be capable of sending a request for User confirmation of a DiagMon operation to the Device, and accepting the response from the Device.	DiagMon Version 1.0
DIAG-SYS-14	The Diagnostics and Monitoring System MUST report errors in Diagnostics and Monitoring querying and reporting in a standardized format.	DiagMon Version 1.0
DIAG-SYS-15	The Diagnostics and Monitoring System MUST verify integrity of Diagnostics and Monitoring data prior to download to Device.	DiagMon Version 1.0
DIAG-SYS-16	The Diagnostics and Monitoring System SHALL rely on features as described in DM v1.2 specifications or higher.	DiagMon Version 1.0
DIAG-SYS-17	The Diagnostics and Monitoring Enabler SHALL be able to provide time stamp information for the collected data or logged events.	DiagMon Version 1.0

Table 8: High-Level System Requirements

Appendix A. Change History (Informative)

A.1 Approved Version History

Reference	Date	Description
OMA-RD-DiagMon-V1_0	20 Dec 2011	Status changed to Approved by TP: OMA-TP-2011-0443-INP_DiagMon_V1_1_ERP_for_Final_Approval