OMTP

ADVANCED DEVICE MANAGEMENT

VERSION: v1_0

STATUS: Approved for publication

DATE OF PUBLICATION: 23rd January 2008

OWNER: OMTP Limited

CONTENTS

This document contains information that is confidential and proprietary to OMTP Limited. The information may not be used, disclosed or reproduced without the prior written authorisation of OMTP Limited, and those so authorised may only use this information for the purpose consistent with the authorisation.

The information contained in this document represents the current view held by OMTP Ltd. on the issues discussed as of the date of publication.

This document is provided “as is” with no warranties whatsoever including any warranty of merchantability, non-infringement, or fitness for any particular purpose. All liability (including liability for infringement of any property rights) relating to the use of information in this document is disclaimed. No license, express or implied, to any intellectual property rights are granted herein.

This document is distributed for informational purposes only and is subject to change without notice. Readers should not design products based solely on this document.

Each Open Mobile Terminal Platform member and participant has agreed to use reasonable endeavours to inform the Open Mobile Terminal Platform in a timely manner of Essential IPR as it becomes aware that the Essential IPR is related to the prepared or published specification. The declared Essential IPR is publicly available to members and participants of the Open Mobile Terminal Platform and may be found on the “OMTP IPR Declarations” list at the OMTP team room.

The Open Mobile Terminal Platform 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 and applicable rules above are set forth in the Schedule to the Open Mobile Terminal Platform Member and Participation Annex Form.

1 INTRODUCTION

1.1 DOCUMENT PURPOSE

As devices become more complex with increasing numbers of capabilities, users are able to configure their devices in ways which can create usage or security problems. These problems may result from any of the following examples:

- Changing default configuration settings
- Incompatibility between different settings
- Incompatibility between applications

When these incidents arise, there should be mechanisms that allow appropriate actions to be taken (e.g. bug fixes, over the air firmware updates, revocation of applications, etc.).

This document defines a set of recommendations for device management elements on the device which allow the operator, manufacturer or third party to resolve the problem on the device.

1.2 SCOPE & RELATIONSHIP WITH SDOS

1.2.1 DOCUMENT SCOPE

The problems defined in the previous section as well the use cases defined in chapter 2 can be used to identify a set of high level functionalities that should be available on mobile platforms:

- **Software Management:** Most of the use cases require the ability to install/uninstall software OTA (over the air) or at least have the possibility to inspect the software that is available on the device.
- **Firmware Update**: The application incompatibility use case will require in some situations to download and install OTA a new firmware in order to avoid any incompatibility with the applications.
- **Diagnostics:** In order to address some of the use cases it is important to have the ability to identify the problem and retrieve related information.
- **Management of Device Capabilities:** Some use cases require having the ability to activate/deactivate or configure OTA many of the device capabilities (e.g. Bluetooth, IR…).

- **DM Smart Card:** Most of the features described in this chapter should only be offered if security is granted. The Smart Card should be used for this security purpose whenever possible.
- **Policy Management:** The policy concept is introduced in the "Corporate IT Security Policy" use case. A policy is a set of rules that determines which operations (e.g. configuration, installation of applications and access to capabilities) can be performed by the end user. The ability to securely modify OTA the policies is also crucial.
- **File Management:** Some use cases require the ability to inspect OTA the device file system. Furthermore in some cases it should be also interesting to have the ability to upload/download/remove files to the device.
- **Process Management:** For some of the use cases it is important to have the possibility to analyse OTA the processes that are being executed. Furthermore it is also important to have the possibility to start/stop applications on the device OTA.

This document defines for each of these high-level functionalities the requirements that they should fulfil in order to address the use cases described before.

1.2.2 RELATIONSHIP WITH SDOS

Most of the high level functionalities described in the previous chapter are being specified within OMA DM group. This section describes which are the related OMA undergoing activities as well as OMTP's role with regards to OMA specifications.

1.2.2.1 Related SDOs

OMA has specified OMA Device Management v1.2 (OMA DM v1.2) that defines protocols and mechanisms that allow managing distributed mobile terminals. The main targets of this standard are to optimise the user experience, reduce the network operating costs and create new business opportunities. Because of its common business rationale with this OMTP task, OMA DM is considered as the most relevant protocol to be analysed within this document.

The OMA DM group decided that many new functionalities not covered in OMA DM Enabler v1.2 would be tackled by new enablers that refer to and interoperate in a consistent manner with OMA DM v1.2. Some of the enablers included in this set that are related with the high level functionalities described are:

- **SCOMO** (Software Component Management Object): The main target of this enabler is to allow Management Authorities to

deliver, install, uninstall, update and remove software components in a secure environment.

- **FUMO** (Firmware Update Management Object): FUMO defines a mechanism to update OTA device's firmware using OMA DM.
- **Diagnostics & Monitoring**: This enabler addresses the definition of mechanisms to enable management authorities to proactively detect and repair troubles in mobile terminals.
- **DCMO** (Device Capabilities Management Object): The primary goal of this enabler is to facilitate the management of many of the capabilities supported by mobile terminals (e.g. Camera, Bluetooth, IR…)
- **DM_SC** (Device Management Smart Card): This enabler defines how a Smart Card should be used to enhance DM capabilities including, for example, secure dynamic provisioning and security extensions for OMA DM enablers using smart cards (as FUMO, SCOMO or DCMO).
- **LAWMO** (Lock and Wipe Capabilities Management Object): This enabler addresses interoperable remote operations, such as Lock/Unlock Device, Wipe Device's Data and Factory Reset provide Management Authorities an effective way to protect data in the device.

1.2.2.2 OMTP / SDOs Interaction

The following table links the high level functionalities with the DM Enablers:

Functionality	OMA Enabler
Software Management	SCOMO
Firmware Update	FUMO
Diagnostics	Diagnostics & Monitoring
Management of Device Capabilities	DCMO
DM Smartcard	DM_SC
Policy Management	None
File Management	None
Process Management	LAWMO

For those areas in which a standard is publicly available, this document will refer to it as much as possible. These recommendations mainly focus in identifying potential gaps and defining the relationship between them (e.g. relationship between DM_SC and SCOMO).

1.3 BUSINESS RATIONALE

If a user has a problem with their device, the first point of contact is generally with the operator. The operator offers the main customer services to users even if the problem has been caused by the users' own actions on the device or by the installation of applications onto that device.. It is very important to correct the problem efficiently, effectively and securely without the need for the customer to return the handset. There will be significant cost savings in proactively monitoring the users' device and enabling capabilities which allow the operator to react quickly to customer problems (which the user may not be able to explain in conversation with the operator).

1.4 INTENDED AUDIENCE

There are two main audiences for these recommendations:

- Mobile Operators: As one of the main targets is reducing requirements fragmentation, OMTP Operators should adopt or reference these recommendations within their requirements specifications.
- OMTP Terminal implementers, i.e. the equipment and technology vendors that will be asked to satisfy OMTP recommendations.

1.5 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 [1].

- MUST: This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.
- MUST NOT: This phrase, or the phrase "SHALL NOT", mean that the definition is an absolute prohibition of the specification.
- SHOULD: This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

- SHOULD NOT: This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.
- MAY: This word, or the adjective "OPTIONAL", mean that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not include a particular option MUST be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides.)

The requirements within this document are uniquely identified using the following format:

ADM-####(.#.#), where:

- ADM (Advanced Device Management) is the acronym identifying the subject of this OMTP document
- #### is a 4 digit number that identifies the requirement (e.g. 0020) and which is to be unique within the document.
- (.#.#) are numbers that indicate sub-requirements (e.g. 00020.1 & 00020.2 which would be sub-requirements of 00020 and 00020.1.1 & 00020.1.2 which would be sub-requirements of 00020.1)

2 USE CASES

2.1 VIRUS

Jo owns a mobile phone and her friend sends Jo a game over Bluetooth. Jo installs the game ignoring a warning that appears to say that the game might be untrusted. Jo plays the game and enjoys being able to send her high score to a website which shows that she is the 5th best player this month. When Jo checks her pre-pay balance she discovers that it has dropped by £45 from what she expects. She calls her operator who informs her that calls and photo messages have been sent by her to several numbers including some at a premium rate. Her operator asks whether she is happy for them to examine her device remotely to determine any potential problems. Upon agreement, the operator remotely installs an agent on the device which looks at all the applications installed and executing on Jo's device. This agent determines that the game is in fact a recognised virus/trojan which can make calls in this way. The application is de-installed. A message is sent to Jo informing her of the risks from viruses to her device and recommending her to use only applications from sources which are trusted.

2.2 APPLICATION INCOMPATIBILITY

Peter downloads a new mapping application from a reputable site. Before the download, the device functions correctly. After the download, the device slows down dramatically even when the mapping application is not being run. Some of the settings for Peter's other applications have also been altered which changes their behaviour. However, Peter just sees a change in behaviour which he has difficulty in associating with the download of the new application which works just fine.

Peter calls customer services and reports the problem in relation to the device slowing down. A diagnostic agent on the device is able to report the status of the device, that all self tests pass and the applications that have been installed on the device. A database recognises an incompatibility problem in relation to two of the applications. Over the phone, Peter is asked whether he will accept the operator removing these applications from the device. Peter accepts and the applications are removed. Any potential loss in data is catered for by a data backup of the applications data. Peter is told about the problem and it is recommended not to install the mapping application. A new firmware build can be downloaded to Peters phone to allow the applications to work together. Under Peter's contract, these updates are free and he accepts the download. He reinstalls the mapping application and the device works normally

2.3 CORPORATE IT SECURITY POLICY

Employees of an enterprise are given mobile devices to help them work more effectively. The IT security department wants to make sure that suitable IT security policies are observed by these mobile devices, just as they do with employees' computers. For instance, they may want to:

- Require that only applications approved by them can be loaded onto the device.
- Allow access to the phone remotely and see what applications are loaded (e.g. make sure there are no games).
- Restrict certain functionality, e.g. disable the camera.
- Mandate the use of a lock code to access the device.
- Enforce Bluetooth policy, e.g. make sure the phone is not visible to other Bluetooth devices.
- Ensure that all internet access goes via the enterprise IT system.

3 GENERAL REQUIREMENTS

REQ. ID	REQUIREMENT
ADM-0010	The device SHALL support OMA DM v1.2 [2].
ADM-0020	The device SHALL support all the DM alerts with user interaction defined in [3].
ADM-0030	The device SHALL support generic alerts as defined in [3].
ADM-0040	The device SHALL be able to receive notifications from a DM server to start DM sessions as defined in [4].
ADM-0050	The Terminal vendor SHALL provide the DDF (Device Description Framework) file describing the Management Tree as defined in [5].
ADM-0050.1	All the functionalities of the DDF entries SHALL be described; example of usage SHALL be provided.

3.1 TRANSPORT SECURITY

Advanced Device Management capabilities can be potentially used for fraudulent purposes: distribution of malware, vandalism… To do so, this chapter defines a set of recommendations that offer security mechanisms for avoiding fraudulent use of ADM capabilities.

The requirements propose the use of certificates for securing OTA DM communications. In order to guarantee the security, and avoid identity spoofing or phishing, DM certificates should be distributed as part of a bootstrap process and cannot be used for any other purpose.

REQ. ID	REQUIREMENT
ADM-0060	The device SHALL support TLS 1.0 [6].
ADM-0070	The device SHOULD support SSL 3.0 [7].
ADM-0080	The device SHALL use a transport layer protocol supporting encryption (e.g. TLS 1.0 [6], SSL 3.0 [7]) for ADM operations performed OTA as recommended in Section 5.5.1.1 of [8].

REQ. ID	REQUIREMENT
ADM-0090	It SHOULD be possible to use dedicated certificates for DM transport layer security (e.g. it should be different from the ones used for application verification or accessing secure web sites).
ADM-0100	The Integrity of the certificates used for transport layer security of DM communications SHALL be assured.
ADM-0110	The certificate used for DM transport layer security SHALL be exposed to authorised servers (according to ACLs as specified in OMA DM TND [5]) in the AAuthData node in the DM Tree as defined in [9].
ADM-0120	The AAuthLevel node linked to a certificate used for DM transport layer security SHALL contain the value “HTTP” as defined in [9] section 5.3.1.19.
ADM-0130	The AAuthType node linked to a certificate used for DM transport layer security SHALL contain the value “TRANSPORT” as defined in [9] section 5.3.1.19.

3.2 BOOTSTRAP PROCESS

Bootstrap is the process of provisioning the device to a state where it is able to initiate a management session to a DM server. Hence, it is essential to guarantee that only trusted entities have the possibility to bootstrap devices. The following set of recommendations is intended to identify the bootstrap mechanisms and the security that should be in place linked to them.

REQ. ID	REQUIREMENT
ADM-0140	The device SHOULD support DM OTA bootstrap using the DM profile as defined in [10].
ADM-0150	If the device does not support DM profile, it SHALL support DM OTA bootstrap using the CP profile method defined in [10].
ADM-0160	If the device supports DM profile, it SHOULD support DM OTA bootstrap using the CP profile method defined in [10].
ADM-0170	When using the CP Profile to bootstrap the device OTA, only the NETWPIN and USERNETWPIN methods as defined in [8] SHALL be supported.

REQ. ID	REQUIREMENT
ADM-0180	When using the CP Profile to bootstrap the device OTA, the USERPIN and USERPINMAC methods as defined in [8] SHALL NOT be supported.
ADM-0190	When using the DM Profile to bootstrap the device OTA, only the NETWORKID and USERPIN_NETWORKID methods as defined in [8] SHALL be supported.
ADM-0200	When using the DM Profile to bootstrap the device OTA, the USERPIN method as defined in [8] SHALL NOT be supported.
ADM-0210	It SHALL be possible to bootstrap the device during manufacture.
ADM-0220	It SHALL be possible to distribute the certificate for DM transport security layer as part of a bootstrap process.
ADM-0230	The device SHALL automatically establish a DM session with the DM server once successfully bootstrapped as soon as practical.

4 FUMO

The possibility of updating the device firmware OTA is a critical part of ADM features. OMA “Firmware Update Management Object” (FUMO) [11] enables firmware updates by specifying the locations in the DM tree where update packages could be downloaded. This section describes additional requirements for the downloading and installation process.

REQ. ID	REQUIREMENT
ADM-0240	The device SHALL support FUMO as defined by OMA [11].

4.1 DOWNLOADING PROCESS

Update package download is the physical downloading of the firmware package which is to be eventually installed onto the device for the update. The OMA standard allows for two methods for package download: download using OMA DM or download using an external protocol. OMTP recommends the use of an external protocol as OMA DM is a heavy protocol, not intended for transferring big amounts of data and does not include session resume support. This section also includes additional requirements for the download process.

REQ. ID	REQUIREMENT
ADM-0250	The device SHALL support server initiated download of firmware update packages.
ADM-0260	The device MAY support client initiated download of firmware update packages using the mechanism defined in section 7 in [11].
ADM-0270	The device SHOULD be able to resume automatically a download that has been interrupted due to reasons beyond user control (e.g. coverage loss, low battery level or terminal being turned off).
ADM-0280	The device SHALL support out of band download of the firmware package (e.g. using OMA-DL) as described in [11].
ADM-0290	The device MAY support in-band download of the firmware package (using OMA-DM) as described in [11].
ADM-0300	Before download process starts, it SHALL be checked if there is enough free memory to store the firmware update package.

4.2 INSTALLATION PROCESS

REQ. ID	REQUIREMENT
ADM-0310	The device SHALL support the automatic start of the installation process once the firmware update package has been downloaded.
ADM-0320	If an error occurs during the firmware update installation process that prevents it from being completed then the device SHALL be able to return to the situation previous to the installation.
ADM-0330	If the firmware update installation process is stopped (e.g. due to battery discharge or extraction) then the device SHALL resume the installation from the point where it was interrupted.
ADM-0340	The device SHOULD support the user deferring the firmware update installation process to a later time (i.e. the installation cannot be deferred for ever).
ADM-0350	The device SHALL report back to the server the status of the firmware update installation process using the Generic Alert mechanism as described in section 6.2 in [11].
ADM-0360	Once the firmware update installation has been successfully completed, the package SHALL be removed from the device to avoid memory shortages.
ADM-0370	Before the firmware update installation starts, it SHALL be checked if there is enough battery life to finish the installation.

4.3 SECURITY

REQ. ID	REQUIREMENT
ADM-0380	Only previously bootstrapped servers SHALL be granted access to FUMO.
ADM-0390	The device SHALL authenticate the server asking to download a package as it is defined in OMA [7].
ADM-0400	The integrity of the firmware package SHALL be checked before installation in the device

REQ. ID	REQUIREMENT
ADM-0410	User data (e.g. DRM, applications, phonebook contacts, messages, notes, etc.) SHALL NOT be modified because of the firmware update process.
ADM-0420	Customisation settings (e.g. melodies, wallpaper, etc.) SHOULD NOT be changed because of firmware update process.
ADM-0430	After the installation process is completed, the device SHALL perform a normal boot sequence as if the device had just been turned on.
DADM-0440	Before installing a package the device SHALL verify that it has been authorised by the Management Authority.

5 SOFTWARE MANAGEMENT

The capability of managing OTA the software components installed on the device is essential to fulfil the use cases defined in Section 2. This section describes the functionalities required for properly addressing those use cases.

REQ. ID	REQUIREMENT
ADM-0450	The device SHALL support all the mandatory requirements defined in OMA SCOMO RD [12].
ADM-0460	For each software component exposed in the DM Tree the following information SHALL at least be available to the DM server: – Name – Identifier – Version – Application Execution Environment – Security Domain
ADM-0470	Information on software components not delivered via DM SHOULD be also available in the DM Tree.
ADM-0480	It SHOULD be possible to use DM for removing software components delivered via non-DM mechanisms.
ADM-0490	Information on the Application Execution Environments (type and version) supported by the device SHALL be available in the DM Tree.
ADM-0500	The device SHALL support verification and signing of software components prior to the installation.

6 INTEGRATION WITH THE SMARTCARD

This chapter defines a set of recommendations that identify how Smartcard capabilities should be used for DM purposes. These requirements apply to devices which support a Smartcard.

REQ. ID	REQUIREMENT
ADM-0510	The device SHALL support DM Smartcard bootstrap using the DM Profile as defined in [10].
ADM-0520	The device MAY support DM Smartcard bootstrap using the CP Profile method defined in [10].
ADM-0530	It SHOULD be possible to distribute the policies defined in section 7 as part of a Smartcard bootstrap process.

7 POLICY MANAGEMENT

Policies are a set of rules that determine the level of access that users have to certain device capabilities. This section defines what the policies that should be possible to set up on devices are and the mechanisms that should be in place for their management.

7.1 POLICY TYPES

REQ. ID	REQUIREMENT
ADM-0540	The device SHALL support policies that determine whether the end-user has the possibility to modify the device connectivity settings or not.
ADM-0550	The device SHALL support policies that determine whether the end-user has the possibility to modify the configuration of embedded MMS settings.
ADM-0560	The device SHALL support policies that determine whether the end-user has the possibility to modify the configuration of embedded PoC settings.
ADM-0570	The device SHALL support policies that determine whether the end-user has the possibility to modify the configuration of embedded VoIP settings.
ADM-0580	The device SHALL support policies that determine whether the end-user has the possibility to modify the configuration of embedded DM settings.
ADM-0590	The device SHALL support policies that determine whether the end-user has the possibility to modify the configuration of WiFi settings.
ADM-0600	If the device supports multiple trust levels, it SHALL support policies that determine at which levels the end-user is allowed to install applications.
ADM-0610	The device SHALL support policies that determine whether the end-user has the possibility to activate/deactivate Bluetooth capabilities.
ADM-0620	The device SHALL support policies that determine whether the end-user has the possibility to activate/deactivate camera capabilities.

REQ. ID	REQUIREMENT
ADM-0630	The device SHALL support policies that determine whether the end-user has the possibility to modify the Location Capabilities operational mode (Emergency Only, Location On, Location Off).
ADM-0640	The device MUST support policies that determine whether the user is required to set a terminal password or PIN.
ADM-0650	The device SHALL support policies that determine which servers are allowed to perform DM operations with the device (e.g. Bootstraps, Software Management…).
ADM-0660	The device SHALL support policies that determine which servers are allowed to perform DM operations without asking for user confirmation.
ADM-0670	The device SHALL support policies that determine which servers are allowed to perform DM operations without notifying the user.

7.2 POLICY LIFECYCLE

REQ. ID	REQUIREMENT
ADM-0680	It SHALL be possible to define the device policies at manufacture.
ADM-0690	Policies defined at manufacture SHALL be persistent in device memory (i.e. the policies must persist after a factory reset). In case multiple policies are provided (manufacturer, operator, enterprise), persistence SHALL NOT imply a conflict of policies during operation of the phone.
ADM-0700	It SHALL be possible to define and modify device policies via DM provided the management authority (i.e. DM Server) has been previously bootstrapped and no existing policy is broken.
ADM-0710	The end-user SHALL NOT be able to delete or modify device policies.

8 FILE MANAGEMENT

Having the possibility to interact with the terminal file system is essential for troubleshooting purposes.

REQ. ID	REQUIREMENT
ADM-0720	Subject to appropriate permissions it SHALL be possible to retrieve the names, sizes and permissions of specified files and folders in the device file system using DM.
ADM-0730	It SHOULD be possible to retrieve the creation, modification and last access dates of specified files and folders in the device file system using DM.
ADM-0740	It SHALL be possible to perform recursively the operations defined in ADM-0720.
ADM-0750	It SHOULD be possible to perform recursively the operations defined in ADM-730
ADM-0760	For file systems that allow file deletion, it SHALL be possible to delete a file using DM.
ADM-0770	For file systems that allow file addition, it SHALL be possible to add a file using DM.

9 PROCESS MANAGEMENT

In many situations the Management Authorities are interested in identifying the characteristics of the executing processes in a Terminal in order to identify problems related with performance. Furthermore in many other cases it is also useful to have the possibility to interact with the process management entity on the Terminal remotely in order to start or stop applications. This chapter describes a set of requirements for identifying what are the key features required for Process Management.

REQ. ID	REQUIREMENT
ADM-0780	It SHALL be possible to start the execution of a process or application in the terminal via DM.
ADM-0790	It SHOULD be possible to stop the execution of a process or application in the terminal via DM.
ADM-0800	It SHALL be possible to get a list of all the processes that are executing in the terminal via DM.
ADM-0800.1	For each executing process the terminal SHALL provide the process ID.
ADM-0800.2	For each executing process the terminal SHALL provide the memory usage.
ADM-0800.3	For each executing process the terminal SHOULD provide the filename the process is loaded from.
ADM-0810	It SHALL be possible to reboot the terminal using DM.
ADM-0820	The device SHALL support all the mandatory requirements defined in OMA LAWMO RD [13].

10 DEVICE CAPABILITY MANAGEMENT

Device Capabilities are physical characteristics and related parameters supported by the device (e.g. Cameras, Bluetooth…). In some situations, enterprises, regulations or operators have policies that restrict the use of some features while allowing others to be available on the mobile device. Hence, it is crucial to have mechanisms for managing remotely the device capabilities (e.g. enablement, disablement, configuration…).

REQ. ID	REQUIREMENT
ADM-0830	The device SHALL support all the mandatory requirements defined in [14].
ADM-0840	In the DM Tree, the device SHALL report, if present, the following hardware capabilities Camera - Bluetooth - WiFi - GPS - Local Connectivity - Memory Card.
ADM-0850	The device SHALL support enablement and disablement of all hardware capabilities reported in the DM Tree (such as Bluetooth and camera) as specified in [14].
ADM-0860	The device SHALL support the configuration of all hardware capabilities reported in the DM Tree (such as Bluetooth and camera) through OMA DM v1.2 [2].

11 DIAGNOSTICS AND MONITORING

In many cases Management Authorities wish to have the possibility to proactively detect and repair problems even before the users are affected or to identify potential problems before they happen.

OMA DM Diagnostics & Monitoring enabler was created in order to 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 problem 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 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.

REQ. ID	REQUIREMENT
ADM-0870	The device SHALL support all the mandatory requirements defined in [15].

12 Definition of Terms

Term	Description
Application Execution Environment	Set of software components (APIs, libraries, security rules…) providing the capabilities necessary to support Application Execution. Examples of different execution environments are the native environment, the browser or a virtual machine (e.g. Java Virtual Machine).
Bootstrap	The process of provisioning the DM client to a state where it is able to initiate a management session to a new DM server.
Cryptographic Mechanisms	Set of algorithms, keys and associated data/protocols used to provide confidentiality and/or integrity and/or authentication of data and/or entities.
Emergency Only	Operational mode in which positioning is only enabled in the context of an emergency services call.
Location On	Operational mode in which positioning is enabled for all services and applications.
Location Off	Operational mode in which positioning is disabled in all contexts including emergency services call.
Management Authority	An entity that has the right to perform a specific device management function on a Terminal 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 Terminal. One Management Authority may own all Terminal resources or may share or delegate all or parts of these with/to other Management Authorities.

TERM	DESCRIPTION
MANAGEMENT OBJECT	A logical element that can contain or represent and manage configurable data and software within a Terminal. The data and/or software includes but is not limited to • Parameters such as connectivity address, user preferences, proxy settings, user Identity, etc. • Software such as applications, applets, drivers, modules, firmware and their updates. A Management Object may represent the complete device configuration or a portion of a Terminal configuration. There may be multiple Management Objects on a Terminal with a pre-specified relationship between them. Each Management Object will support the following operations: • Add/Install – insert new elements into a Management Object. • Replace/Update – modify existing and/or insert new elements into a Management Object. • Delete/Uninstall – remove existing elements from a Management Object. • Query/Enumerate – List all or part of a Management Object.
POLICY	Set of rules that determine the level of access that users have to certain device capabilities.
SMARTCARD	A device with an embedded microprocessor chip. A smartcard is used for storing data and performing typically security related (cryptographic) operations. It is used an alternative term for UICC.
TERMINAL	Used as an alternative term for a cellular telephone or handset.
UNIVERSAL INTEGRATED CIRCUIT CARD	A physically secure device, an IC card (or 'smart card'), that can be inserted and removed from the terminal equipment. It may contain one or more applications. One of the applications may be a USIM [16].

13 ABBREVIATIONS

ABBREVIATION	DESCRIPTION
ADM	Advanced Device Management
API	Application Programming Interface
CP	Client Provisioning
DCMO	Device Capabilities Management Object
DDF	Device Description Framework
DM	Device Management
DM_SC	Device Management Smartcard
DRM	Digital Rights Management
FUMO	Firmware Update Management Object
HTTP	Hyper Text Transfer Protocol
JVM	Java Virtual Machine
IC	Integrated Circuit
IR	Infrared
KPI	Key Performance Indicator
LAWMO	Lock and Wipe Capabilities Management Object
MMS	Multimedia Messaging Service
OMA	Open Mobile Alliance
OMTP	Open Mobile Terminal Platform
OTA	Over The Air
PIN	Personal Identification Number
PoC	Push Over Cellular
RD	Requirements Description

ABBREVIATION	DESCRIPTION
SCOMO	Software Component Management Object
SDO	Standard Developing Organization
SSL	Secure Sockets Layer
TLS	Transport Layer Security
TND	Tree & Description
UICC	Universal Integrated Circuit Card
USIM	Universal Subscriber Identity Module
VoIP	Voice Over IP

14 REFERENCED DOCUMENTS

NO.	DOCUMENT	AUTHOR	DATE
1	RFC 2119 - Key words for use in RFCs to Indicate Requirement Levels http://www.ietf.org/rfc/rfc2119.txt	IETF	March 1997
2	"OMA Device Management V1.2" http://www.openmobilealliance.org/release_program/dm_v1_2A.html	OMA	Feb 2007
3	"OMA Device Management Representation Protocol V1.2" http://www.openmobilealliance.org/release_program/dm_v1_2A.html	OMA	Feb 2007
4	"OMA Device Management Notification Initiated Session V1.2" http://www.openmobilealliance.org/release_program/dm_v1_2A.html	OMA	Feb 2007
5	"OMA Device Management Tree & Description V1.2" http://www.openmobilealliance.org/release_program/dm_v1_2A.html	OMA	Feb 2007
6	RFC 2246, "The TLS protocol, version 1.0" http://www.ietf.org/rfc/rfc2246.txt	IETF	Jan 1999
7	"The SSL 3.0 Protocol"	Netscape Communications Corp	Nov 1996
8	"OMA Device Management Security V1.2" http://www.openmobilealliance.org/release_program/dm_v1_2A.html	OMA	Feb 2007

No.	Document	Author	Date
9	"OMA Device Management Standardised Objects V1.2" http://www.openmobilealliance.org/release_program/dm_v1_2A.html	OMA	Feb 2007
10	"OMA Device Management Bootstrap V1.2" http://www.openmobilealliance.org/release_program/dm_v1_2A.html	OMA	Feb 2007
11	OMA Firmware Update Management Object V1.0 http://www.openmobilealliance.org/release_program/fumo_v1_0A.html	OMA	Feb 2007
12	Software Component Management Object Requirements http://www.openmobilealliance.org/release_program/rd.html	OMA	July 2007
13	"Lock and Wipe Management Object Requirements" http://member.openmobilealliance.org/ftp/public_documents/dm/LAWMO/Permanent_documents/	OMA	2007
14	Device Capability Management Object Requirements http://www.openmobilealliance.org/release_program/rd.html	OMA	June 2007
15	DM Diagnostics & Monitoring Requirements http://www.openmobilealliance.org/release_program/rd.html	OMA	Feb 2007
16	3GPP TR 21.905 "Vocabulary for 3GPP Specifications"	3GPP	Sept 2007

-------- END OF DOCUMENT --------