OMTP

SOFTWARE

DEVICE MANAGEMENT ENABLER REQUIREMENTS

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.

VERSION:	OMTP Device Management Enabler Version 1_0, Release 1_0
STATUS:	Approved
DATE OF LAST EDIT:	12 December 2005
OWNER:	OMTP Software Group

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 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

This documents outlines the technical requirements that a device management enabler must fulfil, as described in OMTP Application Frameworks [1].

1.2 INTENDED AUDIENCE

This document is intended for internal distribution.

1.3 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].

- MUST: This word, or the terms “REQUIRED” or “SHALL”, mean that the definition is an absolute requirement of the specification.[1]
- 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.[2]
- 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

[1] MUST is used in those requirements that are most desired by operators, from a timeline perspective as well as across all phone types.

[2] SHOULD is used in those requirements that are highly desirable, though not needed across all phone segments at this point of time. Those requirements will be time limited to this specific release and will be considered to be raised to “MUST” requirements in future releases.

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 the document are uniquely identified using the following format:

- TADM-GROUP-XX-###.###.### where:
  - ❑ *GROUP* is used to group a set of requirements. Grouping of requirements is used to ease the process of managing requirements. For example TADM-SPMMS-FR-### can be used as a Requirement ID for Requirements on Service Provisioning for the MMS enabler.
  - ❑ *XX* refers to the requirement type (either “FR” for a functionality requirement, “CF” for requirements for the common file format or “IF” for an interfacing requirement).
  - ❑ ### are sequential numbers that identifies the requirement (e.g. 1.1.1). It is only mandatory to include the first number.

2 DEVICE MANAGEMENT ENABLER DESCRIPTION

This chapter describes what a Device Management Enabler is, provides an overview of its responsibilities and the requirements, as defined in this document and relevant references.

2.1 DESCRIPTION

The Device Management Enabler is part of the Services Framework, as defined in the "Application Framework Concept Paper" [1]. The Device Management Enabler will allow third parties to manage the device configuration and other elements on behalf of the end user. OMTP typically focuses on the wireless operators' requirements, but will allow other parties, such as service providers, telephone manufacturers or IT departments of corporations, to also take the role of the third party managing the device.

Device Management will allow these third parties to remotely set parameters, perform troubleshooting on the mobile device and install or upgrade software.

Although some of the requirements refer to user interaction, this enabler will not handle the dialogue with the end user. However the DM enabler is responsible for the management of these interactions.

OMTP Release 1 concentrates only on the requirements for Remote Service Provisioning.

2.2 MOTIVATION

The increased complexity offered by the mobile terminals is a continuous challenge for mobile operators, who are looking for a way to be able to easily manage the whole set of devices using their networks. The Device Management Enabler is defined to fulfil the Functional Requirements as specified by OMTP User Experience requirements. Operators wish not only to be able to provision a mobile device, but also to have the facility to manage certain functionalities on the devices, if required.

2.3 REFERENCES

The Device Management Enabler Requirements gathered in this document are envisioned for the OMTP Release 1 and are based on the Functional Requirements, as outlined in the Specification Of A User Experience Platform "Functional Requirements for Remote Service Provisioning" [2].

The OMA Device Management v1.2 Candidate Enabler [3] is the basis of the OMTP Device Management Enabler specification.

3 ENABLER FUNCTIONALITY

This chapter gathers all the requirements that define the different functionalities that a device management enabler must offer.

3.1 BOOTSTRAP AND SERVICE PROVISIONING

For the first OMTP Release, only the Requirements for Bootstrap and Service Provisioning will be included for the DM Enabler.

In order for a DM enabler to be able to establish a DM session, it MUST be provisioned with the DM settings. The process of provisioning the DM enabler with the information needed to initiate a DM session to a DM server is called bootstrap. Bootstrap can be done in different scenarios: while manufacturing, OTA, at the point of sale and using a SIM card.

The capability of dynamically managing the settings needed to use the different services available in the terminals is called Service Provisioning.

3.1.1 FACTORY BOOTSTRAP

This section defines the requirements for the case when terminals are loaded with OMA DM bootstrap information at the point of manufacture. This mechanism is also called Customised Bootstrap [3].

Although the definition of the mechanism to communicate the bootstrap parameters from operators to manufacturers is outside of the scope of the DM enabler definition, the profiles defined in OMA DM v1.2 are recommended as transport formats.

REQUIREMENT ID	REQUIREMENT	REFERENCES
TADM-BSPFB-FR-1	Terminals MUST be able to be bootstrapped while manufacturing with the basic DM configuration (DM account and connectivity data).	DM5A-F006 DM5A-F012 [2]
TADM-BSPFB-FR-3	The operator DM account MUST be bootstrapped at manufacture as the owner of the DM tree root.	

3.1.2 SIM BOOTSTRAP

This section defines the requirements related to bootstraps performed using the SIM card. The DM enabler must obtain all the information necessary to bootstrap the terminal from the SIM card.

REQUIREMENT ID	REQUIREMENT	REFERENCES
TADM-BSPSIMB-FR-1	DM enabler MUST support the detection of the removal and/or change of the SIM card.	DM5A-F020 [2]
TADM-BSPSIMB-FR-2	When a new SIM card has been inserted, and the device has accepted it, the DM enabler MUST verify that it contains bootstrapping information.[3]	DM5A-F020 [2]
TADM-BSPSIMB-FR-3	When a new SIM card with bootstrapping information has been inserted In a terminal, the DM enabler MUST bootstrap the terminal with this data.	DM5A-F020 DM5A-F021 [2]
TADM-BSPSIMB-FR-4	If the DM servers previously bootstrapped by SIM are no longer available on the SIM card, the DM enabler MUST remove all those DM servers from the terminal DM tree.	DM5A-F017 DM5A-F020 [2]
TADM-BSPSIMB-FR-6	The DM enabler MUST process bootstrapping data from the SIM card in at least one of the standardised data formats defined in OMA DM v1.2 (OMA CP profile and OMA DM profile).	DM5A-F020 [2]
TADM-BSPSIMB-FR-7	If user confirmation is required as indicated in the SIM card data, the DM enabler MUST ask for user confirmation before bootstrapping the terminal.	DM5A-F023 [2]
TADM-BSPSIMB-FR-8	If the bootstrap message defines whether user confirmation is required and is set to “no user confirmation” the device MUST NOT ask for user confirmation.	DM5A-F023 [2]

[3] Although the bootstrap information verification should be done as soon as possible, intervening tasks between SIM acceptance and this verification will be allowed, if necessary

REQUIREMENT ID	REQUIREMENT	REFERENCES
TADM-BSPSIMB-FR-9	The DM enabler MUST initiate a management session with the DM server when the SIM bootstrap has finished.[4]	DM5A-F015 [2]

3.1.3 *SERVER INITIATED BOOTSTRAP*

This section defines the requirements to be applied to bootstraps initiated by a remote server.

REQUIREMENT ID	REQUIREMENT	REFERENCES
TADM-BSPSIB-FR-1	The DM enabler MUST process bootstrapping information received from a remote server in at least one of the standardised data formats defined in OMA DM v1.2 (CP profile and DM profile).	DM5A-F013 DM5A-F014 [2]
TADM-BSPSIB-FR-2	The DM enabler MUST accept only bootstrapping messages coming from an authorised server as defined in [7]. Messages coming from servers not authorised (not using the bootstrap security mechanisms defined in [7]) MUST be ignored.	
TADM-BSPSIB-FR-4	If a non-secure transport mechanism is used to transfer the bootstrap information, the DM enabler MUST accept only requests using transport neutral security mechanisms.	TADM-BSPSIB-FR-2
TADM-BSPSIB-FR-8	In case of transport neutral security, the DM enabler MUST use a shared secret between the SIM card and the remote server (e.g. IMSI) to decide whether a server is authorised or not.	TADM-BSPSIB-FR-4

[4] Although the session initiation should be done as soon as possible, intervening tasks between bootstrap and the beginning of the session will be allowed, if necessary

REQUIREMENT ID	REQUIREMENT	REFERENCES
TADM-BSPSIB-FR-5	The DM enabler MUST ignore non-secure bootstraps (see TADM-BSPSIB-FR-8, TADM-BSPSIB-FR-4, TADM-BSPSIB-FR-5). The user MUST NOT be informed about this circumstance.	TADM-BSPSIB-FR-2
TADM-BSPSIB-FR-6	In case of server initiated CP bootstrap, only mechanisms based on a shared secret (NETWPIN, USERNETWPIN) MUST be accepted.	TADM-BSPSIB-FR-4
TADM-BSPSIB-FR-7	In case of server initiated DM bootstrap, only mechanisms based on a shared secret (NETWORKID, USERPIN_NETWORKID) MUST be accepted by the DM enabler.	TADM-BSPSIB-FR-4

3.1.4 SERVICE PROVISIONING AT MANUFACTURE

REQUIREMENT ID	REQUIREMENT	REFERENCES
TADM-BSPMANSP-FR-1	The DM enabler MUST be able to be configured with all the information related with the services supported by the terminal during manufacture.	DM5A-F013 [2]

3.1.5 SIM CARD SERVICE PROVISIONING

REQUIREMENT ID	REQUIREMENT	REFERENCES
TADM-BSPSIMSP-FR-1	When a new SIM card is inserted in the terminal, the DM enabler MUST be able to incorporate the service settings available in the SIM into the DM tree.[5]	DM5A-F020 [2]

[5] If the SIM/USIM includes the MMS configuration, as specified by 3GPP, the terminal MUST use this information instead of the MMS configuration stored in the DM tree.

3.1.6 CONTINUOUS OTA SERVICE PROVISIONING

REQUIREMENT ID	REQUIREMENT	REFERENCES
TADM-BSPCOTASP-FR-1	The DM enabler MUST process all the DM commands coming from a previously bootstrapped DM server, subject to appropriate security and authentication.	DM5A-F014 DM5A-F016 [2]
TADM-BSPCOTASP-FR-2	The DM enabler MUST request user confirmation before starting any OTA update if the DM server requests it.	DM5A-F025 [2]
TADM-BSPCOTASP-FR-3	The DM enabler MUST inform the user about the progress of an OTA update if the DM server requests it.	DM5A-F023 [2] DM5A-F024 [2]
TADM-BSPCOTASP-FR-4	The DM enabler MUST provide mechanisms to inform the user of the end of an OTA update if the DM server requests it.	DM5A-F029 [2]

3.1.7 DEVICE MANAGEMENT

This section describes the requirements on the DM enabler to manage all the information related to the Device Management Service.

REQUIREMENT ID	REQUIREMENT	REFERENCES
TADM-BSPDM-FR-1	The DM enabler MUST manage the configuration information related to a DM account.	DM5A-F006 [2]
TADM-BSPPDM-FR-2	The DM tree MUST have a Management Object that will be used as a placeholder to store the information related with a DM account. This Management Object MUST meet the specification defined in [6] for DMAcc.	DM5A-F006 [2]
TADM-BSPPDM-FR-3	The DM tree must support the Parameter 'Name' for the DM MO.	

REQUIREMENT ID	REQUIREMENT	REFERENCES
TADM-BSPPDM-FR-4	A link to at least one interior node in the DM tree that contains connectivity parameters MUST be supported.	

3.1.8 MULTIMEDIA MESSAGING SYSTEM[6]

This section describes the requirements on the DM enabler to manage all the information related to MMS connectivity. The definition of the management objects that must be supported in OMTP terminals is defined in the OMA DM Device Description Framework [4].

No Management Object (MO) for MMS has yet been registered with OMNA. It is expected that such an MO registered with OMNA will provide at least the same data as used in the Application Characteristic information used for OMA CP. It is also expected that there will be a mapping of the corresponding parameters between the Application Characteristic and the MO. The requirements given in this section are based on these assumptions.

Please see also the footnote to section 3.1.5.

REQUIREMENT ID	REQUIREMENT	REFERENCES
TADM-BSPMMS-FR-1	The DM enabler MUST manage the configuration information related with the MMS service.	DM5A-F002 [2]
TADM-BSPMMS-FR-2	The DM tree MUST have a Management Object that will be used as a placeholder to store the information related with MMS accounts.	DM5A-F002 [2]
TADM-BSPMMS-FR-3	The leaves of the MMS MO MUST provide the information specified in all mandatory parameters of the w4 Application Characteristics [8] and [9].	DM5A-F002 [2]

[6] Requirements in this section only apply if the terminal supports MMS.

REQUIREMENT ID	REQUIREMENT	REFERENCES
TADM-BSPMMS-FR-5	The MO managed by the DM Enabler that supports an OMA MMS Enabler Release 1.2 [10] based implementation MUST support a leaf containing the information specified in CM parameter, as defined in the w4 Application Characteristic[9].	
TADM-BSPMMS-FR-6	The MO managed by the DM Enabler supporting an OMA MMS Enabler Release 1.3 [11] based implementation MUST support a leaf containing the information specified in CM parameter, as defined in the w4 Application Characteristic [8].	
TADM-BSPMMS-FR-7	A link to at least one interior node in the DM tree that contains connectivity parameters MUST be supported.	

3.1.9 BROWSER[7]

This section describes the requirements on the DM enabler to manage all the information related to the Browser Service.

No Management Object for Browsing has yet been registered with OMNA. It is expected that an MO registered with OMNA will provide at least the same information as used in the Application Characteristic information used for OMA CP. It is also expected that there will be a mapping of the corresponding parameters between the Application Characteristic and the MO. The requirements given in this section are based on these assumptions.

REQUIREMENT ID	REQUIREMENT	REFERENCES
TADM-BSPWEB-FR-1	The DM enabler MUST manage the configuration information related with a Browser.	DM5A-F001 DM5A-F003 [2]

[7] Requirements in this section only apply if the terminal offers browsing capabilities.

REQUIREMENT ID	REQUIREMENT	REFERENCES
TADM-BSPWEB-FR-2	The DM tree MUST include a Management Object to be used as a placeholder to store the information related to the Browser configuration.	DM5A-F001 DM5A-F003 [2]
TADM-BSPWEB-FR-3	The leaves of the Browser MO MUST provide the information specified in all mandatory parameters of the w2 application characteristics [13].	DM5A-F001 DM5A-F003 [2]
TADM-BSPWEB-FR-5	The MO managed by the DM Enabler MUST support a leaf containing the information specified in the 'Name' parameter defined in the w2 Application Characteristics [13].	
TADM-BSPWEB-FR-5	The MO managed by the DM Enabler MUST support a leaf containing the information specified in the 'Startpage' parameter, as defined in the w2 Application characteristics [13].	
TADM-BSPWEB-FR-6	A minimum of 5 Bookmarks MUST be supported.	
TADM-BSPWEB-FR-7	A link to at least one interior node in the DM tree that contains connectivity parameters MUST be supported.	

3.1.10 STREAMING[8]

This section describes the requirements on the DM enabler to manage all the information related with Streaming Services.

No Management Object for Streaming has yet been registered with OMNA. It is expected that an MO registered with OMNA will provide at least the same information as used in the Application Characteristic information used for OMA CP. It is also expected that there will be a

[8] Requirements in this section only apply if the terminal supports streaming capabilities.

mapping of the corresponding parameters between the Application Characteristic and the MO. The requirements given in this section are based on these assumptions.

REQUIREMENT ID	REQUIREMENT	REFERENCES
TADM-BSPSTR-FR-1	When the device supports Streaming, the DM enabler MUST manage the configuration information related to the streaming services.	DM5A-F004
TADM-BSPSTR-FR-2	The DM tree MUST have an MO that will be used as a placeholder to store the information related to a streaming profile.	DM5A-F004 [2]
TADM-BSPSTR-FR-3	The leaves of the Streaming MO MUST support the information specified in all mandatory parameters of the 554 Application characteristics [14].	
TADM-BSPSTR-FR-5	The MO managed by the DM Enabler MUST support a leaf containing the information specified in the 'Name' parameter, as defined in the 554 Application characteristics [14].	
TADM-BSPSTR-FR-6	The MO managed by the DM Enabler MUST support a leaf containing the information specified in 'Max-Bandwidth' parameter, as defined in the 554 Application characteristics [14].	
TADM-BSPSTR-FR-7	The MO managed by the DM Enabler MUST support a leaf containing the information specified in 'Netinfo' parameter, as defined in the 554 Application characteristics [14].	

REQUIREMENT ID	REQUIREMENT	REFERENCES
TADM-BSPSTR-FR-8	The MO managed by the DM Enabler MUST support a leaf containing the information specified in 'Min-UDP-Port' and 'Max-UDP-Port' parameters, as defined in the 554 Application characteristics [14].	
TADM-BSPSTR-FR-9	A link to at least one interior node in the DM tree that contains connectivity parameters MUST be supported.	

3.1.11 EMAIL[9]

This section describes the requirements on the DM enabler to manage all the information related with the email service.

No Management Object for email has yet been registered with OMNA. It is expected that an MO registered with OMNA will provide at least the same information as used in the Application Characteristic information used for OMA CP. It is also expected that there will be a mapping of the corresponding parameters between the Application Characteristic and the MO. The requirements given in this section are based on these assumptions.

REQUIREMENT ID	REQUIREMENT	REFERENCES
TADM-BSPEM-FR-1	The DM enabler MUST manage the configuration information related with the email services.	DM5A-F005 [2]
TADM-BSPEM-FR-2	The DM tree MUST have an MO that will be used as a placeholder to store the information related with email SMTP, POP3 and IMAP accounts.	DM5A-F005 [2]
TADM-BSPEM-FR-3	The leaves of the Email MO MUST provide the information specified in all mandatory parameters of the Email Application Characteristics [15].	

[9] Requirements in this section only apply if the terminal supports email.

REQUIREMENT ID	REQUIREMENT	REFERENCES
TADM-BSPEM-FR-5	The MO managed by the DM Enabler MUST support a leaf containing the information specified in the 'Name' parameter, as defined in the Email Application Characteristics [15].	
TADM-BSPEM-FR-6	The MO managed by the DM Enabler MUST support a leaf containing the information specified in the 'Aauthname' parameter, as defined in the Email Application Characteristics [15].	
TADM-BSPEM-FR-7	The MO managed by the DM Enabler MUST support a leaf containing the information specified in the 'Aauthsecret' parameter, as defined in the Email Application Characteristics [15].	
TADM-BSPEM-FR-8	The MO managed by the DM Enabler SHOULD support a leaf containing the information specified in the 'Rt-Addr' parameter, as defined in the email Application Characteristics [15].	
TADM-BSPEM-FR-9	A link to at least one interior node in the DM tree that contains connectivity parameters MUST be supported.	

3.1.12 DATA SYNCHRONISATION[10]

This section describes the requirements on the DM enabler to manage all the information related to the Data Synchronisation service. The definition of the Management Objects that must be supported in OMTP terminals is done using the OMA DM Device Description Framework [4].

[10] Requirements in this section only apply if the terminal supports data synchronisation capabilities.

No Management Object for DS has yet been registered with OMNA. It is expected that an MO registered with OMNA will provide at least the same information as used in the Application Characteristic information used for OMA CP. It is also expected that there will be a mapping of the corresponding parameters between the Application Characteristic and the MO. The requirements given in this section are based on these assumptions.

REQUIREMENT ID	REQUIREMENT	REFERENCES
TADM-BSPDS-FR-1	When the device supports DS the DM enabler MUST manage the configuration information related to the DS services.	DM5A-F007 [2]
TADM-BSPDS-FR-2	The DM tree MUST have an MO that will be used as a placeholder to store the information related to DS accounts.	DM5A-F007 [2]
TADM-BSPDS-FR-3	The leaves of the DS MO MUST provide the information specified in all mandatory parameters of the w5 Application Characteristics [16].	
TADM-BSPDS-FR-5	The MO managed by the DM Enabler MUST support a leaf containing the information specified in the 'Name' parameter, as defined in the w5 Application Characteristics [16].	
TADM-BSPDS-FR-6	The MO managed by the DM Enabler MUST support a leaf containing the information specified in the 'Resource/Name' parameter, as defined in the w5 Application Characteristics [16].	
TADM-BSPDS-FR-7	The MO managed by the DM Enabler SHOULD support a leaf containing the information specified in the 'CLIURI' parameter, as defined in the w5 Application Characteristics [16].	

REQUIREMENT ID	REQUIREMENT	REFERENCES
TADM-BSPDS-FR-8	A link to at least one interior node in the DM tree that contains connectivity parameters MUST be supported.	

3.1.13 INSTANT MESSAGING AND PRESENCE[11]

This section describes the requirements on the DM enabler to manage all the information related with IMPS.

No Management Object for IMPS has yet been released by OMA. The current draft has been used to define the requirements given in this section.

REQUIREMENT ID	REQUIREMENT	REFERENCES
TADM-BSPPIM-FR-1	When the device supports Instant Messaging and Presence the DM enabler MUST manage the configuration information related to the Presence and Instant Messaging service.	DM5A-F008 [2]
TADM-BSPPIM-FR-2	The DM tree MUST have an MO that will be used as a placeholder to store the information related with IMPS accounts.	DM5A-F008 [2]
TADM-BSPPIM-FR-3	This MO MUST meet the specification, as defined in [12] for IMPS.	DM5A-F008 [2]
TADM-BSPPIM-FR-4	The DM tree MUST support all mandatory nodes from [12].	DM5A-F008 [2]
TADM-BSPPIM-FR-5	The DM tree MUST support the Node ‘Name’ for the IMPS MO.	
TADM-BSPPIM-FR-6	The DM tree MAY support the Node ‘AAccept’ for the IMPS MO.	

[11] Requirements in this section only apply if the terminal supports instant messaging and presence services.

REQUIREMENT ID	REQUIREMENT	REFERENCES
TADM-BSPPIM-FR-7	The DM tree MAY support the Node 'PrefAddrt' for the IMPS MO. It MAY support the Node 'AppAddr' and sub nodes. It MUST support at least one of these nodes.	
TADM-BSPPIM-FR-8	The DM tree MUST support the Node 'AppAuth' with all defined sub nodes for the IMPS MO. This includes AuthName and AuthSecret.	
TADM-BSPPIM-FR-9	The DM tree SHOULD support the Node 'CIDPrefix' for the IMPS MO.	
TADM-BSPPIM-FR-10	A link to at least one interior node in the DM tree that contains connectivity parameters MUST be supported.	

3.1.14 PUSH TO TALK[12]

This section describes the requirements on the DM enabler to manage all the information related with the Push to Talk service.

REQUIREMENT ID	REQUIREMENT	REFERENCES
TADM-BSPPTT-FR-1	The DM enabler MUST be able to manage the configuration information related to the Push To Talk service.	DM5A-F009 [2]
TADM-BSPPTT-FR-2	The DM tree MUST be able to have an MO that will be used as a placeholder to store the information related to a Push to Talk connection. This MO MUST meet the specification, as defined in [5].	DM5A-F009 [2]

[12] Requirements in this section only apply if the terminal supports push to talk.

3.1.15 WiFi[13]

This section describes the requirements on the DM enabler to manage all the information related with WiFi.

A Management Object for WiFi has yet to be specified by a standards body. OMA has started working on a WiFi MO and has sent out two LS to 3GPP and WiFi.

This section will reference to the standardised objects when they become available.

REQUIREMENT ID	REQUIREMENT	REFERENCES
TADM-BSPWIF-FR-1	The DM enabler MUST manage the configuration information related to the WiFi service.	DM5A-F010 [2]
TADM-BSPWIF-FR-2	The DM tree MUST have an MO that will be used as a placeholder to store the information related with the WiFi profile.	DM5A-F010 [2]

3.1.16 CONNECTIVITY INFORMATION

This section specifies the information that MUST be stored in the connectivity MOs (i.e. NAP and PROXY). The standardisation of the whole structure of those objects has not yet been released by OMA. The current drafts have been used to define the requirements given in this section. This chapter should make reference to these standardised objects whenever the standards are released by OMA.

REQUIREMENT ID	REQUIREMENT	REFERENCES
TADM-BSPCON-FR-1	The DM enabler MUST manage the configuration information related with a network access point (NAP).	DM5A-F012 [2] TADM-BSPMMS-FR-5 TADM-BSPDS-FR-7 TADM-BSPPIM-FR-7 TADM-BSPDS-FR-12 TADM-BSPSTR-FR-4 TADM-BSPWEB-FR-3 TADM-BSPWAP-FR-3 TADM-BSPMMS-FR-5

[13] Requirements in this section only apply if the terminal supports WiFi.

REQUIREMENT ID	REQUIREMENT	REFERENCES
TADM-BSPCON-FR-2	The DM tree MUST have an MO that will be used as a placeholder to store the information related with a NAP.	TADM-BSPCON-FR-1
TADM-BSPCON-FR-6	The NAP MO MUST meet the specification, as defined in [17].	
TADM-BSPCON-FR-7	The DM tree MUST support all mandatory nodes from [17] for the NAP Object.	
TADM-BSPCON-FR-8	Dependent on the bearer supported by the device, the DM tree MUST support all mandatory nodes from at least one Bearer Object e.g. if one or more bearer is supported, at least one of the following MOs: • 3GPP PS bearer mandatory nodes from [19] • 3GPP CS bearer mandatory nodes from [20] • 3GPP2 bearer mandatory nodes from [21].	
TADM-BSPCON-FR-4	The DM Enabler MUST manage the configuration information related with a proxy.	TADM-BSPMMS-FR-5 TADM-BSPDS-FR-7 TADM-BSPPIM-FR-7 TADM-BSPDS-FR-12 TADM-BSPSTR-FR-4 TADM-BSPWEB-FR-3 TADM-BSPWAP-FR-3 TADM-BSPMMS-FR-5

REQUIREMENT ID	REQUIREMENT	REFERENCES
TADM-BSPCON-FR-5	The DM tree MUST have an MO that acts as a placeholder to store the information related with proxies.	TADM-BSPCON-FR-4
TADM-BSPCON-FR-9	The Proxy MO MUST meet the specification defined in [17].	
TADM-BSPCON-FR-10	The DM tree MUST support all mandatory nodes from [17] for the PROXY Object.	
TADM-BSPCON-FR-11	The DM tree SHOULD support the ProxyParams node. When the proxy configuration relates to a WAP proxy, the WAP proxy specific MO specified in [18] SHOULD be supported.	

4 RELATIONSHIPS WITH OTHER ENABLERS

This chapter gathers all the requirements for the relationships that the DM enabler must offer to other enablers.

4.1 GENERAL

The solution based on the information exposed in the nodes of the DM tree can be distributed for management by different enablers in the system. This does not prevent an alternative solution where there is an independent storage mechanism e.g. a database or file system. This mechanism is accessed both from the DM enabler — to expose the information to the DM server via the DM tree and manage this data — and the other enabler, either directly or by some other mechanism that accesses the configuration data.

4.2 RELATIONSHIP WITH THE CUSTOMISATION ENABLER

REQUIREMENT ID	DESCRIPTION	REFERENCES
TADM-ENA-IF-1	There SHALL be a relationship with the Customisation enabler that offers the possibility for the Customisation enabler to manage the information contained in one or more nodes in the DM tree.	TACE-IF-1 [22]
TADM-ENA-IF-2	In cases where the customisation enabler is not handling customisation information according to TADM-ENA-IF-1, the customisation information SHOULD be available via an MO in the DM tree to be managed by the DM enabler.	

5 STANDARDS REQUIREMENTS

This chapter includes all the mandatory requirements that are applied to the relevant standards related to DM.

5.1 OMA STANDARDS REQUIREMENTS

REQUIREMENT ID	DESCRIPTION	REFERENCES
TADM-OMADM-ST-1	The DM enabler MUST fulfil the mandatory requirements, as defined in OMA DM v1.2 [3].	
TADM-OMADM-ST-3	The DM enabler MUST support the display alert command, as specified in [3].	TADM-BSPCOTASP-FR-4
TADM-OMADM-ST-4	The DM enabler MUST support the confirmation alert command, as specified in [3].	TADM-BSPCOTASP-FR-2
TADM-OMADM-ST-5	The DM enabler MUST support the user choice alert command, as specified in [3].	CL4-G005 [2]
TADM-OMADM-ST-6	The DM enabler MUST support the progress notification alert command, as specified in [3].	TADM-BSPCOTASP-FR-3
TADM-OMADM-ST-7	The DM enabler SHOULD support the TNDS specification [3].	
TADM-OMADM-ST-8	If DM profile bootstrap is supported the DM enabler MUST support the Inbox Object [6].	

6 DEFINITION OF TERMS

The table below contains the definition of terms used in this document. Cross-referenced words are printed in italics.

TERM	DESCRIPTION
BOOTSTRAP	The process of provisioning the DM enabler with the information needed to initiate a DM session to a DM server.
SERVICE PROVISIONING	The ability to dynamically manage the settings needed to use the different services available in the terminals.

7 ABBREVIATIONS

ABBREVIATION	DESCRIPTION
ACL	Access Control List
CP	Client Provisioning
DM	Device Management
DS	Data Synchronisation
DTD	Document Type Definition
IMAP	Internet Message Access Protocol
IMSI	International Mobile Subscriber Identity
IMPS	Instant Messaging and Presence Services
MMS	Multimedia Messaging System
MO	Management Object
NAP	Network Access Point
OMA	Open Mobile Alliance
OMNA	Open Mobile Naming Authority
OTA	Over The Air
POP	Post Office Protocol
SIM	Subscriber Identity Module
SMTP	Simple Mail Transfer Protocol
TNDS	Tree and Description Serialisation
WAP	Wireless Application Protocol
WIFI	Wireless Fidelity

8 REFERENCED DOCUMENTS

NO.	DOCUMENT	AUTHOR	DATE
1	"OMTP Application Framework Concept Paper 1_0, Release 1" (http://www.omtp.org)	OMTP	July 2005
2	"OMTP Functional Requirements for Remote Service Provisioning, 1_0, Release 1" (http://www.omtp.org)	OMTP	July 2005
3	"Enabler Release Definition for OMA Device Management V1.2", OMA ERELD-DM-V1_2	OMA	July 2005
4	"OMA Device Management Tree and Description, Version 1.2", OMA-TS-DM-TND-V1_2	OMA	July 2005
5	"OMA PoC Control Plane v1.0", OMA-TS-POC-ControlPlane-V1_0	OMA	April 2005
6	"OMA Device Management Standardized Objects v1.2", OMA-TS-DM-StdObj-V1_2	OMA	July 2005
7	"OMA Device Management Security v1.2"	OMA	July 2005
8	"OMA-TS-MMS-W4", OMA-TS-MMS-W4-V1_3	OMA	June 2005
9	"OMA-MMS-W4", OMA-MMS-W4-V1_2	OMA	September 2004
10	"Enabler Release Definition for MMS", OMA-ERELD-MMS-V1_2_1	OMA	April 2005
11	"Enabler Release Definition for MMS", OMA-ERELD-MMS-V1_3	OMA	August 2005
12	"OMA IMPS Management Object", OMA-TS-IMPS-MO-V1.0	OMA	Draft not yet published
13	"OMA-w2-Application-Characteristic-for-Browsing", OMA-w2-Application-Characteristic-for-Browsing-V1_0_0	OMA	July 2004
14	"OMA-Application-Characteristic-for-Streaming", OMA-Application-Characteristic-for-Streaming-V1_0_0	OMA	July 2004

NO.	DOCUMENT	AUTHOR	DATE
15	"OMA-Application-Characteristics-for-Email", OMA-Application-Characteristics-for-Email-1_0_0 documents 110.txt, 143.txt and 25.txt	OMA	July 2004
16	"OMA-w5-Application-Characteristic-for-DS", OMA-w5-Application-Characteristic-for-DS-V1_2	OMA	July 2004
17	"Standardized Connectivity Management Objects ",OMA-TS-DM-ConnMO-V1_0-20051007-D	OMA	Draft October 2005
18	"Standardized Connectivity Management Objects WAP Proxy Parameters ",OMA-TS-DM-ConnMO-WAPProxy-V1_0-20051007-D	OMA	Draft October 2005
19	"Standardized Connectivity Management Objects 3GPP Packet Switched Bearer Parameters", OMA-TS-DM-ConnMO-3GPPPS-V1_0-20051007-D	OMA	Draft October 2005
20	"Standardized Connectivity Management Objects 3GPP Circuit-Switched Data Bearer Parameters", OMA-TS-DM-ConnMO-3GPPCS-V1_0-20051007-D	OMA	Draft October 2005
21	"Standardized Connectivity Management Objects CDMA Packet Data Bearer Parameters", OMA-TS-DM-ConnMO-3GPP2-V1_0-20051007-D	OMA	Draft October 2005
22	"OMTP Customisation Enabler Requirements" 1_0, Release 1	OMTP	Draft, November 2005
23	"User Experience Customisation Functional Requirements: Look and feel, menu customisation and application integration" 1_0, Release 1 (http://www.omtp.org)	OMTP	July 2005