

# OMA DM: Management Object for Device Encryption

Version 1.0; October 1, 2008

OMA Device  
Management

**NOKIA**

Copyright © 2008 Nokia Corporation. All rights reserved.

Nokia and Forum Nokia are trademarks or registered trademarks of Nokia Corporation. Other product and company names mentioned herein may be trademarks or trade names of their respective owners.

#### **Disclaimer**

The information in this document is provided “as is,” with no warranties whatsoever, including any warranty of merchantability, fitness for any particular purpose, or any warranty otherwise arising out of any proposal, specification, or sample. This document is provided for informational purposes only.

Nokia Corporation disclaims all liability, including liability for infringement of any proprietary rights, relating to implementation of information presented in this document. Nokia Corporation does not warrant or represent that such use will not infringe such rights.

Nokia Corporation retains the right to make changes to this document at any time, without notice.

#### **License**

A license is hereby granted to download and print a copy of this document for personal use only. No other license to any other intellectual property rights is granted herein.

## Contents

<b>1</b>	<b>Introduction.....</b>	<b>5</b>
1.1	Notation .....	6
<b>2</b>	<b>Device Encryption management object v1.0 description .....</b>	<b>7</b>
2.1	Commands.....	7
2.1.1	Disable UI.....	7
2.1.2	Encrypt.....	7
2.1.3	Decrypt.....	7
2.2	Node descriptions .....	7
2.2.1	./DevEnc.....	7
2.2.2	./DevEnc/PhoneMemoryCmd .....	7
2.2.3	./DevEnc/MemoryCardCmd .....	8
2.2.4	./DevEnc/PhoneMemoryStatus .....	8
2.2.5	./DevEnc/MemoryCardStatus .....	8
2.2.6	./DevEnc/MemoryCardEncKey .....	9
2.2.7	./DevEnc/UIState .....	9
2.2.8	./DevEnc/PhoneMemoryProgress.....	9
2.2.9	./DevEnc/MemoryCardProgress.....	10
<b>3</b>	<b>Terms and abbreviations.....</b>	<b>11</b>
<b>4</b>	<b>References .....</b>	<b>12</b>
<b>5</b>	<b>Evaluate this resource .....</b>	<b>13</b>

## Change history

October 1, 2008	Version 1.0	Initial document release.

## 1 Introduction

The purpose of this document is to define the “Device Encryption Management Object v1.0” settings format for Open Mobile Alliance (OMA) Device Management (DM) usage. The definition of the parameter settings formats consists of tree structure, instance identifiers, and a detailed description of the management tree.

For information on devices supporting this object version, see the [Forum Nokia Device Specifications](#).

The following document is a Nokia interpretation of the OMA Device Management specification. The intent of the document is to explain the organization of the parameters associated with this functionality.

## 1.1 Notation

In this document the following notation is used to describe the DM Management Object tree model and parameters:

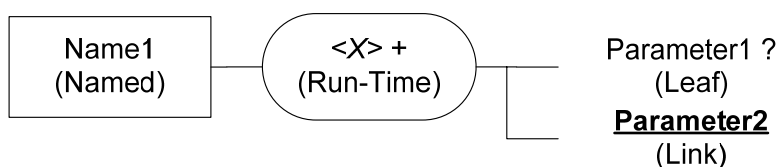


Figure 1: DM Management Object tree model and parameters

### Named parent object

The name of the parent object is fixed. If the parent object's occurrence is One, the object's scope is permanent and cannot be deleted. If parent object's occurrence is ZeroOrOne, the object's scope is dynamic and can be created and deleted at run time by Management Server.

### Run-time object

Run-Time objects can be created and deleted at run-time by Management Server. Run-time objects' scope is dynamic. Run-time objects in the text are represented by an <x> notation where <x> represents the node's instance identifier that is generated dynamically and can have any alphanumeric characters as a value.

### Leaf object

Management objects without any children are called leaf objects. Description framework type for leaf objects in this document is *text/plain*.

### Link object

Link object is a type of Leaf object that has an absolute URI value pointing to another object in the management tree of the same device, that is, always starting from the root node.

Following characters are used in the management object tree diagram to indicate how many instances of a specific node the Management Authority is able to configure in the Management Object Tree:

Character	Meaning
+	One or many occurrences; that is, at least one instance of the parameter needs to exist and be configured.
*	Zero or more occurrences.
?	Zero or one occurrence.
(None)	Occurrence is One; that is, the parameter needs to exist and be configured.

More information about the management tree, object descriptions, and property elements (Occurrence, Scope, Access Type, and Format) can be found from the *OMA Device Management Tree and Description* document [3].

## 2 Device Encryption management object v1.0 description

This chapter defines the management object structure and identifiers needed when managing Device Encryption using OMA DM.

### 2.1 Commands

There are three main command categories that can be activated using OMA DM for Device Encryption.

#### 2.1.1 Disable UI

If the policy for device encryption states that the user is not allowed to remove encryption, the UI can be locked for that action by the administrator. The locking is not dependent on the actual encryption status; that is, the UI lock can also be used to disable encryption on the device. See Section 2.2.7 `"/DevEnc/UIState"` for more information.

#### 2.1.2 Encrypt

Both the device memory and the memory card can be encrypted by the administrator over OMA DM. For the device memory, there is only one option for encryption, that is, the key is generated in the device using random data and it cannot be retrieved.

For the memory card, there are three options:

1. Normal encryption. The key is generated in the device and stored in write-only memory. Restoring factory settings makes the card unreadable.
2. Backup encryption. The key is generated in the device and stored in write-only memory, but a copy of the key remains in the DM adapter to be retrieved by the administrator. This allows restoring the key after a factory reset or making the card readable also in other devices.
3. Restore encryption. The key is not generated in the device, but sent to the device as a part of the DM structure. The key is stored in the device in write-only memory. This operation can be used to restore a key that was retrieved using a Backup encryption operation.

#### 2.1.3 Decrypt

The decrypting operation is the same for both the device memory and memory card, and there are no options or parameters for it.

### 2.2 Node descriptions

#### 2.2.1 `./DevEnc`

Occurrence	Format	Access type
One	Node	Get

The DevEnc node is a parent to all Device Encryption objects. Scope of this node is permanent.

#### 2.2.2 `./DevEnc/PhoneMemoryCmd`

Occurrence	Format	Access type
One	Int	Replace

This permanent node is used for starting a decrypting or encrypting operation on the phone memory.

Write values	Description
0	Start decrypting
1	Start encrypting

### 2.2.3 `./DevEnc/MemoryCardCmd`

Occurrence	Format	Access type
One	Int	Replace

This permanent node is used for starting a decrypting or encrypting operation on the memory card. See Section 2.1.2, "Encrypt" for a detailed explanation of the encryption options.

Write values	Description
0	Start decrypting.
1	Start encrypting.
2	Start backup encrypting; key is generated in the phone and can be retrieved (see Section 2.2.6, " <code>./DevEnc/MemoryCardEncKey</code> ").
3	Start restore encrypting; key is sent to the phone in conjunction with this command (see Section 2.2.6, " <code>./DevEnc/MemoryCardEncKey</code> ").

### 2.2.4 `./DevEnc/PhoneMemoryStatus`

Occurrence	Format	Access Type
One	Int	Get

This permanent node is used for getting the phone memory encryption status.

Read values	Description
8	Phone memory is decrypted (can be encrypted).
9	Phone memory is being decrypted (not possible to encrypt).
10	Phone memory is encrypted (can be decrypted).
11	Phone memory is being encrypted (not possible to decrypt).
12	Phone memory is being wiped.
13	Phone memory is corrupted.

### 2.2.5 `./DevEnc/MemoryCardStatus`

Occurrence	Format	Access type
One	Int	Get

This permanent node is used for getting the memory card encryption status.

Read values	Description
8	Memory card is decrypted (can be encrypted).
9	Memory card is being decrypted (not possible to encrypt).
10	Memory card is encrypted (can be decrypted).
11	Memory card is being encrypted (not possible to decrypt).
12	Memory card is being wiped.
13	Memory card is corrupted.

#### 2.2.6 ./DevEnc/MemoryCardEncKey

Occurrence	Format	Access type
One	B64	Get, Replace

This permanent node is used for getting/setting the memory card encryption key.

Values	Description
< base64-encoded key >	Encryption key for memory card; should be set when using restore encrypting and read when backup encrypting is done.

#### 2.2.7 ./DevEnc/UIState

Occurrence	Format	Access type
One	Int	Get, Replace

This permanent node is used for getting/setting the encryption UI status in the phone.

Values	Description
0	Phone and memory card status can be changed in the phone UI.
1	Memory card status change disabled.
2	Phone memory status change disabled.
3	Both disabled.

#### 2.2.8 ./DevEnc/PhoneMemoryProgress

Occurrence	Format	Access type
One	Int	Get

This permanent indicates the progress of the current en/decryption process. The value of this node is undefined if no phone memory operation is ongoing, that is, state is not 9 or 11.

Value	Description
0..100	Progress status in percent.

## 2.2.9 ./DevEnc/MemoryCardProgress

Occurrence	Format	Access type
One	Int	Get

This permanent indicates the progress of the current en/decryption process. The value of this node is undefined if no memory card operation is ongoing, that is, state is not 9 or 11.

Value	Description
0..100	Progress status in percent.

### 3 Terms and abbreviations

Term or Abbreviation	Meaning
DDF	Device Description Framework
DM	Device Management
DMAcc	Device Management Account
OMA	Open Mobile Alliance
SyncML	Synchronization Mark-up Language

## 4 References

- [1] [OMA Device Management DDF for AP](http://www.forum.nokia.com/), available at [www.forum.nokia.com/](http://www.forum.nokia.com/)
- [2] OMA Device Management Standardized Objects, Open Mobile Alliance Ltd. available at [www.openmobilealliance.com/](http://www.openmobilealliance.com/)
- [3] OMA Device Management Tree and Description, Open Mobile Alliance Ltd. available at [www.openmobilealliance.com/](http://www.openmobilealliance.com/)
- [4] Uniform Resource Identifiers (URI): Generic Syntax [RFC2396], The Internet Engineering Task Force (IETF), available at [www.ietf.org/](http://www.ietf.org/)

## 5 Evaluate this resource

Please spare a moment to help us improve documentation quality and recognize the resources you find most valuable, by [rating this resource](#).