LAWMO Requirements

Candidate Version 1.0 – 10 June 2008

Open Mobile Alliance

OMA-RD-LAWMO-V1_0-20080610-C

Contents

Tables

1. Scope (Informative)

This document defines the requirements for Lock and Wipe Management functionality, which leverage OMA DM enabler and makes use of the functionalities provided by OMA DM protocol **Error! Reference source not found.**.

2. References

2.1 Normative References

[RFC2119] "Key words for use in RFCs to Indicate Requirement Levels", S. Bradner, March 1997, URL:http://www.ietf.org/rfc/rfc2119.txt

2.2 Informative References

[OMADICT] "Dictionary for OMA Specifications", Version 2.6, Open Mobile Alliance™, OMA-ORG-Dictionary-V2_6, URL:http://www.openmobilealliance.org/

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

3. Terminology and Conventions

3.1 Conventions

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in [RFC2119].

All sections and appendixes, except “Scope” and “Introduction”, are normative, unless they are explicitly indicated to be informative.

3.2 Definitions

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	see [OMADICT]
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
End User	see [OMADICT]
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 Operator	see [OMADICT]
Service Provider	An entity that provides and administers a service to a Subscriber and/or User. The Network Operator is often a Service Provider.
Subscriber	see [OMADICT]
User	see [OMADICT]
LAWMO Operations	Lock Device, Unlock Device, Wipe Device’s Data and Factory Reset operations which may be invoked on a Lock and Wipe MO.
Lock Device	To render the device fully or partially inoperable from unauthorised usage according to which lock level is chosen. Two lock levels are defined: Partially Lock Device and Fully Lock Device.
Fully Lock Device	To render the device fully inoperable from unauthorised usage except for functions mandated by law (e.g. emergency calls) and participating LAWMO sessions as well as other data sessions that aid in the recovery of the device.
Partially Lock Device	To render the device inoperable from unauthorised usage except for receiving incoming calls, functions mandated by law (e.g. emergency calls), and participating in LAWMO sessions as well as other data sessions that aid in the recovery of the device.
Unlock Device	To re-enable all Device functionalities previously locked by Lock Device operation.
Wipe Device’s Data	The act to permanently erase personal and/or enterprise-related data from the device
Factory Reset	The act to reset the device to its initial factory state.

Abbreviations

OMA	Open Mobile Alliance
DM	Device Management
DMS	Device Management Server
LAWMO	Lock And Wipe Management Object
MO	Management Object

4. Introduction (Informative)

The mobile device is becoming a pocketable private information database which contains various user data and enterprise-related data. There are several scenarios user may need to remotely lock and/or wipe the device as follows:

- If the device was lost or stolen, there is a risk of data being compromised either maliciously or by accident. User may request to lock the device and wipe all the data from the device. If the device is returned, the user can also request to unlock the device.
- If the device was hand over or sold to other users, the owner may request to clean all user and enterprise-related data in the device or reset it to factory state.

There are more use cases and scenarios that may require LAWMO Operations, such as Lock/Unlock Device, Wipe Device's Data and Factory Reset.

This specification collects the use cases and corresponding requirements to develop a standardized approach to fulfil the above market needs.

5. Use Cases (Informative)

5.1 Wiping Device's Data

5.1.1 Short Description

1) Wiping Device's Data with user request

An end user wants to upgrade his device and sell the old one on the internet. He wishes to permanently wipe all his personal and/or enterprise-related data from device. His device either does not provide a user-accessible wipe function or the wipe function is hard to use. In this case, wiping data by Device Management Server is welcome.

2) Wiping a device without user request:

When an employee uses a personal phone and decides to terminate his contract with his employer. Prior to terminating his employment, the enterprise commands the device to wipe enterprise-sensitive data.

5.1.2 Actors

- **Management Authority: Customer Care**
- **Device Management Server**
- **User: End User**

Actor Specific Issues

- **Management Authority:** Management Authority would like to help subscribers deal with their data remotely and easily.
- **Device Management Server:** Device Management Server issues and handles the commands in the service.
- **User:** User would like to permanently wipe his data from his device.

Actor Specific Benefits

- **Management Authority:** Management Authority can provide good service experience for their subscribers
- **User:** User can permanently erase his personal data and protect his privacy.

5.1.3 Pre-conditions

- Customer Care can request the Device Management Server send wipe command(s).
- The device is able to establish a DM session with the Device Management Server.
- Personal and/or enterprise-related data in the device can be wiped.
- The Device Management Server can optionally provide a user prompt for approving the wipe process.
- User is able to request Customer Care to help him wipe his data from device and Customer Care can confirm the user's identity.

5.1.4 Post-conditions

All sensitive data in the device is permanently wiped by the Device Management Server.

5.1.5 Normal Flow

1. End User contacts Customer Care and requests personal data be wiped from his device
2. Customer Care validates and confirms the User's identity.
3. Customer Care sends, via the Device Management Server, command(s) to the device to wipe data.
4. The device issues a prompt to the User to confirm this operation.
5. Upon confirmation by the User, the device wipes user's data.
6. The device reports the results to the Device Management Server. Customer Care is notified of the results and informs the User.

Alternative Flow 1

This alternate flow describes the scenario that no user prompt is required by the device holder:

2. End User contacts Customer Care and requests personal data be wiped from his device without user confirmation
3. Customer Care validates and confirms the User's identity
4. Customer Care sends, via the Device Management Server, command(s) to the device to wipe data.
5. The device consumes the command and wipes user data without user confirmation.
6. The device reports the results to the Device Management Server. Customer Care is notified of the results and informs the User.

5.2 Resetting Device to Factory Clean State

5.2.1 Short Description

Non-end users, such as mobile network operators, device manufacturers, or resellers of second-hand devices, require the capability to reset devices to the factory clean state automatically and easily. Even they wish to deal with devices in bulk.

We can take it into account as one special wipe scenario.

5.2.2 Actors

- **Enterprise Management Authority: Who have authority to reset device via Device Management Server.**
- **Device Management Server**
- **User: Non-end user such as mobile network operators, device manufactures, or resellers of second-hand devices**

5.2.3 Pre-conditions

- Enterprise Management Authority can request Device Management Server to send command.
- The device is able to establish a DM session with the Device Management Server.
- The device can be reset to factory clean state.

- The factory clean state has been defined by the device manufacture.

5.2.4 Post-conditions

The device is reset to factory clean state.

5.2.5 Normal Flow

1. Enterprise Device Management Authority sends via Device Management Server command(s) to the device to reset device to factory clean state.
2. The device consumes the command and reset to factory clean state.

5.3 Locking/Unlocking Device Use Case

5.3.1 Short Description

1) Locking device with user request:

Jack comes to his office and finds he has left his mobile Device in a taxi just minutes ago. He contacts the Device Management Authority, who may be his service provider's Customer Care, at once and asks for his device to be Partially Locked. Customer Care staff first confirms his identity then requests the Device Management Server send a command to Partially Lock his device. Jack's device is now protected from fraudulent use and his personal information cannot be perused. Jack calls his device hoping the person in possession of it will return it to him. The taxi driver answers and Jack arranges to pick up his device. After picking up his device he calls Customer Care to unlock his device and return it to full functionality.

2) Locking device without user request:

An enterprise distributes phones to employees. An employee resigns but fails to return his phone. The enterprise (who is the Management Authority in this case) locks the former employee's phone. Many similar use cases exist ie, the employer may wish to lock the phone when the employee goes on a leave of absence, or on weekends, etc.

5.3.2 Actors

- **Device Management Server**
- **Device Management Authority: Customer Care**
- **User A: Jack who lost his device**
- **User B: Someone who holds the lost device**

Actor Specific Issues

- **Customer Care**: Customer Care helps subscribers to deal with their device and data remotely.
- **Device Management Server**: Device Management Server issues and handles the commands in the service.
- **User:** Neither User A or User B can unlock the device locally.

Actor Specific Benefits

- **Customer Care:** Customer Care can provide good service experience for their subscribers and protect against fraudulent service use.

- **User A:** User can effectively protect his privacy and avoid fraudulent use of his device without having to terminate his service account. Upon retrieving his device he can have it returned to its normal working state.

5.3.3 Pre-conditions

- The device is able to establish a DM session with the Device Management Server.
- Customer Care can confirm the identity of Jack, who asks for his device to be locked, and can request the Device Management Server send device lock and unlock command(s).
- The device can be locked and unlocked.

5.3.4 Post-conditions

The device is locked/unlocked by the Device Management Server.

5.3.5 Normal Flow

- After losing his device in a taxi, User A (Jack) makes a call to Customer Care to request Partially Locking his device. Customer Care first confirms his identity and then requests the Device Management Server to send a command to Partially Lock Jack's device.
- The device consumes the operations and partially locks the device.
- The device reports the results to the Device Management Server, and Customer Care is notified of the results and informs Jack.
- Jack dials up his device to contact User B, the current holder, to arrange return of his device. User B answers and Jack arranges to retrieve his device.
- After retrieving his device, Jack calls Customer Care and requests his device to be unlocked. Customer Care confirms Jack's identity, then requests the Device Management Server to send command(s) to unlock Jack's device
- The device consumes the operation and unlocks Jack's device.
- The device reports the results to the Device Management Server and Customer Care is notified of the results and informs Jack.

5.3.6 Alternative Flow

In this alternate flow, Jack realizes his device has been stolen and requests his device to be fully locked.

1. After realizing his device has been stolen, User A (Jack) makes a call to Customer Care to request Fully Locking his device. Customer Care first confirms his identity and then requests the Device Management Server send a command to Fully Lock Jack's device.
2. The device consumes the operations and fully locks the device.
3. The device reports the results to the Device Management Server, and Customer Care is notified of the results and informs Jack.

6. Requirements (Normative)

6.1 High-Level Functional Requirements

Label	Description	Enabler Release
LAWMO-HLFR-1	The LAWMO enabler SHALL support all LAWMO Operations.	LAWMO 1.0
LAWMO-HLFR-2	The LAWMO enabler SHALL support a mechanism for the Management Authority to specify whether the user is to be informed of LAWMO operations performed in the Client.	LAWMO 1.0
LAWMO-HLFR-3	The LAWMO enabler SHALL support a mechanism to notify the result of LAWMO Operations except Factory Reset to Device Management Server.	LAWMO 1.0
LAWMO-HLFR-4	Only the Authorised LAWMO Server that invoked a Lock Device Operation on a Device SHALL be authorised to perform the corresponding Unlock Device Operation.	LAWMO 1.0

Table 1: High-Level Functional Requirements

6.1.1 Security

Label	Description	Enabler Release
LAWMO-SEC-1	Only authenticated Device Management Server SHALL be able to perform LAWMO Operations.	LAWMO 1.0
LAWMO-SEC-2	Only authorized Device Management Server SHALL be able to perform LAWMO Operations.	LAWMO 1.0
LAWMO-SEC-3	The LAWMO enabler SHALL reuse the security mechanism defined in DM v1.2 [DMPRO] or later release.	LAWMO 1.0

Table 2: High-Level Functional Requirements – Security Items

6.1.1.1 Authentication

None

6.1.1.2 Authorization

None

6.1.1.3 Data Integrity

None

6.1.1.4 Confidentiality

None

6.1.2 Charging

None

6.1.3 Administration and Configuration

None

6.1.4 Usability

Label	Description	Enabler Release
LAWMO-USA-1	**The LAWMO enabler SHALL support execution of LAWMO Operations on the device with or without user's permission.**	**LAWMO 1.0**
LAWMO-USA-2	**The LAWMO Enabler SHALL support prompting the user for confirmation prior to executing LAWMO operations if the user confirmation is requested by the Device Management Server using the mechanisms provided by OMA DMv1.2 or higher.**	**LAWMO 1.0**

Table 3: High-Level Functional Requirements – Usability Items

6.1.5 Interoperability

None

6.1.6 Privacy

None

6.2 Overall System Requirements

Label	Description	Enabler Release
LAWMO-OSR-01	The LAWMO enabler SHALL rely on features as described in OMA DM v1.2 specifications or higher.	LAWMO 1.0
LAWMO-OSR-02	The LAWMO enabler SHALL support vendor extensions.	LAWMO 1.0

Table 4: High-Level System Requirements

6.2.1 Device Management Server

Label	Description	Enabler Release
LAWMO-OSR-DMS-01	The Device Management Server SHALL support Partially Lock Device operation.	LAWMO 1.0
LAWMO-OSR-DMS-02	The Device Management Server SHALL support Fully Lock Device operation.	LAWMO 1.0
LAWMO-OSR-DMS-03	The Device Management Server SHALL support Unlock Device operation.	LAWMO 1.0
LAWMO-OSR-DMS-04	The Device Management Server SHALL support Wipe Device's Data operation.	LAWMO 1.0
LAWMO-OSR-DMS-05	The Device Management Server SHOULD support Factory Reset operation.	LAWMO 1.0
LAWMO-OSR-DMS-06	The Device Management Server SHALL be able to receive notifications about result of LAWMO operations from the Device	LAWMO 1.0

Table 5: DMS Requirements

6.2.2 Device

Label	Description	Enabler Release
LAWMO-OSR-Device-01	The Device SHALL support Partially Lock Device operation.	LAWMO 1.0
LAWMO-OSR-Device-02	The Device SHALL support Fully Lock Device operation.	LAWMO 1.0
LAWMO-OSR-Device-03	The Device SHALL support Unlock Device operation.	LAWMO 1.0
LAWMO-OSR-Device-04	The Device SHALL support Wipe Device's Data operation.	LAWMO 1.0
LAWMO-OSR-Device-05	The Device SHOULD support Factory Reset operation.	LAWMO 1.0

LAWMO-OSR-Device-06	The Device SHALL be able to send notifications about result of LAWMO operations to the Device Management Server	LAWMO 1.0

Table 6: Device Requirements

Appendix A. Change History (Informative)

A.1 Approved Version History

Reference	Date	Description
n/a	n/a	No prior version –or- No previous version within OMA

A.2 Draft/Candidate Version <current version> History

Document Identifier	Date	Sections	Description
Draft Versions OMA-RD-LAWMO-V1_0-20070417-D	17 April 2007	3.2, 5, 6	Incorporates agreed document: OMA-DM-2007-0052R02-INP_use_case_for_wiping_data.doc
Draft Versions OMA-RD-LAWMO-V1_0-20070704-D	4 July 2007	1	Incorporates agreed document: OMA-DM-LAWMO-2007-0007-CR_Scope.doc
	4 July 2007	4	Incorporates agreed document: OMA-DM-LAWMO-2007-0006R01-CR_Introduction.doc
Draft Versions OMA-RD-LAWMO-V1_0-20070803-D	3 August 2007	3.2	Incorporates agreed document: OMA-DM-LAWMO-2007-0003R01-CR_Factory_Reset_Definition.doc
	3 August 2007	3.2	Incorporates agreed document: OMA-DM-LAWMO-2007-0005R01-CR_Wipe_User_Data_Definition.doc
	3 August 2007	3.2	Incorporates agreed document: OMA-DM-LAWMO-2007-0011R04-CR_Lock_UnLock_Device_Definition.doc
	3 August 2007	5	Incorporates agreed document: OMA-DM-LAWMO-2007-0012R02-CR_Locking_Unlocking_Device_Use_Case.doc
Draft Versions OMA-RD-LAWMO-V1_0-20070905-D	3 Sep 2007	2,3.2,3.3	Incorporates agreed document: OMA-DM-LAWMO-2007-0014R03-CR_Abbreviation_Definition_Reference.doc
	3 Sep 2007	6.2	Incorporates agreed document: OMA-DM-LAWMO-2007-0015R02-CR_Overall_System_Requirements.doc
Draft Versions OMA-RD-LAWMO-V1_0-20071025-D	25 Oct 2007	6.1,6.1.1,6.1.4	Incorporates agreed document: OMA-DM-LAWMO-2007-0022R01-CR_Client_Notification_Requirement.doc OMA-DM-LAWMO-2007-0018R01-CR_HLFR_Update.doc
	25 Oct 2007	5.1.3	Incorporates agreed document: OMA-DM-LAWMO-2007-0020R01-CR_Wiping_Precondition.doc
	25 Oct 2007	3.2,4,5.1.1,5.3.6	Incorporates agreed document: OMA-DM-LAWMO-2007-0019-CR_LAWMO_RD_bugfix.doc
Draft Versions OMA-RD-LAWMO-V1_0-20071212-D	12 Dec 2007	All	Incorporates agreed document: OMA-DM-LAWMO-2007-0025-CR_Enrich_RD_Use_Cases.doc OMA-DM-LAWMO-2007-0024-CR_Updates_HLFR.doc OMA-DM-LAWMO-2007-0023R01-CR_RD_Cleanup_For_Closure_Review.zip
Draft Versions OMA-RD-LAWMO-V1_0-20080226-D	26 Feb 2008	3.1,5.1.3,6.1.4	Incorporates agreed document: OMA-DM-LAWMO-2008-0002-CR_RD_corrections.doc
Candidate Version OMA-RD-LAWMO-V1_0-20080610-C	10 June 2008	n/a	Status changed to Candidate by TP TP ref# OMA-TP-2008-0195-INP_LAWMO_v1_0_RD_for_Candidate_Approval