Lock and Wipe Management Object

Candidate Version 1.0 – 27 Jan 2009

Open Mobile Alliance

OMA-TS-LAWMO-V1_0-20090127-C

Contents

Figures

1. Scope

This document defines the Lock and Wipe Management Object employed in a Lock and Wipe management process that leverages OMA DM protocol [DMPRO]. It also defines LAWMO Client and LAWMO Server-side behaviour associated with Lock and Wipe Management Object necessary to remotely manage the Device.

The mechanisms defined in this document fulfils the functional requirements needed to support LAWMO enabler as described in the LAWMO requirements document [LAWMO-RD] and comply to the architecture defined in LAWMO Architecture document [LAWMO-AD].

2. References

2.1 Normative References

[DMPRO]	"OMA Device Management Protocol", Version 1.2, Open Mobile Alliance, OMA-TS-DM_Protocol-V1_2, URL: http://www.openmobilealliance.org/
[DMREPRO]	"OMA DM Representation Protocol", Version 1.2, Open Mobile Alliance, OMA-TS-DM_RepPro-V1_2, URL: http://www.openmobilealliance.org/
[LAWMO-AD]	"LAWMO Architecture", Version 1.0, Open Mobile Alliance, OMA-AD_LAWMO-V1_0, URL: http://www.openmobilealliance.org/
[LAWMO-RD]	"LAWMO Requirements", Version 1.0, Open Mobile Alliance, OMA-RD_LAWMO-V1_0, URL: http://www.openmobilealliance.org/
[RFC2119]	"Key words for use in RFCs to Indicate Requirement Levels", S. Bradner, March 1997, URL: http://www.ietf.org/rfc/rfc2119.txt
[RFC4234]	"Augmented BNF for Syntax Specifications: ABNF". D. Crocker, Ed., P. Overell. October 2005, URL: http://www.ietf.org/rfc/rfc4234.txt
[SCRRULES]	"SCR Rules and Procedures", Open Mobile Alliance™, OMA-ORG-SCR_Rules_and_Procedures, URL: http://www.openmobilealliance.org/

2.2 Informative References

[OMADICT]	"Dictionary for OMA Specifications", Version 2.7, Open Mobile Alliance™, OMA-ORG-Dictionary-V2_7, 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

Device	see [OMADICT]
Factory Reset	The act to reset the device to its initial factory state.
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.
LAWMO Alert	LAWMO-specific alerts which convey the result of LAWMO Operations via the DM Generic Alert mechanism [DMPRO].
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.
Management Object	A data model for information which is a logical part of the interfaces exposed by DM components.
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.

3.3 Abbreviations

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

4. Introduction

The mobile device is becoming a pocketable private information database which contains various user data and enterprise-related data. There are several scenarios where a 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. A User may request to lock the device and/or wipe sensitive data from the device. If the device is returned, the user can also request to unlock the device.

- If the device was given or sold to another user, the owner may request to erase all sensitive 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 defines the Lock and Wipe Management Object and associated LAWMO Client and LAWMO Server-side behaviour for LAWMO Operations.

This specification is expected to meet all the requirements defined in [LAWMO-RD] and to comply with [LAWMO-AD].

4.1   Version 1.0

The OMA LAWMO Enabler v1.0 supports the following functionality:

- Lock the Device – partially or fully.

- Unlock the Device

- Wipe the data from the Device – personal or/and enterprise.

- List the available data that can be wiped from the Device.

- Configure the data to be wiped from the Device.

- Trigger remotely a Factory Reset of the Device.

- Report the result of LAWMO Operations to LAWMO Server

- Notify the user with the LAWMO Operation result when LAWMO Operation is executed

5. Lock and Wipe Management Object

5.1   Figure of the Management Object   (Informative)
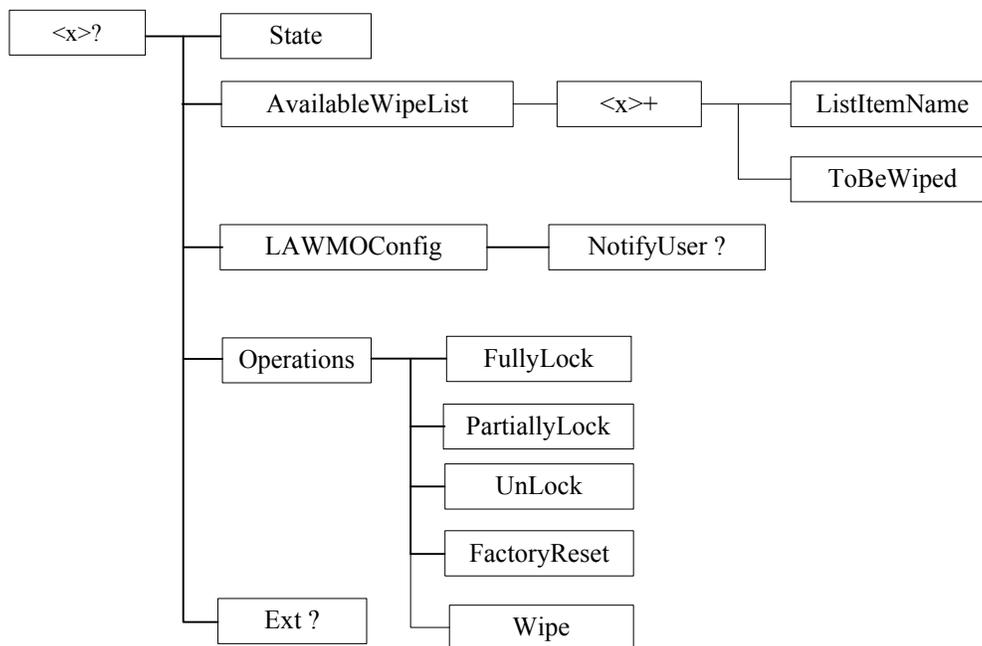
Figure 1: Lock and Wipe Management Object

5.2   Lock and Wipe Management Object Parameters

Lock and Wipe Management Object consists of following parameters:

<x>

Status	Occurrence	Format	Min. Access Types
Required	ZeroOrOne	node	Get

This interior node groups together the parameters of a LAWMO. The ancestor elements of this node define the position in the DM tree of this MO.

The type of this node MUST be the LAWMO MOI 'urn:oma:mo:oma-lawmo:1.0'.

<x>/ State

Status	Occurrence	Format	Min. Access Types
Required	One	int	Get

This leaf node specifies the state for the Device. The value of this node is one of the following:

Integer Value	State	Description
10	Fully Locked	The device is in Fully Locked state.
20	Partially Lock	The device is in Partially Locked state.
30	Unlocked	The device is in Unlocked state.

<x>/AvailableWipeList

Status	Occurrence	Format	Min. Access Types
Required	One	node	Get

This node is the placeholder for the lists of data that can be wiped from the Device and also contains the configuration for which data will be wiped from the Device. The LAWMO Server can get the list to determine what data are available on the Device. It can also set the configuration that which data will be wiped from the Device when Wipe Operation is executed.

<x>/ AvailableWipeList/<x>

Status	Occurrence	Format	Min. Access Types
Optional	OneOrMore	node	Get

This node is the placeholder for a list item.

<x>/ AvailableWipeList/<x>/ListItemName

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

This node specifies a specific category of data that can be wiped from the Device.

<x>/ AvailableWipeList/<x>/ToBeWiped

Status	Occurrence	Format	Min. Access Types
Required	One	bool	Get, Replace

This node specifies whether the specific category of data will be wiped when Wipe Operation is executed. If the value is "true", the data will be wiped when Wipe Operation is executed. If the value is "false", the data will not be wiped when Wipe Operation is executed.

<x>/LAWMOConfig

Status	Occurrence	Format	Min. Access Types
Required	One	node	Get

This interior node groups together the configuration parameters for the LAWMO.

<x>/LAWMOConfig/NotifyUser

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	bool	Get

This leaf node specifies whether the user is notified with the LAWMO Operation result when FullyLock/PartiallyLock/Unlock/Wipe/FactoryReset Primitive is executed. If the node is not present or the value is 'false', the user SHALL NOT be notified about the result of the operation. If the node is present and the value is 'true', the user SHALL be notified about the result of the operation.

<x>/Operations

Status	Occurrence	Format	Min. Access Types
Required	One	node	Get

This node is a parent node for Operations that can be executed for LAWMO in the device.

<x>/Operations/FullyLock

Status	Occurrence	Format	Min. Access Types
Required	One	null	Exec

This node is used with Exec command to Fully Lock the device.

<x>/Operations/PartiallyLock

Status	Occurrence	Format	Min. Access Types
Required	One	null	Exec

This node is used with Exec command to Partially Lock the device.

<x>/Operations/UnLock

Status	Occurrence	Format	Min. Access Types
Required	One	null	Exec

This node is used with Exec command to re-enable all device functionalities previously locked by Lock Device operation.

<x>/Operations/FactoryReset

Status	Occurrence	Format	Min. Access Types
Required	One	null	Exec

This node is used with Exec command to reset the device to its initial factory state.

<x>/Operations/Wipe

Status	Occurrence	Format	Min. Access Types
Optional	One	null	Get, Exec

This node is used with Exec command to permanently erase data from the device. For those data whose "ToBeWiped" value is "true" will be wiped from the Device when Wipe Operation is executed.

<x>/Ext

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

This node designates a branch of the <x> sub-tree into which vendor extensions MAY be added, permanently or dynamically. Ext sub tree provides flexible points of extension for vendor-specific parameters. However, vendor extensions MUST NOT be defined outside of Ext sub-tree.

6. Behavior associated with the Management Object

6.1 Exec command semantics

In the LAWMO tree the Exec command is only allowed to target Primitives under Operations nodes. After an Exec command to one of the Primitives under Operations node, the LAWMO Client MUST send response to the LAWMO Server in either of the following ways:

1. Asynchronously if the Exec command is acceptable and will be executed asynchronously.

   • The LAWMO Client MUST return status code 202 ("Accepted for processing") for Exec command, as defined in [DMREPRO]

   • Upon completion of the asynchronous operation, the LAWMO Client MUST send an alert back to the server by using the Generic Alert defined in [DMPRO].

2. Synchronously If the Exec command is acceptable and executed synchronously.

   • If the Exec command is performed, the LAWMO Client MUST return appropriate LAWMO Result Code in <Status>/<Data> element for Exec command as defined in section 6.4.

Before receiving the Exec command, the following Pre-Condition needs to be satisfied:

   • At least the following nodes need to be set with an appropriate value:

      o <X>/Operations/… (at least one Operation sub-node for the Primitive to be executed)

The Exec command targeting a child node of an Operations node starts the execution of a chosen Primitive. For example:

```
<Exec>
    <CmdID>3</CmdID>
    <Item>
        <Target>
            <LocURI>./LW/Operations/FullyLock</LocURI>
        </Target>
    </Item>
</Exec>
```

If the Exec command is targeting FullyLock/PartiallyLock Primitive, the LAWMO Client MUST Fully/Partially Lock the device.

If the Exec command is targeting Unlock Primitive, the LAWMO Client MUST re-enable all device functionalities previously locked by Lock Operation.

If the Exec command is targeting Factory Reset Primitive, the LAWMO Client MUST reset the device to its initial factory state. In this case only the status code for Exec command will be returned to LAWMO Server within the same DM session. It is not possible to report result back.

There are two purposes for the <x>/AvailableWipeList branch:

   • The LAWMO Client uses it to expose the list of data supported on the Device to LAWMO Server and receive configuration from LAWMO Server at the same time. In this case, the LAWMO Client MUST create the <x> and its child nodes under <x>/AvailableWipeList node for each supported list in advance. Then the LAWMO Server can

obtain the list using <Get> command and set the value of "ToBeWiped" node to specify whether a specific list will be removed when Wipe Primitive is executed.

- The LAWMO Server uses it to configure the list of data supported on the Device to LAWMO Server only.In this case, the LAWMO Server MUST create the <x> and its child nodes under <x>/AvailableWipeList node for each list and set the value of "ToBeWiped" node to specify whether a specific list will be removed when Wipe Primitive is executed.

6.2   Synchronous Result Reporting

If the Exec command is executed synchronously, the LAWMO Client MUST send result for Exec command as described below:

- The <Data> element MUST contain a valid LAWMO Result Code defined in section **Error! Reference source not found.**4

- The URI of the Primitive node on which the Exec command was invoked – Used to identify the source MUST be included in the <Source>/<LocURI> of <Status>/<Item> element.

The following is the example message:
```
<Status>
  <MsgRef>1</MsgRef>
  <CmdRef>2</CmdRef>
  <Cmd>Exec</Cmd>
  <Data>1200</Data>        <!--LAWMO Result status Code -->
  <Item>
    <Source>
      <LocURI>./LAWMO/Operations/Lock</LocURI>
    </Source>
  </Item>
</Status>
```

6.3   Asynchronous Result Reporting Using Generic Alert

If the Exec command is executed asynchronously, the LAWMO Client MUST send a LAWMO Alert to the LAWMO Server about the result of the operation via a Generic Alert message [DMPRO]. The alert message includes the following data:

- The URI of the Primitive node on which the Exec command was invoked MUST be included in the <Source>/<LocURI> element

- An integer Result Code – Used to report result of the operation. The appropriate LAWMO Result Code defined in section 6.4 MUST be included in an Item/Data element.

- The alert type MUST be included in <Meta>/<Type> element.

LAWMO Alerts that are reporting an error or failure condition SHOULD report an importance level defined in [DMPRO] higher than Informational in the Mark field of the Meta information. The following is the example message:
```
<Alert>
  <CmdID>2</CmdID>
  <Data>1226</Data>        <!-- Alert Code for Generic Alert -->
  <Item>
    <Source>
      <LocURI>./LAWMO/Operations/FullyLock</LocURI>
    </Source>
    <Meta>
      <Type xmlns="syncml:metinf"> urn:oma:mo:oma-lawmo:operation:1.0</Type>
```

```
        <Format xmlns="syncml:metinf">text/plain</Format>
        <Mark xmlns="syncml:metinf">warning</Mark>
      </Meta>
      <Data>1401</Data>     <!-- LAWMO Result Code -->
    </Item>
  </Alert>
```

6.4   LAWMO Result Code

The LAWMO Result Code MUST be sent as an integer value in <Item>/<Data> element of the LAWMO Alert message or in response to an Exec command in case of synchronous execution. The Result Code MUST be one of the values defined below:

Result Code	Result Message	Informative Description of Status Code Usage
1200	Operation Succeeded	Operation is completed successfully
1400	Client Error	Client error – based on User or Device behaviour
1401	User cancelled	User chose not to accept the operation when prompted
1402	Fully Lock Device Failed	The Fully Lock Device Operation failed
1403	Partially Lock Device Failed	The Partially Lock Device Operation failed
1404	UnLock Device Failed	The UnLock Device Operation failed
1405	Wipe Device's Data Failed	The Wipe Device's Data Operation failed
1450-1499	Client Error – Vendor Specific	Client Error encountered for Operation with Vendor Specified Result Code

6.5   Alert Types for LAWMO

The following alert types MUST be used in a Generic Alert [DMPRO] message originating from a Lock And Wipe Management Object. The alert type is used to identify the operation that was performed on the Device.

urn:oma:mo:oma-lawmo:operation:1.0: This alert type is used to claim that the alert message conveys the result of LAWMO Operation(s) that was performed on the device.

6.6   User Interaction Commands

This section deals with the LAWMO Client behavior associated with user interactions commands sent to the Device.

6.6.1 Requesting User Confirmation

The LAWMO Server MAY request user confirmation before performing LAWMO operations within the Device. However it is important to ensure that the LAWMO Client supports the ability to handle the user confirmation request.

In particular the LAWMO Client:

- SHOULD support DISPLAY Alert as described in [DMPRO].

- SHOULD support CONFIRM OR REJECT Alert as described in [DMPRO].

- SHOULD support USER INPUT Alert as described in [DMPRO].

- SHOULD support USER CHOICE Alert as described in [DMPRO].

The LAWMO Server SHOULD support all these Alerts.

Appendix A.   Change History   (Informative)

A.1   Approved Version History

Reference	Date	Description
n/a	n/a	No prior version

A.2   Draft/Candidate Version 1.0 History

Document Identifier	Date	Sections	Description
Draft Versions OMA-TS-LAWMO-V1_0	28 Mar 2008	All	Incorporates agreed CR: OMA-DM-LAWMO-2007-0026R02
	08 May 2008	5	Incorporates agreed CR: OMA-DM-LAWMO-2008-0005R02
	01 Jun 2008	5 Appendix B	Incorporates agreed CRS: OMA-DM-LAWMO-2008-0010 OMA-DM-LAWMO-2008-0009R02
	08 Jul 2008	5.1,5.2	Incorporates agreed CR: OMA-DM-LAWMO-2008-0010R01
	14 Oct 2008	2.1,6.1 6.2,6.3,6.4,6.5 6.6	Incorporates agreed CRs: OMA-DM-LAWMO-2008-0018R03 OMA-DM-LAWMO-2008-0019R01 OMA-DM-LAWMO-2008-0020
	15 Oct 2008	All	Editorial clean up
	22 Oct 2008	4.1	Incorporates agreed CR: OMA-DM-LAWMO-2008-0024R02
	11 Nov 2008	5.2,6.3,6.4,6.5	Incorporates agreed CR: OMA-DM-LAWMO-2008-0025
	12 Jan 2009	5.2	Incorporated agreed CR: OMA-DM-LAWMO-2009-0001
Candidate Versions OMA-TS-LAWMO-V1_0	27 Jan 2009	n/a	Status changed to Candidate by TP TP ref# OMA-TP-2009-0010- INP_LAWMO_V1_0_ERP_for_Candidate_Approval

Appendix B.   Static Conformance Requirements   (Normative)

The notation used in this appendix is specified in [SCRRULES].

B.1   SCR for LAWMO Tree Structure

Item	Function	Reference	Requirement
LAWMO-T-001-M	Use of appropriate Management Object identifier for the LAWMO node	Section 5.2	
LAWMO-T-002-M	Support for Required nodes under root node	Section 5.2	
LAWMO-T-003-O	Support for Optional nodes	Section 5.2	
LAWMO-T-004-M	Support for Required nodes under an Optional node if the Optional node is supported	Section 5.2	

B.2   SCR for LAWMO Client

Item	Function	Reference	Requirement
LAWMO-C-001-M	Support for FullyLock Operation	Section 6.1	
LAWMO-C-002-M	Support for PartiallyLock Operation	Section 6.1	
LAWMO-C-003-M	Support for UnLock Operation	Section 6.1	
LAWMO-C-004-M	Support for FactoryReset Operation	Section 6.1	
LAWMO-C-005-O	Support for Wipe Operation	Section 6.1	
LAWMO-C-006-M	Support for listing available data which can be wiped	Section 6.1	
LAWMO-C-007-M	Support for creation of <x>/ AvailableWipeList/<x> and sub-nodes to list the available data which can be wiped from the Device	Section 6.1	
LAWMO-C-008-M	Support for modification of the list of data to be wiped	Section 6.1	
LAWMO-C-009-M	Support for modification of <x>/ AvailableWipeList/<x>/ ListItemName	Section 6.1	
LAWMO-C-010-M	Support for modification of <x>/ AvailableWipeList/<x>/ ToBeWiped	Section 6.1	

B.3   SCR for LAWMO Server

Item	Function	Reference	Requirement
LAWMO-S-001-M	Support for the Lock and Wipe Management Object	Section 6.1	
LAWMO-S-002-M	Support for obtain the list of the data to be wiped from the Device	Section 6.1	
LAWMO-S-003-M	Support for modification on <x>/AvailableWipeList to specify which data will be wiped from the Device	Section 6.1	