IOTA Device Management for cdma2000 Systems

Stage 1 Requirements

COPYRIGHT NOTICE
3GPP2 and its Organizational Partners claim copyright in this document and individual Organizational Partners may copyright and issue documents or standards publications in individual Organizational Partner’s name based on this document. Requests for reproduction of this document should be directed to the 3GPP2 Secretariat at secretariat@3gpp2.org. Requests to reproduce individual Organizational Partner’s documents should be directed to that Organizational Partner. See www.3gpp2.org for more information.
EDITOR
Paul Oommen, Nokia
+1-972-894-4876
paul.oommen@nokia.com

Soma Sanhiveeran, Openwave Systems
+1-650-480-6723
soma.santhiveeran@openwave.com

REVISION HISTORY

<table>
<thead>
<tr>
<th>Rev. number</th>
<th>Content changes</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Initial Publication</td>
<td>22 April 2004</td>
</tr>
</tbody>
</table>
Table of Contents

1 INTRODUCTION ................................................................. 4
2 REFERENCES ................................................................. 4
3 DEFINITIONS AND ABBREVIATIONS ................................. 4
4 Support for OMA (SyncML) Device Management in Addition to Current MMC Commands ...................................................... 6
  4.1 Overview of the Proposal ................................................ 6
  4.2 Advantages of DM ......................................................... 7
  4.3 DM Protocol ................................................................. 7
  4.4 Management Tree ........................................................ 7
  4.5 Device Description Framework ...................................... 8
  4.6 Bootstrap Mechanism ..................................................... 8
  4.7 SyncML DM MIME Types .............................................. 8
  4.8 SyncML DM Commands ................................................ 8
  4.9 Notification Message .................................................... 8
  4.10 Access Control and Security ......................................... 8
  4.11 Transport Bindings ....................................................... 9
  4.12 Requirements ............................................................ 9
5 Firmware Over-the-Air Upgrades ........................................ 10
  5.1 Overview of the Proposal ................................................ 10
  5.2 Reference Architecture ................................................. 11
  5.3 Requirements ............................................................ 13
List of Tables

1
2
3
List of Figures
1 INTRODUCTION

This document specifies the stage-1 Mobile Station (MS) and Operator requirements for the next release of IP Based Over-the-Air Handset Configuration standard [1].

Current release of IOTA standard allows Service Providers to remotely manage handset configuration. It provides a standardized method to remotely read and write to the Mobile Station (MS) memory in a secure manner. This method may be extended beyond handset configuration management. This document specifies requirements to support the following:

- Support for OMA (SyncML) Device Management in Addition to Current MMC Commands
- Firmware Over-the-Air (FOTA) Upgrades

2 REFERENCES


3 DEFINITIONS AND ABBREVIATIONS

Abbreviations
Definitions

Bootstrap The process by which a device or mobile station in un-provisioned state is transformed to a state where it can establish a management session with a trusted Management Server.

DDF The Device Description Framework (DDF) document is an XML document which describes the properties of management objects in the device.

Device Management The Management of configuration and other managed objects in the devices by authorized management entities. Device management includes initial provisioning and continuous management of information in devices. It also allows the processing of alarms originating from the devices.

DM Client The DM Client processes the DM messages and commands, performs authorization, and handles access to the management tree.

DM Server The IOTA DM Server is the entity in the network managing the services and applications in a MS. It issues DM commands and correctly interprets responses from the DM client.

Firmware Firmware is defined as all software that is non-downloadable i.e. operating systems, device drivers, DSP or other coprocessor codes, call processing stack, user interface and other applications.
S.R0101-0 v1.0 IOTA-DM Stage 1

Firmware Installer  MS resident software that installs the firmware in the MS storage after over-the-air download.

Firmware Over-the-Air  A process of delivering firmware to the MS over-the-air.

IOTA DM  IP Based over-the-air device management is the process of managing mobile stations or mobile devices over-the-air using IP based protocols.

Management Objects  Management objects consist of parameters, software objects, configuration data blocks etc., which are associated with applications and services. Management Objects are organized as logically related groups (or subtrees) in a hierarchical tree.

Mobile Device  Same as Mobile Station.

Management Server  Same as DM Server.

4  Support for OMA (SyncML) Device Management in Addition to Current MMC Commands

4.1  Overview of the Proposal

As the functionality of mobile devices grows at an increasing rate, configuring and maintaining the services and features on the devices becomes a complex and time-consuming task. For instance, CDMA service provisioning and enabling WAP, and data connectivity requires configuration of multiple settings. Even with limited features of today, many customers do not know how to configure their phones. Operators should ensure that phone configuration is quick and easy for the customer. Another use case is over-the-air (OTA) provisioning and management of new services to mobile devices. Advanced mobile services such as browsing, multimedia messaging, mobile e-mail, and calendar synchronization requires accurate mobile phone settings. The process of remotely managing a plurality of device settings and applications is called Device Management.

Device Management will help the widespread adoption of mobile services, as it provides a mechanism for the users to easily subscribe to new services. For the operators this enables a fast and easy way to introduce new services and manage provisioned services, by dynamically adjusting to changes and ensuring a certain level of quality of service.

The SyncML Initiative has developed an open standard for Device Management called SyncML Device Management (DM). SyncML DM provides an integrated and extensible framework for OTA management needs of 3G mobile devices and beyond. The standard includes the protocol specification and the framework for mobile device management. The release 1.1.1 of the standard is already available. The standard is optimized for OTA management - one of the foundations in SyncML Initiative has been to take into account the resource and bandwidth limitations of mobile devices. On November 1, 2002, the SyncML Initiative was consolidated with the Open Mobile Alliance (OMA), which will continue to develop technologies for device management. OMA DM 1.1.2 specifications based on SyncML DM was published recently.

OMA DM, as a mechanism, is very versatile and can be used to manage different types of data objects. Some of the data objects are simple numeric or textual parameters, while others are binary. Numeric objects may include connectivity parameters, such as access point addresses and proxy configurations. Binary objects may be security keys, blocks of data or software modules.
The protocol leverages WAP 2.0 bootstrap for initial provisioning and the set of OMA DM protocol specifications for continuous management after the initial provisioning.

The purpose of this document is to describe high-level requirements for OTA Management of CDMA devices, using OMA DM protocol. OMA DM can be adopted to meet CDMA IP based over-the-air management (IOTA) requirements; hence bringing interoperability to IOTA management of CDMA Mobile Stations (MS).

### 4.2 Advantages of DM

The following are some of the advantages of using OMA DM.

- Beyond configuration management, supports other management functions, such as diagnostics, large data handling etc.
- Extensible framework – allows support for new management features with minimum or no changes to the messaging protocol.
- Open solution - uses SyncML DM/ OMA DM command set and representation.
- Supports provisioning of new services
- Support management of parameters after initial provisioning
- XML based command set Support diagnostics - remote reading of data.
- Supports large data handling.
- Several levels of securitySupports management over several bearers – HTTP, WAP, OBEX (Bluetooth) and SMS

### 4.3 DM Protocol

The OMA DM Protocol defines a management framework and a set of messages exchanged between the mobile device and an entity in the network called the management server. This section describes briefly the core components of OMA DM.

### 4.4 Management Tree

OTA Management of services or applications in the DM framework requires accessing corresponding objects in the mobile device in a secure way. The management objects are logically grouped in a tree like structure called the management tree. The runtime tree is implemented in the device. Thus, the management of a service or application in the DM framework requires accessing locations in the management tree corresponding to the service or application.

The management tree is structured on the basis of services, and applications. Each location or node in the management tree is referenced using the URI scheme as described in the Tree and Descriptions specification [9].

Using the Device Description Framework (DDF) of the management tree, described in section 3.2, and the Tree exchange mechanism [9], the management server knows the URI of the location to be referenced for a specific management action.

In the management tree, CDMA objects would be under a specific subtree. Similarly application objects form other subtrees of the management tree.
4.5 Device Description Framework

The management objects implemented in the runtime tree are made known to the management server using the DDF (Device Description Framework) to describe these objects. The DDF description is an XML document, which is updated to the management server over-the-air or over the network in an offline manner. The Device Description DTD specified in [9] is used to describe management objects.

The DDF description gives the properties, such as type, format, description etc of each object, and their relative location in the runtime management tree. The server learns about the management objects and how to manage the objects from the DDF description.

The DDF framework provides a flexible mechanism, allowing management of customized and new features in the device.

Features common to a class of mobile devices can be standardized for interoperability. The management tree for CDMA objects can be represented using the DDF DTD.

4.6 Bootstrap Mechanism

The OMA DM uses the WAP bootstrap for initial provisioning. The bootstrap mechanism is defined in the OMA DM Bootstrap specification [7].

4.7 SyncML DM MIME Types

In OMA DM, set of messages, exchanged between the DM client and the management server, are conceptually combined into a package. In most situations a package corresponds to a single message, but when large objects are involved in the transfer, each package is sent over multiple DM messages. A DM message is a well-formed XML document with header and body. The XML specification for OMA DM is described in the protocol specifications.

4.8 SyncML DM Commands

OMA DM protocol allows commands to be executed on a node in the management tree, resulting in a specific management action. Management action can be create, read, update, delete etc. OMA DM Management commands are used to represent the management actions and associated data elements that are transferred between the DM client and the management server.

The OMA DM commands are in XML form. See the OMA SyncML Representation Protocol, Device Management Usage [6].

4.9 Notification Message

The DM notification message causes the client to initiate a connection to the management server and begin a management session. The notification is a signed message, which the client can authenticate. There are several fields in the notification message, for example there is a field for specifying user interaction when the client receives the notification.

Notification message can also originate within the device, thus triggering the establishment of a session, for example when a timer expires.

The format and security mechanism for the OMA DM notification message are described in the Notification Initiated Session specification [10].

4.10 Access Control and Security

The OMA DM framework provides security at several levels:

- Access control mechanism to control the access to management objects
• Protocol security mechanism to ensure confidentiality of data
• Ensuring the integrity of the data
• Authentication between the mobile device and the management server.

The access control mechanism defined in the OMA DM standards controls access to parameters and management objects in the mobile device. Only the management server with appropriate rights can modify the management objects. Since the management objects are organized as a tree, it is possible to define access control list (ACL) to the node and leaf objects in the management tree to describe who has the access to e.g. modify or delete an object in the management tree. The ACL applies on a per-command basis to any node or leaf in the management tree.

Confidentiality ensures that only the intended recipient can interpret the contents of a management message. Authentication is achieved through the exchange of credentials in a secure way. Either the client or the server may send credentials to each other or challenge the other to send them.

Integrity of management data transferred between the device and the server is important, since deliberate or accidental corruption data can occur. Integrity of SyncML DM data is achieved using a hashed message authentication code used on each message.

The OMA DM security mechanism is defined in the Security specification [11].

4.11 Transport Bindings

The DM framework allows management over different protocols like HTTP, WSP, OBEX (Bluetooth, IrDA), SMS, etc. HTTP bindings are defined in the OMA SyncML HTTP bindings specification [3]. WSP and OBEX bindings are specified in [12] and [4] respectively.

4.12 Requirements

This section describes the requirements for adopting OMA DM for IP based over-the-air device management (IOTA DM) in cdma2000® systems.

4.12.1 General Requirements

IOTA-DM-0: The system shall be able to support one or more IOTA-DM servers which SHALL be able to handle SyncML DM messages as defined in [5].

IOTA-DM-1: The IOTA-DM Server SHALL manage the parameters and objects in the MS assigned to it.

IOTA-DM-2: It SHALL be possible to represent all CDMA related parameters and objects managed by an IOTA-DM server using the SyncML DM management tree mechanism defined in SyncML DM Tree and Descriptions specification [9].

IOTA-DM-3: The MS SHALL be able to handle SyncML DM messages.

IOTA-DM-4: The IOTA-DM Management Server SHALL be able to initiate an IOTA-DM Management Operation.

---

1 cdma2000® is the trademark for the technical nomenclature for certain specifications and standards of the Organizational Partners (OPs) of 3GPP2. Geographically (and as of the date of publication), cdma2000® is a registered trademark of the Telecommunications Industry Association (TIA-USA) in the United States.
IOTA-DM-5: The MS SHALL be able to initiate an IOTA-DM Management operation. The MS sends its capability information at the beginning of a management session so that the IOTA DM Server can tailor the contents and operations to suite the capabilities of the MS.

IOTA-DM-6: The IOTA DM system SHALL support the provision as defined in C.S0016-B or later revisions.


The IOTA-DM system is designed to manage parameters that reside in the MS, including their modification, deletion, or creation, using the SyncML DM protocol mechanism. The IOTA-DM server introducing new parameters MAY NOT be same as the IOTA-DM server managing these parameters.

IOTA-DM-8: The IOTA-DM system SHALL be able to support modifications, deletions, and additions of parameters in the MS, e.g., as a result of the user subscribing to a new service offered by an Operator or Service Provider.

4.12.2 Security Requirements


IOTA-DM-SEC-2: An authorized IOTA DM Server SHALL be able to access and manage a specific management object in the MS.

IOTA-DM-SEC-3: It SHALL be possible for the IOTA DM to learn enough details about parameters and objects in the MS so as to successfully manage these parameters and objects.

5 Firmware Over-the-Air Upgrades

5.1 Overview of the Proposal

Firmware Over-the-Air (FOTA) is a method of updating the MS firmware over-the-air in order to fix or enhance the firmware. Firmware is defined as all software that is non-downloadable i.e. operating systems, device drivers, DSP or other coprocessor codes, call processing stack, user interface and other applications.

The FOTA feature is intended to provide the following benefits in the event that firmware on mobile stations needs to be updated:

- Save costs to the mobile station vendors, mobile carriers and the end users.
- Quick deployment of new services
- Increase revenue from increased use of impacted services
- Improve and enhance user experience

FOTA technology enables Service Providers and MS vendors to save such costs by upgrading the firmware over-the-air, without requiring the MSs be brought back to the service centers for firmware update.

Proposed scope of the FOTA standard includes:

- Standardize over-the-air delivery of firmware. This will enable carriers to distribute firmware in a multi-vendor environment.
• Backing up the mobile station or user specific data prior to upgrades
• Firmware update package validation
• Recovery of mobile station in case of errors or exceptions in order to restore operations
• Security mechanism
• End-user interactions

5.2 Reference Architecture

Figure below illustrates entities in the Firmware OTA architecture sequence.
**5.2.1 DM Protocol**

DM protocols such as OMA DM [5] and IOTA [1] enable secure and reliable provisioning of mobile stations with data/voice/application settings, read mobile station settings and diagnostics information and download of large objects such as screen savers, software modules, etc.

For Firmware OTA, IOTA Protocol may be used for:

- User interaction and confirmation process before firmware upgrades
- Mobile station diagnostics for identifying appropriate firmware
- Reliable over-the-air delivery of firmware packages
- Security
- Integrity of the firmware

**5.2.2 Firmware OTA Server**

Server side implementation of firmware security & management, target mobile station identification, scheduling and over-the-air delivery of Firmware using DM protocol.

**5.2.3 DM Client**

This entity is mobile station side implementation of DM protocol. Manages user confirmation, security, download, status reporting, etc.

**5.2.4 Firmware Installer**

Firmware Installer is an embedded application in the mobile station, that installs the software and updates the status of the install.
5.3 Requirements

FOTA-1: 3GPP2 to adopt Firmware OTA specifications as developed by OMA with following additional requirements.

FOTA-2: While changing the firmware or any associated configuration or application, FOTA protocol shall comply with Service Programming Lock security as specified in IS-683 protocol [2] section 3.3.6.

FOTA-3: While changing the firmware or any associated configuration or application, FOTA protocol shall comply with Subscriber Parameter Administration Security Management procedure as specified in IS-683 protocol [2] section 3.3.7.