Device Management Requirements

Candidate Version 1.2 – 07 Jun 2005

Open Mobile Alliance

OMA-RD-DM-V1_2-20050607-C

Contents

1. Scope (Informative)

The scope of this document is a requirements description for Device Management (for the definition of Device see section 3.2). This document describes a set of functional requirements (partly on an abstract level) for the management of a Device's changeable parameters, as seen from the Management Authority's points of view.

This document contains information applicable to Network Operators, terminal and network manufacturers, enterprises, independent software vendors, content providers, and service providers.

This document covers the requirements needed to supply the core Device Management service. Additional, related functionality not described here may involve requirements outside the scope of this document. This additional functionality shall not interfere with the core service described in this document.

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

None.

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].

3.2 Definitions

Archiving of applications	The process initiated by the Device Management System or the Device itself that, together with DRM policies, allows applications to be moved to an offline or online storage medium. These remotely stored applications may run on request by the User, and be transparently restored to the device or the User may take explicit action to restore the application. The process includes all actions required to temporarily replace applications on demand.
Backup and Restore	The secure and reliable offline storage of personal information, parameters and applications that can be used at a later date to restore the device. The backup copy can be stored locally, remotely or as a combination of both.
Bootstrap Provisioning	The process of installing parameters and/or applications on a Device to establish a given service for the first time, or for the purposes of resetting a Device to initial settings.
Content Provider	An entity that provides data which forms the basis of a service.
Continuous Provisioning	The process where a Device is updated with new data, parameters, or application upgrades to replace pre-existing versions.
Device	In this context, a Device is a voice and/or data terminal that uses a Wireless Bearer for data transfer. Device types may include (but are not limited to): mobile phones (GSM, CDMA, 3GSM, etc.), data-only terminals, PDAs, laptop computers, PCMCIA cards for data communication, unattended data-only Devices (e.g., vending machines), and smart cards if associated with these Devices. If within a particular context an associated smart card should not be regarded as part of a Device this is marked explicitly.
Device Discovery	A mechanism to allow devices to identify each other for the purposes of performing some data exchange.
Device Query	The process of polling a mobile Device for a specific piece of information.
Device Reporting	The process whereby a Device sends specific information to a management server in the network. This can occur as a response to a Device Query (pull) or it can occur autonomously in response to a state change in the Device (push). The information that is sent may either be parameters stored in data fields in the Device, information about the configuration of the Device, information about the capabilities of the Device, or data that has been collected, stored, and assembled for later forwarding (e.g., performance metrics).
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
Device Management System	A background system capable to interact with a (set of) Device(s) for the purpose of Device Management.
Enterprise	A business with deployment and Management Authority for WLAN Bearers, Local Wired Bearers, computers, Devices, software, and employees.
Enterprise Device Management Server	Part of the Device Management System that is under administration of an Enterprise Management Authority.
Friendly Name	A human readable string which is created by the user.

Local Wired Bearers	Serial, USB, Ethernet
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
Management Object	A logical element that can contain or represent and manage configurable data and software within a Device. The data and/or software includes but is not limited to • Parameters such as connectivity address, User preferences, proxy settings, User Identity, etc. • Software such as applications, applets, drivers, modules, firmware and their updates. A management object may represent the complete device configuration or a portion of a device configuration. There may be multiple Management Objects on a Device with a pre-specified relationship between them. Each Management Object will support the following operations. • Add/Install – insert new elements into a Management Object. • Replace/Update – modify existing and/or insert new elements into a Management Object. • Delete/Uninstall – remove existing elements from a Management Object. • Query/Enumerate – List all or part of a Management Object.
Network Bearers	Wireless Bearer and Local Wired Bearers
Network Device Management Server	Part of the Device Management System that is under administration of a Network Management Authority
Network Operator	An entity that is licensed and allocated frequency to operate a public mobile wireless telecommunications network for the purpose of providing publicly available commercial services.
Network Unique Name	A full qualified domain name.
Parameters	In this context, parameters are service-related data elements that are stored in the Device and can be manipulated (i.e., changed, added, or deleted) over Network Bearers. For example, system parameters can be used to establish or maintain a bearer session, and application parameters can be used to specify the profile of a particular service, or some parameters may be related with performance characteristics.
PC Agent	Application running on a PC or PC-like device in User's proximity, not the Device itself, that facilitates Device Management functionality, and which MAY involve a logical association with a DMS.
Policy	The set of Service configuration settings and installed applications which are mandated by the Management Authority.
Provisioning Mechanisms	Network bearers, smart card, and Media card
Regulatory Agency	A governmental agency (typically) that regulates the use and/or sale of Devices. For example the FCC in the USA.
Regulatory Agency Label	A digital signature or digital certificate that securely identifies a piece of software and/or data as being approved by a particular Regulatory Agency.
Removable Media Card	A removable card for the purpose of storing and/or exchanging mass data as e.g., music, video.
Radio Software	The software within a Device that is coupled with the radio hardware to derive the overall "radio" functionality. Radio software is not to be confused with User applications and content, but has certain commonality for functional requirements for

	device management.
Service Provider	An entity that provides and administers a service to a Subscriber and/or User. The Network Operator is often a Service Provider.
Software Originator	The entity that creates, directly or through a third party, software and/or data targeted for use in a Device, Platform or Base Station. In the event that the software and/or data is controlled by a Regulatory Agency, the Software Originator is responsible for obtaining any Regulatory Agency license and Label.
Subscriber	The individual or organisation that is paying for service.
User	The individual who is in possession of and operates the Device.
Wireless Bearer	WAN Network Bearers (e.g. GPRS, GSM Data, CDMA), WLAN Bearers (802.1x), Local Wireless Network Bearers (e.g. Bluetooth, IR)

3.3 Abbreviations

APN	Access Point Name
CDMA	Code Division Multiple Access
CPU	Central Processing Unit
DHCP	Dynamic Host Configuration Protocol
DM	Device Management
DMS	Device Management Server
DRM	Digital Rights Management
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communication
HTTP	HyperText Transfer Protocol
HTTPS	HTTP Secure
HW	Hardware
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IR	InfraRed
MMS	Multimedia Messaging Service
OTA	Over The Air
PC	Personal Computer
PCMCIA	Personal Computer Memory Card International Association
PDA	Personal Digital Assistant
RAN	Radio Access Network
SSDP	Simple Service Discovery Protocol
SW	Software

UC	Use Case
UI	User Interface
USB	Universal Serial Bus
WAN	Wide Area Network
WAP	Wireless Application Protocol
WLAN	Wireless Local Access Network
XML	Extensible Markup Language

4. Introduction (Informative)

As differentiation between Device types grows and Device functionality broadens, the difficulty in provisioning these Devices with service-specific parameters and software increases.

In addition, Device administration servers and systems face an increasingly difficult task in keeping track of the status and configuration of the Devices they manage.

A Device is any User terminal which is primarily used in mobile scenarios. They may be equipped with a smart card (where applicable), which is under the sphere of influence of a specific Management Authority. The scope of Device Management includes both the Device itself and smart card. A Device could be, for example, a WAP- or MMS-capable handheld, a smart phone, PDA, or a notebook computer. PDAs, handhelds, smart phones and notebooks can be attached to a wireless modem via hardware integration, cable, IR, and Bluetooth.

Each of the requirements may limit the target Device to the specific subset of capabilities of a Device considering the fact that each of the Devices has different constraints from each other due mainly to capabilities in particular for mobile phone handset. When such requirements or use cases are specified, the capabilities of Device(s) that each requirement or use case is targeting should clearly be described in this specification. *Devices which are under the control of a Management Authority should support transparent forced setting of all parameters covered by the Management Authority Control.*

The actors involved in Device Management include Management Authorities (including Network Operators, Enterprise Managers, Service Providers), Device Management Systems, Subscribers and Users.

The objective of this document is to develop a standardized approach to Device Management.

This document defines the requirements for Device Management as a framework to enable such functionality as:

- Bootstrap provisioning of configuration data to a Device
- Remote maintenance of configuration data of a Device
- Reporting of Device capabilities and configuration to a Management Authority
- Downloading/Updating and Retrieving status of Management Authority's software, or operating system components/firmware to a Device
- Device diagnostics, performance reporting, and fault management
- Secure transmission of exchanged data to and from the Device
- Access rights management
- Cost-effective administration of configuration and software data on the Management Authority's side
- Easy handling or virtual invisibility of diagnostic/update actions on the Subscriber's side
- Device conformance to policy established by the OMA

- Segregation of management ownership between one ore more entities. For example, the operator and enterprise can share management responsibilities

- Device conformance to Policy established by the Management Authority(s)

- Transfer of Management Authority. For example, the management rights are partially or fully transferred between Management Authorities

- Integration of new software (downloaded or otherwise) into the existing Device Management framework

- Management, download and installation of software at all levels above hardware to the Device in the form of complete code, patching and deltas as applicable in communication with the Device Management Server via wired and unwired mechanisms

5. Description of Use Cases (Informative)

The use cases are classified into the following categories:

- **Provisioning**
- **Configuration Maintenance/Management**
- **Software management**
- **Fault Detection, Query and Reporting**
- **Non-application Software Download**

In the sub-clauses that follow describing the use cases, further flows may be required where they are required to meet functional, security, usability or business needs. For the sake of clarity these have been omitted.

5.1 Provisioning

5.1.1 New Device Purchase

A new Device (e.g., a handset or PDA) is purchased by a network Subscriber in an authorised retail store and provisioned with parameters. The Device is powered on and store personnel at the retail outlet use a Device Management system to provision the Device with network-specific parameters (e.g. gateway addresses, etc.) that enable delivery of subscribed services, as well as User-specific preferences (e.g. message headers, etc.) as defined by the User. The Device provisioning can be done via a local or public transport mechanism, e.g. IR, Bluetooth, local, or non-local, wired, or wireless network. The new Device and all accompanying services are fully operational when the Subscriber leaves the store.

As a minimum, the retail store shall be able to provision the parameters described in section 7.

5.1.1.1 Actors and Data Authority

- User/Subscriber. The User/Subscriber is authorised to define and change the User Preference parameters.
- Network Operator. The Network Operator is authorised to define and change the Network Parameters.
- Authorised agent of the Network Operator

5.1.1.2 Pre-Conditions

- User is the Subscriber and has purchased a service contract with the Network Operator.
- Authorised agent (e.g. a retail outlet) has a Device Management system for provisioning Devices.
- Device is capable of interfacing with the Device Management system.

5.1.1.3 Post-Conditions

- Device is provisioned with parameters necessary to obtain the services the User/Subscriber has purchased.
- Device is configured with User-specific parameters as defined by the User.
- Network and service provider end points recognise the device as having authorisation to use the purchased services.
- Device and all purchased services are fully operational.

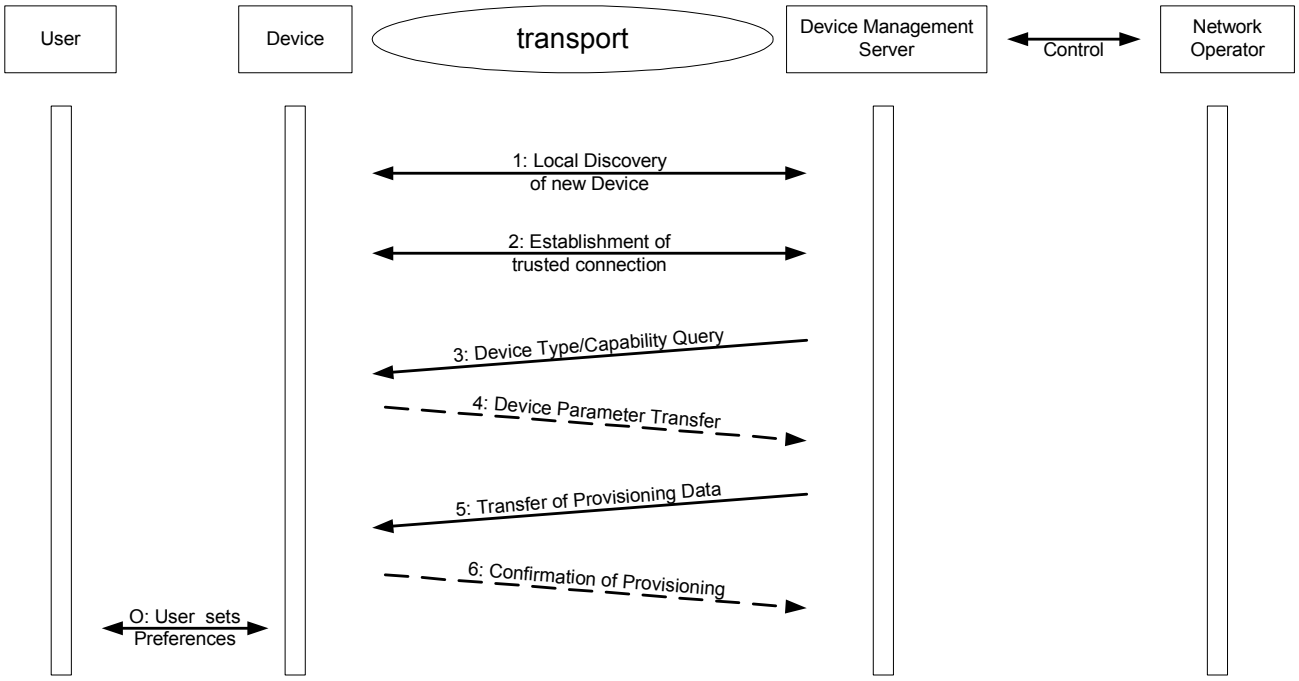
5.1.1.4 Variations

The user purchases a device in retail market, on power on the device is automatically provisioned over the air.

5.1.1.5 Normal Flow

1. Device is discovered by local Device Management infrastructure.
2. Trusted Relationship is established.
3. Device is queried for Type and Capabilities.
4. Type and Capabilities are transferred.
5. Provisioning data is transferred to Device.
6. Provisioning is confirmed.

O : Optional the User overwrites the predefined values for the User's preferences.



Provisioning of a new purchased Device

Remarks: The User Preference parameters should be changeable for the User in a comfortable way. The network parameters should be altered only by an authorized Management Server.

If pre-configured Devices are brought in bulk by the operator, it should be possible for the operator to give a simple "Provisioning Content" XML file to the Device manufacturers, so that the Device (or the smart card) can be provisioned in factory.

5.1.2 New Enterprise Device Purchase

A new Device (e.g., a handset or PDA) is purchased by an Enterprise Management Authority from a Device vendor. The Enterprise management system has also obtained Network parameters and software from the Network Operator and uses these with Enterprise specific parameters (as appropriate), Enterprise policy/preferences, Enterprise applications, and Enterprise security credentials to enable Enterprise use of the device. All this data is then used to create a set-up program for the device. The User receives and powers on the Device. The User then configures their device using the set-up program created by the Enterprise management authority. This set-up program can be communicated to the device using a removal media card, USB, Fire Wire, wireless network etc . The setup program is automatically executed and after a few seconds the Device is provisioned with WAN Network and all accompanying services/applications are fully operational after setup is complete.

5.1.2.1 Actors

- User
- Network Operator Management Authority
- Enterprise Management Authority
- Enterprise Administrator

5.1.2.2 Pre-Conditions

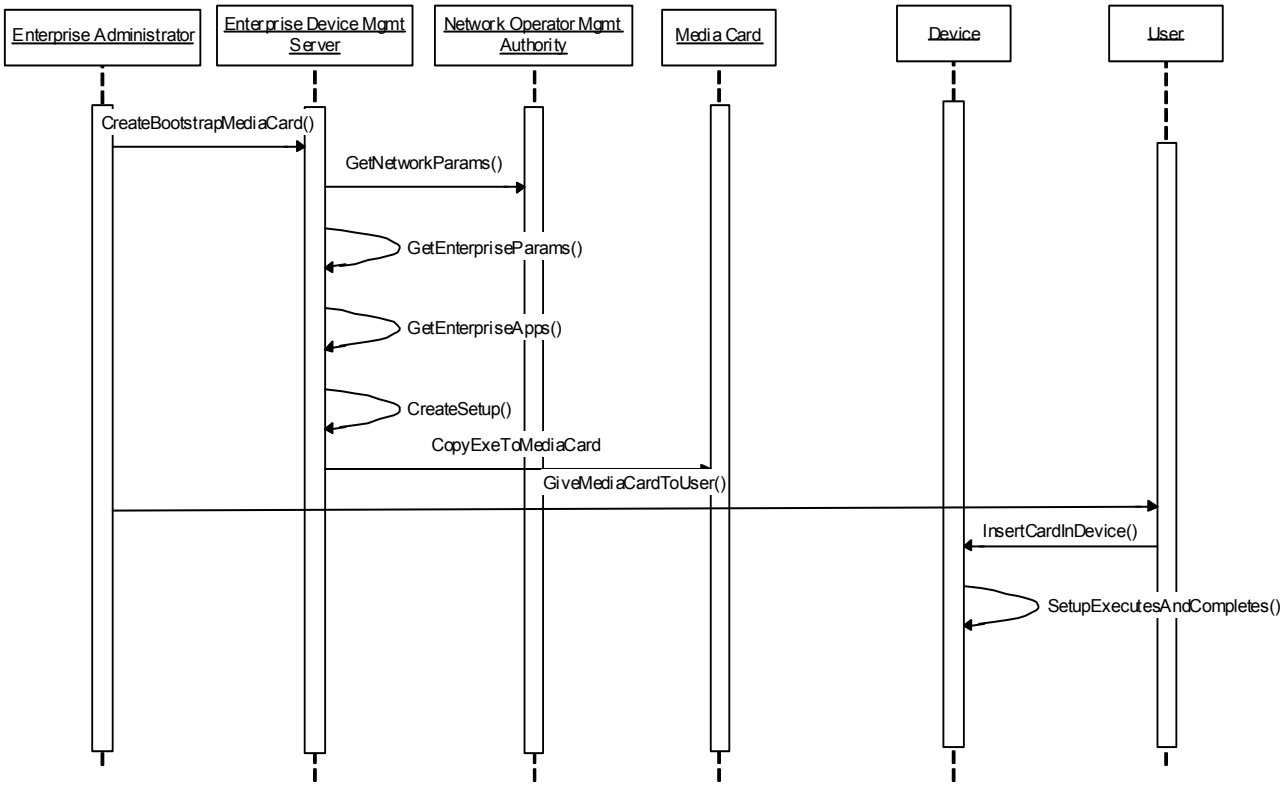
- User may be a Subscriber and has purchased a service contract with the Network Operator.
- The Enterprise has a Device Management system.
- Device is capable of interfacing with the Device Management system.
- The Enterprise Management Authority has programmatic access to the appropriate WAN Network Bearer parameters established by the Network Operator Management Authority. This may involve partial transfer of Management Authority.

5.1.2.3 Post-Conditions

- Device is provisioned with parameters and applications necessary to connect to the enterprise network and run the installed enterprise applications.

5.1.2.4 Normal Flow

1. Enterprise Administrator creates the contents of a removable media card.
    a. Device Mgmt Server (DMS) obtains the Network settings from the Network Operator.
    b. DMS obtains Enterprise parameters and applications.
    c. DMS writes the appropriate data and instructions to the media card.
2. Enterprise Administrator gives the media card to a User.
3. The User inserts the media card into a Device.
4. The setup runs and the device is appropriately configured.



New Enterprise Device Purchase

5.1.3 Smart Card based Provisioning

A smart card is inserted into the Device for the first time. The smart card contains pre-configured service parameters that enable access to a Service Provider's infrastructure and a key that allows to establish a trust connection to the Device Management system. The User inserts the smart card into the Device and the Device is provisioned (with optional user interaction) with parameters from the smart card. Upon use, the Device then establishes a relation to the Service Provider's management server in the network.

5.1.3.1 Actors and Data Authority

- User/Subscriber
- Service Provider

5.1.3.2 Pre-Conditions

- The User/Subscriber has established a contractual relationship with the Service Provider for service and has obtained a pre-configured smart card with a key (Issuing aspects of the smart card are not within scope of this document).
- The Device is equipped with a Device Management User Agent
- The Device is equipped with an User Agent associated with the pre-configured service, if required (or the Device has the ability to download such a User Agent)

5.1.3.3 Post-Conditions

- The Device is fully provisioned with parameters necessary to allow delivery of the purchased service.

5.1.3.4 Variations

a) Instead of having parameters pre-configured on the smart card, the card could contain only a key that enables establishment of a trust relationship with the Service Provider's management server. Service parameters could then be subsequently provisioned onto the Device by the Service Provider over the air.

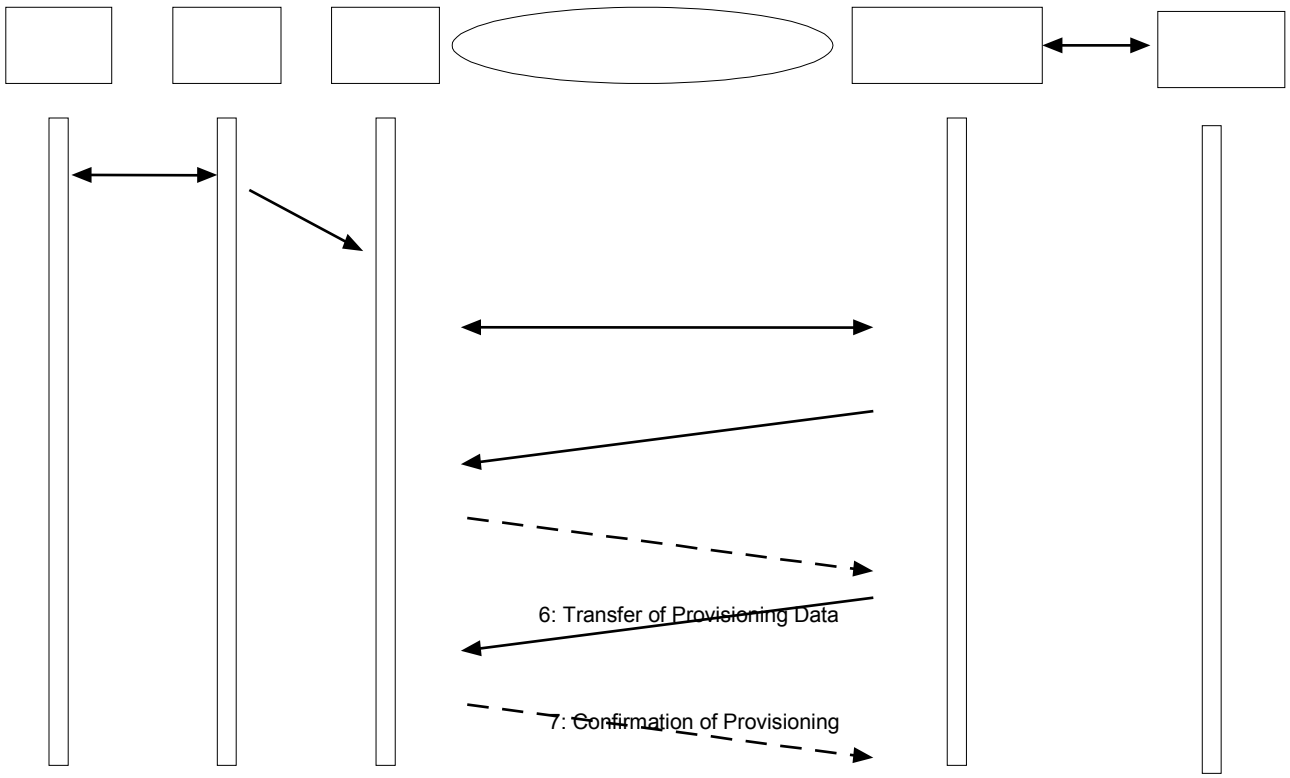
b) Instead of purchasing a new smart card with a Device, a Subscriber could purchase a service from a Service Provider and have their existing smart card configured with parameters or keys by an entity with Management Authority of the smart card.

5.1.3.5 Normal Flow

1. The User inserts the smart card into the Device.
2. If applicable (parts of) provisioning data is transferred from the smart card to the Device.
3. With the key on the smart card a trusted connection is established between the Device and the Device Management server.
4. The Device Management server queries the Device for actual configuration.
5. The Device responses to the query.
6. The relevant provisioning data is downloaded towards the Device.
7. The Transfer of the Provisioning data is confirmed.

5.1.3.6 Alternative Flow

As described in variation a) the trusted relationship can be established without prior transfer of provisioning data from the smart card to the Device (omission of step 2).



Smart Card based Provisioning including a partial transfer of provisioning data (Normal Flow)

5.1.4 Bootstrap Provisioning for used Devices

A Subscriber acquires a Device outside the operator's normal sales lines, e.g. second-hand. An inappropriate configuration in this case is very likely. The only connection to the operator is the smart card, where applicable. The Subscriber's first time use of the Device is detected automatically by the operator's infrastructure.

Alternatively the Subscriber asks explicitly for a configuration parameter set, e.g. by Customer care call or an abbreviated dialling request. The characteristics of the Device (e.g., Device capabilities, resident applications, configuration parameters) are determined and transmitted to the operator's management server. The appropriate provisioning parameters are transferred to the Device; optionally after a confirmation by the Subscriber. In addition User-specific preferences are defined by the User.

Difference to the use case in section 5.1.3 is that here already inserted configuration data has to be overridden; the Device is not in a 'fresh' state, but might be highly mis-configured, so standard values do not necessarily apply.

5.1.4.1 Actors and Data Authority

- Subscriber: The Subscriber has decided to connect to a particular Network Operator.
- User : The User is authorised to define and change the User Preference Parameter.
- Network Operator: The selected Network Operator is authorised to define and change the Network Configuration Data.

5.1.4.2 Pre-Conditions

- The Subscriber has purchased a service contract with the Network Operator.
- Device is capable of interfacing with the Device Management system.

5.1.4.3 Post-Conditions

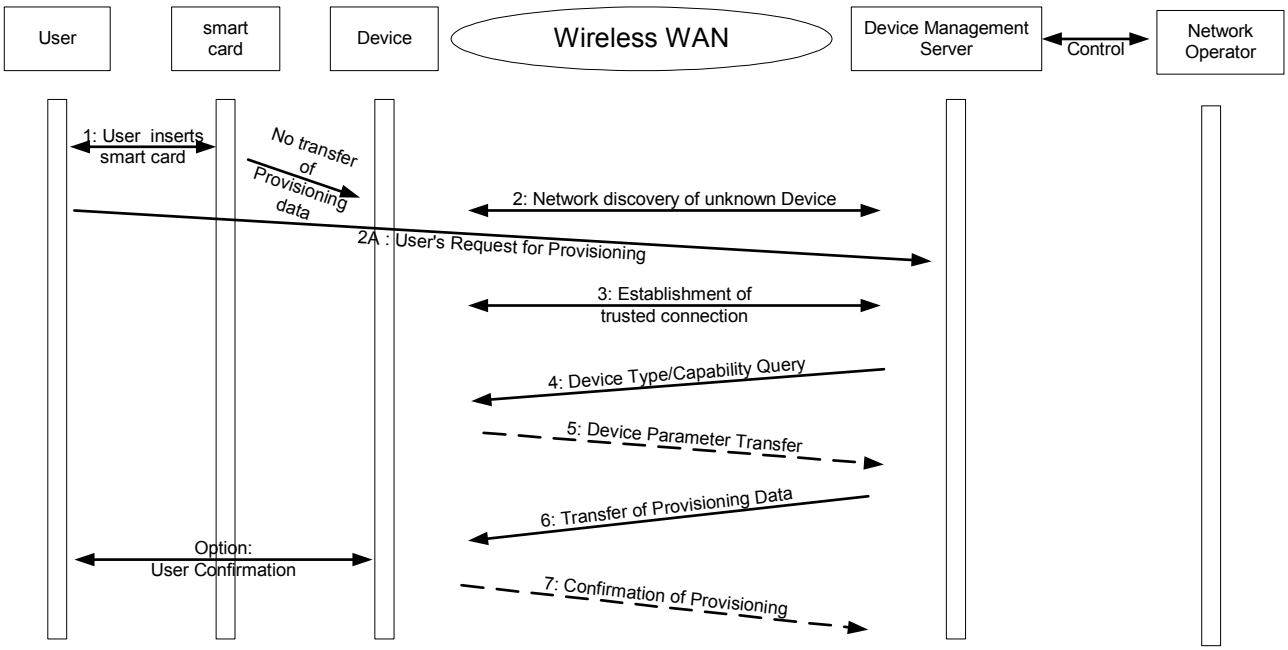
- Device is provisioned with parameters necessary to obtain the services the User/Subscriber has purchased.
- Device is configured with User-specific parameters as defined by the User.
- Device and all purchased services are fully operational.

5.1.4.4 Normal Flow

1. User inserts smart card (where applicable)
2. Radio Network detects a new combination of Subscriber (e.g. IMSI) and Device (e.g. IMEI).
3. Establishment of trusted relationship between Device and Device Management Server.
4. Management server queries the Device for its capabilities
5. Device responses to the request
6. Appropriate configuration is transferred by the Device Management Server.
7. The provisioning of the Device is confirmed.

5.1.4.5 Alternative Flow

The Device Management data transfer is triggered by the User. In this case step 2 is replaced by the User's request.



Provisioning for used Devices including network detection (Normal Flow)

5.1.5 Subscriber provisioning through the PC

A new Device is purchased by the User via the Internet from a Device vendor. The User receives the Device from the vendor.

To provision the Device the User places the new Device in proximity to their PC. The PC Agent discovers the Device. The User is prompted to ask if they wish to provision the Device, after an affirmation of consent the PC Agent connects to the Network Management Authority.

The User is then presented with options on the PC UI and is stepped through the process of provisioning the Device via a secure Network connection. The User selects to configure network settings, add additional prepaid minutes and selects the game service. The User enters their personal and credit card information and confirms the transaction. Upon completion of a credential check the Network Management Authority provisions the device via the PC Agent.

5.1.5.1 Actors

- User
- Network Operator Management Authority
- PC Agent

5.1.5.2 Pre-Conditions

- User may be a Subscriber and has purchased a service contract with the Network Operator.
- PC Agent is capable of interfacing with the Network Management Authority.
- PC Agent is capable of interfacing with the Device.
- PC Agent has obtained mechanism to access the Network Management Authority.
- PC Agent is present on the PC.
- Device is capable of interfacing with the Network Management Authority (variation 1).
- User has obtained mechanism to access and log into Network Management Authority website (variation 1).

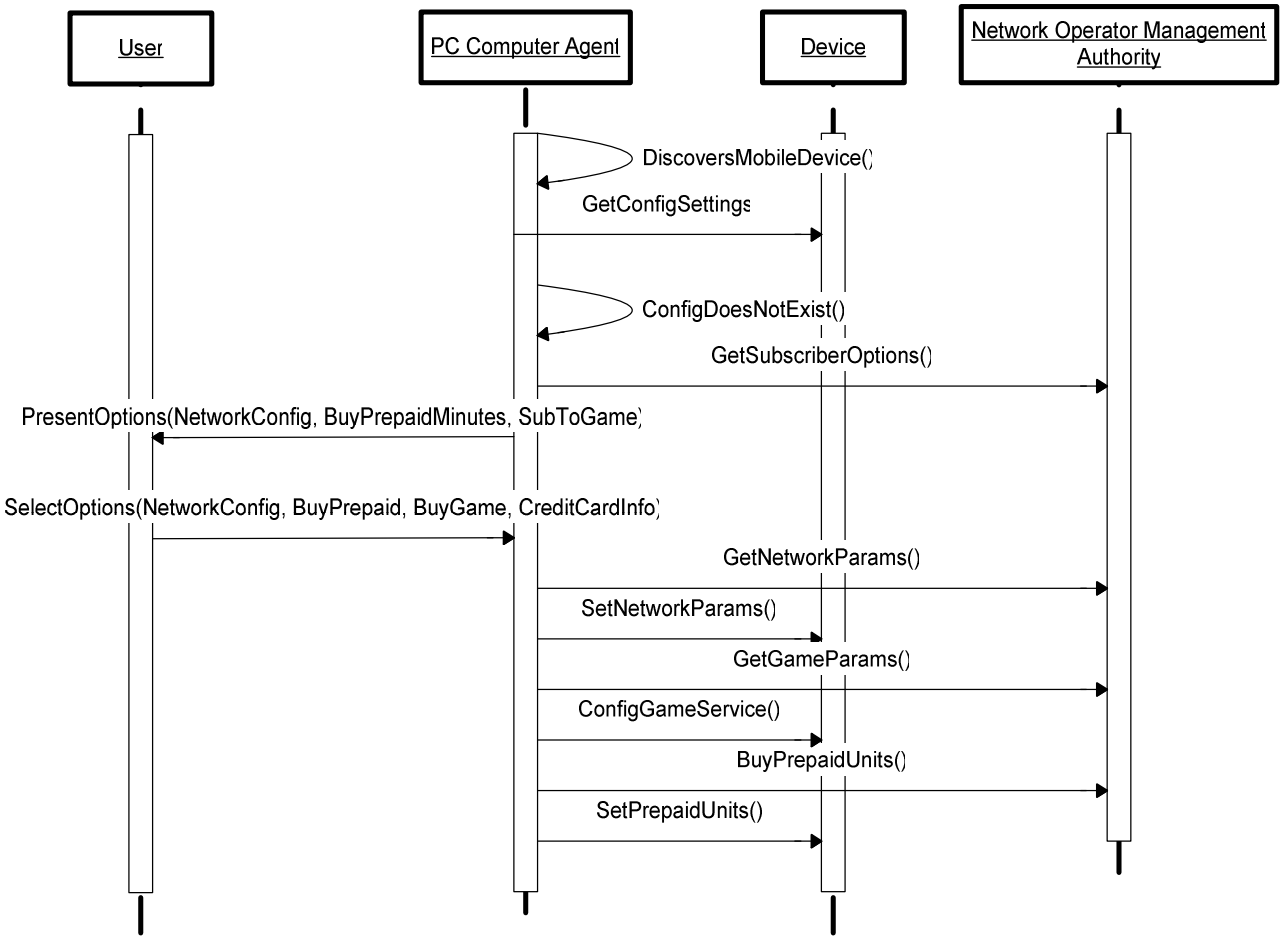
5.1.5.3 Post-Conditions

- The Device has network connectivity.
- The Subscriber has more prepaid minutes on their account.
- The appropriate applications are installed and server side service provisioning is complete.

5.1.5.4 Variations

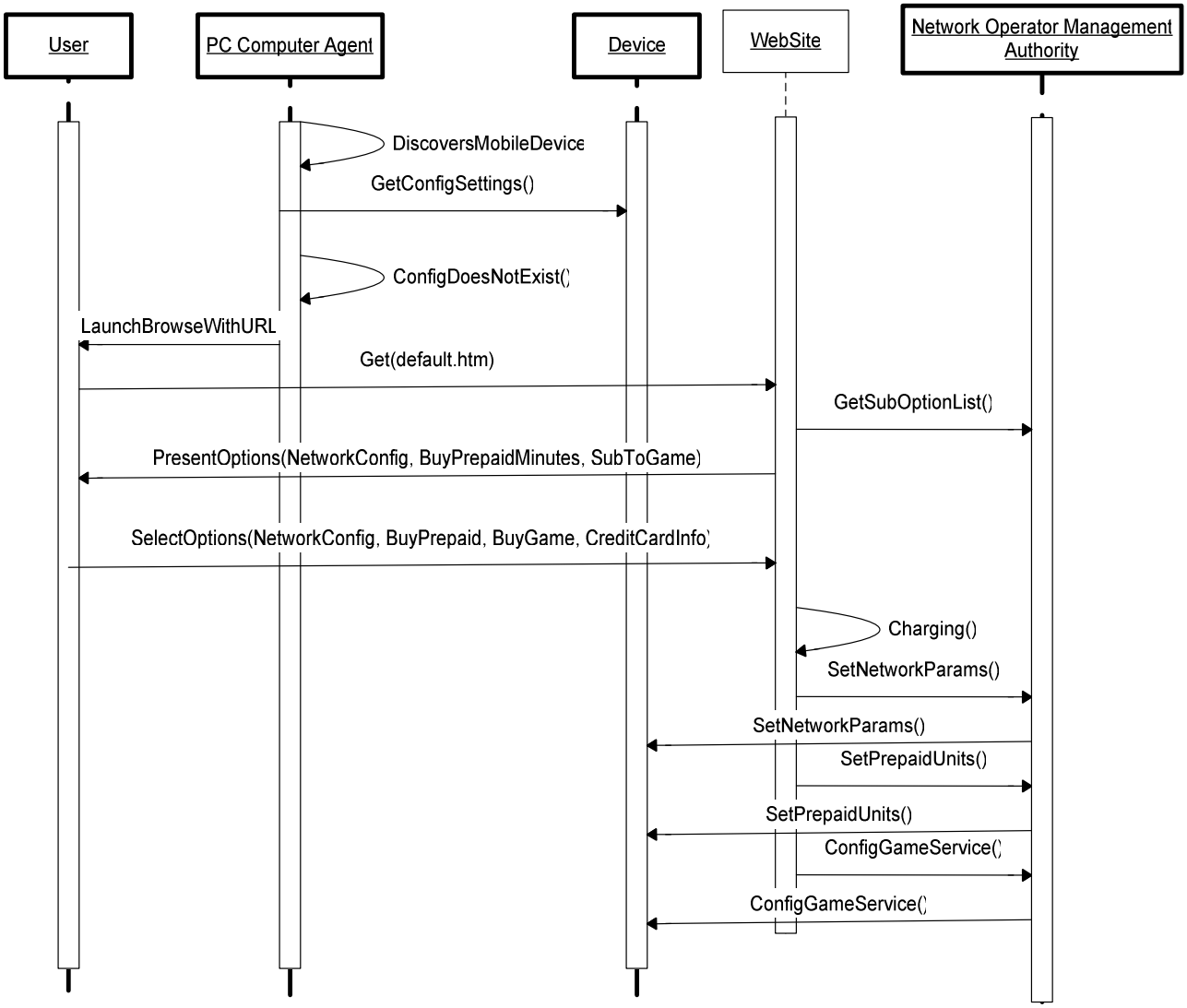
1. The Device provisioning can be performed via an OTA mechanism between the Network Management Authority and the Device.
2. The User while sitting in front of their computer places the Device in proximity of the PC. The PC Agent discovers the Device and interrogates the Device for the number of available service minutes. If the service minutes are below a preconfigured limit the PC Agent prompts the User if they wish to top up the number of service minutes.

5.1.5.5 Normal Flow



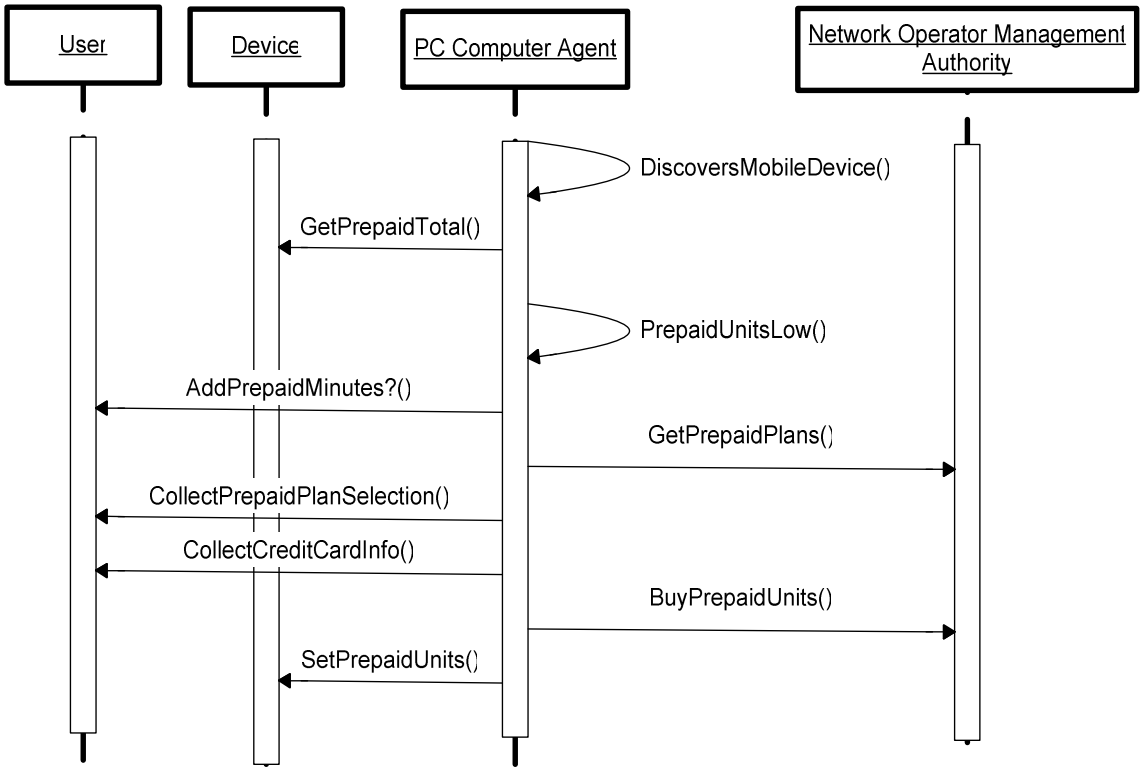
Provisioning via Computer Agent

5.1.5.6 Variation 1 Flow



Provisioning via OTA

5.1.5.7 Variation 2 Flow



Low prepaid detection

5.2 Configuration Maintenance/Management

5.2.1 Remote Configuration initiated by the management server

An operator changes its platform infrastructure for a data service, e.g. the IP-address of WAP gateway changes. Manual configuration of the new parameters by the Subscriber with assistance of Customer care is a lengthy and cumbersome procedure. Either the attempt to access the operator's infrastructure with the old parameter set triggers the transfer of the new parameter set, or all affected Devices are identified and automatically updated over the air, regardless of the actual usage of the service.

The management server receives the parameters for the client Device to be updated. The management server determines the Device information in order to potentially customise the configuration. The management server sends the configuration information to the Device. The Device stores the data in the configuration context associated with the management server without any User interaction and reports the status as requested by the management server. Optionally an User confirmation may be requested. The Device interacts with the User. If the User confirms the operation, the Device stores the data in the configuration context associated with the management server.

5.2.1.1 Actors and Data Authority

- User: User-specific preferences are not altered
- Management Authority: The Management Authority is authorised to define and change the Configuration Data

5.2.1.2 Pre-Conditions

- Configuration Data has/will become obsolete.
- Device is capable of interfacing with the Device Management system.

5.2.1.3 Post-Conditions

- Device is provisioned with effective parameters necessary to conserve/improve the services the User/Subscriber has purchased.
- Device is configured with User-specific parameters as previously defined by the User.
- Device and all purchased services are fully operational.

5.2.1.4 Variations

- A Enterprise Management Authority changes a Device policy setting. Using the Enterprise Device Management system the administrator deploys the policy change to all Devices. The next time the Users connect to the corporate network, the new policy is applied.

- A Customer experiencing problems with their handset calls customer care. While the call is still active, the customer care agent is able to read:
  - the Device information;
  - other available Device settings, including as a minimum those described in section 6.10;
  - the application inventory.

  The agent detects a fault in the settings and resets the incorrect parameters remotely via the management server.
- The Network Operator reads the Device settings listed in the above bullet outside of the context of a customer care call, as part of pro-actively solving problems.
- A new service is to be enabled for legacy Devices. This may require a new APN to be configured in the handset, a new bookmark to be added etc.

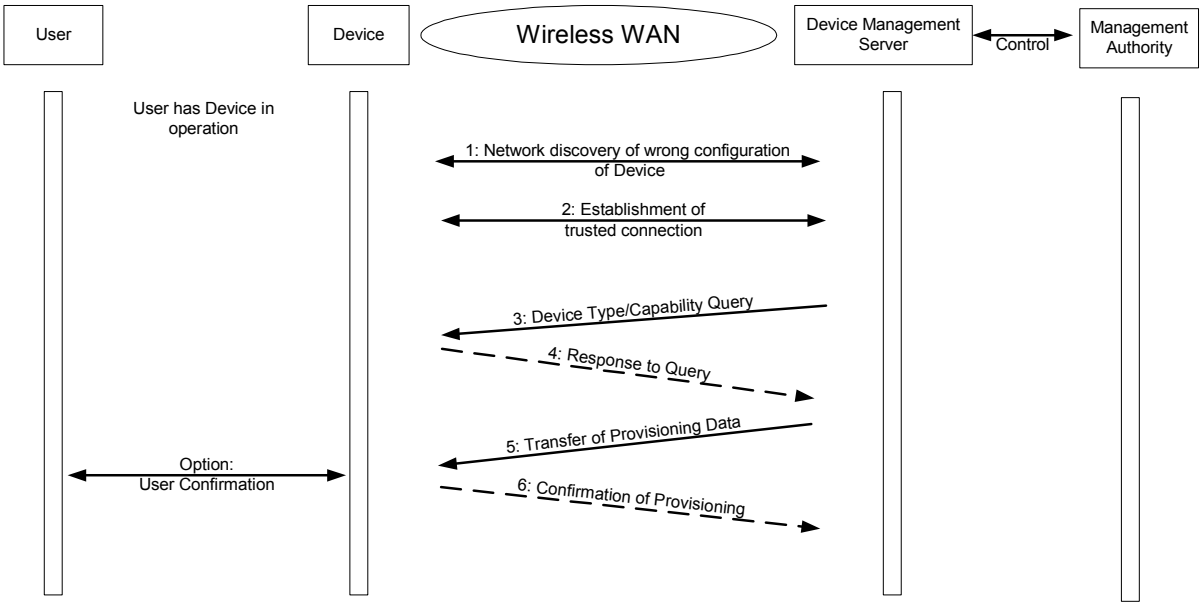
Remarks: High volume remote configuration of Devices should be possible in a short time period, so the interruption/duplication of a service is short. In order to avoid User confusion in this case the configuration affirmation should be abandoned.

5.2.1.5 Normal Flow

1. Detection of Device with obsolete configuration settings, e.g. by addressing wrong URL or IP-address. Alternatively query for the Device settings actively, e.g. triggered by customer care call.
2. Establishment of trusted relationship between Device and Device Management Server.
3. Management servers queries the Device for actual configuration.
4. The Device responses to that query.
5. The effective configuration data is transferred to the Device.
6. The update of the configuration data is confirmed.

5.2.1.6 Alternative Flow

- If settings should be overwritten unconditionally, the transfer of old configuration in the Device can be omitted (step 3 and 4).



Remote Configuration by management server (Normal Flow).

The Device Query (step 3) and the corresponding transfer of capabilities/configuration (step 4) could be omitted if the wrong configuration is detected in the network or if the configuration is distributed to a mass of Devices unconditionally

5.3 Software management

5.3.1 Software upgrade/update/installation initiated by the management server/User:

The management server requests the software/hardware inventory of the Device. The Device returns appropriate inventory data to the management server (with optional User interaction). The management server analyses the data, and initiates the transfer of the required software. The Device receives and installs the software using the mechanisms that are applicable to that type of software. Upon completion, the Device reports the status to the management server as requested by the management server. Software may be transferred as an upgrade package that is not in itself the complete software component being updated. Software updated in this way may be indistinguishable from software updated in its entirety.

5.3.1.1 Actors and Data Authority

- Provider: The Service/Content Provider assigns what application software should be installed by default on a specific Device type. The provider is authorised to define and change the default software on a Device type.
- User authorises request from the Management Server.

5.3.1.2 Pre-Conditions

- Installed software (or SW versions) on a Device is incorrect or incomplete or non-existent or is to have added functionality applied or is to be enhanced for security or performance reasons.
- Device is capable of interfacing with the Device Management system.

- Security constraints imposed by Device Management Server and any Device Client are met.

5.3.1.3 Post-Conditions

- All software and/or software updates target at the device have been delivered and installed.
- Device and all purchased services are fully operational.

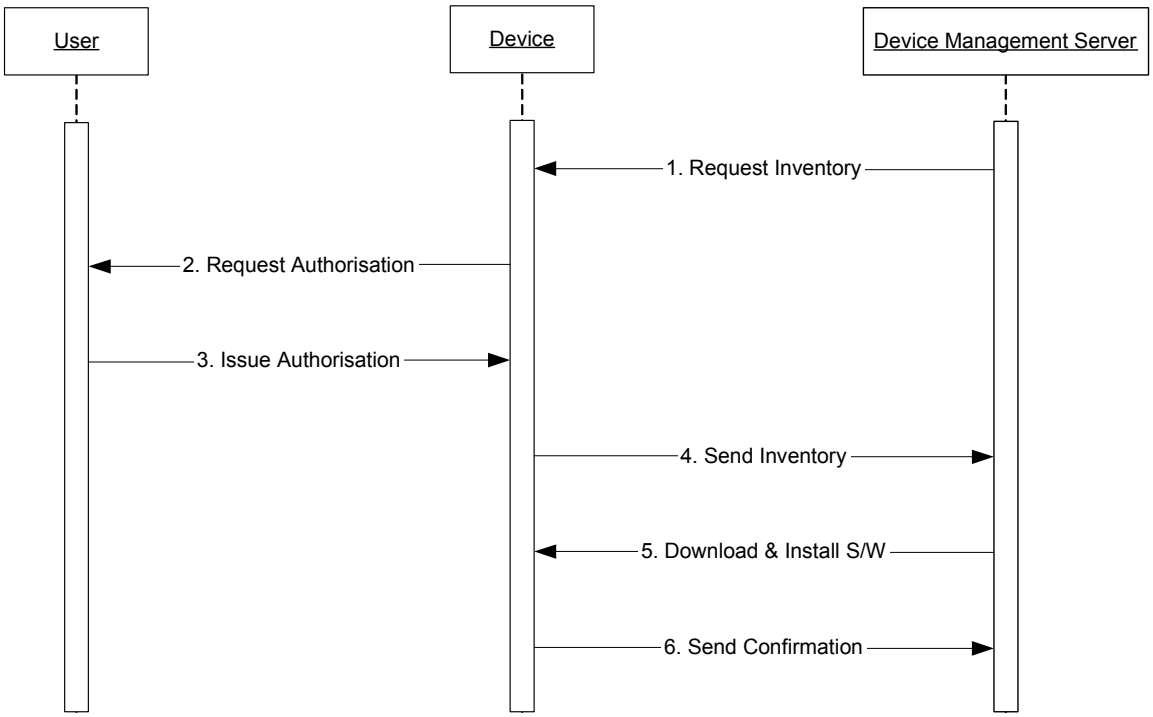
5.3.1.4 Variations

- The servers request (inventory) is replaced by an User request (directly or indirectly via a web service for example). Furthermore the User may request additional software over the default software installation. The portfolio of these additional software is authorized by the provider.
- The service/content provider may suggest updates and/or additional software. User acceptance would lead to device query and download of update.
- The management server may be able to trigger the remote execution of the application securely, i.e. after authentication of the management server and with assured integrity of the executed code.

Remark: The management server shall be able to stop the execution of an application intended to be upgraded.

5.3.1.5 Normal Flow (for initialisation by the server)

1. The Device Management Server issues a request to the Device for an inventory of installed software
2. The Device issues a request to the User for authorization to send a response to the Device Management Server containing an inventory of installed software and authorization to install upgrades
3. Upon confirmation by the User, the Device sends the response to the Device Management Server
4. The Device Management Server initiates software download, installation, and execution
5. The Device sends a confirmation back to the Device Management Server



Software Upgrade/Update

5.4 Fault Detection, Query and Reporting

5.4.1 Helpdesk problem determination

A Subscriber calls the operator's customer care facility or corporate help desk complaining that their Device is reporting an error, or a service is failing to work. The corporate help desk or operator's Customer care server Help Desk agent can query the Device to determine key information, e.g.:

- Device type
- Serial number
- Operating system version
- Capabilities
- Installed applications
- Connectivity/application configuration
- Event/performance logs

Based upon this information, the Help Desk agent may be able to determine the cause of the issue, and take Device Management actions that resolve it.

5.4.1.1 Actors and Data Authority

- Subscriber (User or Corporate Customer): A Corporate Customer may be able to specify aspects of the configuration and issue resolution procedures for its Devices.
- Device: The Device protects its configuration from unauthorized access.
- Management Authority: The Management Authority can access the Device configuration, and change it.

5.4.1.2 Pre-Conditions

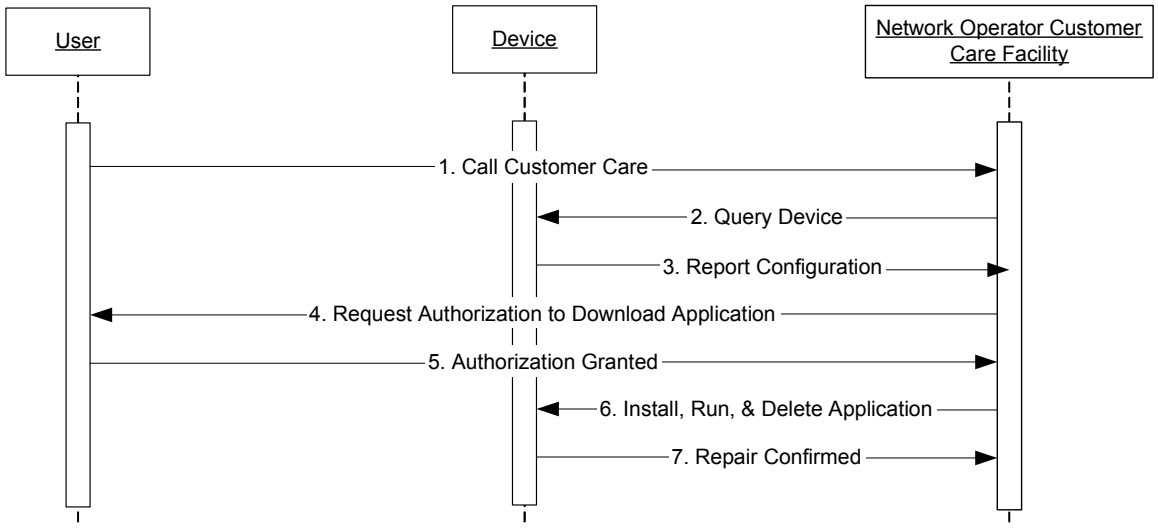
- Devices support Device Management queries and actions from the management server.
- The Network Operator has a Device Management server supporting Device Management queries and actions.

5.4.1.3 Post-Conditions

N/A

5.4.1.4 Normal Flow

1. User calls Customer Care
2. Customer Care sends query to Device
3. Device reports its configuration information to the Customer Care server
4. Customer Care sends request to User for authorisation to download application to Device
5. User grants authorisation
6. Customer Care downloads application to device, installs and executes it
7. Device sends acknowledgement to Customer Care server



Fault Detection, Query, and Reporting

5.5 Non-application Software Download

Non-application software download is the process of delivering new executable code to a device to modify its operation or performance.

Examples of non-application software include but are not limited to device operating system, drivers, radio software and firmware. While the following Use Case is intended to be generic it should be noted that the software being updated may have its own requirements and that these requirements may be outside the scope of OMA. What is being described here is the need for the ability to update non-application software and provide a means to do so. We are not defining the elements but a mechanism to update them.

5.5.1 Bug Fixes for Operational Improvement

5.5.1.1 Short Description

The increased complexity of Devices has increased the likelihood for device recalls due to software. There is a strong business case for over-the-air software download to correct software deficiencies including non-applications software. The manufacturer is responsible for developing software for correcting "bugs" in their software and for seeking approval from the appropriate regulatory agency for every software version to be installed and executed on any wireless hardware device.

5.5.1.2 Actors and Data Authority

- **User/Subscriber**: The end User may request a download of software to fix "bugs" in non-application software.
- **Network Operator/Service Provider**: The Network Operator/Service Provider may initiate software download to correct "bugs" in the software.

5.5.1.3 Pre-Conditions

- **Manufacturer**: Must include non-application software reconfiguration capabilities in the design of the device.
- **User/Subscriber**: Must initially configure Device to accept software download for non-application software reconfiguration.
- **Network Operator/Service Provide**: Works with the manufacturer to identify and solve deficiencies in non-applications software.

5.5.1.4 Post-Conditions

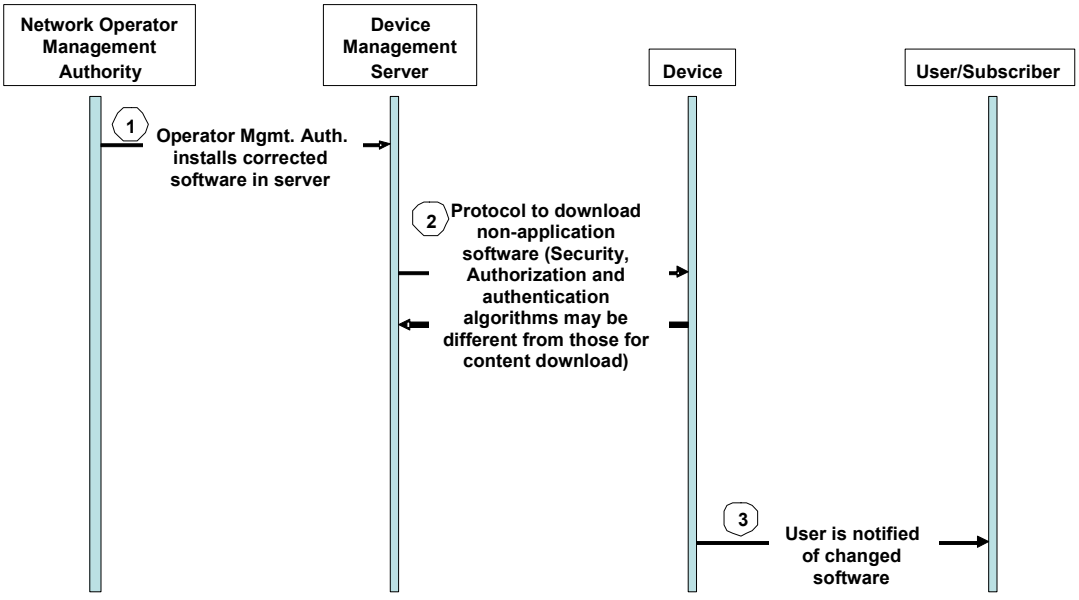
- Mobile device has corrected operational non-applications software

5.5.1.5 Variations

- The download may be accomplished either over-the-air or by other mechanisms (e.g., service technician at a kiosk).
- Either the Network Operator/Service Provider or the User/ Subscriber may initiate this action.

5.5.1.6 Normal Call Flow

1. Operator Management authority installs corrected software in server.
2. Software is downloaded to the device using a standardized protocol. This protocol includes device discovery, capability exchange, authentication, authorization and security and other software download functions.
3. The User is notified of changed software.



Call flow for bug fixes use case

6. Requirements (Normative)

6.1 High Level Functional Requirements

6.1.1 Security

6.1.1.1 General security requirements

1. The authentication procedure MUST be strong enough to ensure that is not be possible for a third party to masquerade as a Device management server by spoofing its identity. **2.** The client and sever MUST be capable of detecting replay attacks. **3.** Architecture supports traversal of corporate firewalls and Network translation Devices (Use Case 5.1.2)

4. If end user confirmation is indicated by the Device Management Server, the Device will prompt for user confirmation before incorporation of configuration data. (Use Case 5.1.5)

5. Except for establishing the initial trust relationship (bootstrap) over the air, if end user confirmation is not indicated by the Device Management Server, the Device MUST NOT ask for user confirmation before incorporation of configuration data. (Use Case 5.1.5)

6. The non-repudiation of the session MUST be ensured. (Use Case 5.4.1)

6.1.1.2 Authentication

Before any Device management operations can be carried out on the Device, it must conform to the following:

1. The client MUST successfully authenticate the Device Management server (Use Case 5.2.1).

2. If the Device management operation is related to personal information then the user MUST successfully authenticate himself to the Device management server (Use Case 5.2.1).

3. The Device Management Server May also authenticate the Device (Use Case 5.1.1., 5.1.3, 5.4.1)

4. Whenever there is communication between Device Management Servers the Device Management Servers MUST mutually authenticate (Use Case 5.1.2).

5. With local wireless interfaces, discovery is controlled between the PC Agent and Device. Secure association and authentication MUST be supported. The first connection requires a secure association be created between the Device and PC. (Use Case 5.1.5)

6.1.1.3 Authorisation

Before the Device Management server can carry out any Device management operations on the Device, it must conform to the following:

1. The Device Management server MUST be authorised to carry out any Device management operations on the Device (Use Case 5.2.1).

2. With local wireless interfaces, discovery is controlled between the PC Agent and Device. Secure association and authorisation MUST be supported. The first connection requires a secure association be created between the Device and PC. (Use Case 5.1.5)

6.1.1.4 Integrity protection

1. All data communication between the Device Management Server and a Device MUST be integrity protected. (Use Case 5.1.1, 5.1.3, 5.4.1)

2. All data communication between Device Management Server MUST be integrity protected. (Use Case 5.1.2)

3. The Data Link between the Software Originator (or agent) and the Device Management Server MUST maintain data integrity. (Use Case 5.5.1)

4. The inventory SHALL be secure from alteration when sent by the appropriate integrity protection. (Use Case 5.3.1)

5. The downloaded software SHALL be secure from alteration by the appropriate integrity protection. (Use Case 5.3.1)

6.1.1.5 Confidentiality protection

1. All data communication between the Device Management Server and a Device, that is personal to the user or confidential to the owner of the information (e.g. some network operator settings) MUST be confidentiality protected. (Use Case 5.1.1, 5.1.3, 5.4.1)

2. All data communication between Device Management Servers MUST be confidentiality protected. (Use Case 5.1.2)

3. The Data Link between the Software Originator (or agent) and the Device Management Server MAY maintain data confidentiality. (Use Case 5.5.1)

4. The Data Link between the Device Management Server and the Device MAY maintain data confidentiality, where appropriate. (Use Case 5.5.1)

6.1.1.6 Smart card security

1. Provisioning data on smart card SHALL be protected against unauthorized modification. (UC 5.1.3)

2. It SHALL NOT be possible for the Smart Card to reveal any secret keys it holds (UC 5.1.3)

6.1.2 Recording

1. The Device Management System SHALL provide sufficient information so that queries from the Device Management Server, reports from Devices, data downloads, and acknowledgements MAY be billed and tracked accordingly. (Use Case 5.1.1, 5.1.3, 5.4.1)

2. If a management authority causes delegation to occur among several Device Management Servers, the Management Authority MAY request from each DMS, and each DMS SHALL provide, reports of the operations performed in a device for tracking purposes (Use Case 5.1.1, 5.1.3, 5.4.1)

3. The session MUST be identified as customer-care-related. (Use Case 5.4.1)

4. The session MUST be uniquely identified. (Use Case 5.4.1)

5. If transactions are logged, server MUST log transactions with success indicator. (Use Case 5.4.1)

6.1.3 Administration and Configuration

1. The DMS SHALL provide a standardized mechanism for publishing session/message transactions, such as confirmation requests and results, etc.

(Use Case 5.1.1, 5.1.3, 5.4.1)

2. Confirmation request messages SHALL be uniquely identified and contain at least the subscriber id, data or data summary, and date/time.

(Use Case 5.4.1)

3. Confirmation result messages SHALL be uniquely identified and correlated to the request.

(Use Case 5.4.1)

4. Management Authority MAY be delegated by a primary Management Authority (one that has domain over a given set of Management Objects) to a secondary Management Authority. (Use Case 5.1.1)

5. The first connection MUST involve a secure association be created between the Device and PC. (Use Case 5.1.5)

6. The DMS shall send a notification of the update/upgrade to the appropriate management authority. (Use Case 5.3.1)

6.1.4 Usability

1. If user confirmation is indicated by smart card data, the Device SHALL ask for user confirmation before incorporation of provisioning data (stored on smart card).

2. If user confirmation is not indicated by smart card data, the Device MUST NOT ask for user confirmation before incorporation of provisioning data (stored on smart card). (UC 5.1.3)

3. If indicated by smart card data, the Device SHALL establish the connection to Device Management Server autonomously. (UC 5.1.3)

4. If user confirmation is indicated by the Device Management Server, the Device SHALL ask for user confirmation before incorporation of configuration data (transferred by Device Management Server).

5. Except for establishing the initial trust relationship configuration (bootstrap) over the air, if user confirmation is not indicated by the Device Management Server, the Device MUST NOT ask for user confirmation before incorporation of configuration data (transferred by Device Management Server). (UC 5.1.3, 5.1.4, 5.2.1)

6. The Device SHALL be capable for being contacted by the Device Management Server, if the Device is switched on and has radio coverage by its subscribed network operator and is not busy by a voice link. (UC 5.2.1)

7. The Device MAY be capable for being contacted by the Device Management Server, if the Device is busy by a voice link. (UC 5.2.1)

8. User is not prompted if there is no work to be done (Use Case 5.1.5)

9. Management Authority MAY clarify implications of subsequent actions (query, etc.) to the User. (Use Case 5.4.1)

10. User voice calls MUST NOT be terminated upon reception of the query. (Use Case 5.4.1)

11. User voice calls MUST NOT be terminated upon reception of the authorization request. (Use Case 5.4.1)

12. Authorization MUST be clear esp. regarding privacy issues and warranty. (Use Case 5.4.1)

13. User MAY be informed that the process is over. (Use Case 5.4.1)

14. The user SHALL be asked for confirmation to proceed before any software is updated. (Use Case 5.3.1)

15. The user SHALL be informed that the update/upgrade has been completed. (Use Case 5.3.1)

16. The Device MUST NOT send an inventory list of applications installed in the Device without either this optional feature being added by the user or the Device asks for permission from the user when needed.

6.1.5 Interoperability

1. The DMS MAY be interfaced with a Customer Care application. (Use Case 5.4.1)

2. Errors MAY be reported to a Customer Care application. (Use Case 5.4.1)

6.1.6 Privacy

Requirements covered in other sections

6.2 Overall Systems Requirements

1. The Device Management infrastructure MAY be based on a distributed architecture, wherein functional elements of the system (e.g., the Device Management Server) MAY consist of one or more coordinated, but physically separate entities. (Use Case 5.1.1)

2. The overall system SHALL support a distributed system architecture (Use Case 5.1.2)

3. Device Discovery by the Device Management Server MUST be clearly defined (e.g. SMS, push.). (Use Case 5.4.1)

5. The Device Management System SHALL make provision for different Management Authorities (e.g. Enterprise, Network Operator) to manage different data sets or applications in a single device. Each Management Authority can control data sets and applications owned by that Management Authority.

6.3 System Elements

6.3.1 Device

1. The Device SHALL be capable of discovering the presence of nearby, active Device Management system elements if those elements are using compatible local bearers. (Use Case 5.1.1)

2. The Device SHALL be able to communicate all of its relevant properties (e.g., manufacturer, model, firmware, etc.) to the Device Management Server on demand. (Use Case 5.1.1, 5.1.3, 5.4.1)

3. The Device SHALL be able to communicate its capabilities and configuration (e.g., WAP/MMS settings, installed software applications, etc.) to the Device Management Server on demand. (Use Case 5.1.1, 5.1.3, 5.4.1)

4. The Device SHALL be capable of autonomously (i.e., without User interaction) accepting and storing downloaded Management Objects (e.g., parameters, software, etc.) after the one time initial trust relationship configuration (bootstrap) is performed. (Use Case 5.1.1, 5.1.3, 5.4.1)

5. Obsolete/outdated configuration data transferred/stored by any other Management Authority MUST NOT prevent the incorporation of the current data (UC 5.1.4).

6. The data tree for containing Device management objects on the Device SHALL be capable of being modified (i.e., nodes or data fields added or deleted), read from, and/or written to. (Use Case 5.1.1, 5.1.3, and 5.4.1)

7. The Device SHALL be capable of receiving and displaying a command from the DM Server to request User confirmation for a management action. (Use Case 5.4.1)

8. The Device SHALL be capable of accepting User input regarding confirmation of a proposed management action, and sending the result of that confirmation to the DM Server. (Use Case 5.4.1)

9. The Device SHALL be able to acknowledge the receipt and installation of data downloaded from the Device Management Server. (Use Case 5.1.1, 5.1.3, 5.4.1)

10. The Device SHALL be capable of detecting the presence of provisioning data on an installed, activated Smart Card. (Use Case 5.1.3)

11. The Device SHALL be capable of autonomously establishing a data link with the Device Management Server, using connectivity information stored on the Smart Card. (Use Case 5.1.3)

12. The Device SHALL be capable of participating in a mutual authentication with the Device Management Server, using authentication credentials (e.g., a challenge response) stored on or derived from the Smart Card. (Use Case 5.1.3, 5.4.1)

13. Device SHALL retrieve and incorporate relevant configuration data stored on the smart card into the Device's DM structure. (UC 5.1.3)

14. Each Device MUST support standardized dynamic IP allocation when the Device is first connected to the network. If an IP address cannot be allocated from the network, then the Device MUST use automatic IP addressing (Auto-IP) to obtain an address. (Use Case 5.1.5)

15. The Device SHOULD announce itself on the network to all control points it detects. The act of announcement does not imply the Device will receive rights, since assignment of rights is an expression of the user's decision. When the Device is added to the network, the discovery protocol allows that Device to advertise its services to control points on the network. The fundamental exchange in both cases is a discovery message containing a few, essential specifics about the Device e.g., its type, identifier, and a pointer to more detailed information. (Use Case 5.1.5)

16. The Device MUST support the assignment of a friendly name in relation to a network unique name(Use Case 5.1.5)

17. The mapping from friendly name to unique name MUST be the function of each user's user interface in the case where the Device is shared. (Use Case 5.1.5)

18. A method SHOULD be available by which a Device MAY automatically configure an interface with an IPv6 link-local address, IPv4 address in the 169.254/16 range that is valid for link-local communication on that interface, or both. On top of this there is a requirement to be able to define the link-local configuration to enable hosts that support multi-homing (more than one active interface and/or, more than one active address per interface, both IPv4 and IPv6 addresses, or a combination of these).This requirement is especially valuable in environments where no other configuration mechanism such as DHCP is available. (Use Case 5.1.5)

19. The Device SHOULD support IP based Device discovery based on the SSDP [http://www.upnp.org/download/draft_cai_ssdp_v1_03.txt]. The Device SHOULD support a 30 minute suggested timeout for when a Device is added or disappears from the network. (Use Case 5.1.5)

20. If end user confirmation is indicated by the Device Management Server, the Device will prompt for user confirmation before incorporation of configuration data. (Use Case 5.1.5)

21. PC Agent SHALL be capable of changing the DM tree on the Device and install the application (Use Case 5.1.5)

22. The Device MAY support concurrent voice calls and data exchanges. (Use Case 5.4.1)

23. The Device MUST support at least one wireless data bearer. (Use Case 5.4.1)

24. The Device MUST respond to query. (Use Case 5.4.1)

26. The Device MUST verify integrity of data before execution. (Use Case 5.4.1)

27. The Device MUST report to Server errors that occur during the parameter or software download. (Use Case 5.4.1)

28. The Device MUST be capable of determining that the Server is authorized to provide the software and/or data. (Use Case 5.5.1)

29 The Device MUST be capable of exchanging security information with the Server. (Use Case 5.5.1)

30. The Device MUST be capable of storing the software that is downloaded. (Use Case 5.5.1)

31. The Device MUST be able to independently verify the validity of the Software Originator of the Software and/or Data downloaded. (Use Case 5.5.1)

32. The Device MAY be able to verify, with the help of a Trusted Authority, the validity of the Software Originator of the Software and/or Data downloaded. (Use Case 5.5.1)

33. The Device MUST be able to verify that the downloaded Software and/or Data is targeted to the Device. (Use Case 5.5.1)

39. The Device SHALL send an inventory of its installed software to the Device Management Server. (Use Case 5.3.1)

40. The Device SHALL receive the software update/upgrade. (Use Case 5.3.1)

6.3.1.1 Interface to other Devices

1. Data links between the Devices SHALL be over standardized, local and/or remote, wired and/or wireless bearers (e.g., Bluetooth, IR, USB, Ethernet, GPRS, etc.). (Use Case 5.1.1)

2. Protocols used SHALL be generally accepted and standardized (e.g. TCP/IP, http, https, Universal Plug and Play, etc) (Use Case 5.1.5)

6.3.1.2 Interface to Device Management Servers

1. Data links between the Device Management Server and Devices SHALL be over standardized, local and/or remote, wired and/or wireless bearers (e.g., Bluetooth, IR, USB, Ethernet, GPRS, etc.). (Use Case 5.1.1, 5.1.3, 5.4.1)

2. Interface MUST support traversal of corporate firewalls and Network Address Translators (Use Case 5.1.2)

3. Interface MUST be discoverable (Use Case 5.1.2)

4. The Device Management Server MUST support secure connectivity via HTTPS. (Use Case 5.1.5)

5. Protocols used SHALL be generally accepted and standardized (e.g. TCP/IP, http, https, Universal Plug and Play, etc) (Use Case 5.1.5)

7. The Device Management Server and the Device MUST be able to exchange their respective capabilities and select a set to be used for the download. (Use Case 5.5.1)

8. The Device MUST be able to notify the server that it has accepted and successfully saved the downloaded software and/or data. (Use Case 5.5.1)

6.3.2 Smart Card

1. The Smart Card SHALL be capable of storing Management Objects (e.g., network address(es)). (Use Case 5.1.3)

2. The Smart Card SHALL be able to securely store authentication parameters, such keys, encryption mechanisms, etc. (Use Case 5.4.1)

3. The smart card MAY store data-allowing the establishment of a secure connection to the Device Management Server (UC 5.1.4).

4. Device Management Server SHALL be capable of manipulating a Device's Management object

(Use Case 5.1.3)

5. The data tree for containing Device management objects on the Smart Card SHALL be capable of being modified (i.e., nodes or data fields added or deleted), read from, and/or written to. (Use Case 5.1.3)

6. The Device Management Server SHALL be capable of manipulating a Management object resident on a Smart Card

(Use Case 5.1.3)

7. Smart card SHALL provide mechanism that allows efficient detection of its DM structure. (UC 5.1.3)

8. If the Smart Card is present, the Smart Card MAY be used to ensure authenticity, integrity and non-repudiation of session between Device and DMS. (Use Case 5.4.1)

9. The Smart Card MAY be used to store data in a secure fashion. (Use Case 5.4.1)

6.3.2.1 Interface to Device Management Servers

1. The Device Management Server SHALL be able to establish a data link with a Smart Card installed in a Device. (Use Case 5.1.3)

6.3.3 PC Agent

1. The PC agent SHALL to be able to support discovery of Devices so that it can identify those that should receive access rights to Devices in the local security domain. The PC MUST be able to authenticate and authorize further Device interaction. The PC is responsible for granting access rights to Devices under its control via the user's decision. (Use Case 5.1.5)

2. The mapping from friendly name to network unique name SHALL be the function of each user's user interface in the case where the Device is shared. (Use Case 5.1.5)

3. The PC agent SHALL be capable of launching the browser with an appropriate URL. (Use Case 5.1.5)

6.3.3.1 Interface to Devices

1. Any interested PC Agent SHALL be capable of listening to the standard multicast address for notifications that new Devices are available. (Use Case 5.1.5)

2. Protocols used SHALL be generally accepted and standardized (e.g. TCP/IP, http, https, Universal Plug and Play, etc) (Use Case 5.1.5)

3. Data links to Devices SHALL be over standardized, local and/or remote, wired and/or wireless bearers (e.g., Bluetooth, IR, USB, Ethernet, GPRS, etc.). (Use Case 5.1.5)

6.3.4 Overall Device Management Server

1. The Device Management Server SHALL be capable of discovering the presence of nearby, active Device Management clients if those elements are using compatible local bearers. (Use Case 5.1.1)

2. The Device Management Server SHALL support mutual authentication with the Device. (Use Case 5.1.1, 5.1.3, 5.4.1)

3. The Device Management Server SHALL be capable of querying Devices for information about Device properties, configuration, and capabilities. (Use Case 5.1.1, 5.1.3, 5.4.1)

4. The Device Management Server SHALL be capable of querying the Smart Card for information about Device properties, configuration, and capabilities. (Use Case 5.1.3)

5. The Device Management Server SHALL be capable of manipulating a Device's Device Management Object. (Use Case 5.1.1, 5.1.3, 5.4.1)

6. The Device Management Server SHALL be capable of manipulating a Management Object resident on a Smart Card'. (Use Case 5.1.3)

7. The Device Management Server SHALL be capable of capable of add/deleting/editing the fields of the Device's Device Management Object. (Use Case 5.1.1, 5.1.3, 5.4.1)

8. The Device Management Server SHALL be capable of add/deleting/editing the values of the Management Object present on a Smart Card. (Use Case 5.1.3)

9. The message from the Device acknowledging a device management operation SHALL contain an indication of success/failure of the operation. (Use Case 5.1.1, 5.1.3, 5.4.1)

10. The Message from the Device acknowledging a device management operation SHALL contain an indication of success/failure of the operation. (Use Case 5.1.3)

11. The DM Server SHALL be capable of sending a request for User confirmation to the Device, and accepting the response from the Device. (Use Case 5.4.1)

12. The DMS SHOULD be capable of receiving fault messages from a Device, and if supported the DMS SHALL provide a standardized mechanism for publishing the messages. (Use Case 5.4.1)

13. The management server SHOULD be able to poll devices for faults. (Use Case 5.4.1)

14. The Device Management Server SHALL be able to establish a secure data connection to the Device. (UC 5.1.3, 5.1.4, 5.2.1)

15. The Device Management Server SHALL support group addressing of Devices in order to transfer the changed management objects for them. (UC 5.2.1)

16. For the Device Management Server to be able to differentiate between the new and current configuration of a Device, Management Object data definitions SHALL specify canonical value representations and associated rules for unambiguous comparison. (UC 5.2.1)

17. Management Object data definitions SHOULD be composed from a common set of basic data types rather than by specifying new data types.

18. The Device Management Server SHOULD support at least one wireless data bearer. (Use Case 5.4.1)

19. The Device Management transactions SHOULD be annotated with sufficient information to enable the Device Management Server to detect the lack of response of Device in a specified time interval. (Use Case 5.4.1)

21. The Device Management Server MUST report errors in a standardized format. (Use Case 5.4.1)

22. The Device Management Server MUST verify integrity of data prior to download to Device. (Use Case 5.4.1)

23 The Device Management Server MUST be able to verify that software and/or data is from an approved Software Originator or agent thereof. (Use Case 5.5.1)

24. The Device Management Server MUST be able to detect when a Device that needs a software and/or data update. (Use Case 5.5.1)

25. The Device Management Server MUST be capable of determining that the Device is authorized to receive the software and/or Data. (Use Case 5.5.1)

26. The Device Management Server MUST be capable of interrogating the Device as to its capabilities and to determine from this information if the Device is capable of receiving the software/data download using a mutually agreed upon method and format. (Use Case 5.5.1)

27. The Device Management Server MUST be capable of exchanging security credentials with the Device. (Use Case 5.5.1)

28. The Device Management Server MUST be capable of transmitting the software and/or data to the Device. (Use Case 5.5.1)

29. The Device Management Server SHOULD be able to verify, either independently or with the help of a Trusted Authority, the validity of the Software Originator of the Software and/or Data to be downloaded. (Use Case 5.5.1)

30. The Device Management Server SHOULD be able to verify that the downloaded Software and/or Data is targeted to a particular Device. (Use Case 5.5.1)

32. The Device Management Server SHALL be able to query a Device for an inventory of its installed software.

33. The Device Management Server SHALL support group addressing of Devices in order to query multiple Devices for the purposes of a common update/upgrade to those Devices. (Use Case 5.3.1)

34. The software inventory reported from the Device SHALL be in standardised format. (Use Case 5.3.1)

6.3.4.1 Interface to Devices

1. Data links between the Device Management Server and Devices SHALL be over standardized, local and/or remote, wired and/or wireless bearers (e.g., Bluetooth, IR, USB, Ethernet, GPRS, etc.). (Use Case 5.1.1, 5.1.3, 5.4.1)

2. Network/Device Management Server SHALL be capable to discover a new combination of Subscriber and Device attached in the Network (UC 5.1.4).

3. Interface supports traversal of corporate firewalls and Network Address Translators (Use Case 5.1.2)

4. The DMS MUST support secure connectivity via HTTPS. (Use Case 5.1.5)

5. Protocols used SHALL be generally accepted and standardized (e.g. TCP/IP, http, https, Universal Plug and Play, etc) (Use Case 5.1.5)

7. The Device Management Server and the Device MUST be able to exchange their respective capabilities and select a set to be used for the download. (Use Case 5.5.1)

9. The Device Management Server MUST be able to process the response from the Device indicating the success or failure of the download. (Use Case 5.5.1)

6.3.4.2 Interface to other Device Management Servers

1. Interface SHALL support traversal of corporate firewalls and Network Address Translators (Use Case 5.1.2)

2. Interface SHALL be discoverable (Use Case 5.1.2)

3. The Device Management Server MUST support secure connectivity via HTTPS. (Use Case 5.1.5)

4. The Device Management Server SHALL expose a standard interface for obtaining Network parameters (Use Case 5.1.2)

6.3.4.3 Interface to External

1. Device Management Server SHALL provide an interface for receiving subscriber data remotely, which is needed to identify the Device or smart card of new subscriber. (UC 5.1.3)

2. Device Management Server SHALL provide an interface that allows the user to trigger the transfer of configuration data (UC 5.1.4).

3. Device Management Server SHALL provide an interface that allows the Management Authority to initiate the transfer of (updated) configuration data. (UC 5.2.1)

6.3.5 Network Interfaces

Requirements covered in other sections

7. Resources to be managed in the Device (Informative)

This section provides an overview of the resources which are candidates for being managed using the Device Management mechanism. Categories of parameters and the parameters themselves that are listed in association with a resource are **informative only** – they are meant to provide guidance, and are not an exhaustive list of required parameters for particular capabilities, applications, or other Device characteristics.

There may be some special conditions or expectations around the presence, access, or manipulation of managed resources that should be taken into account when defining parameters and some of those conditions are noted here:

- Note that not all resources may be available at a given time depending on a number of factors, such as the presence of accessories or permissions associated with a resource. For example, in Devices with a smart card, some parts of the resources managed in the Device may be specific to a certain IMSI, for example the username & password associated with a bearer. These shall only be active if the specified IMSI is inserted in the Device.

- Time-sensitive resources shall be noted as such and their configurability specified such that it is possible to ascertain when such settings apply. For instance, some settings may have one or more time periods with distinct start and stop clock times. Other such settings may only be active for a period measured by cumulative use.

- For operationally critical resources it shall be possible to locally or remotely revert the handset back to using a previously working value of the resources, should the new settings fail (e.g. software defined radio). Critical resources should be supported by adequate fault management on or off the Device as appropriate.

- Management data may be set originally by OMA bootstrap methods, then read and maintained via Device Management. Subsequent to booting, resources may be created, added, deleted, or modified in accordance with any implementation of Device Management or OA&M mechanisms.

7.1 Applications Requiring Managed Resources

- Following is a non-exhaustive list of common mobile applications that are expected to be supported by managed resources. The list of applications may be appended and special requirements pertaining to their managed resources may be noted in this section. However, the categories of managed resources presented in a subsequent section are intended to be applicable to the Applications listed here as well as additional applications that are added. The addition or modification of managed resource parameters should reference back to specific applications or use cases as presented in this document. The current list of Applications are:

- Multi-Media Messaging Service

- E-mail

- Instant Messaging

- Internet Browser

- Device Synchronization

- Device Management Agents

7.2 Application and Service Resource Categories

The categories of Managed Resources required by some or all of these Applications are detailed in this section and are comprised of:

- Connectivity
- Device Physical
- Security
- Performance
- Billing
- User Preferences & Customization
- Other

In the following tables the Default Actor "Management Authority" is abbreviated **MA**.

Change Policy has generic settings as follows:

- Without Authorization, implying no or weak authentication. Usually applies to User or Subscriber modifiable resources – abbreviated **W/O A**
- With Authorization, implying data integrity required, authentication with cryptographic means. Usually associated with Network or Service Provider Management Authorities, Enterprise/IT Administrators, or other MA Delegates. – abbreviated **W/A**
- Unknown (which may mean it's ambiguous) – abbreviated **Unk**

Application	Resource Category	Application-specific Parameters	Notes
MMS	Connectivity	MMS Relay/Server address MMS Bearer Type MMS NAP Address MMS Gateway Address MMS Port Number	
	Security	MMS Server Authentication Params MMS Gateway Authentication Params	
	User preferences	MMS User Preferences Profile Name MMS Sender Visibility MMS Issuance of a Delivery Report MMS Receipt of a Read Report MMS Message Priority MMS Message Time of Expiry MMS Earliest Delivery Time for Message	

Application	Resource Category	Application-specific Parameters	Notes
IMPS	Application Specific	IMPS Application ID IMPS Application Provider ID IMPS Authentication Type (e.g. two-way) IMPS Address Type (e.g. E164)	
	Connectivity	IMPS Server Address IMPS Address Type (e.g. absolute, E164) IMPS Proxy Address IMPS NAP ID	
	Security	IMPS Application Authentication	
E-Mail	Connectivity	Service name Incoming Server Address Outgoing Server Address Reply Address Connection type (e.g. TLS, SSL)	
	User Preferences	Contacts List Address Book Download Headers	
	Security	Account Name Signature	
Internet Browser	Connectivity	Proxy used to access bookmark	
	User Preferences	Bookmarks/Favorites (e.g.,Title, Description URI, Icon, NAP)	
Data Synch	Connectivity	Database URL	
	User Preferences	DB Name, Content Types and Versions	
	Security	DB authentication username and password	

7.2.1 Application Data Resources

Resource	Parameters	Default Actor	Change Policy (Easy, Hard, Unknown)	Notes
Device Management settings	TBD	MA	W/A	
Data Synchronization settings	Application Service Access	User,	W/O A	

	Point, Server Name, Access Point Link, Proxy Information Link	Subscriber		

7.2.2 Connectivity

The following resources are mainly based on the OMA client provisioning data.

Resource	Parameters	Default Actor	Change Policy	Notes
Supported packet bearer settings - The information model associated with GPRS bearer settings is described in the OMA client provisioning Network Access Point parameter, for the case where the bearer relates to GPRS.	Packet Bearer (e.g. GPRS, SMS, …),	MA	W/A	The management authority may, for example, use this object to modify or add an APN definition in the Device.
Circuit switched data settings - The information model associated with circuit switched data settings is described in the OMA client provisioning Network Access Point parameter, for the case where the bearer relates to circuit switched data.		MA	W/A	
Proxy settings - The information model associated with this resource is described in the OMA client provisioning PXLOGICAL parameter..	WAP Gateway,	MA	W/A	
Application connectivity data - Application-specific protocol connectivity parameters are specified in Sec. 7.1	Application Service Access Point (address and port), Bearer, Server Name, Access Point Information Link, Proxy Information Link, URI Domain	MA	W/A	The Device may support fallback connectivity parameters in case the preferred connectivity profile fails. (See OMA-REQ-2002-0078, LS from MSIG). For any combination of: (a) application, (b) port number and (c) requested URI domain it shall be possible

				to specify the network access point (including bearer) and/or proxy to be used. Reference the information model in the OMA client provisioning APPLICATION and ACCESS parameters.

7.2.3 Device Physical

Resource	Representative Parameters	Default Actor	Change Policy	Notes
Device information - Device information gives a view on the parameters which identify and describe the Device.	Device Make, Device Model, OS Version, Memory Configuration, Display Characteristics, IMEI, IMSI, Phone Number, Connectivity Supported (e.g. GPRS, BlueTooth, 802.11x, etc.), Current Connectivity	MA	Unknown	Reference existing Device information management object defined by SyncML.
Time and Date - Needed to allow authorised parties to set the time and date on behalf of the customer.	Time Zone, Time, Time Format, Date, Date Format	MA, User	W/A, W/O A?	Useful in those cases where network identification and time zone is not supported by the visited network.
Peripheral Profile - List of peripheral support and their current usage	Peripheral List, Usage	MA, User	W/A, W/O A	

7.2.4 Security

Security Resources listed here are assumed to be generic, Device-wide attributes, whereas it is presumed that any Device Management system will define security models for the manipulation of the actual managed objects representing the resources.

Resource	Parameters	Default Actor	Change Policy	Notes
Certificate – A list of parameters that are required in order to provision the Device with security certificates:	Base64 Encoded Certificate, Certificate hash (used as the ID to identify the cert), Private key (If it is a client cert, the private key of the cert need to be specified separately when being transmitted to the Device together with the certificate), Owner (define who logically own this certificate, operator, corp, end user, etc), Certificate category (specify whether this is a root cert, a cert for application execution, a personal cert, etc)	MA	W/A	
Keys - One or more keys as required by Device, Applications, or Management Authority in general		MA	W/A	Separate keys per usage are possible.
Cryptographic Algorithms - Available cryptographic algorithms (and specification of how to access them)	Crypto Algorithm List	MA	W/A	
Trust Levels - Specification of the available trust level available and/or desired on the Device as a whole, useful for authentication choices	Available Trust Levels, Current Trust Level	MA	W/A	
Hardware Security Support - Identification of non-software security support, such as a built-in random number generator	Hardware Security List,	MA	W/A	Some question about how this may map to other Security parameters such as Trust Level (what does it enable?)
Authentication Profile - Authentication is used to verify the identity of the user or application. Base resource to be re-used by Applications, Services, or protocols. Multiple authentication mechanisms	Authentication level (specify the authentication is for which layer: app layer, transport layer, etc), Authentication Protocol	MA	W/A	

and associated parameters are anticipated.	(specify the auth protocol, such as Kerberos v5, NTLM, RADIUS, EAP, HTTP BASIC Auth, etcNote: different layer could have different auth protocols.			
Policy - Policies around how the security features of the Device are used. For instance, what level of trust is required for certain transactions or for different connections.	Trust Policy, Transaction Policy, Updates Policy, Connections Policy,	MA, User	W/A	
Authorization and Access Control – covers access to other resources at various levels in Device Management from applications and services to the managed resources themselves	Managed Resource ACLs, White List, Black List	MA	W/A	For particular applications there may be the need to allow (whitelist) or block (blacklist) connections explicitly, e.g. allowing only a predefined SMSC sender number for WAP Push.

7.2.5 Performance

Performance measurements can take multiple forms. For example, they may be high or low-water marks, accumulators, discrete samples, etc.

Resource	Parameters	Default Actor	Change Policy	Notes
Alarm Log - Reports on recent Device alarms	Log ID, Subscribers, Policy, Enabled Flag, Reports	MA	W/A	Local policy may be defined to account for retention or storage limits .
Fault Log - Reports on recent Device faults	Log ID, Subscribers, Policy, Enabled Flag, Reports, Severity Counts, Metrics	MA	W/A	Local policy may be defined to account for retention or storage limits .
Connectivity Bandwidth	Unit of Measure, Available,	MA	W/A	

	Preferred, Actual			
Traffic Load - Measurement(s) of network activity (bytes, packets, etc.)	Unit of measure (bytes, packets, …), Current Load, Historical Load, Dropped Packets	MA	W/A	
Application Load - Measurement indicating relative application usage of the Device	Number of Apps, Processor Utilization	MA	W/A	
Policy - One or more policies governing performance monitoring or acquisition	Schedules, Sample Rates, Logging Policy	MA	W/A	

7.2.6 Accounting and Billing

Resource	Parameters	Default Actor	Change Policy	Notes
Billing Information - Settings and data that are relevant both to the Device user's account with Network and Service Providers as well as billing descriptions utilized by such Providers.	Service Name, Trust Policy, Rate Name, Basis (time, volume, usage, etc.), Measurement Unit, Rate, Rate Unit	MA, User	W/A	For example, for handset based prepay solutions, resources may be defined to allow update of minutes remaining and the purchase thereof. See use case: 5.1.5.4. There may be different sets of data, some visible by user, some only by MA.
Policy - One or more policies governing authentication, usage limits, and so on.	Expiration, Trust Levels, Logging	MA	W/A	

7.2.7 User Preferences & Customization

Resource	Parameters	Default Actor	Change Policy	Notes
Background Picture	Picture File	User	W/O A	

Background Lighting	Color, Intensity	User	W/O A	
Audio	Volume, Tone, Output Component	User	W/O A	
Signature	Signature List, Application List, Current Choice	User	W/O A	
Language	Language List, Current Choice	User	W/O A	
Ring Tone	Ring Tones, Current Choice	User	W/O A	

7.2.8 Non-applications software and firmware

Resource	**Parameters**	**Default Actor**	**Change Policy (Easy, Hard, Unknown)**	**Notes**
System software	Operating system firmware, middleware, libraries and drivers	User, MA	W/A	These are resources that can be managed with standardized software download protocols, mechanisms and interfaces coupled with proprietary software to actually manage the Device.

7.2.9 Operator Menu

Resource	**Representative Parameters**	**Default Actor**	**Change Policy**	**Notes**
Operator Menu	Set of menu items on User Interface for list of services S_1, S_2 ,S_3 ,...	MA; i.e. the User is not able to modify the operator's menu.	W/A	The operator is able to download a complete menu system or part of a menu system to the Device via the Device Management System. The operator is able to select amongst the following options: - whether or not the user needs to accept the new or changed menu system - whether or not the new or changed menu system is activated as the primary user interface

7.2.10 Other Resources

The following are resources that do not fit neatly into other categories, but are worth taking into consideration.

Resource	Representative Parameters	Default Actor	Change Policy	Notes
Data Synchronization settings	Application Service Access Point, Server Name, Access Point Link, Proxy, Information Link	User, Subscriber	W/O A	
Application and Service Profile – List of applications currently installed, along with optional specific attributes	Upgrade version date, License information, Usage data, In use flag, Resources consumed (e.g. storage), Archived flag	MA	W/A	Not all applications are required to possess all attributes, though some small set might be mandatory. Needed to allow authorised parties, such as customer care or a software management server, to determine the current status of the applications authorised party has access right to.
Proximity & Social context	Proximity to Physical or Network services, Social Context	MA	W/A	Social context is a user-centric concept that covers the user's situation. Examples are being in a meeting (where documents may be made available), restaurant (and it's meal time), office vs. home (different connectivity or permissions), etc.

Appendix A. Change History (Informative)

A.1 Approved Version History

Reference	Date	Description
OMA-RD-DM-V1_0_0-20030902-A	02 Sep 2003	Approved by TP R&A

A.2 Draft/Candidate Version 1.2.0 History

Document Identifier	Date	Section	Description
Draft Versions OMA-RD-DM-V1_2	21 Jan 2005	All	Added informative appendix for requirements coverage.
	25 Jan 2005	All	Editorial changes.
	26 Jan 2005	All	Updated to correct template. Applied CR 2004-0133R2.
	03 May 2005	Filename Title page	Version changed from 1.2.0 to 1.2
Candidate Versions OMA-RD-DM-V1_2	07 Jun 2005	n/a	Candidate version approved by TP R&A OMA-TP-2005-0137R01-DM-V1_2-for-Candidate-approval

Appendix B. Additional Information

The requirements related with non-urgent use cases were transferred to another document OMA-REQ-2003-0342.

Appendix C. Requirements Coverage (Informative)

This appendix presents a table with the list of requirements and their coverage in the DM 1.2, DM 1.1.2 and CP 1.1 enablers. The possible coverages are: Fulfilled, Partly Fulled, Not Fulfilled, and Not Applicable.

Requirement	DM 1.1.2	DM 1.2	CP 1.1
1. Requirements			
1.1 High Level Functional Requirements			
1.1.1 Security			
1.1.1.1 General security requirements			
1. The authentication procedure MUST be strong enough to ensure that is not be possible for a third party to masquerade as a Device management server by spoofing its identity.	f	f	f
2. The client and sever MUST be capable of detecting replay attacks.	f	f	f
3. Architecture supports traversal of corporate firewalls and Network translation Devices (Use Case 5.1.2)	f	f	n/a
4. If end user confirmation is indicated by the Device Management Server, the Device will prompt for user confirmation before incorporation of configuration data. (Use Case 5.1.5)	f	f	n/a
5. Except for establishing the initial trust relationship (bootstrap) over the air, if end user confirmation is not indicated by the Device Management Server, the Device MUST NOT ask for user confirmation before incorporation of configuration data. (Use Case 5.1.5)	n/a	n/a	n/a
6. The non-repudiation of the session MUST be ensured. (Use Case 5.4.1)	f	f	n/a
1.1.1.2 Authentication			
Before any Device management operations can be carried out on the Device, it must conform to the following:			
1. The client MUST successfully authenticate the Device Management server (Use Case 5.2.1).	f	f	f
2. If the Device management operation is related to personal information then the user MUST successfully authenticate himself to the Device management server (Use Case 5.2.1).	n/a	n/a	f

3. The Device Management Server May also authenticate the Device (Use Case 5.1.1., 5.1.3, 5.4.1)	f	f	n/a
4. Whenever there is communication between Device Management Servers the Device Management Servers MUST mutually authenticate (Use Case 5.1.2).	nf	nf	nf
5. With local wireless interfaces, discovery is controlled between the PC Agent and Device. Secure association and authentication MUST be supported. The first connection requires a secure association be created between the Device and PC. (Use Case 5.1.5)	n/a	n/a	n/a
1.1.1.3 Authorisation			
Before the Device Management server can carry out any Device management operations on the Device, it must conform to the following:			
1. The Device Management server MUST be authorised to carry out any Device management operations on the Device (Use Case 5.2.1).	f	f	n/a
2. With local wireless interfaces, discovery is controlled between the PC Agent and Device. Secure association and authorisation MUST be supported. The first connection requires a secure association be created between the Device and PC. (Use Case 5.1.5)	n/a	n/a	n/a
1.1.1.4 Integrity protection			
1. All data communication between the Device Management Server and a Device MUST be integrity protected. (Use Case 5.1.1, 5.1.3, 5.4.1)	f	f	n/a
2. All data communication between Device Management Server MUST be integrity protected. (Use Case 5.1.2)	n/a	n/a	n/a
3. The Data Link between the Software Originator (or agent) and the Device Management Server MUST maintain data integrity. (Use Case 5.5.1)	n/a	n/a	n/a
4. The inventory SHALL be secure from alteration when sent by the appropriate integrity protection. (Use Case 5.3.1)	n/a	n/a	n/a
5. The downloaded software SHALL be secure from alteration by the appropriate integrity protection. (Use Case 5.3.1)	n/a	n/a	n/a
1.1.1.5 Confidentiality protection			
1. All data communication between the Device Management Server and a Device, that is personal to the user or confidential to the owner of the information (e.g. some network operator settings) MUST be confidentiality protected. (Use Case 5.1.1, 5.1.3, 5.4.1)	f	f	nf
2. All data communication between Device Management Servers MUST be confidentiality protected. (Use Case 5.1.2)	n/a	n/a	n/a
3. The Data Link between the Software Originator (or agent) and the Device Management Server MAY maintain data confidentiality. (Use Case 5.5.1)	n/a	n/a	n/a

4. The Data Link between the Device Management Server and the Device MAY maintain data confidentiality, where appropriate. (Use Case 5.5.1)	f	f	nf
1.1.1.6 Smart card security			
1. Provisioning data on smart card SHALL be protected against unauthorized modification. (UC 5.1.3)	f	f	f
2. It SHALL NOT be possible for the Smart Card to reveal any secret keys it holds (UC 5.1.3)	n/a	n/a	n/a
1.1.2 Recording			
1. The Device Management System SHALL provide sufficient information so that queries from the Device Management Server, reports from Devices, data downloads, and acknowledgements MAY be billed and tracked accordingly. (Use Case 5.1.1, 5.1.3, 5.4.1)	pf	pf	n/a
2. If a management authority causes delegation to occur among several Device Management Servers, the Management Authority MAY request from each DMS, and each DMS SHALL provide, reports of the operations performed in a device for tracking purposes (Use Case 5.1.1, 5.1.3, 5.4.1)	n/a	n/a	n/a
3. The session MUST be identified as customer-care-related. (Use Case 5.4.1)	n/a	n/a	n/a
4. The session MUST be uniquely identified. (Use Case 5.4.1)	f	f	n/a
5. If transactions are logged, server MUST log transactions with success indicator. (Use Case 5.4.1)	n/a	n/a	n/a
1.1.3 Administration and Configuration			
1. The DMS SHALL provide a standardized mechanism for publishing session/message transactions, such as confirmation requests and results, etc. (Use Case 5.1.1, 5.1.3, 5.4.1)	nf	nf	n/a
2. Confirmation request messages SHALL be uniquely identified and contain at least the subscriber id, data or data summary, and date/time. (Use Case 5.4.1)	pf	pf	n/a
3. Confirmation result messages SHALL be uniquely identified and correlated to the request. (Use Case 5.4.1)	f	f	n/a
4. Management Authority MAY be delegated by a primary Management Authority (one that has domain over a given set of Management Objects) to a secondary Management Authority. (Use Case 5.1.1)	f	f	n/a
5. The first connection MUST involve a secure association be created between the Device and PC. (Use Case 5.1.5)	n/a	n/a	n/a
6. The DMS shall send a notification of the update/upgrade to the appropriate management authority. (Use Case 5.3.1)	n/a	n/a	n/a

1.1.4 Usability			
1. If user confirmation is indicated by smart card data, the Device SHALL ask for user confirmation before incorporation of provisioning data (stored on smart card).	nf	pf	nf
2. If user confirmation is not indicated by smart card data, the Device MUST NOT ask for user confirmation before incorporation of provisioning data (stored on smart card). (UC 5.1.3)	n/a	pf	n/a
3. If indicated by smart card data, the Device SHALL establish the connection to Device Management Server autonomously. (UC 5.1.3)	pf	f	pf
4. If user confirmation is indicated by the Device Management Server, the Device SHALL ask for user confirmation before incorporation of configuration data (transferred by Device Management Server).	f	f	n/a
5. Except for establishing the initial trust relationship configuration (bootstrap) over the air, if user confirmation is not indicated by the Device Management Server, the Device MUST NOT ask for user confirmation before incorporation of configuration data (transferred by Device Management Server). (UC 5.1.3, 5.1.4, 5.2.1)	n/a	n/a	n/a
7. The Device MAY be capable for being contacted by the Device Management Server, if the Device is busy by a voice link. (UC 5.2.1)	n/a	n/a	n/a
8. User is not prompted if there is no work to be done (Use Case 5.1.5)	f	f	n/a
9. Management Authority MAY clarify implications of subsequent actions (query, etc.) to the User. (Use Case 5.4.1)	f	f	n/a
10. User voice calls MUST NOT be terminated upon reception of the query. (Use Case 5.4.1)	nf	nf	n/a
11. User voice calls MUST NOT be terminated upon reception of the authorization request. (Use Case 5.4.1)	n/a	n/a	n/a
12. Authorization MUST be clear esp. regarding privacy issues and warranty. (Use Case 5.4.1)	n/a	n/a	n/a
13. User MAY be informed that the process is over. (Use Case 5.4.1)	f	f	n/a
14. The user SHALL be asked for confirmation to proceed before any software is updated. (Use Case 5.3.1)	n/a	n/a	n/a
15. The user SHALL be informed that the update/upgrade has been completed. (Use Case 5.3.1)	n/a	n/a	n/a
16. The Device MUST NOT send an inventory list of applications installed in the Device without either this optional feature being added by the user or the Device asks for permission from the user when needed.	n/a	n/a	n/a

### 1.1.5 Interoperability			
1. The DMS MAY be interfaced with a Customer Care application. (Use Case 5.4.1)	n/a	n/a	n/a
2. Errors MAY be reported to a Customer Care application. (Use Case 5.4.1)	n/a	n/a	n/a
### 1.1.6 Privacy			
Requirements covered in other sections			
## 1.2 Overall Systems Requirements			
1. The Device Management infrastructure MAY be based on a distributed architecture, wherein functional elements of the system (e.g., the Device Management Server) MAY consist of one or more coordinated, but physically separate entities. (Use Case 5.1.1)	f	f	f
2. The overall system SHALL support a distributed system architecture (Use Case 5.1.2)	f	f	f
3. Device Discovery by the Device Management Server MUST be clearly defined (e.g. SMS, push.). (Use Case 5.4.1)	f	f	f
5. The Device Management System SHALL make provision for different Management Authorities (e.g. Enterprise, Network Operator) to manage different data sets or applications in a single device. Each Management Authority can control data sets and applications owned by that Management Authority.	f	f	f
## 1.3 System Elements			
### 1.3.1 Device			
1. The Device SHALL be capable of discovering the presence of nearby, active Device Management system elements if those elements are using compatible local bearers. (Use Case 5.1.1)	n/a	n/a	n/a
2. The Device SHALL be able to communicate all of its relevant properties (e.g., manufacturer, model, firmware, etc.) to the Device Management Server on demand. (Use Case 5.1.1, 5.1.3, 5.4.1)	f	f	n/a
3. The Device SHALL be able to communicate its capabilities and configuration (e.g., WAP/MMS settings, installed software applications, etc.) to the Device Management Server on demand. (Use Case 5.1.1, 5.1.3, 5.4.1)	pf	pf	n/a
4. The Device SHALL be capable of autonomously (i.e., without User interaction) accepting and storing downloaded Management Objects (e.g., parameters, software, etc.) after the one time initial trust relationship configuration (bootstrap) is performed. (Use Case 5.1.1, 5.1.3, 5.4.1)	f	f	n/a

6. The data tree for containing Device management objects on the Device SHALL be capable of being modified (i.e., nodes or data fields added or deleted), read from, and/or written to. (Use Case 5.1.1, 5.1.3, and 5.4.1)	f	f	n/a
7. The Device SHALL be capable of receiving and displaying a command from the DM Server to request User confirmation for a management action. (Use Case 5.4.1)	f	f	n/a
8. The Device SHALL be capable of accepting User input regarding confirmation of a proposed management action, and sending the result of that confirmation to the DM Server. (Use Case 5.4.1)	f	f	n/a
9. The Device SHALL be able to acknowledge the receipt and installation of data downloaded from the Device Management Server. (Use Case 5.1.1, 5.1.3, 5.4.1)	pf	f	n/a
10. The Device SHALL be capable of detecting the presence of provisioning data on an installed, activated Smart Card. (Use Case 5.1.3)	pf	f	f
11. The Device SHALL be capable of autonomously establishing a data link with the Device Management Server, using connectivity information stored on the Smart Card. (Use Case 5.1.3)	pf	f	pf
12. The Device SHALL be capable of participating in a mutual authentication with the Device Management Server, using authentication credentials (e.g., a challenge response) stored on or derived from the Smart Card. (Use Case 5.1.3, 5.4.1)	pf	pf	f
13. Device SHALL retrieve and incorporate relevant configuration data stored on the smart card into the Device's DM structure. (UC 5.1.3)	pf	f	f
14. Each Device MUST support standardized dynamic IP allocation when the Device is first connected to the network. If an IP address cannot be allocated from the network, then the Device MUST use automatic IP addressing (Auto-IP) to obtain an address. (Use Case 5.1.5)	n/a	n/a	n/a
15. The Device SHOULD announce itself on the network to all control points it detects. The act of announcement does not imply the Device will receive rights, since assignment of rights is an expression of the user's decision. When the Device is added to the network, the discovery protocol allows that Device to advertise its services to control points on the network. The fundamental exchange in both cases is a discovery message containing a few, essential specifics about the Device e.g., its type, identifier, and a pointer to more detailed information. (Use Case 5.1.5)	n/a	n/a	n/a
16. The Device MUST support the assignment of a friendly name in relation to a network unique name(Use Case 5.1.5)	n/a	n/a	n/a

17. The mapping from friendly name to unique name MUST be the function of each user's user interface in the case where the Device is shared. (Use Case 5.1.5)	n/a	n/a	n/a
18. A method SHOULD be available by which a Device MAY automatically configure an interface with an IPv6 link-local address, IPv4 address in the 169.254/16 range that is valid for link-local communication on that interface, or both. On top of this there is a requirement to be able to define the link-local configuration to enable hosts that support multi-homing (more than one active interface and/or, more than one active address per interface, both IPv4 and IPv6 addresses, or a combination of these).This requirement is especially valuable in environments where no other configuration mechanism such as DHCP is available. (Use Case 5.1.5)	n/a	n/a	n/a
19. The Device SHOULD support IP based Device discovery based on the SSDP [http://www.upnp.org/download/draft_cai_ssdp_v1_03.txt]. The Device SHOULD support a 30 minute suggested timeout for when a Device is added or disappears from the network. (Use Case 5.1.5)	n/a	n/a	n/a
20. If end user confirmation is indicated by the Device Management Server, the Device will prompt for user confirmation before incorporation of configuration data. (Use Case 5.1.5)	f	f	n/a
21. PC Agent SHALL be capable of changing the DM tree on the Device and install the application (Use Case 5.1.5)	f	f	n/a
22. The Device MAY support concurrent voice calls and data exchanges. (Use Case 5.4.1)	n/a	n/a	n/a
23. The Device MUST support at least one wireless data bearer. (Use Case 5.4.1)	f	f	n/a
24. The Device MUST respond to query. (Use Case 5.4.1)	f	f	n/a
26. The Device MUST verify integrity of data before execution. (Use Case 5.4.1)	f	f	n/a
27. The Device MUST report to Server errors that occur during the parameter or software download. (Use Case 5.4.1)	f	f	n/a
28. The Device MUST be capable of determining that the Server is authorized to provide the software and/or data. (Use Case 5.5.1)	f	f	n/a
29 The Device MUST be capable of exchanging security information with the Server. (Use Case 5.5.1)	f	f	n/a
30. The Device MUST be capable of storing the software that is downloaded. (Use Case 5.5.1)	n/a	n/a	n/a
31. The Device MUST be able to independently verify the validity of the Software Originator of the Software and/or Data downloaded. (Use Case 5.5.1)	nf	nf	n/a
32. The Device MAY be able to verify, with the help of a Trusted Authority, the validity of the Software Originator of the Software and/or Data downloaded. (Use Case 5.5.1)	nf	nf	n/a

33. The Device MUST be able to verify that the downloaded Software and/or Data is targeted to the Device. (Use Case 5.5.1)	f	f	n/a
39. The Device SHALL send an inventory of its installed software to the Device Management Server. (Use Case 5.3.1)	nf	nf	n/a
40. The Device SHALL receive the software update/upgrade. (Use Case 5.3.1)	nf	pf	n/a
1.3.1.1 Interface to other Devices			
1. Data links between the Devices SHALL be over standardized, local and/or remote, wired and/or wireless bearers (e.g., Bluetooth, IR, USB, Ethernet, GPRS, etc.). (Use Case 5.1.1)	n/a	n/a	n/a
2. Protocols used SHALL be generally accepted and standardized (e.g. TCP/IP, http, https, Universal Plug and Play, etc) (Use Case 5.1.5)	f	f	f
1.3.1.2 Interface to Device Management Servers			
1. Data links between the Device Management Server and Devices SHALL be over standardized, local and/or remote, wired and/or wireless bearers (e.g., Bluetooth, IR, USB, Ethernet, GPRS, etc.). (Use Case 5.1.1, 5.1.3, 5.4.1)	n/a	n/a	n/a
2. Interface MUST support traversal of corporate firewalls and Network Address Translators (Use Case 5.1.2)	n/a	n/a	n/a
3. Interface MUST be discoverable (Use Case 5.1.2)	n/a	n/a	n/a
4. The Device Management Server MUST support secure connectivity via HTTPS. (Use Case 5.1.5)	n/a	n/a	n/a
5. Protocols used SHALL be generally accepted and standardized (e.g. TCP/IP, http, https, Universal Plug and Play, etc) (Use Case 5.1.5)	f	f	f
7. The Device Management Server and the Device MUST be able to exchange their respective capabilities and select a set to be used for the download. (Use Case 5.5.1)	f	f	f
8. The Device MUST be able to notify the server that it has accepted and successfully saved the downloaded software and/or data. (Use Case 5.5.1)	f	f	n/a
1.3.2 Smart Card			
1. The Smart Card SHALL be capable of storing Management Objects (e.g., network address(es)). (Use Case 5.1.3)	pf	f	f
2. The Smart Card SHALL be able to securely store authentication parameters, such keys, encryption mechanisms, etc. (Use Case 5.4.1)	nf	nf	pf
3. The smart card MAY store data-allowing the establishment of a secure connection to the Device Management Server (UC 5.1.4).	nf	f	pf

4. Device Management Server SHALL be capable of manipulating a Device's Management object (Use Case 5.1.3)	f	f	n/a
5. The data tree for containing Device management objects on the Smart Card SHALL be capable of being modified (i.e., nodes or data fields added or deleted), read from, and/or written to. (Use Case 5.1.3)	nf	nf	pf
6. The Device Management Server SHALL be capable of manipulating a Management object resident on a Smart Card (Use Case 5.1.3)	nf	nf	n/a
7. Smart card SHALL provide mechanism that allows efficient detection of its DM structure. (UC 5.1.3)	pf	f	f
8. If the Smart Card is present, the Smart Card MAY be used to ensure authenticity, integrity and non-repudiation of session between Device and DMS. (Use Case 5.4.1)	nf	nf	nf
9. The Smart Card MAY be used to store data in a secure fashion. (Use Case 5.4.1)	n/a	n/a	n/a
1.3.2.1 Interface to Device Management Servers			
1. The Device Management Server SHALL be able to establish a data link with a Smart Card installed in a Device. (Use Case 5.1.3)	nf	nf	n/a
1.3.3 PC Agent			
1. The PC agent SHALL to be able to support discovery of Devices so that it can identify those that should receive access rights to Devices in the local security domain. The PC MUST be able to authenticate and authorize further Device interaction. The PC is responsible for granting access rights to Devices under its control via the user's decision. (Use Case 5.1.5)	nf	nf	n/a
2. The mapping from friendly name to network unique name SHALL be the function of each user's user interface in the case where the Device is shared. (Use Case 5.1.5)	nf	nf	n/a
3. The PC agent SHALL be capable of launching the browser with an appropriate URL. (Use Case 5.1.5)	n/a	n/a	n/a
1.3.3.1 Interface to Devices			
1. Any interested PC Agent SHALL be capable of listening to the standard multicast address for notifications that new Devices are available. (Use Case 5.1.5)	n/a	n/a	n/a
2. Protocols used SHALL be generally accepted and standardized (e.g. TCP/IP, http, https, Universal Plug and Play, etc) (Use Case 5.1.5)	n/a	n/a	n/a
3. Data links to Devices SHALL be over standardized, local and/or remote, wired and/or wireless bearers (e.g., Bluetooth, IR, USB, Ethernet, GPRS, etc.). (Use Case 5.1.5)	f	f	f

1.3.4 Overall Device Management Server			
1. The Device Management Server SHALL be capable of discovering the presence of nearby, active Device Management clients if those elements are using compatible local bearers. (Use Case 5.1.1)	f	f	n/a
2. The Device Management Server SHALL support mutual authentication with the Device. (Use Case 5.1.1, 5.1.3, 5.4.1)	f	f	n/a
3. The Device Management Server SHALL be capable of querying Devices for information about Device properties, configuration, and capabilities. (Use Case 5.1.1, 5.1.3, 5.4.1)	f	f	n/a
4. The Device Management Server SHALL be capable of querying the Smart Card for information about Device properties, configuration, and capabilities. (Use Case 5.1.3)	nf	nf	n/a
5. The Device Management Server SHALL be capable of manipulating a Device's Device Management Object. (Use Case 5.1.1, 5.1.3, 5.4.1)	f	f	n/a
6. The Device Management Server SHALL be capable of manipulating a Management Object resident on a Smart Card'. (Use Case 5.1.3)	nf	nf	n/a
7. The Device Management Server SHALL be capable of capable of add/deleting/editing the fields of the Device's Device Management Object. (Use Case 5.1.1, 5.1.3, 5.4.1)	f	f	n/a
8. The Device Management Server SHALL be capable of add/deleting/editing the values of the Management Object present on a Smart Card. (Use Case 5.1.3)	nf	nf	n/a
9. The message from the Device acknowledging a device management operation SHALL contain an indication of success/failure of the operation. (Use Case 5.1.1, 5.1.3, 5.4.1)	f	f	n/a
10. The Message from the Device acknowledging a device management operation SHALL contain an indication of success/failure of the operation. (Use Case 5.1.3)	f	f	n/a
11. The DM Server SHALL be capable of sending a request for User confirmation to the Device, and accepting the response from the Device. (Use Case 5.4.1)	f	f	n/a
12. The DMS SHOULD be capable of receiving fault messages from a Device, and if supported the DMS SHALL provide a standardized mechanism for publishing the messages. (Use Case 5.4.1)	pf	pf	n/a
13. The management server SHOULD be able to poll devices for faults. (Use Case 5.4.1)	pf	pf	n/a
14. The Device Management Server SHALL be able to establish a secure data connection to the Device. (UC 5.1.3, 5.1.4, 5.2.1)	f	f	n/a

15. The Device Management Server SHALL support group addressing of Devices in order to transfer the changed management objects for them. (UC 5.2.1)	n/a	n/a	n/a
16. For the Device Management Server to be able to differentiate between the new and current configuration of a Device, Management Object data definitions SHALL specify canonical value representations and associated rules for unambiguous comparison. (UC 5.2.1)	f	f	n/a
18. The Device Management Server SHOULD support at least one wireless data bearer. (Use Case 5.4.1)	n/a	n/a	n/a
19. The Device Management transactions SHOULD be annotated with sufficient information to enable the Device Management Server to detect the lack of response of Device in a specified time interval. (Use Case 5.4.1)	n/a	n/a	n/a
21. The Device Management Server MUST report errors in a standardized format. (Use Case 5.4.1)	n/a	n/a	n/a
22. The Device Management Server MUST verify integrity of data prior to download to Device. (Use Case 5.4.1)	n/a	n/a	n/a
23 The Device Management Server MUST be able to verify that software and/or data is from an approved Software Originator or agent thereof. (Use Case 5.5.1)	n/a	n/a	n/a
24. The Device Management Server MUST be able to detect when a Device that needs a software and/or data update. (Use Case 5.5.1)	pf	pf	n/a
25. The Device Management Server MUST be capable of determining that the Device is authorized to receive the software and/or Data. (Use Case 5.5.1)	f	f	n/a
26. The Device Management Server MUST be capable of interrogating the Device as to its capabilities and to determine from this information if the Device is capable of receiving the software/data download using a mutually agreed upon method and format. (Use Case 5.5.1)	pf	pf	n/a
28. The Device Management Server MUST be capable of transmitting the software and/or data to the Device. (Use Case 5.5.1)	f	f	n/a
29. The Device Management Server SHOULD be able to verify, either independently or with the help of a Trusted Authority, the validity of the Software Originator of the Software and/or Data to be downloaded. (Use Case 5.5.1)	n/a	n/a	n/a
30. The Device Management Server SHOULD be able to verify that the downloaded Software and/or Data is targeted to a particular Device. (Use Case 5.5.1)	n/a	n/a	n/a
32. The Device Management Server SHALL be able to query a Device for an inventory of its installed software.	pf	pf	n/a
33. The Device Management Server SHALL support group addressing of Devices in order to query multiple Devices for the purposes of a common update/upgrade to those Devices. (Use Case 5.3.1)	n/a	n/a	n/a
34. The software inventory reported from the Device SHALL be in standardised format. (Use Case 5.3.1)	nf	nf	n/a

1.3.4.1 Interface to Devices			
1. Data links between the Device Management Server and Devices SHALL be over standardized, local and/or remote, wired and/or wireless bearers (e.g., Bluetooth, IR, USB, Ethernet, GPRS, etc.). (Use Case 5.1.1, 5.1.3, 5.4.1)	f	f	f
2. Network/Device Management Server SHALL be capable to discover a new combination of Subscriber and Device attached in the Network (UC 5.1.4).	n/a	n/a	n/a
3. Interface supports traversal of corporate firewalls and Network Address Translators (Use Case 5.1.2)	f	f	n/a
4. The DMS MUST support secure connectivity via HTTPS. (Use Case 5.1.5)	n/a	n/a	n/a
5. Protocols used SHALL be generally accepted and standardized (e.g. TCP/IP, http, https, Universal Plug and Play, etc) (Use Case 5.1.5)	n/a	n/a	n/a
7. The Device Management Server and the Device MUST be able to exchange their respective capabilities and select a set to be used for the download. (Use Case 5.5.1)	f	f	n/a
9. The Device Management Server MUST be able to process the response from the Device indicating the success or failure of the download. (Use Case 5.5.1)	nf	f	n/a
1.3.4.2 Interface to other Device Management Servers			
1. Interface SHALL support traversal of corporate firewalls and Network Address Translators (Use Case 5.1.2)	f	f	n/a
2. Interface SHALL be discoverable (Use Case 5.1.2)	n/a	n/a	n/a
3. The Device Management Server MUST support secure connectivity via HTTPS. (Use Case 5.1.5)	n/a	n/a	n/a
4. The Device Management Server SHALL expose a standard interface for obtaining Network parameters (Use Case 5.1.2)	n/a	n/a	n/a
1.3.4.3 Interface to External			
1. Device Management Server SHALL provide an interface for receiving subscriber data remotely, which is needed to identify the Device or smart card of new subscriber. (UC 5.1.3)	n/a	n/a	n/a
2. Device Management Server SHALL provide an interface that allows the user to trigger the transfer of configuration data (UC 5.1.4).	pf	pf	n/a
3. Device Management Server SHALL provide an interface that allows the Management Authority to initiate the transfer of (updated) configuration data. (UC 5.2.1)	n/a	n/a	n/a
1.3.5 Network Interfaces			
Requirements covered in other sections			