(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
7 May 2009 (07.05.2009)

PCT

(10) International Publication Number
WO 2009/056148 A2

(51) International Patent Classification:
H04L 29/06 (2006.01)

(21) International Application Number:
PCT/EE2008/000025

(22) International Filing Date: 27 October 2008 (27.10.2008)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
200700055 29 October 2007 (29.10.2007) EE

(71) Applicant (*for all designated States except US*): FROMDISTANCE AS [EE/EE]; Uus 2-4, EE10111 Tallinn (EE).

(72) Inventor: VIERUMÄKI, Jouko; Uus 2-4, EE10111 Tallinn (EE).

(72) Inventor; and
(75) Inventor/Applicant (*for US only*): VIERUMÄKI, Jouko [—/EE]; Uus 2-4, EE10111 Tallinn (EE).

(74) Agent: NELSAS, Tõnu; Aaa Patendibüroo Ou, Tartu mnt 16, EE10117 Tallinn (EE).

(81) Designated States (*unless otherwise indicated, for every kind of national protection available*): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

(54) Title: MOBILE DEVICE MANAGEMENT SYSTEM

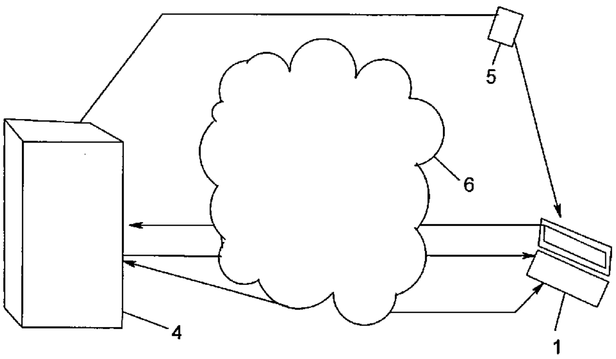

FIG 1

(57) Abstract: Mobile device management system comprises a mobile device, where is OMA DM (Open Mobile Alliance Device Management) interface, and a server. Management of the mobile device is executed through a proprietory OMA DM server. Using the management system of the invention it is possible to configure mobile phones, smart phones and computers, install, uninstall applications, set up restrictions to the end user, make backup copies, perform the inventory of the devices and applications and support the end users in trouble. Mobile device management system can be installed into client server or it can be as a remote service. In addition mobile device management system can be used for distribution of software (including silent install), sending messages to users (with secure, reported delivery), generation of reports, taking back-ups of devices (and restoring data to devices), accessing devices remotely, and other similar. MDM client is normally invisible to the end user.

Mobile device management system

Field of the invention

The present invention relates to management of mobile devices, especially mobile phones.

Background

US2005055397 discloses method and system that extends the functionality of the Open Mobile Alliance (OMA) Device Management (DM) standard to manage vendor specific configuration parameters and settings. An OMA DM structure is provided as an extension to the tree structure of the OMA DM standard. The OMA DM extension allows selected vendor specific parameters and settings to be managed under the OMA DM protocol.

In prior art the management of mobile device uses Open Mobile Alliance (OMA) Device Management (DM). Existing mobile device management system includes a mobile device, having (OMA) (DM) support, and (OMA) (DM) server.

Between the (OMA) (DM) interface of the mobile device 1 (look figures 1 and 3) and resources of the device there takes place continuous data exchange. In need (OMA) DM server 4 sends a SMS 5 to the (OMA) DM client and initiates a session. Proprietary DM session can also be initiated manually by the user or it can be a scheduled connection (time schedule is saved in the (OMA) DM client device). Request from (OMA) DM client's device is sent via wireless network 6 (WLAN, CSD (GSM Data), GPRS, EDGE, WCDMA/UMTS (3G), Bluetooth) into server 4 to carry out an inventory of the user's resources (settings, user data, etc.).

In response to the session server transmits to the user's device necessary settings, themes, policies, software packages, requests for information, etc. There may be several requests and responses during proprietary DM session.

Solutions known in the prior art do not provide sufficient functionality for management of the devices.

Summary of the invention

In organisations are many mobile phones, smartphones and computers that can use mobile device management (MDM) system of the present invention, enabling information management or service provider of an enterprise to configure devices, install and uninstall applications, set restrictions for end users, take backups, collect inventory of devices and applications and support end users in case of trouble.

MDM system of the present invention is a client server solution with secure interface between the two. MDM system server may be installed on customer's server or it may be offered remotely as service.

All parameters related to device management are configured on MDM system server:

- Device security settings;
- Device connection settings;
- Blacklist of applications;
- List of mandatory applications;
- List of mandatory access points;
- Access point restrictions;
- E-mail settings;
- OMA DM operations;
- other similar.

All these settings can be set for individually selected devices and on bases of device models and/or user groups. Furthermore, MDM system can be used for:

- Distribution of software (including silent install);
- Sending messages to users (with secure, reported delivery);
- Transferring files to/from devices;
- Generation of reports;
- Taking back-ups of devices (and restoring data to devices);
- Restricting user activities;
- Accessing devices remotely (VNC, Virtual Network Computing);
- other similar.

MDM system client is normally invisible to the end user. It, however, monitors the device and its usage and is invoked in following situations:

- Blacklisted applications are either installed or run;
- Mandatory applications are not installed or running;
- Security settings of the device are compromised;
- A message is sent from the administrator to the end user;
- User should address an issue (like low memory).

MDM server is considered an administrator tool.

MDM client can be distributed in two ways:

1. Sending a link to MDM client using MDM server. MDM server has tool for sending OTA (Over-The-Air) SMS messages. Sending a link to MDM client installation package enables end user to open the link and install MDM client with very little effort. After installation, MDM client is activated either manually or by SMS.

2. Software package delivery

MDM client can be installed by the end users of the devices just like any application. In this case, the administrator needs to send MDM client to end users and to add their devices to the MDM server database. MDM clients are activated either manually or by SMS.

The method selected for distribution of MDM client normally depends on whether the devices get to their users via administrator or not.

After its first connection with the MDM server, MDM client shall continue connecting the server. Connection intervals are defined on MDM server - they can also be overridden by a manually given date and time. Also the user of the device may initiate a session with the MDM server manually.

All additional settings on the devices are controlled and/or deployed within normat client-initiated sessions remotely.

Server-initiated sessions

When MDM server needs to initiate a session with MDM client SMS is used to trigger the session. The need for server-initiated activity may be caused by some of the following reasons:

1. Connectivity (access point) settings on mobile device need to be altered in order to connect to MDM server.

2. Confidential data on mobile device needs to be erased in case of theft or loss

3. Server access information (server address and/or password) needs to be changed unexpectedly.

4. Sessions need to re-scheduled (a session should take place immediately).

5. Remote device access session is started. In this case, after receiving the SMS, an SSH tunnel is opened from device to MDM Server. This allows VNC connection to be established between device and Java-based VNC client.

Deployment and monitoring of security settings

Security settings of devices are fundamental for any security scheme deployed within an enterprise. These settings include parameters related to Bluetooth settings as well as deployment of lock codes of the devices. The company policy on these settings can be defined in MDM server, while MDM client takes care of deployment of the defined policy. It is up to the administrator to decide whether end-user needs to approve the policy prior to deployment or not. Should the user need to approve changes, MDM client will ask for his/her approval and make the settings automatically. In no case the administrator has a need to write device-specific instructions for the users in order to deploy a security policy.

All security settings may be targeted to defined device models and/or user groups as well as individually selected devices.

Distribution and monitoring of applications installed and/or run on devices

MDM makes provisioning of software to mobile devices easy and efficient. MDM Server offers tools for making software available for devices - furthermore, it allows administrators to monitor applications that have been installed and run on devices. Silent installation and uninstallation of software is supported.

Different software packages may be targeted to different device models and different user groups as well as individually selected devices.

MDM server generates a report that helps the administrator to understand the install base of applications. This is particularly helpful when purchasing or managing software licences.

Messaging

The messaging function of MDM is a complementary channel for getting messages to end users. The messages are delivered within normal MDM sessions, making them a cost-efficient way to broadcast messages.

MDM follows delivery of messages, enabling the administrator to see when messages have been sent to users and when they actually become read.

Remote access to device

MDM system according to the invention facilitates remote desktop access to mobile devices. This feature is particularly useful for helpdesk and troubleshooting. Like in the screenshot below, device doesn't need to have 3G or WLAN connectivity.

Remote access is based on VNC and it allows administrator to access all device functionalities. User's permission is always prompted before remote access session is established for privacy reasons.

File transfers

Selected MDM clients may be commanded to fetch any files from MDM server in a secure manner. Also, files may be pulled from selected devices to server side; files and folders may be created and deleted etc. No user involvement is needed. After each transaction - if administrator chooses so - a message written by administrator is displayed to the user. Delivery and execution of each file command is tracked.

File commands may be executed in batches where execution of a command is conditional to successful execution of the previous command.

Back-up/restore

Key personal data - like contacts, calendar (with meeting notes) and messages - can be backed up over the air. Back-ups may be taken from one type of device and restored to another. For instance, data backed up from a Windows Mobile device may be restored to a Series 60 mobile device device or vice versa. No user involvement whatsoever is required for either back-up or restore. Back-up and restore commands may be executed for selected device(s) or the whole device base.

Execution of commands on selected devices

Any application on selected devices may be executed automatically, with or without parameters. Also, any file may be launched on the device; application associated with the corresponding file extension will be used to process the file.

Certificates may be installed on devices, OMA DM (Open Mobile Alliance Device Management) commands may be executed, devices may be rebooted etc. Progress of execution commands is tracked.

Country information

When a device arrives to a new country and registers itself to any mobile network (not necessarily yet being able to connect to the Internet), MDM client displays a country-specific message written by administrator. The contents of these messages are automatically pushed to all devices during normal connections.

With these country-specific messages it is possible - for instance - to instruct users to use a specific network or warn them of problems with GPRS roaming etc. In many cases significant savings can be achieved by selecting correct network for roaming.

Detonation of confidential data

MDM can be used to detonate confidential data on lost or stolen devices. This task can be executed by sending a special-content SMS to the device. Detonation of confidential data can also be performed during the course of a normal (client-initiated) session. This is the only option when device's SIM card has been replaced with another SIM card by an unauthorized device holder. Detonation erases all data from both device memory and memory card.

Technical notes

MDM Server is written with PHP, making it practically independent on the server platform to be used. It only requires (besides the PHP support) an SQL database (like MySQL, MS SQL Server or Oracle) and a web server (like Apache or IIS). Requirements for the hardware depend on number of devices and selected software environment (operating system, database, web server). However, any modern server with decent software environment is capable of handling a device base of thousands of devices with typical connection intervals. The user interface of MDM server is browser-based, so a web browser with JavaScript support is needed. For remote device access, also Java applets need to be supported by the browser.

Brief description of the drawings

Figure 1 depicts a prior art mobile device management system.

Figure 2 depicts a preferred embodiment of the mobile device management system according to the present invention.

Figure 3 depicts a prior art mobile device schematic diagram.

Figure 4 depicts a preferred embodiment of the mobile device schematic diagram according to the present invention.

Detailed description of the preferred embodiment

A preferred embodiment of the invention depicted in the figure 2 comprises (OMA) DM compatible device like for example mobile device 7, which is connected to proprietary device management server 9 via communication network 8. Between the (OMA) DM of the mobile device 7 and server 9 there is continuous data exchange. In need (OMA) DM server 9 sends to (OMA) DM client SMS 10 and initiates a session. Proprietary DM session can also be initiated manually by the user or it can be a scheduled connection (time schedule is saved in the (OMA) DM client device). Request from (OMA) DM client's device is sent via wireless network 8 (WLAN, CSD (GSM Data), GPRS, EDGE, WCDMA/UMTS (3G), Bluetooth) into the server 9 to carry out an inventory of the user's resources (settings, user data, etc.). In response to the session the server 9 transmits to the user's mobile device 7 necessary settings, themes, policies, SW packages, requests for information, etc. There may be several requests and responses during proprietary DM session. MDM system server 9 may be installed on customer's server or it may be offered remotely as service. MDM system server 9 may be based for example on OS Windows or Unix/Linux, data base of the MDM server may be based on known SQL database (like MySQL, MS SQL server or Oracle). MDM server 9 is connected to Administration interface 12, which is browser based interface for administering MDM server and for accessing devices remotely. The browser-based interface of MDM Server is used to monitor and control the device base equipped with MDM Clients. Into the mobile device 7 of the present invention in addition to the OMA DM interface 2 and device's resources 3 is also incorporated OMA DM server 13 and proprietary DM server interface 14 (see figure 4). In that specific solution the broader device management framework together with the smart DM client can be used as the overall framework - the more narrow OMA DM framework works in the mobile device 7 as a subset.

OMA DM interface can be used in two ways:

1) One can change settings of mobile device 7 using the framework and passing the necessary instructions from the DM server 9 to DM client (mobile device 7). The DM client then decides whether the changes on device are performed directly by the DM client by accessing/writing device resources - or, if it instructs OMA DM client to connect with the virtual OMA DM server 2 from where OMA DM client gets the necessary instructions and communicates them with device resources (look figure 4).

2) OMA DM instructions can be encapsulated (wrapped) into the DM server/client communication and passed directly to OMA DM client through the virtual OMA DM server 2. The difference to the previous option is that in this case the DM client doesn't necessarily understand the meaning of the instructions as such - it's just being used as a transport of the instructions between device and server-side infrastructure.

On device, proprietory DM client may access and write device 7 resources by itself (B), or it can invoke (OMA) DM client (A) to connect to local (OMA) DM server 2 and instruct the local (OMA) DM server (D) to feed/fetch necessary data (E) to/from device. Local (OMA) DM server 2 may also access/write device resources independently (C).

Claims

1. Mobile device management system that consists of a mobile device (1), which is connected OTA (over-the-air) to an OMA DM server (4) via the OMA DM interface (2), **characterized in that**, it has the OMA DM server on the mobile device and the management system contains the owner's OMA DM server (9).

2. Mobile device management system according to the claim 1, **characterized in that**, the mobile device (1) is connected to the owner's OMA DM server (4) so that with one session the DM server can send an unlimited number of OMA DM commands to a mobile device.

3. Mobile device management system according to the claim 1, **characterized in that**, the mobile device is configured to use its existing files as OMA DM commands parameters without having to resend the OTA.

4. Mobile device management system according to the claim 1, **characterized in that**, the mobile device is configured to create an OMA DM sessions without an external data connection.

5. Mobile device management system according to the claim 1, **characterized in that**, a proprietary DM client is configured to independently to manage mobile device resources.

6. Mobile device management system according to the claim 1, **characterized in that**, a proprietary DM client is configured to command OMA DM clients to connect to local proprietary OMA DM server and to read/write necessary mobile device information.

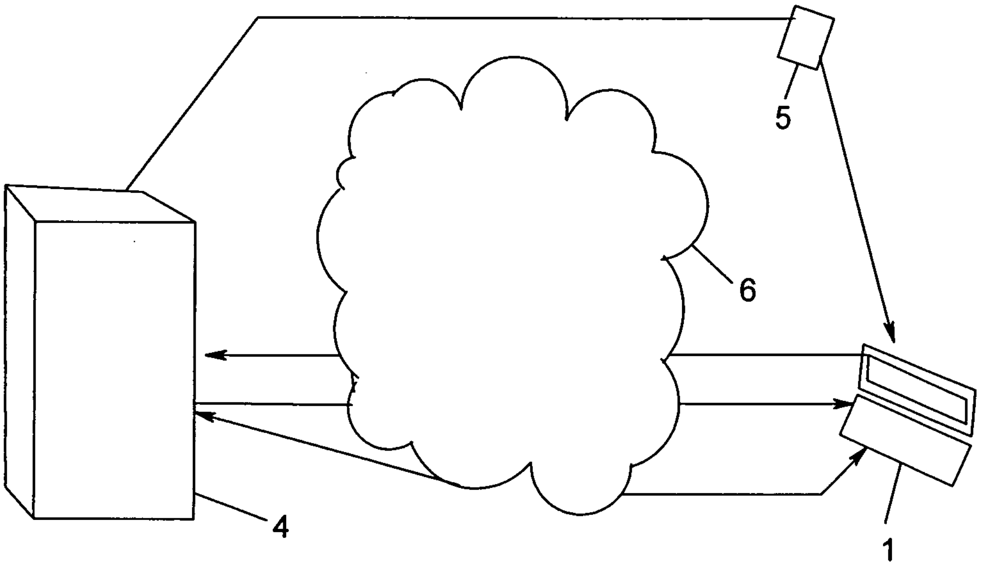

FIG 1

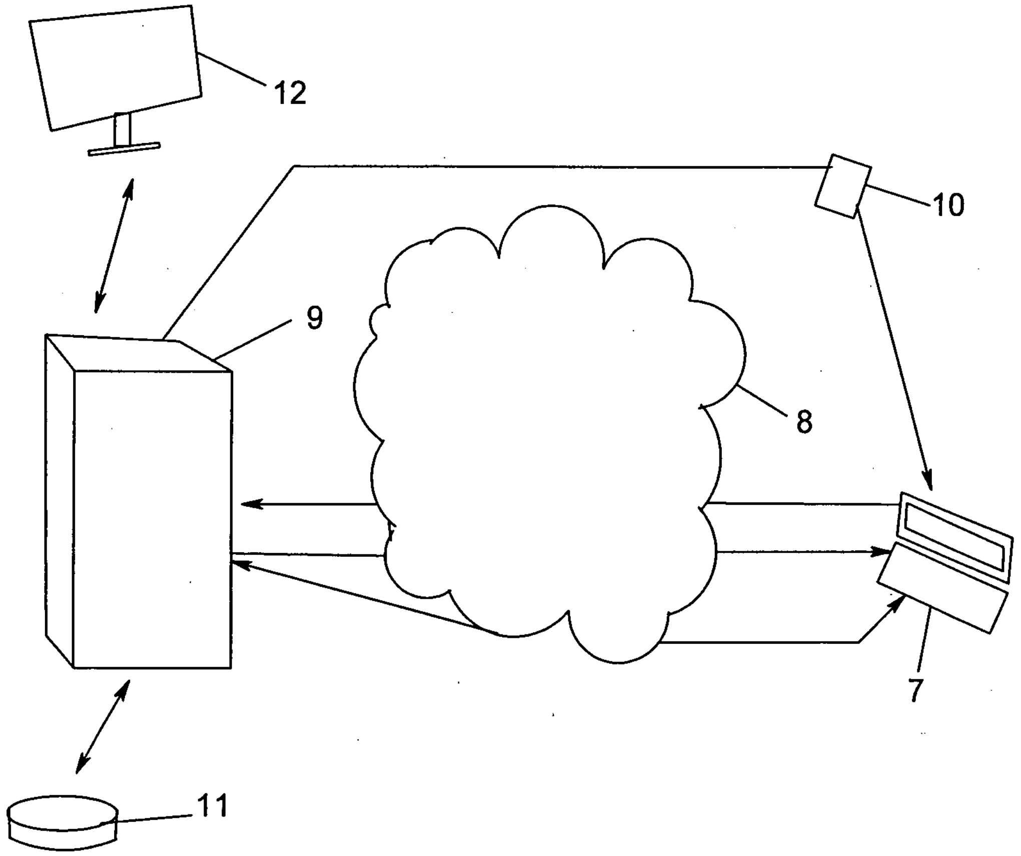

FIG 2

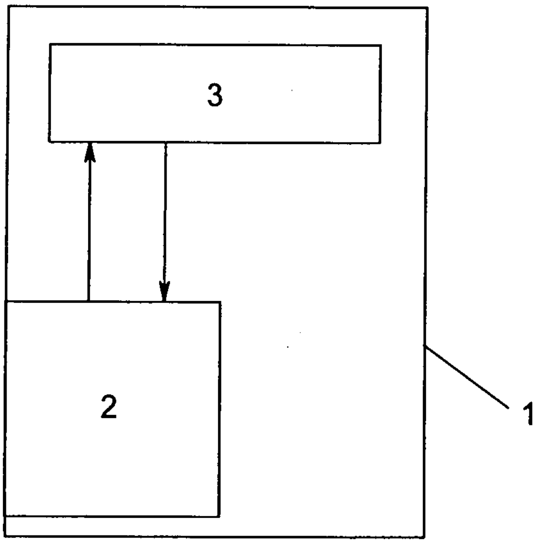

FIG 3

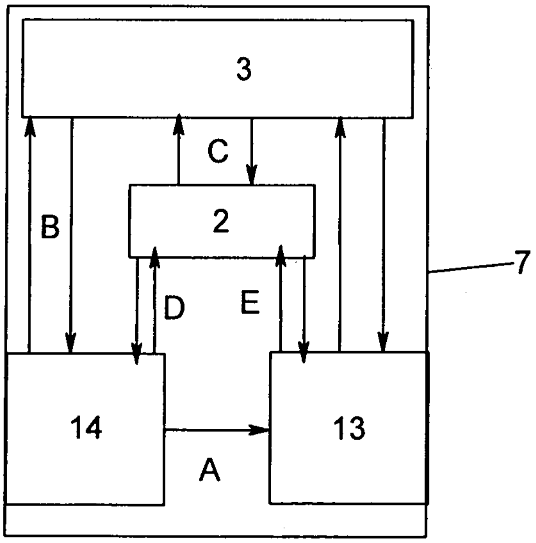

FIG 4