Emmanuel Dujardin

Device Management in 3G

With mobile handsets becoming increasingly powerful, computerised and complex, there are some new parameters to be configured to ensure the usability of Universal Mobile Telecommunications System (UMTS) and all related services. For many users these configurations might be a tricky undertaking. This might yield lower usage and revenue forecast from new services, or make things costlier for the customer. The sophisticated features of third-generation (3G) user equipment will require flexible means to support management of the user equipment, satisfying the need of end-users.

Working groups of the Third Generation Partnership Project (3GPP) and Open Mobile Alliance (OMA) are currently developing the standardisation of device management. Therefore, in order to ensure the success of this work, it is important to examine what requirements developed by standards can offer to the operators and manufacturers.

The complexity of 3G mobile terminal equipment is greater than the existing 2G equipment. Therefore, there is a higher risk that future terminals will include service-affecting problems and restricted functionality. This paper shows that *device management* can offer the basis for achieving the performance needed in 3G mobile. It also points to the remaining issues that must be solved for achieving a complete working system. It starts with a general description of device management, goes on to give an overview of functional requirements and device management features, and concludes by discussing industrial proposals and open issues.

What is the Scope of Device Management?

In the past few years the mobile Internet has developed impressively with the convergence of information technology (IT) activities. Small electronic devices with integrated operating system, extended memory and faster processing power have overflowed the market. Moreover, mobile devices like PDAs, phones (UMTS, GPRS/WLAN, UMTS/WLAN…) will be increasingly specialised and users may have lots of them. As far as many new data-oriented services like multimedia messaging service (MMS) and other multimedia systems are to be deployed in the future, provisioning will become a critical point. *Device management* will enable remote parameter manipulation or configuration, like wireless application protocol (WAP) settings and content delivery, on mobile devices. For the customers, it will improve the customer experience by providing devices with more features, applications and services. The services will be more relevant and more localised. And the potential configuration problems will be solved by a more efficient helpdesk. It will improve the management of mobile devices and enhance the mobile working efficiency. Moreover for operators, it will increase the service uptake and decrease the customer care cost while enhancing service level.

Why do Operators need Device Management?

The only acceptable means to manage the increasing numbers of mobile devices, including high-end smart phones and communicators, traditional phones, personal digital assistants, and embedded devices residing in such places as motor vehicles and soda machines, is remotely.

Next-generation terminals (advanced in chipsets, radio and communication protocols, operating systems, and application software) will support a multitude of new and complex services such as messaging, Internet access, streaming media, secured transaction and interactive multimedia. One should expect that problems with configuring or using services would limit the uptake of next-generation services. These devices will require new management and security capabilities.

Just as with today's PCs, mobile devices will require significant configuration and management mechanisms. The improvement of processes for fulfilment and assurance operations through automation of configuration management and remote diagnostics will enable devices to function effectively, reliably and securely.

Early mobile handling will intend to give to the vendors a way of handling early mobiles in case problems occur because of insufficient testing. It will enable the mobile network operator and other actors (telecom equipment manufacturer, independent

Author
Emmanuel Dujardin
France Telecom
Tel: +33 1 45 29 64 80
Email: emmanuel.dujardin@francetelecom.com

software vendor…) to manage the inherent problems associated with uncertainties in the introduction of new 3G technologies by supporting terminal reconfiguration.

Device management enables better protection of access network resources from attacks from rogue devices, roaming users and malicious users.

So the benefits of device management to the operator are:

- the ability to deliver new services to existing and new customers at lower costs;
- improved understanding of the customer environment and customer behaviours;
- concerning the terminal equipment, problem analysis at source and problem correction;
- faster time to market of new terminal devices with lower financial risks;
- enhanced brand recognition; and
- the ability to be able to market new functionality on new and existing devices.

Functional Requirements

This section identifies device management requirements in terms of provisioning, configuration, fault management, performance management and security.

Provisioning

Here, different user cases provide a good overview on provisioning:

A new device is purchased by a network subscriber in an authorised retail store and is provisioned with parameters. The device provisioning can be done via a local transport mechanism (IR, Bluetooth, local, wired, or wireless network).

A company purchases a new device via the Internet from a device vendor. The device is provisioned via a WAN bearer. The company obtains network parameters from the network operator before creating a setup program with enterprise-specific parameters (enterprise security, enterprise applications policy and preferences…) via a media card.

A new device is purchased which comes packaged with a smart card. The user inserts the smart card into the device and the user equipment is automatically provisioned with parameters from the smart card.

A customer purchases a new device via the Internet from a device vendor. To provision the device, the user places the new device in proximity to his/her PC that connects to the user equipment manager. The user equipment manager provisions the device via a secure network connection.

A subscriber acquires a device outside the operator's normal sales line. In this case an inappropriate configuration is very likely. The characteristics of the device are determined and transmitted to the operator's management server. (the subscriber's first time use of the device is detected automatically by the operator's infrastructure). The appropriate provisioning parameters are downloaded to the device.

Terminal configuration

Here, mobile terminals will be reconfigured to protect and optimise the use of access network resources. In addition, operating system (OS) upgrades may be necessary to enable deployment of new services. Some of these reconfigurations may be done without the consent of the mobile terminal user.

The radio channel in the terminal could be reconfigured manually or automatically to enable users to connect to access networks with a different radio interface to that originally configured in the terminal. (modify modulation techniques, wide-band or narrow-band operation and waveform).

Telecom firmware may be reconfigured automatically (based on a request from the service provider) to stop for example disruption on the access network by incompatible firmware in the terminal or to optimise access to the network.

The terminal OS and associated applications programming interfaces (APIs) may be reconfigured manually or automatically to enable the installation and operation of new services.

Application and service configuration

In this topic, mobile terminals may be reconfigured to download or disable/remove an application, upgrade applications, archive applications to a PC in case of memory limitation and backup/restore user data. The applications and user data can be stored in either the mobile terminal itself or a universal subscriber identity module (USIM). Furthermore the operator must be able to uninstall applications to the mobile terminal. And the operator must be informed whether the application has completed its tasks successfully.

Fault management

Error tracing is a procedure to determine if the terminal equipment is the cause when a problem is identified in the network.

Reports of significant events detected by the device are made available to the management system. The network operator determines a set of key events to be monitored by devices (hardware, software, connection, protocol, content, security errors).

The operator must be able to identify and locate the appropriate diagnostic/remedial application.

The remote terminal diagnostics procedures are used to collect diagnostic information from the mobile terminal, which may be used later for testing, fault localisation and recovery procedures. This requirement should not disrupt the service operation. Remote diagnostics may include signal strength, location, memory, applications, battery level, processor, signal quality, etc.

Performance management

The tracked enrolled devices will allow a customer service representative in the help desk to deal with queries more efficiently and will also allow measures to be taken to prevent the customer from having problems with services. The feature requires a set of the terminal equipment information that needs to be known: software version, applications resident on the terminal, application on the terminal, software parameter settings and configuration files, hardware configuration information, capacity of the memory and processor, network parameters, radio configuration settings, messaging configuration settings and security settings (PKI, passwords, etc.).

Moreover, the network operator's user equipment management (UEM) server periodically queries the customer's fielded user equipment (UE), which returns stored, time-tagged performance metrics and fault reports. The end-user may play a role in authorising or enabling the service provider to gather data about the terminal and its applications.

Security parameters and virus detection and control

As the terminals become ever more complex, there is a risk of viruses being spread through terminals. If terminals are affected, UEM must facilitate the virus detection to ensure the viruses are not spread. UEM must facilitate the testing of terminals and assist in the removal and restoration of data and applications resident on the user equipment. The virus detection and control procedure should use the application and service reconfiguration procedures to recover data and applications in the terminal.

Device Management Features

Actors

Figure 1 describes the interaction between the different entities involved in device management: user equipment supplier, user equipment manufacturer, the service provider content and the network operator (and its own customer care).

Figure 1 Interaction between actors in device management

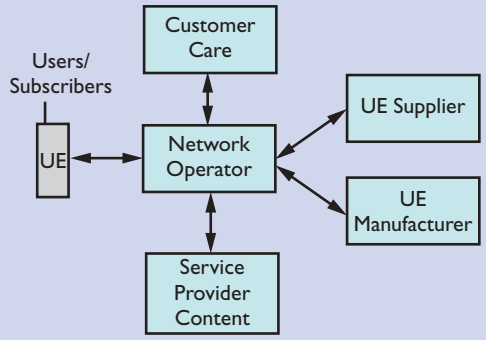
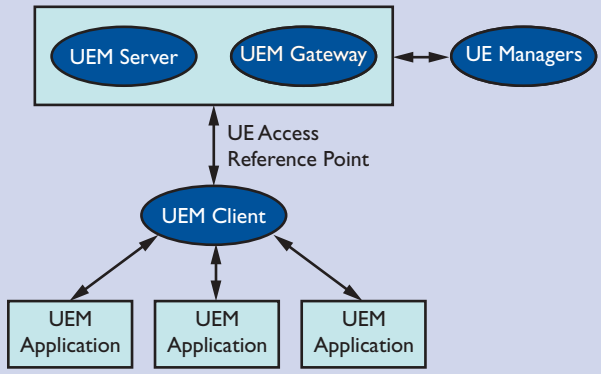


Figure 2 Logical architecture



Logical architecture

Several types of architecture can be used. Figure 2 is an example of the architecture and associated interfaces based on the client/server concept.

Components involved

Regarding Figure 2, the *UEM client* is the component required in the *user equipment* to collaborate with the management server to manage the *mobile equipment* and the *USIM*. It includes the *user equipment management application* that is executed on the user equipment to provide UEM functionality. The *UEM server* maintains the management clients' session information and forwards the results to the different *UE managers*: it enables the UE reconfiguration (but also service and application reconfiguration), the application error tracing, the remote UE diagnostics, the remote application diagnostics, performance measurements and virus detection and prevention. The UE managers use the *UEM gateway* to access the UEM clients. We can note that UE managers may be numerous. It gathers customer self-care service of the network operator, handset manufacturers, service and content providers, IT support, enhanced and application services, etc.). The UEM gateway provides access to the UE client from various UE managers. It is assumed that the network operator will own the UEM gateway and the UEM server.

Interfaces

The realisation of the UE access reference point enables the information exchange between the UEM server and clients. Based on the extent of UE equipment capability, this interface may be realised using various connection media and protocols.

Interfaces between UEM gateway and UEM managers are not standardised at this time (maybe never).

Protocols

The SyncML Dev Man is an available standard regarding protocol. Currently, all the interoperability testing is done on SyncML1.0, which basically focuses on synchronising personal information management (PIM) like address book/calendar to the mobile device. Exhibitions on device management have been shown at various events based on a SyncML client installed on the phone and communicating over the air with a SyncML DM server. For example, Motorola has demonstrated in the last SyncML congress in Amsterdam a device management application enabling the remote change of the volume and ring tone value and the clock/time zone value. Nokia and Ericsson have demonstrated device management applications enabling the remote change of the language used, the background of the screen, the remote change/set of the WAP configuration.

There is an initiative called *SyncML DM* in OMA that is focused on changing configuration parameters in the mobile device. Currently, this specification is under discussion; a meeting in Finland in June 2003 discussed more on interoperability testing: There is a proposal in SyncML DM to support firmware/binary update over the air.

Industry Proposals

It takes time for the standards to be released. So other proprietary device management solutions are developed.

What we called 'proprietary device management solutions' are, generally speaking, solutions that are not specified by an international body.

Possible solutions and key vendors on the market

Three solutions have been developed:

- *SIM-based solution (STK and/or Java card)*
  This solution is under control of the network operator independently of handset manufacturers. It needs IMEI (international mobile equipment identity), and update database. Its features are limited. This is a near-term solution. Examples include card providers' solutions like Gemplus STK based 'GemConnect', etc.
- *Terminal-based solution*
  A terminal-based solution can cover more features. It needs manufacturers' cooperation and this solution is a mid- and long-term solution. Several manufacturers' solutions are developing. For example, one of them may provide a solution based on the SyncML Device Management protocol. It could include configuration parameters that enable Internet connectivity, email connectivity, WAP connectivity, MMS settings, etc.
- *'Patch' solution*
  Patch solutions are also available but are manufacturer specific with limited features; for example, Sagem is a vendor of this solution.

Partnership with operators

Currently, operators are looking for an over-the-air (OTA) solution to set handset parameters, provision services, perform device software update—bug fixing, software version update—, improve device distribution/personalisation flexibility, perform handset remote diagnostic, network optimisation, etc. All these solutions may limit the impact on the operator network and be close to the standardisation specifications.

Today, an automatic solution with massive update capability able to address the majority of handsets—to come or already deployed—is urgent, even if there is currently no standard.

Even if operators have the best visibility in terms of a set of parameters/protocols used for devices which are going to be deployed, they are waiting for a maximum of autonomy from their solution provider: close relations with handset manufacturers.

To progress further on device management, vendors (Motorola, Siemens, Nokia, etc.), vendors' partners (DoOnGo, Bitfone,

Mformation, OpenPlug, etc.), handset manufacturers and network operators may organise meetings to progress on a global solution (handset management via OTA, standard API above OS handset, etc.).

Mutual Action Between Fora

3GPP SA5 UEM

User equipment management (UEM) is a capability that will allow the network and customer care operator, the service provider, the user equipment manufacturer, subscriber and user to manage the user equipment.

The Release 5 User Equipment Feasibility Study (TR 32.802) shows that user equipment management would bring a number of benefits to all the actors.

We can observe that 3GPP Release 6 UEM would be directed towards the three following capabilities:

- UE configuration query capability, which allows UE configuration information to be remotely requested and retrieved;
- UE reconfiguration capability, which builds upon the UE configuration query capability in that it allows configuration changes to be made to the UE remotely; and
- remote UE diagnostics capability to run diagnostic applications on the user equipment to aid fault resolution.

In June 2003, Release 6 was reviewed to avoid overlap between standards groups (see OMA versus UEM).

OMA Dev Man

A group called *Device Management* (DevMan) is working on the management of the handset. This working group has provided a quick analysis of the device management functional requirements.

It is one technical working group specifying DM specifications but the requirements are defined in the OMA Req group. The OMA DM group is responsible for implementing the new requirements.

Regarding the next version, the release timeline has not yet been set. The intention was to have an approved requirements specification in May 2003. Part of the use cases are already included in the SyncML DM and WAP client provisioning release.

The use cases covered by DevMan include: UC provisioning, UC remote configuration, UC software management, UC fault detection, query and reporting, UC backup and restore.

WAP and SyncML activities are now part of OMA. WAP Forum has released WAP client provisioning and SyncML has released SyncML DM. WAP 2.0 and SyncML DM 1.1.1 will be released by OMA.

OMA versus UEM

According to SA5 Chairman, even if OMA take in charge completely the work on device management, SA5 will still need to do additional work to apply device management to the 3GPP networks, and so a new work item is necessary. OMA may well be specifying the details of device/user equipment management from the device perspective, but SA5 will have to ensure that the management is integrated with the rest of the 3GPP O&M solution.

Further work in SA5 will include 3GPP telecom management infrastructure aspects including the UEM manager, UEM gateway and charging.

Other Fora (TMF and MMF)

Other standards bodies are also involved in the definition of device management:

The goal of TMF (TeleManagement Forum) is to help service providers and network operators automate their business processes in a cost- and time-effective way. In a Catalyst Project, the Mobile Terminal Equipment Management group is deliberating on activities (like configuration (including software versions)) required to deliver in time for early deployments of UMTS technology.

The Mobile Management Forum has identified some activities to define the future standards for mobile device management and provisioning (DMaP). Their work items include:

- creating a mobile device management and provisioning requirements and issues document;
- creating scenarios to reflect the mobile device management boundary less information flow;
- creating proposals for the definition of new standards and the enhancement of existing standards that have a bearing on the management of mobile devices; and
- creating a set of device management and provisioning certification requirements and issues to support the proposed standards.

Strength and Weakness

From most operators' point of view, the user management framework covers mainly the following needs. Each point covers requirements in near/mid and long term:

- provisioning (the automatic configuration of parameters in the handset);
- monitoring and diagnostics;
- bug fixing (which should be of interest to the handset manufacturers);
- software back-up and restore (data synchronisation, etc.);
- software update (applications, services, but also in the SIM card (this last point joins the provisioning part), etc.) and
- OS update and firmware update (to remotely repair software).

To sum-up the opportunities are:

- reduce cost regarding customer care, terminal validation, bug fixing;
- network optimisation;
- enhancement usage (service distribution and feature update);
- improvement of operator's branding.

The weakness and threats are:

- The radio resource consumption (when we use OTA case configuration).
- Needs in term of more detailed (IMEI…) and unified (parameters and infrastructure data, shared data and personal data) database regarding the user profile. (Develop mutual action with generic user profile developed by 3GPP.)
- Lack of clear responsibility between operators and manufacturers. We need to separate operators' needs from handset manufacturers' needs. Stakes for the operator are provisioning and configuration, service distribution and update but also software and feature update. Stakes for handset manufacturers are bug fixing and firmware management.
- Fragmentation of solutions (such as Sagem with patch solution regarding software (which includes application and software solution), Motorola with the provisioning, card provider solution (Gemplus based 'GemConnect'), and many other vendors like Redbend with firmware update and M-formation with monitoring, tracking and provisioning solution). In fact it is difficult to find a solution that covers all needs.
- Security risk (concerning download applications, OS and firmware update, etc.)
- Delay in standardisation. Needs are now significant but no target architecture is defined. It could be a good opportunity to increase synergy with related group in 3GPP and OMA, and develop discussion/lobbying between manufacturers and operators.

Conclusion

The network operator is not the only actor involved in handset management. Device management should enable new services through enhanced UE functionality and several actors could be involved. Device management is a capability that will allow the network operator, service provider and/or UE manufacturer to remotely manage UE. Device management will assist the mobile network operator to reach new business opportunities (differentiation from competition, acquire new customers, increase of the average revenue per user (ARPU), etc.).

This paper has given an overview of device management for the management of future handsets. Some work remains to be done to quickly achieve such management.

The work within the 3GPP is still ongoing; OMA will in the future play a more important role. The management of user equipment (mobile equipment and (U)SIM) will be a part of the mobile operator's core business. Operators must ensure that users' equipment is configured correctly to access the right services in the right way through the right network. Device management is a key to achieving revenue potential and maximising the return on investment, and will enable to new services to be launched more easily.

Bibliography

1 3GPP TR 32.802 V5.1.0 (2002-09): User Equipment Management feasibility study.

2 3GPP TR 21.905: Vocabulary for 3GPP Specifications.

3 3GPP TR 22.240: Service Aspects, Service requirement for the 3GPP GUP.

4 3GPP TS 23.240: 3GPP Generic User Profile (GUP) Architecture R6.

5 3GPP TS 22.057: Mobile Execution Environment (MExE): Service description.

6 3GPP TS 23.227: Application and User interaction in the UE – Principles and specific requirements.

7 OMA draft v0.94x (AWS): Requirements Specification: Stage 1 Device Management.

8 TMF 515v1.0 MTEM Team Business Agreement.

Biography

Emmanuel Dujardin
France Telecom

Emmanuel Dujardin received the degree in telecommunications engineering from the ENST Bretagne (France) and a D.E.A. in Optical Technologies from the Université de Bretagne Occidentale in 2001. In October 2001, he started working in France Telecom as a research and development engineer. During the last two years, he has been involved in testing UMTS equipment in the operation, administration and maintenance domain. He represents Orange in the 3GPP working group SA5 and OMA related to subscription management and device management in 3G.

Mobile Device Management. Empower easy and secure mobility across your enterprise. Overview.Â Weâ€™ve teamed with leaders in mobile device management (MDM) technologies and services to help you streamline and protect mobility across your business. Be sure to get all of your MDM solutions directly from Verizon, so we can help you integrate them into your current mobile strategy and systems. Whether you deploy in the cloud or onsite, weâ€™ve got you covered. How does Mobile Device Management work? Verizon MDM solutions integrate enterprise firmware over-the-air (FOTA) management, device diagnostics and endpoint management into a single, unified and intuitive user experience.