

# Terminal Management and Control Platform System

*In recent years, there has been demand for averting the risk of information leaks and address the use needs of corporations. We developed a terminal management and control platform system that provides unified terminal management functions such as remote initialization and remote customization according to diverse forms of use, including corporate use, consumer use, and communication operator use, and various kinds of mobile terminals, including open platform terminals.*

Core Network Development Department

*Michiko Wakui**Nobuo Takeuchi*

Product Department

*Akihiro Ichinose**Masashi Onogi*

## 1. Introduction

In recent years, there has been a demand for a suitable response to the risk of information leaks by loss of mobile terminals (hereinafter referred to as “terminal”) and for monitoring terminals for appropriate use by employees according to the company contract. Communication operators, too, need functions for diagnostic checking for proper operation of increasingly complex terminal functions, measuring the frequency of function use, and remote collection of network quality information from the terminal for improving user satisfaction with network quality, and various functions for remote control of the terminal in general.

NTT DOCOMO provides terminals

that have enhanced remote data initialization and remote function controls for corporate users, who place importance on security functions. However, concern for security is also increasing among general users, and to respond to that demand, NTT DOCOMO provides a FOMA terminal that has a function for remote locking of a lost terminal [1] and is developing various other services. The same demand is also assumed for Open Platform (OPF) terminals<sup>\*1</sup>, beginning with smart phones, for which future market growth is expected.

Those facts point to the need for a terminal management and control platform system (hereinafter referred to as “platform system”) that provides comprehensive management of services that

involve different kinds of terminal management, regardless of the terminal platform, and at the same time can add functions immediately as needed in instant response to user requests.

In this article, we describe a platform system developed for rapid response to diverse needs for terminal management. This system provides unified terminal management and is also compatible with the Open Mobile Alliance-Device Management (OMA-DM)<sup>\*2</sup> international standard terminal management and control method that includes OPF terminals and is widely used.

## 2. Platform System

The platform system consists of a set of functions for unified management

<sup>\*1</sup> **OPF terminal:** A cell-phone-like information terminal that allows functional improvement and customization by free addition of applications as well as use of free use of native hardware-dependent applications.

<sup>\*2</sup> **OMA-DM:** OMA is an organization involved in standardizing applications related to mobile communication. DM refers to remote control functions of mobile device.

and execution of processing for various kinds of remote control such as initialization of data in terminals.

## 2.1 System Design Concept

The main features of the platform system design concept are described here.

- Modularization of functions limits the scope of effects of functions added to comply with user needs and new specifications from international standardization activities, thus shortening the implementation of added services.
- A terminal control management module for management across multiple services to reduce the load on the terminal for priority decisions and other such contention processing.
- Use of user information stored by the core network to determine from the terminal serial number (International Mobile Equipment Identity (IMEI)) and the subscriber number (Mobile Subscriber ISDN Number (MSISDN)) whether or not the terminal is the target of control and provision of added value such as resending the terminal control request when the Subscriber Identity Module (SIM) is inserted into the terminal.
- Implement terminal control for the target terminal with an optimum protocol that identifies the device type of the terminal to be controlled

to enable control from a FOMA terminal to an OPF terminal without putting constraints on the device type/OS/application, etc.

## 2.2 System Configuration

The platform system configuration is shown in **Figure 1**.

### (1) Control receive and respond module

This module receives various service control requests and responds to them to execute the control of terminals provided to company employees or control of user terminals by the NTT DOCOMO support system according to notification from individual users. There may be multiple control request systems, depending on the number of services, so the control receive and respond module was established to provide a central point for receiving control requests. That function absorbs the differences in the request protocols used

by multiple control request systems and at the same time controls the receiving of control requests from multiple systems at one time.

### (2) Terminal control management module

This module manages remote initialization, remote customization or other such control requests sent from the control receive and respond module to a terminal across services. When multiple simultaneous control requests are sent to a single terminal, a priority is assigned to them and the priority is compared to the priority of the control processing in progress. When the terminal control management module receives a control request, it checks the contract, and retrieves the terminal status from the terminal status DB. It then checks the IMEI DB to determine whether or not the terminal is the control target and thus verify the validity of the

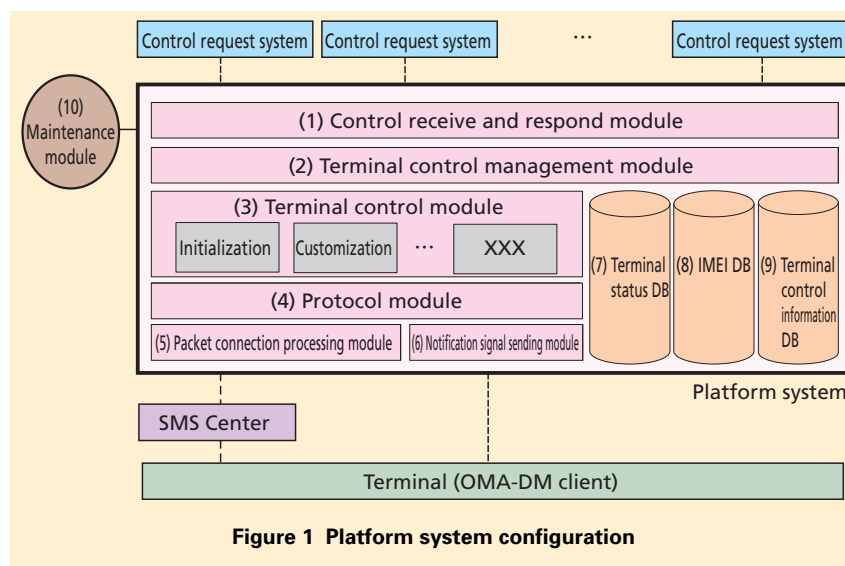


Figure 1 Platform system configuration

control request. It also performs resend processing in cooperation with core network functions such as location registration. For example, if terminal control fails, the next location registration or power-on event is detected and the control is resent.

### (3) Terminal control module

This module receives control requests sent by the terminal control management module. It checks the terminal control information DB for the functions that can be controlled for each device type and the applicable control protocols. It then executes the control. The terminal control module comprises functional units that execute remote initialization, remote customization and other such terminal controls. For OMA-DM control services, various management functions for the Lock And Wipe Management Object (LAWMO)<sup>\*3</sup> and the Device Capability Management Object (DCMO)<sup>\*4</sup> etc. specified by OMA are applied. The terminal control module has also a mechanism for adding management functions as needed to comply with new specifications from the standardization process.

### (4) Protocol module

This module executes the terminal control protocol processing. For terminals equipped with an OMA standard DM client, it can select the

protocol for OMA-DM control, etc.

### (5) Packet connection processing module

This module establishes an Secure Socket Layer (SSL)<sup>\*5</sup> connection between the terminal and the platform system and at the same time determines whether packet communication charges processing and connection are possible. The platform system is used by multiple services, so the charging method is expected to differ according to the service (form of function use and contract status). Therefore, the connection destinations (Access Point Names (APN)) specified by the terminal when connecting to the platform system are divided into service units that have different charging methods and connection to those multiple APN is permitted by the packet connection processing module.

### (6) Notification signal sending module

When terminal control is implemented by OMA-DM, a DM Notification (DMN)<sup>\*6</sup> is sent to the terminal by Short Message Service (SMS) and a packet connection from the terminal to the platform system is started. Specifically, the notification signal sending module generates the DMN and sends it by SMS to the terminal.

### (7) Terminal status DB

This DB stores the terminal states that are controlled by the plat-

form system (camera lock, browser lock, etc.). It is accessed to determine whether or not terminal control is possible for a terminal state.

### (8) IMEI DB

This DB stores information on the IMEI and MSISDN combinations that are in use. It is accessed to determine whether or not the control target terminal is in use when executing a terminal control.

### (9) Terminal control information DB

This DB stores the terminal device type information needed for terminal control and the applicable protocols. When the applicable protocol is OMA-DM, the Management Object (MO)<sup>\*7</sup> specified by OMA-DM is stored, so control is enabled by simply registering the MO.

### (10) Maintenance module

This module performs remote monitoring and control of the platform system and handles inquiries from users, etc. It also maintains the terminal control log.

## 3. Services Using the Platform System

NTT DOCOMO provides remote customization, remote initialization, remote locking, and remote initial value setting services that use the platform system. Of those services, remote customization and remote initialization were offered as options under the Business Mopera Security Manager terminal

\*3 **LAWMO**: A function for managing remote terminal locking and initialization.

\*4 **DCMO**: A function that determines whether or not the use of a terminal function can be controlled remotely.

\*5 **SSL**: A protocol for secure communication between a client and server, mainly using the Internet. It provides functions for encryption, authentication and detection of tampering.

\*6 **DMN**: Information specified by OMA-DM for notification of the invocation of terminal con-

trol.

\*7 **MO**: The terminal structure that is the target of control in OMA-DM terminal control.

management service for corporate users on November 19, 2008 [2].

1) Remote Customization

The remote customization service is offered a flexible way for the company's terminal manager to remote set up the minimum required functions for use by employees to restrict non-business use of the terminal and reduce the risk of information leaks by controlling terminal use according to company policy. The functions available for custom setup are shown in **Table 1**.

2) Remote Initialization

The remote Initialization service

**Table 1 Functions available for remote customization**

Remote customization control items (as of October 1, 2009)
Camera use
Music and video player use
One seg use
Mailer use
Browser (i-mode/ full browser) use
i-appli use
i-appli autostart setting
Forced manner mode (direct control)
Dialed call restriction
Reject calls from numbers not in phone book
Phone book use
Data transfer by Bluetooth <sup>*1</sup> , USB, Ir or FeliCa <sup>*2</sup>
Data BOX use
External memory use
Browse or move phone book or SMS data in FOMA card
Bio-authentication only
Key lock (ON/OFF)
IC card lock (ON/OFF)
GPS position provision setting

\*1 Bluetooth®: Registered trademark of Bluetooth SIG, Inc.  
 \*2 FeliCa®: Registered trademark of the Sony Corp.

can remotely delete user data such as phone book and mail information and reset the terminal to restore it to the state when it shipped from the factory to prevent leaking of information when a terminal is lost. The data that can be deleted includes the content of the memory card and SIM card as well as the user data in the terminal itself. Each device can be selected individually for data deletion.

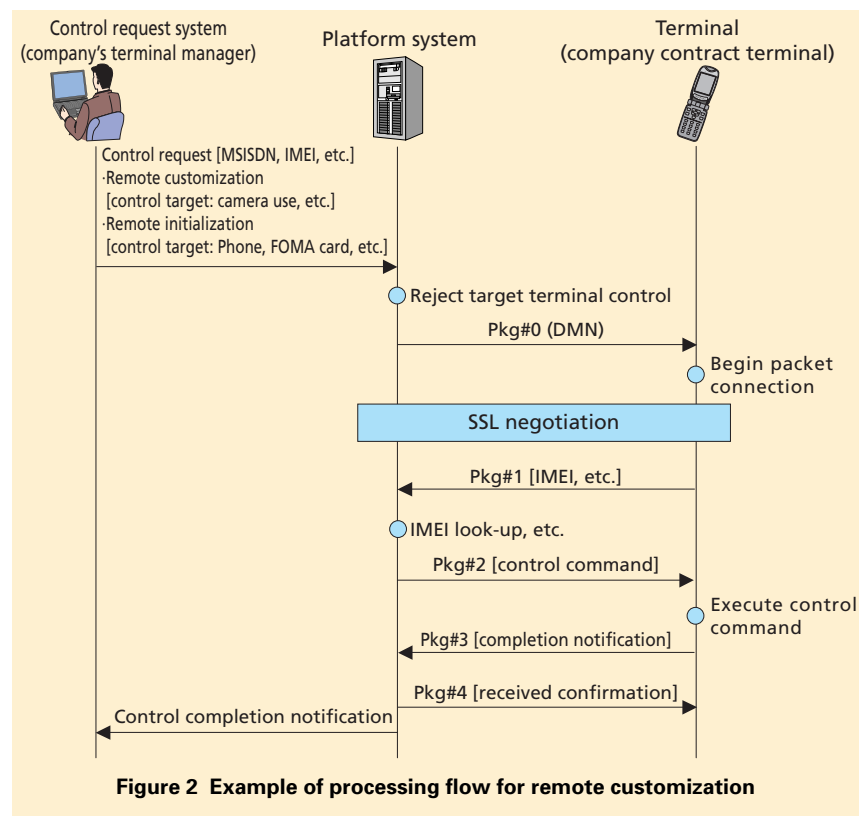
**3.1 Service Processing Flow**

An example of the processing flow in the remote customization service is shown in **Figure 2**. This service is implemented with OMA-DM. It works in much the same way as the remote

initialization service.

The company terminal manager sends a remote customization control request to the platform system, specifying the MSISDN and IMEI of a terminal that has been registered in advance with the management site for corporate users.

When the platform system receives the control request and control is permitted for the specified terminal, it sends a Package<sup>\*8</sup> (Pkg) #0 (DMN) to the terminal as a message to start DM control. When the terminal receives Pkg#0 (DMN), it established a packet connection and performs SSL negotiation. After establishing a session, the terminal sends the IMEI and other ter-



**Figure 2 Example of processing flow for remote customization**

\*8 Package#X: An OMA-DM processing message. X represents the sequence number of the processing message (0, 1 to 4).

terminal information to the platform system in Pkg#1. When the platform system receives Pkg#1, it determines from the IMEI whether or not the terminal is the specified control target. Then, it sends the control command to the terminal in Pkg#2. When the terminal receives Pkg#2, it executes the control according to the control command. After the terminal completes execution of the control, it notifies the platform system by sending Pkg#3. The platform system acknowledges the message by sending Pkg#4 to the terminal, which then recognizes that Pkg#3 was received by the platform system and ends the DM control. At the same time, the platform system sends a control completion notification to the corporate user management site and ends the control.

When the control ends, the terminal setting status is registered in the terminal status DB and the terminal manager can check the customization status by using the corporate user management site.

### 3.2 Terminal Software Configuration

The terminal software configuration is shown in **Figure 3**. The remote customization and remote initialization services use the OMA-DM method, so the OMA standard DM client is used. The DM client only executes the Pkg data processing, so the customization and initialization processing execution mod-

ule and the control target application invocation module are implemented as terminal functions.

An overview of the processing done within the terminal in this service is given below.

When Pkg#0 (SMS) is received from the platform system, the application invocation module determines the function invocation conditions and invokes the DM function (Fig. 3 (1) and (2)). The DM client generates or parses the Pkg data exchanged with the platform system (Fig. 3 (3)), notifies the customization and initialization processing execution module of the instructions from the platform system. The execution module then executes the customization and initialization processing (Fig. 3 (4)).

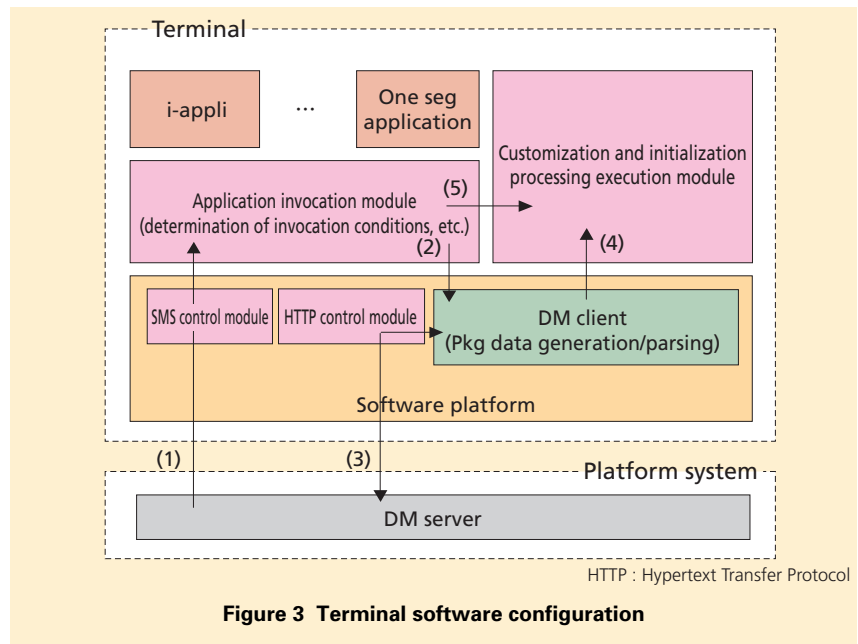
When the control target application is invoked, the application invocation

module either invokes or restricts the relevant application according to the customization status (Fig. 3 (5)).

### 3.3 Processing for Conflict with Other Functions

In a server-startup type platform system such as this service, control packet communication begins with Pkg#0 (SMS). Thus, control may begin while the terminal is being used. In the OMA-DM, DM processing can be executed forcefully when Pkg#0 is received or the user can select whether or not the control is to be executed, and either case can be specified by the manager.

In the remote initialization and remote customization services described here, instructions from the manager are given highest priority to reduce risk, and the control is executed



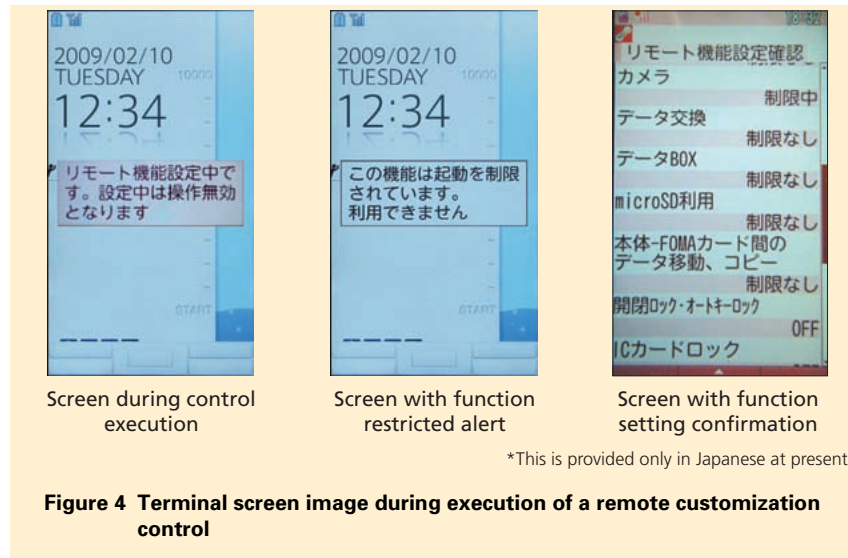
**Figure 3 Terminal software configuration**

during terminal use regardless of the user's desire. Thus, forced execution of the DM processing is set. To prevent interference with this function by the execution of other functions, particularly during packet communication, functions other than voice calls and emergency functions are in principle terminated and the DM processing is executed.

There may be future cases in which priority is given to other functions by the addition of services in the future. In such cases, for example, priorities can be set for each service by adding private parameters to the operator's extended data area in Pkg#0.

### 3.4 User Interface

The terminal screen during execution of the remote customization control is shown in **Figure 4**. If the user tries to invoke a restricted function after the control has been completed, the "Restricted function" alert is displayed and that function is disabled. Also, the restricted function is grayed out or disabled message is displayed when the



**Figure 4** Terminal screen image during execution of a remote customization control

function is invoked. The control status of the function can be checked from the function menu remotely from the PC of a company manager.

## 4. Conclusion

We have described a terminal management and control platform system that we developed for rapid response to diverse requirements for terminal management, as well as remote initialization and remote customization functions as services that use the system. In future work, too, we plan to implement addi-

tional terminal management functions to meet user needs and comply with changes in OMA specifications.

### REFERENCES

- [1] W. Sakurai et. al: "Remote-terminal-management Infrastructure Technology for Safe and Secure Life-Style Mobile — Keitai Shitei Lock Function," NTT DoCoMo Technical Journal, Vol. 10, No. 1, pp. 37-41, Jun. 2008.
- [2] NTT DOCOMO Press Release: "More Functions for the Business Mopera Security Manager," Nov. 2008.