Safe and Secure | Terminal Management | Remote Control

Technology Reports

Special Articles on Technology toward Further Diversification of Life-Style Mobile

Remote-terminal-management Infrastructure Technology for Safe and Secure Life-Style Mobile — Keitai Shitei Lock Function —

Core Network Development Department *Wataru Sakurai*
Takashi Morita
Hironori Chikura

As more and more functions are being added to mobile terminals, they are becoming an indispensable tool for daily life. In order to make better use of these functions, NTT DoCoMo is developing a terminal-management infrastructure which makes it possible to control specific terminals via the network. Using this infrastructure, we are providing the "Keitai Shitei Lock" function to provide additional safety, and security for users by allowing control of specific mobile terminals.

1. Introduction

NTT DoCoMo has developed various functions to promote the safety and security of users, including "Area mail," which is able to send notifications to users in a specified area in times of emergency without being affected by network congestion, secure services like "imadoco search," which allows people to check their location or that of family members through i-mode and other means, and functions that can notify emergency services of the location of the caller when someone calls for emergency help.

Also recently, with the increasing number of functions in mobile terminals, we have provided functions like "Omakase Lock," which can remotely lock terminal functions or erase sensitive data to prevent data leaks, or limit use of FeliCa®[*1] functions to help minimize the risk when a terminal is lost or stolen. In addition to these types of controls, for controlling terminals when they have been lost, there is further demand for a remote control function that allows administrators to remotely enable and disable individual functions such as the camera or external-device interfaces to help prevent information leaks. Thus the need for terminal-control functions is increasing, particularly in the security field.

When controlling a terminal remotely, a control request must be sent specifying either the phone number stored in the User Identity Module (UIM)[*2] currently inserted in the mobile terminal or the International Mobile Subscriber Identity (IMSI)[*3]. However, since the UIM can be changed in a mobile terminal, and a user may use more than one terminal, it is desirable to be able to specify the terminal itself when performing remote control operations. We have developed the terminal-management infrastructure in order to address this issue, making it possible to specify the mobile terminal itself when

[*1] **FeliCa®**: A contactless IC card technology developed by Sony Corp. A registered trademark of Sony Corp.

[*2] **UIM**: An IC card storing subscriber information including the phone number and the IMSI (see *3). Inserted into the mobile terminal and used to identify the user.

[*3] **IMSI**: A number used by Global System for Mobile communications (GSM) and Third-Generation networks to distinguish individual users, but not known to users. Preserved in the UIM.

performing remote control operations.

In this article, we provide an overview of the terminal management infrastructure, and of how the Keitai Shitei Lock service was implemented as an example application of this infrastructure.

2. IMEI and Terminal Management

2.1 IMEI Overview

The International Mobile Equipment Identity (IMEI) is a unique identifier for mobile terminals that is retained by the terminal itself. As shown in **Figure 1**, it is composed of an 8-digit Type Allocation Code (TAC), identifying the terminal type, a 6-digit Serial NumbeR (SNR), specifying indivisual terminal, and a single spare digit. Actually, in addition to the IMEI there is also an IMEI Software Version (IMEISV), which is the actual data maintained by the network in some cases, but for this article we will refer to them uniformly as the IMEI.

Using this IMEI, the type of terminal can be determined from the TAC, and operations that are specific to the functions supported by the terminal can be performed.

The 3rd Generation Partnership Project (3GPP) has defined a logical node, called the Equipment Identity Register (EIR)[*4], which uses the IMEI as a key for storing data, and this is used by some network operators to provide control over specific mobile terminals by registering the IMEI of each illicit terminal in the EIR.

2.2 The Need for Terminal Management Infrastructure

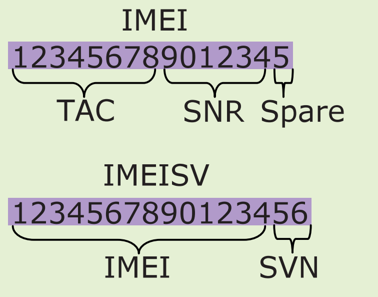
Mobile terminals are able to move freely in and outside of the network area. In order to communicate with these terminals which could be anywhere, it is necessary for the network to maintain information about where and whether terminals are on the network. Current mobile communication systems use a combination of the phone number registered in the UIM and the IMSI, and the mobile terminal registers these with the network at its current location to control communication.

In order to control a specific mobile terminal, the phone number or IMSI (hereinafter we assume the phone number is acquired) must be derived from the IMEI, but this presents the following issues:

Issue 1: It is not possible to determine the node where the terminal is currently located

Issue 2: It is not possible to uniquely identify an IMEI

For the first issue, it is not possible to identify the particular node where the terminal with the desired IMEI is currently located. The IMEI is stored as part of the network-location information by the Visitor Location Register (VLR)[*5] and the Serving General packet radio service Support Node (SGSN)[*6], but it is not known which VLR/SGSN the terminal is currently under, so in order to determine the phone number for a particular IMEI, inquiries must be made to each VLR/SGSN sequentially (**Figure 2**).



*The IMEI in the IMEISV doesn't include the spare digit

Figure 1 Structure of IMEI and IMEISV

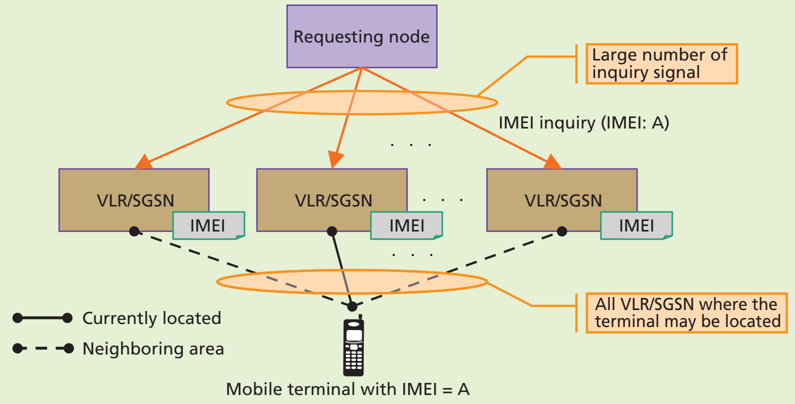


Figure 2 First issue with extending the existing method

[*4] **EIR**: A logical node defined by the 3GPP with functions for managing IMEIs.

[*5] **VLR**: A logical node defined by the 3GPP with functions for managing network-location information for subscribers.

[*6] **SGSN**: A logical node defined by the 3GPP with functions for handling packet communications.

Maintaining a mapping between IMEI and phone number in the Home Location Register (HLR)[*7] has been considered, but since the HLR uses phone numbers and IMSI as keys to hold related data and uses these number ranges to determine which equipment physically stores the data, requests would have to be sent to each HLR to determine whether it holds the desired IMEI. While this may be less of a load than querying each VLR/SGSN, it would still be significant. Considering the current number of FOMA subscribers, processing load, and time that would be required to identify the phone number being used, this approach is not considered practical.

For the second issue, there will be cases where multiple phone numbers are maintained with the same IMEI, so the IMEI cannot be uniquely identified with a phone number. There are cases, when changing the UIM, as when removed while out of the service area, when communication with the VLR/SGSN cannot be done, so the VLR/SGSN cannot detect whether the UIM has been changed, and cannot delete the IMEI data. Because of this, until the old UIM is inserted in a different terminal and communication with the VLR/SGSN is initiated, the IMEI registered for the old user will be the same as that registered for the new user. Thus, it is not possible to uniquely determine which phone number is being used with the IMEI (**Figure 3**).

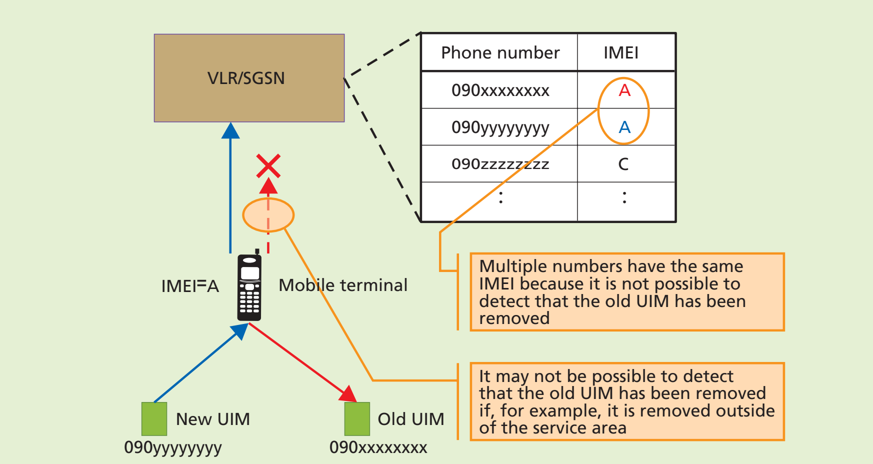
To create a terminal-management infrastructure as an extension to current systems and capable of determining the current phone number efficiently from the IMEI, we needed to resolve these types of issues with real-time response and processing. We built the IMEI-DB, a new database using the IMEI as a key and deriving the phone number currently in use.

We used the phone number as the data derived from the IMEI so that it could be referenced from the IMEI-DB even if the referring equipment does not hold the IMSI.

3. Overview of the Terminal-management Infrastructure

3.1 Overall Structure and Main Function

The overall structure of the terminal-management infrastructure is shown in **Figure 4**, and the main functions are shown in **Table 1**.



Phone number	IMEI
090xxxxxxxx	A
090yyyyyyyy	A
090zzzzzzzz	C
:	:

Multiple numbers have the same IMEI because it is not possible to detect that the old UIM has been removed

It may not be possible to detect that the old UIM has been removed if, for example, it is removed outside of the service area

Figure 3 Second issue with extending the existing method

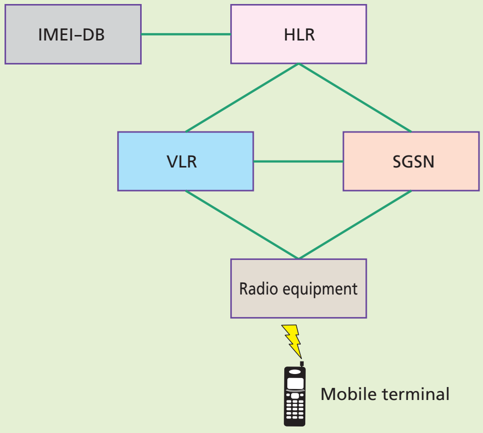


Figure 4 Overall structure

[*7] **HLR**: A logical node defined by the 3GPP with functions for managing subscriber information and call processing.

The newly-created IMEI-DB stores the IMEI data, The HLR manages updates to IMEI data, and the VLR and SGSN handle IMEI changes and notifications.

3.2 Phone Number in Use Update Function

An IMEI update is performed when a change of IMEI is detected by the VLR/SGSN. The VLR/SGSN notifies the HLR by setting the IMEI in the current-location registration signal. Then, when the VLR/SGSN detects an IMEI change, it notifies the HLR. The HLR holds the IMEI, and if the location registration signal received from the VLR/SGSN contains a different IMEI than the one in the HLR, the IMEI-DB is updated with the new IMEI.

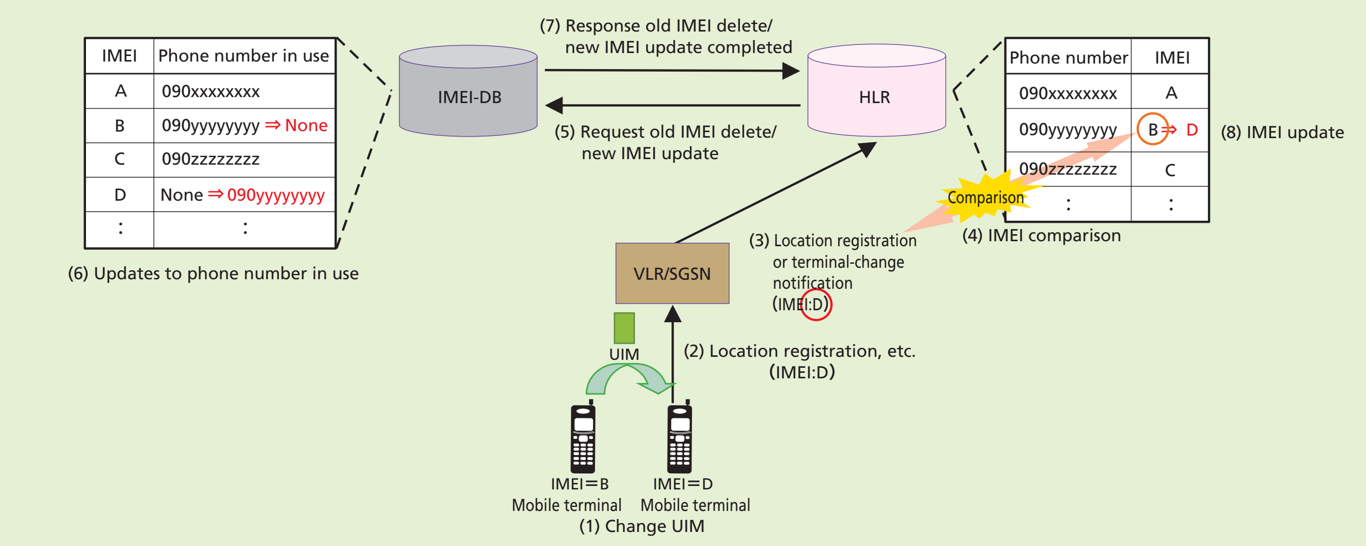
Table 1 Main functions per node

Logical node	Main functions
IMEI-DB	• IMEI-DB management • Referencing in-use phone numbers
HLR	• IMEI update management
VLR	• IMEI change management/notifications
SGSN	• IMEI change management/notifications

The update operations when a UIM is moved to a new mobile terminal are shown in **Figure 5**. The user with phone number 090yyyyyyyy removes the UIM from a terminal with the IMEI B, and inserts it in a terminal with IMEI D (Fig. 5 (1)), and the new terminal notifies the VLR/SGSN of the IMEI (Fig. 5 (2)). The VLR/SGSN receiving the location registration signal recognizes the change of IMEI, and sends a terminal-change notification to the HLR (Fig. 5 (3)). The HLR receiving this signal compares the old IMEI in its profile with the new IMEI received in the location registration signal (Fig. 5 (4)), and if they are the same, continues with normal location-registration processing. If they are not the same, an update to IMEI-DB is done, indicating that the phone number in use for that IMEI has changed. If the HLR had been retaining a different IMEI, it sends a delete/update request for this old IMEI to the IMEI-DB (Fig. 5 (5)).

When the IMEI-DB receives the delete/update request, it deletes the old IMEI and updates the new one (Fig. 5 (6)). When the HLR receives the response from the delete/update request (Fig. 5 (7)), it updates the IMEI in its own profile (Fig. 5 (8)).

The IME-DB is updated based on the IMEI maintained by the VLR/SGSN. It could also be possible to update the IMEI-DB directly from the VLR/SGSN, but this would complicate processing on the VLR/SGSN, as well as increasing the amount of signal processing required on the IMEI-DB, increasing the total cost of the implementation over all equipment (VLR/SGSN and IMEI-DB). Because of this, we decided to use the existing IMEI notification signal sent from the VLR/SGSN to the HLR, and have the



IMEI	Phone number in use
A	090xxxxxxxx
B	090yyyyyyyy ⇒ None
C	090zzzzzzzz
D	None ⇒ 090yyyyyyyy
:	:

Phone number	IMEI
090xxxxxxxx	A
090yyyyyyyy	B ⇒ D
090zzzzzzzz	C
:	:

IMEI-DB
HLR
(7) Response old IMEI delete/ new IMEI update completed
(5) Request old IMEI delete/ new IMEI update
(8) IMEI update
Comparison
(4) IMEI comparison
(6) Updates to phone number in use
VLR/SGSN
(3) Location registration or terminal-change notification (IMEI:D)
UIM
(2) Location registration, etc. (IMEI:D)
IMEI＝B Mobile terminal
IMEI＝D Mobile terminal
(1) Change UIM

Figure 5 IMEI-DB Updates

HLR determine whether an update to the IMEI-DB was needed or not. As a result, we were able to minimize the cost of IMEI-DB equipment with no added equipment for the VLR/SGSN or HLR. Also, the database is structured so that the IMEI is a unique key, and updates are performed whenever the terminal communicates, so there is no danger of a single IMEI holding multiple phone numbers.

3.3 Referencing a Currently-in-use Phone Number

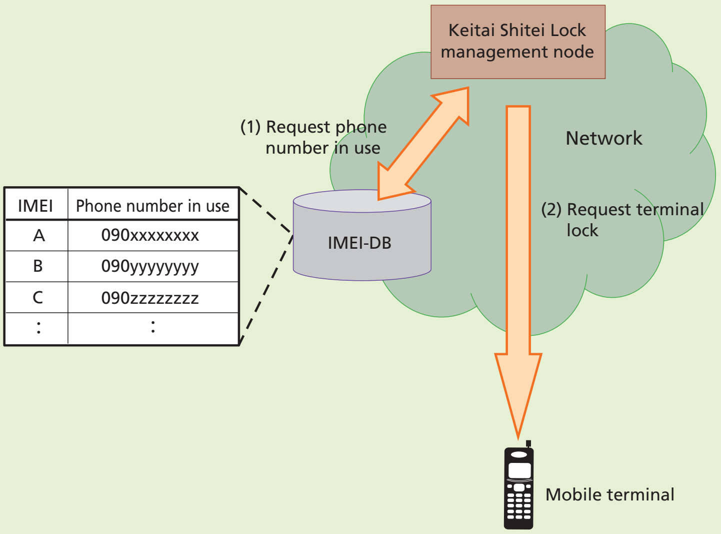
The requesting node sends a request to the IMEI-DB using the IMEI as the key. The IMEI-DB searches for the phone number currently in use by the terminal with the given IMEI and returns the result to the requesting node.

4. Example Service

We now describe the "Keitai Shitei Lock" service as an example of using the terminal-management infrastructure. This is a locking service similar to "Omakase lock" that can be applied to a pre-registered mobile terminal by applying for the Keitai Anshin Pack (Mobile Phone Security Package).

The Keitai Shitei Lock service allows a specific mobile terminal to be locked by specifying the IMEI, rather than the UIM for the terminal to be locked. In other words, using this service, the mobile terminal can be locked against users even if they change the UIM in the terminal.

An overview of the process is shown in **Figure 6**. A Keitai Shitei Lock management node sends a request to the IMEI-DB for the phone number being used on the terminal with a specified IMEI key. The IMEI-DB responds, returning the phone number it has stored corresponding to the IMEI to the Keitai Shitei Lock management node. If the IMEI-DB does not currently have a phone number for the given IMEI, it replies that the number does not exist, but keeps track of this fact, and notifies the Keitai Shitei Lock management node of the phone number if it later detects the registration of a phone number for that IMEI.


Keitai Shitei Lock management node
Network
(1) Request phone number in use
(2) Request terminal lock
IMEI-DB
Mobile terminal

IMEI	Phone number in use
A	090xxxxxxxx
B	090yyyyyyyy
C	090zzzzzzzz
:	:

Figure 6 Keitai Shitei Lock overview

In this way, even if for some reason no number exists in the IMEI-DB for the IMEI of the mobile terminal to be locked, the Keitai Shitei Lock management node will be notified as soon as the terminal performs a location registration on the network and the lock can then be applied immediately.

After obtaining the phone number being used, the Keitai Shitei Lock management node can request that the terminal be locked using the phone number as the key.

5. Conclusion

We have described a method for implementing a terminal-management infrastructure, as well as a "Keitai Shitei Lock" service as an example application of this infrastructure.

Introduction of the IMEI-DB as part of the terminal-management infrastructure will enable various types of management and control applications for mobile terminals, and contribute to development of new services in the future.