Technology Reports

903i Application Functions

Junko Hiraishi, Ema Tohriyama, Eiji Yano and Yoshimasa Nishimura

The FOMA 903i Series supports a number of new application functions, notably the Kisekae Tool, Machi-chara function, support for non-DoCoMo digital authentication certificates, and a function to handle SMS junk mails, and realizes an attractive lineup of mobile terminals providing safety and security in communications.

1. Introduction

The scope of mobile terminal use has expanded to the point where many users are unable to do without a mobile terminal, and users now require terminals to be both attractive and provide safe and secure communications. To satisfy these requirements, the FOMA 903i Series has been developed to target users requiring highly functional and high-performance mobile terminals, and as such provides a number of application functions including the Kisekae Tool, Machi-chara function, support for non-DoCoMo digital authentication certificates, and a function to handle Short Messaging Service (SMS)[*1] junk mails.

The Kisekae Tool and Machi-chara function allow the user to customize the mobile terminal according to personal preference, while support for non-DoCoMo digital authentication certificates and the SMS junk mail handling function are designed to provide greater safety and security in mobile terminal communications.

This article describes an overview of these four new functions.

2. Kisekae Tool

2.1 Service Concept

When customizing the standby screen and ringtone with the content of user's choice, it is important that the users are able to

*1 SMS: A service supporting the sending and receiving of short text messages, primarily between mobile terminals.

select from wider variety of contents and easy to be installed. In addition, more users wish to customize their mobile terminals while maintaining a uniform display theme, such as installing content using the same characters in a variety of areas.

The Kisekae Tool allows customizing with downloaded content particularly for the highly-used areas, and providing a diverse expression with a variety of content. A function for batch downloading and installing of content in multiple customizable areas is also supported, allowing the user to maintain a uniform display theme on the mobile terminal through simple operation.

The expanded customizing function and the batch downloading and installation supported by the Kisekae Tool are described below.

2.2 Expanded Customizing Function

The Kisekae Tool enables the installation of Flash®*2 menu content downloaded to the top menu screen. The Flash menu allows mobile terminal functions to be started directly from the content. This leads the content to be readily created by anyone using commercially available Flash content, and apprehension over creating junk content arises, only pre-installed content may be used with existing models. The Kisekae Tool therefore handles content not as normal Flash content, but as packages (described later) which may be downloaded without apprehension of encountering junk content. Thus, the user can customize the top menu screen from a greater range of content, not only from pre-installed content. Consequently, it is now possible to customize with downloaded content, primarily to display useful information for the user, such as remaining battery charge and antenna status.

The ability to download this content and expand the customizable area enables customization by selecting from a more diverse range of content to suit user preference.

2.3 Batch Downloading and Installation of Content

The Kisekae Tool permits the ready customization of a variety of areas. Content is packaged for the Kisekae Tool to allow the batch downloading and installing of multiple content for a variety of areas. **Figure 1** shows an overview of the batch

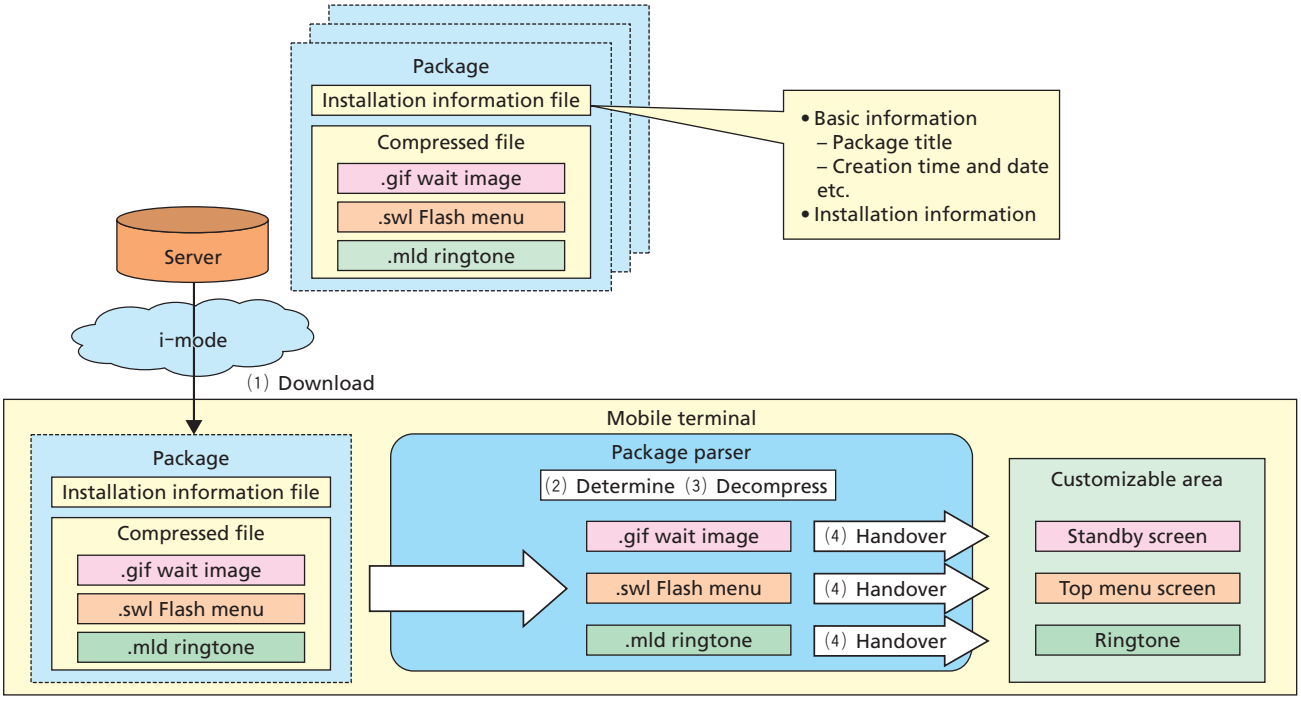

Figure 1 Batch download and installation

*2 Flash®: Software used to create content that combines audio and vector graphics animation or the created content itself.
Flash is a trademark and registered trademark of Adobe Systems Inc. in the United States of America and other countries.

download and installation function.

Packaged content (hereafter referred to as a 'package') is supplied in the form of a compressed file containing such basic information as the package title, setup information specifying the customizing area in which to install the content, and the content itself.

A package is downloaded using the i-mode browser (Fig. 1 (1)). The downloaded package is installed using the package parser pre-installed on the mobile terminal. This package parser is a module which makes a determination on the installation information file and decompresses compressed files. When installing a package, the module determines the location at which to install individual content based on the installation information file (Fig. 1 (2)), and then passes the decompressed content (Fig. 1 (3)) to the relevant customizable area (Fig. 1 (4)). The received content is installed in the appropriate customizing area; thus, multiple content may be batch downloaded and installed.

3. Machi-chara Function

3.1 Service Concept

The service concept is focused on the expansion of customizing functions (such as changing the standby screen) to let users customize mobile terminals according to personal preference. However, a function to continuously display the same content on multiple function screens (e.g., standby screen, menu screens), in addition to expanding the customizable area, was not previously available. Since an increase in provided content can be expected due to greater involvement by users and expanded development of the Content Provider's (CP) scope of business, the use of character content was investigated. The continuous superimposition of character images on the differing function screens (e.g., standby screen, menu screens) as the background image is implemented as the Machi-chara function.

Characters may be in either 2D or 3D format, and the superimposed character display can be switched to accommodate changes in mobile terminal status (such as a missed call). **Photo 1** shows the standby screen for the Machi-chara function. For example, when a missed call occurs under normal conditions

(a) Normal status (b) Missed call status

Photo 1 Standby screen displaying Machi-chara

(Photo 1 (a)), the mobile terminal transitions to missed call status and the missed call character (Photo 1 (b)) is displayed.

Character data for the Machi-chara function may be freely created and provided by the CP as i-mode content.

3.2 Overview of Configuration Technology

The Machi-chara function is comprised of three functions: "management of character display coordinates", "management of changes in selection of character images", and "change in appearance of characters according to time information".

1) Management of Character Display Coordinates

By controlling the display position of a character, it is possible to move the character on the mobile terminal screen. Controlling the display position permits the display of lifelike characters with changing activity patterns and the speed of movement, and to avoid simply repeated movement of the character along a fixed path, there are two methods of movement available for the CP to combine as follows:

- Patterned movement: The CP determines the path of character movement. This allows the CP to control movement.
- Automatic movement: The path of movement is generated on mobile terminals. This avoids repeated movement over the same path.

2) Management of Changes in Selection of Character Images

This function changes character images and manages the priority order of various statuses to accommodate changes in mobile terminal status (e.g., missed call, reception of mails).

The CP can prepare character images for use when status

changes (e.g., to missed call) and movements occur.

3) Change in Appearance of Characters According to Time Information

This function changes the appearance of a character according to the current time and the time during which the character content is used. Character appearance may be changed by changing the texture[*3] used in the character data, or by substituting all of the character data. Changing the texture enables such small changes in perception as switching from a suit by day to pajamas by night, and requires little additional data to effect this change in appearance. The changing of texture is only applicable to 3D character data. Substituting all of the character data facilitates large changes in perception such as switching from a child to an adult, and requires a large amount of additional data to effect said change in appearance. The substituting of all character data is applicable to both 2D and 3D character data.

4. Support for Non-DoCoMo Digital Authentication Certificates

4.1 Service Concept

Secure communications services on mobile terminals previously used only digital certificates (FirstPass) issued by DoCoMo; however, the increased number of digital certificates issued by the Certificate Authority (CA) offices and private companies has necessitated the requirement for a secure service with which each office of the CA authenticates FOMA users under its own policy.

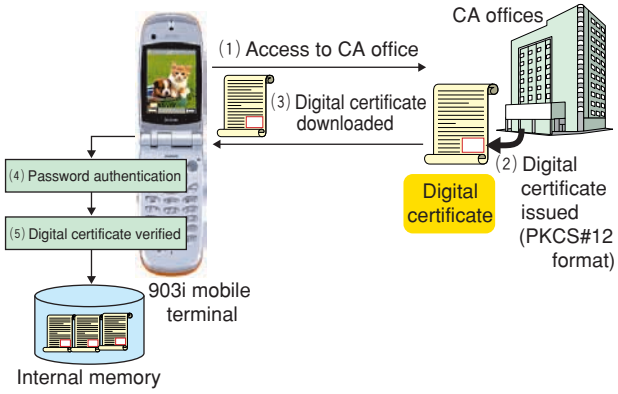

Figure 2 Downloading non-DoCoMo digital certificates

In order to raise the level of sophistication of security functions on mobile terminals and expand the business market, this function provides a means of acquiring and storing digital certificates issued by the CA offices and private companies from mobile terminals, and permits the use of secure communications and digital signatures with these digital certificates.

4.2 Acquisition and Storage of non-DoCoMo Digital Certificates

Digital certificates are generated by the CA offices and private companies as data in standard Public Key Cryptography Standards#12 (PKCS#12)[*4] data format, and acquired as PKCS#12 data downloaded from the issuing Website of the CA offices to the mobile terminal by using the browser (**Figure 2** (1) to (3)).

The PKCS#12 data includes a private key that forms a pair with the digital certificate, and since the private key is very secure information, the CA office encrypts it with a password. When acquiring PKCS#12 data, the password determined by the CA office must be entered on the mobile terminal to prevent the acquisition of illegal data (Fig. 2 (4)).

Since the use of digital certificates on mobile terminals has conventionally been limited to those installed at the time of purchase, and those issued by DoCoMo (FirstPass), it was possible to verify the validity of the data format of a digital certificate with DoCoMo prior to downloading and using it on the mobile terminal. However, since this function handles digital certificates issued by CA offices (i.e., non-DoCoMo digital certificates), DoCoMo cannot verify the validity of such certificates before downloading. Since the various CA offices have different policies and issue digital certificates with differing data formats, a mechanism whereby only digital certificates usable for secure communications can be stored is required, thus preventing the storage of unnecessary and illegal digital certificates. A function is therefore supported to enable verifying the validity of a downloaded digital certificate when storing it on a mobile terminal. In practice, the data format of the digital certificate, suitability of the chain formation[*5] between PKCS#12 data included in the digital certificate and the higher-order certificate

*3 Texture: An image applied to the surface of an object to provide the sense of hand feeling in 3D data.

*4 PKCS#12: A standard data format used for the exchange and transmission of certificates and private keys.

*5 Chain formation: A method of verifying whether a digital certificate has been issued by the relevant CA office.

(i.e., Root certificate, sub-Root certificate), and the public and private pairs of keys are verified to guarantee usability in secure communications (Fig. 2 (5)).

4.3 Use of Non-DoCoMo Digital Certificates

Downloaded digital certificates are used with secure communications services. The Secure Sockets Layer (SSL)[*6] and Transport Layer Security (TLS)[*7] communications functions are already supported with this model, and used with digital signatures. The use of these functions is explained below.

1) Use with SSL/TLS Communications

Non-DoCoMo digital certificates downloaded with the mobile terminal browser and i applications may be used for SSL and TLS communications.

The digital certificates used are compatible with the Root certificate list specified from the server in SSL protocol, and automatically extracted at the mobile terminal. Convenience is therefore improved by displaying only usable digital certificates for selection by the user.

Moreover, when a digital certificate is sent to the server, the signature must be processed with a private key; however, since the private key is very secure information, personal verification is required by the mobile terminal user. This function therefore requires entry of the existing mobile terminal code number, thus achieving personal verification while reducing the amount of software development work necessary. Biometric technology as a means of improving personal verification is now being investigated.

2) Use with Digital Signatures

Digital certificates downloaded with this function may be used with the digital signature function according to existing Java applications. A digital signature is encrypted using a private key that is paired with digital certificate, primarily for transaction data between the mobile terminal and server, and encrypted data is provided with the transaction data to prevent the alteration of data and facilitate personal verification.

Since a private key is used when generating a digital signature, the terminal code number must be entered (as with SSL/TLS communications) from the mobile terminal for personal verification of the user.

5. SMS Junk Mail Handling Function

5.1 Service Concept

Sending restrictions have been placed on SMS operators as a means of handling increasing junk mails sent via the SMS system. However, the possibility of SMS junk mails reaching the user has not been completely eliminated. Since SMS uses a phone number as the message destination, greater damage is possible and immediate measures are required. A new SMS junk mail filtering function using a security scan has therefore been implemented in the mobile terminals to ensure safety and security in use. This function provides the user with a warning when the body of a received SMS message includes a phone number or URL, and the user is therefore able to prevent inadvertent connection to the offending SMS operator. An overview of the technology adopted in implementing this function is described below.

5.2 User-customizable Messages

SMS messages containing phone numbers and URLs in the body are detected as a potential problem using the existing security scan function; however, since the warning displayed at detection is of fixed format, the system lacks flexibility in the measures available to deal with SMS junk mail. A function that enables all content of the warning to be freely customized is therefore provided so that messages appropriately customized for the problem detected may be displayed. The security scan function has been expanded to permit the display of freely customizable messages upon the detection of a problem.

1) Expansion of Pattern Data Format

Data format has been expanded to allow storage of the message displayed upon detection of a problem is detected in pattern data as part of the data itself. Updated pattern data may therefore be downloaded, allowing the user to add, modify, and delete messages for display, in addition to the problem detection pattern, thus providing the flexibility to accommodate new messages as necessary when a new type of SMS junk mail appears.

Both Japanese and English messages may be stored simulta-

*6 SSL: A protocol used for the encryption of communications and detection of alterations to data, and secure communications when communicating between clients and servers, primarily using the Internet.

*7 TLS: An expanded protocol that specifies SSL as standard Internet technology. The encryption algorithm and error message specifications have been expanded beyond that of SSL.

Table 1 Problem level values and displayed messages

Problem level value	Displayed message
Level 0	Message A
Level 1	Message B
Level 0	Message C
Level 1	Message D

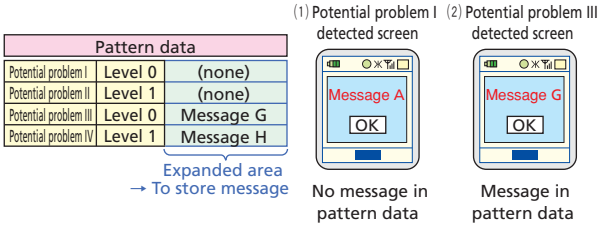

Figure 3 Screens displayed with expanded pattern data and problem detection

neously on the mobile terminal, allowing for installation of either as necessary.

2) Changing the Method of Displaying Messages when a Potential Problem is Detected

The existing security scan function provides a mechanism to display messages of fixed format, each corresponding (**Table 1**) to a level value unique to each problem included in the scanning pattern data (**Figure 3** (1)). Mobile terminal operation has been changed so that upon the detection of a type of problem for which a message is stored in pattern data, that message is displayed instead of a fixed message (Fig. 3 (2)).

5.3 Other Related Functions

SMS junk mail warnings provide the user with cautions related to specific SMS messages. For users who are well aware of the potential problems of SMS junk mails, a menu is available to allow the user to switch on/off the warnings, separately from the security scan function on/off option. To avoid the lowering of security level, the menu is designed so that the warning setting may only be changed when the security scan function is valid.

6. Conclusion

This article has described a number of new application functions supported by the 903i Series: the Kisekae Tool, the Machichara function, compatibility with non-DoCoMo digital authentication certificates, and a function to handle SMS junk mails. The installation of these functions has resulted in a greater ability to customize mobile terminals and improvements in security functions.

A greater variety of customizing functions and more sophisticated security functions will be implemented in the future as part of the process to satisfy a wider range of user requirements for mobile terminals.