505i Series Mobile Terminals with New Functions

Hidetoshi Yazaki, Tetsu Saito, Naoki Naruse,
Takayuki Orii, Masato Takeshita,
Fukiko Maeda and Yuichi Ichikawa

This article describes the 505i series, which is equipped with the i-appli DX service, the enhanced access functions of the i-appli services, and Macromedia Flash™ that allows displaying rich, expressive contents such as animations.
With this series, in addition to incorporation of the functions above, we have achieved a configuration that will be able to support the future diversification of the i-mode service, such as performance improvement of the basic devices and equipment of an external memory slot as standard. Moreover, improved security is also taken into consideration; some of the models have a fingerprint authentication function.

Development Reports

1. Introduction

The Personal Digital Cellular (PDC) digital mobile phone system started in 1993 and has mainly been targeted at voice communication so far. Recently, however, the traffic of data communication such as character- and image-based information is increasing. Through the introduction of the i-mode service in February 1999, it became possible to browse web sites, use e-mails and download images for stand-by display and music ring tones from mobile terminals. Moreover, the Java Runtime Environment was incorporated in the 503i series [1] launched in 2001, and the i-appli service that makes it possible to download application contents such as games to mobile terminals had started. As the functionality of mobile terminals improves, the needs for high-performance contents are increasing. Due to such synergy, the demands for data communication have been increasing. The continued diversification and advancement of the i-mode service will be critical factors in promoting increase of data communication traffic in the future as well. Development of mobile terminals that can support such high-performance contents, thus, has been highly demanded.

In development of the 505i series, we enhanced the func-

tions, which includes performance improvement of basic devices such as liquid crystal display screens and cameras, incorporation of the i-appli DX service, an enhanced version of the i-appli service, and inclusion of Macromedia Flash™ that permits various forms of animation. In addition to this, we mounted an external memory slot as standard equipment to allow the user to back up his/her personal data stored in the mobile terminals. Moreover, we improved the security by implementing a fingerprint authentication function in some of the models.

This article explains the specifications of the basic devices incorporated in the 505i series that we have developed this time, and the newly built-in functions, as well as the new services implemented thereby.

2. Features

Photo 1 shows the external appearance of the newly developed 505i series. **Table 1** shows a comparison of the functions with conventional mobile terminals. The development for this series can largely be classified into two parts: performance improvement of the basic devices of the mobile terminals and newly added functions. This chapter provides an overview of these features.

Photo 1 505i Series (D505i, SO505i, SH505i, N505i, F505i and P505i from the left)

2.1 Performance Improvement of the Basic Devices

The main purpose of the performance improvement of the basic devices is to support i-appli contents, because the usage of such contents is expected to become more diversified and advanced.

For the liquid crystal display screens, a high-definition liquid crystal display technology called Quarter Video Graphics Array (QVGA) was employed for the first time. With this technology, the 505i series is able to display contents including various animations (detailed characters, still images and video) in a more beautiful manner and at higher definition than before. For the camera function, we built a CCD camera with a resolution of over 1 million pixels into some of the models to improve the quality of acquired images. Moreover, we installed a function to read Japan Article Number (JAN) barcodes and Quick Response (QR) codes. It is expected that the inclusion of this feature will make net shopping via i-appli applications more comfortable.

The memory capacities were also enlarged. The capacity of the scratch pad for the i-appli service was increased from the conventional maximum of 100 kB to 200 kB; the capacity of contents that can be used with mobile terminals was thus doubled. The capacity of the browser was expanded from the maximum 10 kB to 20 kB per page and the browser display performance was enhanced. The capacity for downloading music ring tones was also doubled, to a maximum of 20 kB; it has thus

Table 1 Main features of the 505i series

	505i series	Conventional PDC mobile terminal
i-appli DX	○	×
Macromedia Flash™	○	×
External memory slot	○	Some models only
Fingerprint authentication function	F505i only	×
QVGA	○	×
Camera with a resolution of over 1 million pixels and barcode reader function	Some models only	×
Infrared remote controller function	○	Some models only
Capacity of i-appli scratch pad	Maximum 200 kB	Maximum 100 kB
Browser capacity per page	Maximum 20 kB	Maximum 10 kB
Capacity to download music ring tones	Maximum 20 kB	Maximum 10 kB
i-mode mail selective reception	○	×

become possible to utilize a richer selection of music ring tones than before.

An infrared remote controller function has been implemented in some of the conventional models. This function allows sending remote control data to external devices (TVs, VCRs etc.). The 505i series is equipped with an infrared remote controller function based on the i-appli service as standard.

2.2 Enhancement of Conventional Functions

First of all, the "selective reception function" of i-mode mail that can be used with Freedom Of Mobile multimedia Access (FOMA) terminals has become standard with the 505i series. With this function, it is possible to check the number of i-mode mails, names of senders and date/time of reception, and then download only mails deemed necessary by the recipient to the mobile terminals. This can be used as an effective means of filtering out junk mails, which have been increasing rapidly in recent years.

Secondly, an external memory slot was mounted as standard equipment. Recently, the amount of personal information stored in mobile terminals (e.g., phonebooks, mails, schedulers and images taken by cameras) has been continuously increasing. The memory capacity in a mobile terminal is limited, however, so it is usually not a good idea to save such information only in the mobile terminal on a permanent basis. In addition, providing means to back up such information is considered to contribute to the recycle rate of mobile terminals. The models in the 505i series thus come with an external memory slot as standard equipment, a feature that was implemented only in some of the conventional models.

In order to address the demands for smaller, thinner and lighter mobile terminals, we adopted Memory Stick Duo and miniSD cards, which are highly compact media. As a result, the 505i series successfully meet the above demands without having greater volume and weight than conventional mobile terminals. Moreover, we assumed that the external memory is used to 1) back up personal information, 2) transfer phonebook data etc. to other models, and 3) transfer images to printing devices. Based on this assumption, we unified the folder structures and file formats used for storing contents within the external memories, such as phonebooks and image files, for each memory medium to secure data compatibility among different models. Furthermore, the file format of images taken by the built-in camera of the 505i series conforms to the Exchangeable image file format (Exif) and Design rules for Camera File system (DCF) standards that are adopted in the majority of commercially available digital cameras. The images can thus easily be printed out using existing printing devices.

The third enhancement is the inclusion of the i-appli DX service as a standard feature. With conventional mobile terminals, access to functions and personal information such as phonebooks inside mobile terminals via i-appli applications has been uniformly restricted for security purposes. Moreover, i-appli applications were allowed to communicate only with servers and ports from which they were downloaded. For this reason, the serviceability of i-appli applications has been somewhat impaired since the usage range was limited due to security considerations. Thus, the downloading method and activation control have been improved for the i-appli DX service compared to the i-appli service. The service allows access to functions and personal information such as phonebooks inside mobile terminals from an i-appli DX application and enables it to communicate with servers and ports other than those from which the application was downloaded, while maintaining the required security. Furthermore, linking with i-mode mails was made possible as well. With these function enhancements, it has become possible to connect to various sites as shown in **Figure 1**, and the serviceability and marketability of i-appli applications were heightened. How the security is maintained when using i-appli DX applications will be explained in detail in chapter 3.

2.3 Newly Implemented Functions

New functions implemented in the 505i series include Macromedia Flash™ and a fingerprint authentication function. The former is implemented in all models as standard, while the latter is implemented only in some of the models (F505i).

Contents utilizing Macromedia Flash™ have already become widespread on the Internet and the use of rich contents (Flash) using various forms of animation are increasing on PC web browsers. i-mode browsers on conventional PDC terminals support HyperText Markup Language (HTML) and both Graphic Interchange Format (GIF) and Joint Photographic Experts Group (JPEG) formats as image formats. In other words, web sites for i-mode are primarily text-based and can only handle still image or simple animations (animated GIF) comprised of approx. 10 frames as images. By implementing Macromedia Flash™ in the 505i series, various forms of anima-

Compared to conventional i-appli, i-appli DX has enhanced linkage with native functions of terminals.

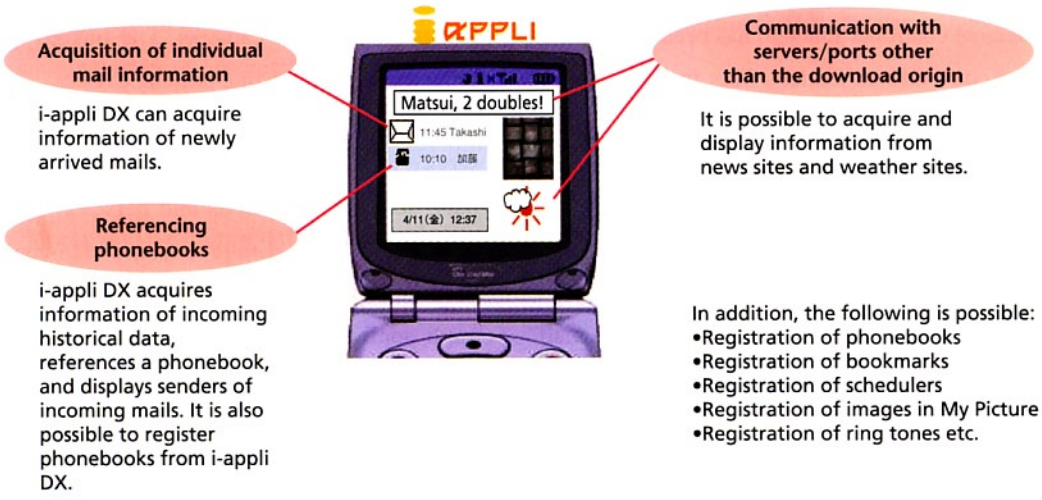


Figure 1 Service image of i-appli DX (example)

tion were made possible on i-mode browsers and it has become possible to use conventional text-based screens as more expressive and interactive interfaces. Chapter 4 provides an installation overview of Macromedia Flash™ on mobile terminals.

On the other hands, as mobile terminals become advanced, much more personal information, such as phonebooks, mails and camera images, is being stored in internal memories of mobile terminals. Such personal information can be protected via various lock functions, such as dial lock and phonebook lock. Furthermore, the fingerprint authentication function implemented in F505i as an optional function not only provides enhanced security of the mobile terminals themselves via a fingerprint sensor, but also simplifies operations of these lock functions and achieves improved operability linked with the i-appli DX service. Chapter 5 provides an overview of the fingerprint authentication function implemented in F505i.

3. Maintaining Sufficient Security in the i-appli DX Service

3.1 Operation/Management of i-appli DX Applications

Mobile terminals supporting i-appli applications are equipped with an application manager Java Application Manager (JAM). The JAM manages downloaded i-appli applications and the Virtual Machine (VM). When downloading an i-appli applications, the JAM judges whether or not it can be downloaded based on the information described in an Application Descriptor File (ADF). **Figure 2** shows the download sequence of an i-appli DX application to a mobile terminal of the 505i series. The Security Descriptor File (SDF) download processing is a new download function that has been added starting from the 505i series. This SDF is a file that describes functions that are allowed to be accessed from an i-appli DX application. It is issued by DoCoMo uniquely for each i-appli DX application and managed on the i-mode server. Mobile terminals can access functions only permitted by the SDF.

At the time of downloading an application and acquiring the ADF, the JAM judges whether or not the i-appli application in question is an i-appli DX application, and if it is, the JAM acquires the SDF from the i-mode server. After acquiring the SDF, the JAM acquires the Java ARchive (JAR) file and then allows the i-appli DX application to use functions made available by the SDF. Moreover, if the i-appli DX application attempts to access a function not permitted by the SDF during execution, the i-appli DX application is forced termination. i-appli DX applications can thus be managed and operated via SDFs issued by DoCoMo.

3.2 Verification of Validity and Upgrading of i-appli DX Applications

In order to allow controlling downloaded i-appli DX applications, a process has been added to conduct an SDF check regularly when activating i-appli applications. In such an SDF check, it is checked whether or not it is allowed to start a given i-appli DX application at the time connection to the i-mode server is established. The JAM judges whether or not to perform an SDF check according to the number of times the i-appli DX application was activated and the elapsed time described in the SDF. If the application is activating more times than what is

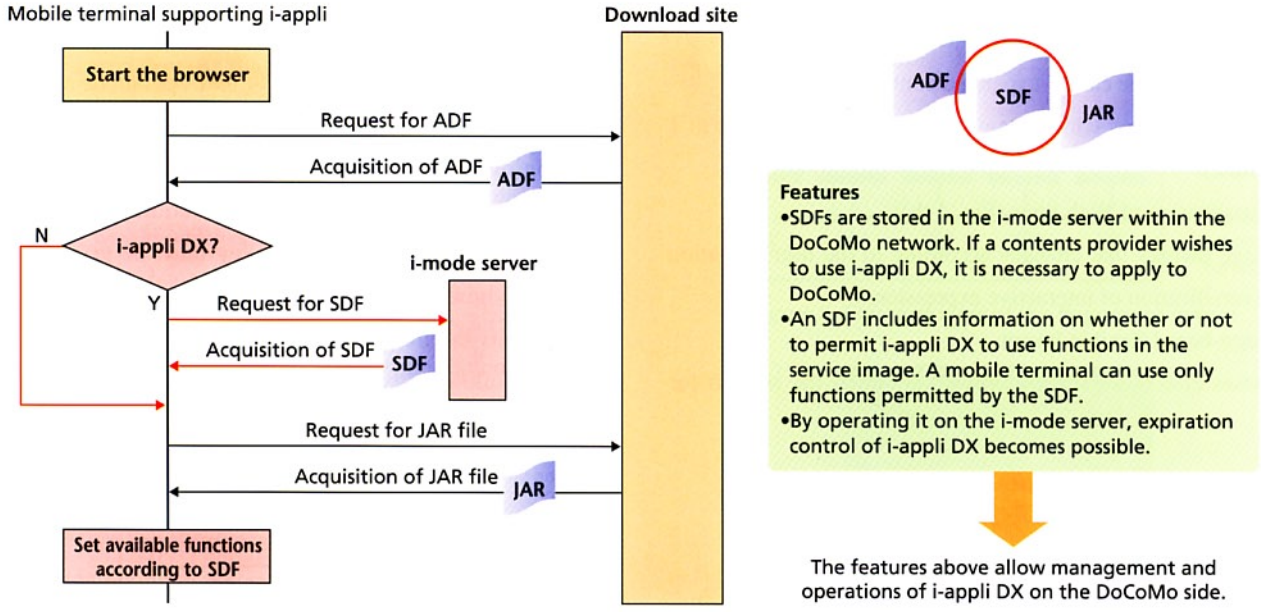


Figure 2 How to download i-appli DX

specified in the SDF or if the time elapsed from the time the JAM judged that the SDF was valid the last time exceeds the time specified in the SDF, an SDF check is performed when the i-appli application is activated. If the response result from the i-mode server is "valid," the activation of the i-appli application is allowed. If the response result from the i-mode server is "expired," the i-appli application is prohibited from activating. Moreover, if the response result from the i-mode server is "upgraded," the i-appli application is upgraded.

Thus, to sum up, the security of i-appli DX applications is maintained by managing and operating the applications according to information described in SDFs.

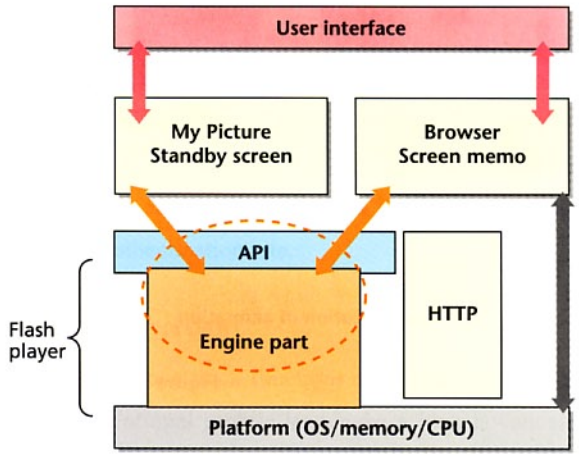


Figure 3 Software configuration

4. Embedding Macromedia Flash™

In order to allow playing Flash files, we have obtained a ported version of the Flash player from Macromedia Inc. and embedded it in the mobile terminals. This chapter explains how the Flash player was embedded and the operation modes.

4.1 Embedding Flash Player

The Flash player is linked to various modules within a mobile terminal and used to play Flash files. At this point, the host application controls the processing between the Flash player and the user interface devices such as screen, speakers and buttons, as well as HTTP communication processing. **Figure 3** shows the configuration of the user interfaces, browser and Flash player on the mobile terminal platform. In addition to the browser, it is only the screen memo (offline browser), My Picture (image viewer) and standby screen that can use the Flash player as host application. The number of applications to which the Flash player is made available, are limited to these in order to avoid multiple startups of the player.

Two parts are defined for the Flash player: an engine part that performs analysis, calculation and rendering of files, and an interface part between the engine part and host application. Since it is embedded in various different models, the engine part is customized to conform to each platform of the 505i series.

4.2 Play Mode Definition

Effects obtained by implementation of Macromedia Flash™ can largely be divided into the following two categories.

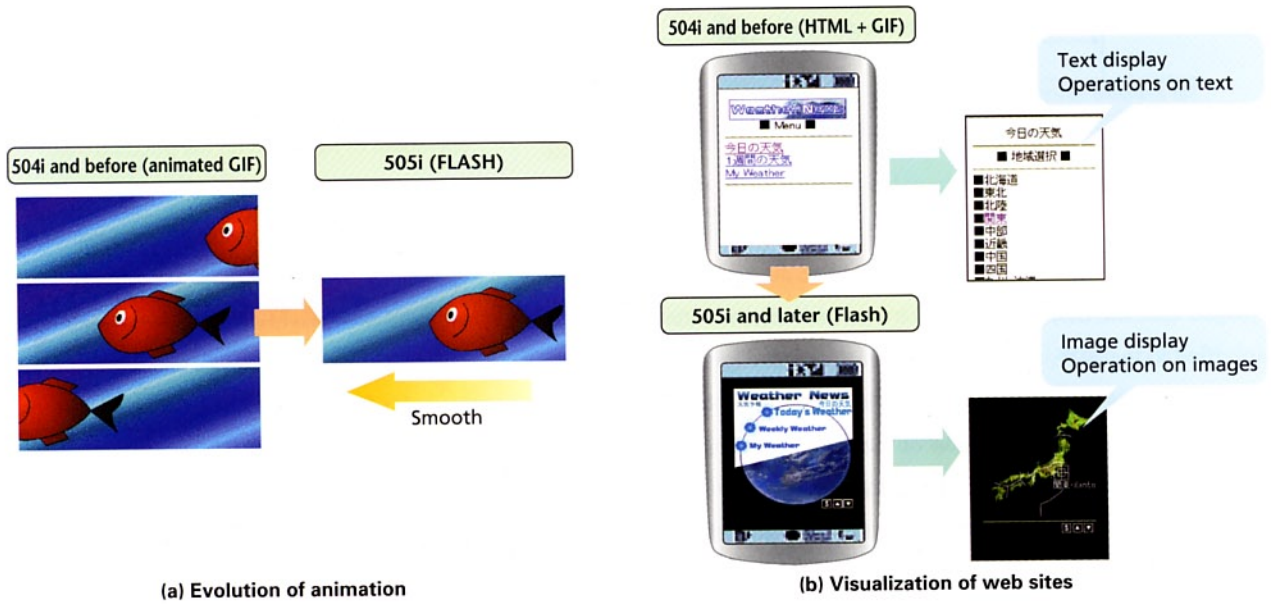
(1) Evolution of Animation

- Smooth play (**Figure 4 (a)**)
- The display size can be expanded/contracted.
- Long animations with plots are possible (* 30 seconds to 1 minute).

(2) Visualization of Web Sites (Fig. 4 (b))

- Image display that changes according to the user operation (diversification of interactive expressions)
- Image-based flexible layout

Theses effects are mainly brought about by the support for vector-based graphics functions and use of scripting language, which are features of the Flash player. The Flash player allows interactive playing that responds to user operations and, on PC browsers, operating targets are selected and executed with a pointing device such as the mouse in most cases. In order to perform similar operations on mobile terminals, an interface device such as the cross-shaped key must be used. Existing functions, however, have already been assigned to the key, which limits the freedom of operation. In order to supplement this, the following two play modes (**Figure 5**) are defined.



(a) Evolution of animation

(b) Visualization of web sites

Figure 4 Improved expression by Macromedia Flash™

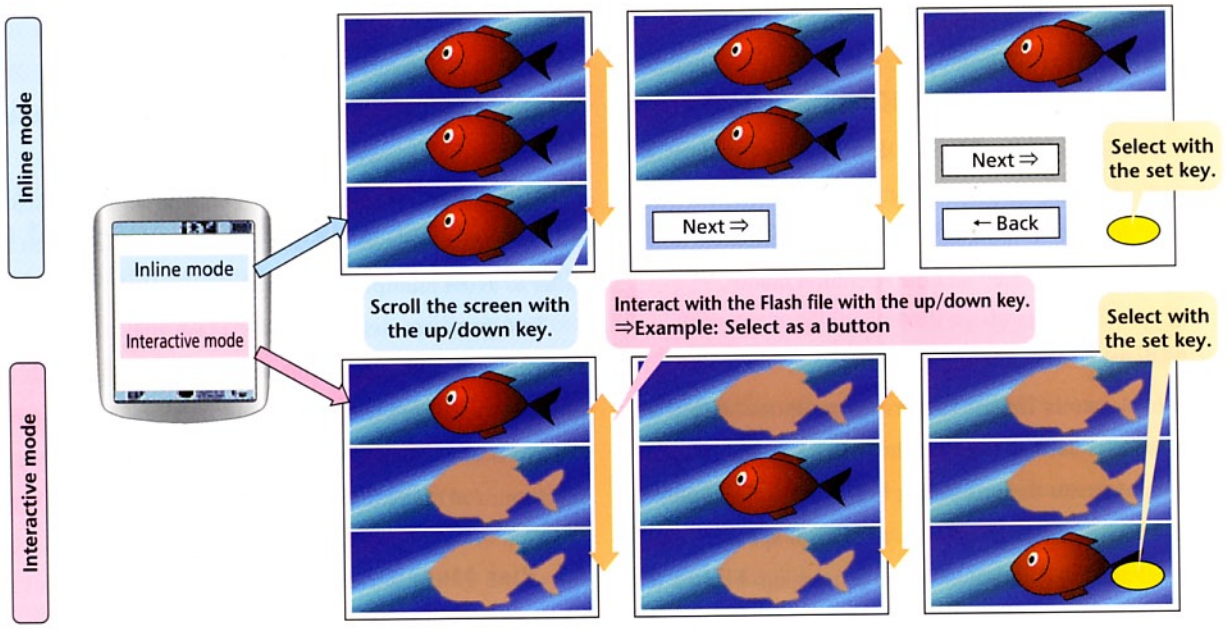


Figure 5 Play modes

Switching between the play modes is judged by descriptions in HTML tags and the chosen acquisition method of Flash files; the contents providers can thus determine the play mode.

1) Inline mode

There is no change to the way the cross-shaped key and other keys work. A Flash file is treated as one image file in the same way as a GIF or JPEG file.

2) Interactive mode

The cross-shaped key and other keys interact with Flash files. It becomes possible to perform operations on each object within the Flash file displayed.

These two modes allow content providers to use the two types of features of Macromedia Flash™, evolution of animation and visualization of web sites, for best uses in contents according to their purposes.

5. Fingerprint Authentication Function (F505i)

5.1 Fingerprint Sensor

Every person in the world has a unique fingerprint, and one's fingerprint does not change till one's dying day. Technologies that take advantage of such characteristics to allow accurate personal authentication are widely known as biometrics. Fingerprint authentication is also suited for implementation on mobile terminals because the input sensor can be made small. Fingerprint input sensors can be of different types, based on their input methods: "optical," "capacitance-based" and "weak electric field detection-based." F505i employs a "weak electric field detection-based" system that permits a small sensor size and achieves a high authentication rate. **Figure 6** shows the structure of the fingerprint sensor and operation principle.

The "weak electric field detection-based" sensor detects the electric field of the water layer at the boundary surface between the epiderm (A) and corium (B) below the epiderm, rather than actual epiderm of a finger. As shown in fig. 6, when a finger is placed on the outer edge of the sensor (the bezel part), a weak current is conducted to the finger, and the sensor detects the variations in the electric field generated by the irregularity of fingerprint ridges. The sensor then converts these measurements to a signal pattern allowing a fingerprint image to be generated.

In order to implement this system on mobile terminals, the reading part of the sensor had to be miniaturized to 6.6 mm square (**Photo 2**). This degree of miniaturization raised some concerns that the authentication rate might be lowered because the resultant area of the fingerprint read might become too small. For this reason, F505i employs a unique authentication algorithm that integrates a "pattern matching system," which directly evaluates the similarity of two images, and a "Minutia system," which extracts and contrasts characterizing points to improve the authentication rate.

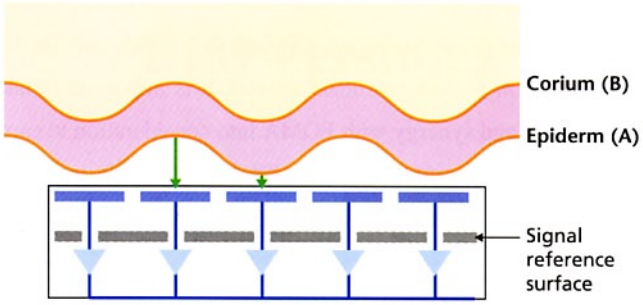


Figure 6 Enlarged view of the fingerprint sensor

Photo 2 Fingerprint sensor (F505i)

5.2 Function Overview

F505i can cancel lock functions via fingerprint authentication. In conventional mobile terminals, a lock is canceled by entry of a 4-digit secret number. With mobile terminals equipped with the fingerprint authentication function, on the other hand, a lock can be canceled either by entry of 4-digit secret number or fingerprint authentication, aiming to improve the security and operability.

Moreover, with F505i, it is possible to use a function for acquiring query results of fingerprint authentication via i-appli, assign different actions for each query result, and activate corresponding functions. For example, fingerprint authentication can be used as a shortcut key, such as "authentication of my index finger means sending a mail to Mr. A" or "authentication of my middle finger means creating a mail for Mr. B."

6. Conclusion

This article explained new functions and services (i-appli DX, Macromedia Flash™, external memory slot and fingerprint

authentication) implemented in the 505i series. We are planning to implement these functions and services developed for the 505i series on FOMA terminals as well. It is important to take consistency and synergy with FOMA into consideration to carry forward development of new functions and mobile terminals that allow new services implementation in the future as well.

REFERENCES

[1] Yazaki, et al: "Special Article on Advanced i-mode Mobile Phones," NTT DoCoMo Technical Journal, Vol. 3, No. 1, PP.4–36, Jun. 2001.

ABBREVIATIONS

ADF: Application Descriptor File
DCF: Design rule for Camera File system
Exif: Exchangeable image file format
FOMA: Freedom Of Mobile multimedia Access
GIF: Graphic Interchange Format
HTML: HyperText Markup Language
JAM: Java Application Manager
JAN: Japan Article Number
JAR: Java ARchive
JPEG: Joint Photographic Experts Group
PDC: Personal Digital Cellular
QR: Quick Response
QVGA: Quarter Video Graphics Array
SDF: Security Descriptor File
VM: Virtual Machine