PIN Secure MultiMediaCard to Support the Secure Ubiquitous Information Society

Akira Kanehira
Jun Miyake
Takashi Totsuka

OVERVIEW: Security is fundamentally important in this new emerging era of ubiquitous availability and access to information. Hitachi, Ltd. has now developed PIN Secure MultiMediaCard (PIN-SMMC), a flash memory card product that securely protects confidential content such as copyrighted material and personal and corporate data against unauthorized access. The product features a public-key encryption scheme like other MultiMediaCards, but also incorporates a user authentication function that provides a new level of security. Sensitive data cannot be accessed unless the user is authenticated by correct PIN input, an additional security feature that prevents data from falling into the wrong hands even if the device is lost or stolen. By installing the card in the expansion slot of a PDA or other mobile handheld device, this will provide a powerful tool supporting sales force automation in a mobile environment by enabling sales people in the field to access customer and product related data anytime and anywhere. Management of keys is handled by each individual system, so use of the PIN-SMMC can be flexibly tailored to accommodate different security level requirements.*

INTRODUCTION

IN the ubiquitous information age, people will be able to access networks and obtain the information they need anytime and anywhere. The tradeoff for this flexibility and convenience is that it heightens the risk of personal or corporate data falling into the wrong hands, and indeed this risk only increases with the proliferation of broadband and wireless networks.

Thus, concern for security becomes more important than ever before in the age of ubiquitous information. To achieve a truly secure environment, one would ideally have to implement security measures at every step along the way from the network servers and network line down to the terminal equipment and storage cards. However, to implement such an ideal security system would create a major hardship on users in terms of cost and flexibility. A more typical real-world system therefore consists of an ordinary general-purpose terminal to receive information and a storage card with security features for protecting personal and corporate data.

In this paper we will give an overview of Hitachi's PIN-SMMC (personal identification number Secure MultiMediaCard), a flash memory card with a user authentication function for protecting personal and corporate data on mobile handheld devices, and describe a number of applications for the secure memory card.

NEED TO PROTECT PERSONAL AND CORPORATE DATA

As the ubiquitous information society continues to unfold, we are seeing an enormous upsurge in demand for security capabilities that can protect personal or corporate data and prevent the information from being accessed by unauthorized strangers. Designed to address this need is Hitachi's PIN-SMMC featuring a user authentication function to provide a new level of security for protecting personal and corporate data on mobile handheld devices.

The MultiMediaCard (MMC) is a large-capacity removable flash memory card that can be used to store a diverse range of digital content. By adding a function supporting secure communication between a server and encoder to the card, Hitachi began mass producing Secure MultiMediaCards (SMMC) in November 2000 that are capable of protecting a wide range of content such as music, digital images, and copyrighted materials (see Fig. 1).

*: MultiMediaCard is a trademark of Infineon Technologies AG, Germany, and is licensed to MMCA (the MultiMediaCard Association).

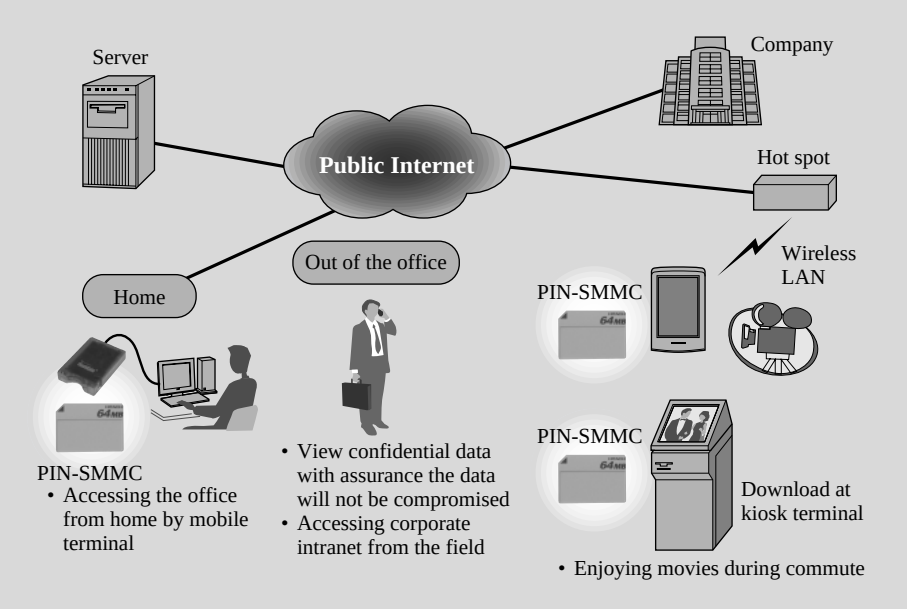

Fig. 1—Envisioned Applications for the PIN Secure MultiMediaCard. Whether from home or on a business trip, one can easily access critical company-related information. We envision that people will soon be able to watch movies on their PDAs while commuting back and forth to work and school.

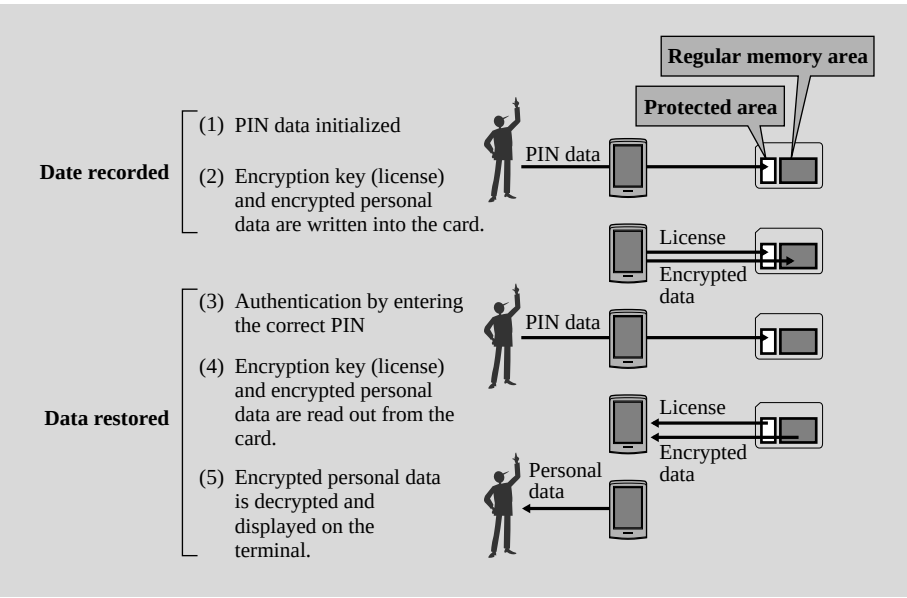

Fig. 2—Process of Protecting Data on a PIN-SMMC. User's authentication PIN is established when data is first recorded, and the PIN must be entered to later view the data. The encryption key can only be accessed and the data decrypted and displayed on the terminal after the user is authenticated by correct PIN input.

Because confidential data such as copyrighted materials and personal records are stored in encrypted form on the card, the new function ensures that data security will not be compromised even if the memory card or the PDA (personal digital assistant) is lost or falls into the wrong hands.

OVERVIEW AND FUNCTIONS OF THE PIN-SMMC

PIN-SMMC Data Protection Process Flow

As with other types of SMMC, Hitachi's PIN-SMMC also employs the cryptographic processes and technologies of the public key infrastructure (PKI). Sensitive data is protected by encrypting the confidential information with an encryption key and storing the data in the flash memory part of the SMMC, while the encryption key is stored along with other incidental data in a protected hardware tamper-resistant module (TRM) in the memory card. The PIN user authentication function adds another level of protection by ensuring that the license keys can only be accessed from the SMMC after the user is authenticated by correct PIN input. The confidential content can only be decrypted and displayed on the terminal after the

license key has been successfully accessed.

The basic PIN-SMMC data protection process is shown in Fig. 2: first (1) a PIN is initialized when confidential data is recorded, then (2) the encrypted data and encryption key are read into the card. Then, when the user wants to access the data, (3) the user is authenticated by entering the correct PIN from the terminal, (4) the encrypted data and encryption key are read out, and (5) the data is decrypted and displayed on the terminal.

If the management of content and the license keys is more complex than just a handheld device equipped with an SMMC and involves the use of personal computers and servers, operations will vary depending on how the system is being used. In the case of a single user, initializing the PIN and managing the encryption license keys are of course done by the individual. In the case of a corporation, on the other hand, the license keys are generally managed by a system administrator using a network system made up of PCs and servers. Employees have PINs set up for them in advance by the administrator, and receive license keys in the PIN-SMMCs they are provided. An employee can use the license key to encrypt and decrypt his own personal data or any shared files of groups to which the employee belongs. This allows the user to view and use these files even when away from the office as long as he has a PDA or other mobile device equipped with the PIN-SMMC on which the encryption license key and the content are stored.

PIN-SMMC Configuration

Fig. 3 shows a block diagram of the PIN-SMMC. The card consists of (1) the basic flash memory making up the card, (2) the CPU that manipulates the flash memory based on MMC commands from the host computer, (3) a tamper-resistant module where the flash memory control circuitry and the card's secret key and shared key for the components making up the MMC interface to the host computer, and (4) the encryption processing circuitry that performs security processing based on security processing commands from the host computer. One will note that the flash memory control is stored in the TRM that is able to withstand intense cryptoanalysis. PIN verification for the card also takes place in the TRM, thus providing even more robust security than authentication processing on the host computer.

User Authentication Function

The PIN-SMMC user authentication function works in such a way that the license key stored in the TRM can only be accessed and read out on the terminal after the user is authenticated by correct PIN input. The card's authentication capability is implemented by the five functions listed in Table 1.

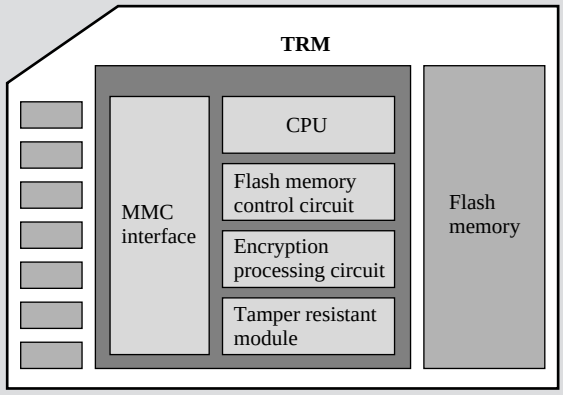

Fig. 3—PIN-SMMC Functional Block Configuration. User authentication by verifying the user's PIN takes place in the TRM that is able to withstand intense cryptoanalysis, thus providing better security than authentication on the host terminal.

TABLE 1. PIN-SMMC User Authentication Functions
This shows the user authentication functions incorporated in the PIN-SMMC. The functions can be used to manage and control the users' access to license key portion of the card.

Function	Description
Verify PIN	Function allowing user to access license key by correct PIN input. If the wrong PIN is entered, the retry counter is incremented by 1. If the verification try limit is reached, the user authentication function ceases without providing the license key or initializing the PIN.
Update PIN	Function allowing the user to update the PIN that is set in the TRM. User must be authenticated by the old PIN before the PIN can be undated.
Update number of verification tries	Function allowing the user to change the number of PIN verification tries that is set in the TRM. User must be authenticated by the old PIN before the number of PIN verification tries can be undated.
Initialize license area	Function allowing a license key specified by the user to be deleted, and a new PIN and retry counter value to be set.
Reset retry counter	Performs PIN verification of specified license area, and restores retry counter initial value. At the same time, this updates the retry counter reset PIN.

Authentication Mode and License Access Control

The PIN-SMMC features an expanded license area that has been independently added to the license area used of protected content distribution on the standard SMMC. In addition, the authentication requirements to access the license to this expanded license area can be further strengthened by combining PIN verification described above with machine certification verification, the requirement that the license can only be read out on a particular machine. These options are selected in advance in accordance with system security requirements when the administrator sets the license area and access conditions. These authentication functions can be flexibly combined and configured in various ways to protect sensitive data with different security requirements ranging from individuals to corporate or governmental database management systems.

APPLICATION SYSTEMS EMPLOYING PIN-SMMC

System Features

One of the most remarkable features of systems based on the secure memory card is that management of the key is left to the system itself. This means that, since the system itself is its own certification authority, the whole system of certifying cards and terminals has been drastically simplified and is administered without setting up a separate certification authority.

Another noteworthy feature of the product is that the key and encrypted data can be distributed separately. This would permit an arrangement in which anyone can download encrypted data from a system with access to the data and the key is distributed separately. For example, one might envision an arrangement in which the key is distributed to a user by being entered into the card in advance.

One can also set data access restrictions on the key, thereby only giving a user access to images, music, or other specific types of data.

Application Example (1)

For our first example, let us consider a PDA equipped with the PIN-SMMC.

Mobile handheld PDAs have seen widespread and growing popularity, and in combination with Hitachi's PIN-SMMC, would make a highly effective system for business purposes. For example, customer data or CAD data for a construction site could be encrypted and stored on a company's server, and employees could gain free access to the data over the company intranet using their PDAs. The administrator could then separately distribute keys to employees that would provide access to portions of the data based for example on data category, the particular duties of the employee, or other criteria. This would provide a highly secure system in which the data would not be compromised even if the memory card or the PDA was lost or stolen, and employees could not gain access to data that was not covered by the key they were given.

Application Example (2)

Further improvement in the performance of PDAs will permit these handheld devices to smoothly play back video, and this allow commuters to enjoy movies on their PDAs on their way back and forth to work and school. With this capability, we might envision a change in the video rental business so that commuters could download encrypted movies and games to their flash memory cards at kiosks conveniently located at convenience stores or on train platforms. Then, by purchasing the key corresponding to the encrypted content either at the same kiosk or by downloading it using a cell phone, users could play games or watch movies on their PDAs. The key could be programmed to restrict the number of times the content could be viewed, so there would be no reason or need to return the content, a fundamental change that could be the basis for a new rental video system (see Fig. 4).

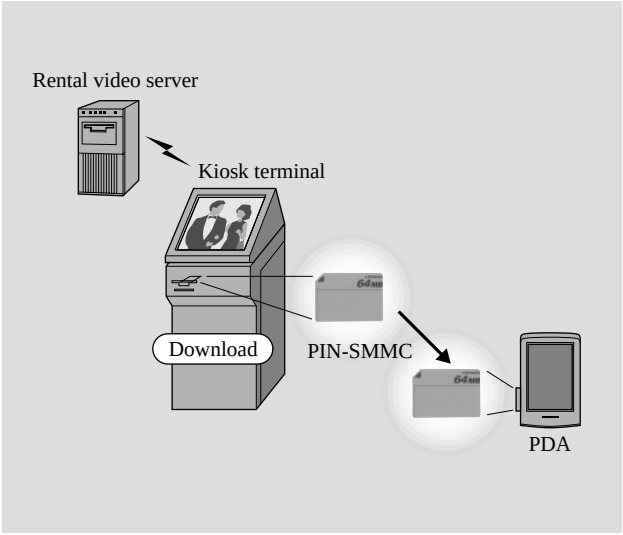

Fig. 4—Rental Video System Based on PDAs.
Movies and other types of content can be downloaded to a PDA from a kiosk terminal located in a convenience store or other public location. Limits can easily be set on the number of times the content can be viewed, so it is not necessary to return the content, a feature that could be the basis of a new rental system.

Hitachi's Actual PDA-based System

Finally, let us consider an actual application: a retail customer support system based on Hitachi's PDA, the NPD-10JWL, with the PIN-SMMC that went on the market in June 2002. (NPD-10JWL is currently on sale only in Japan.)

Unique with the NPD-10JWL is that it comes equipped with a wireless LAN interface as a standard feature. The system was designed to free sales personnel from having to constantly come back to main sales station computer for information so that they can remain at their assigned places throughout the store. All essential data including customer data (accumulated points based on purchases in the past, contact information, etc.), price information, and product availability can be viewed on the clerk's PDA which they carry around. Considering that this is confidential information, the PDAs are equipped with the PIN-SMMC.

Initially, all of the above information is encrypted by the company's server at headquarters. The key used in the process is then distributed to the various sales people using their ID numbers. In other words, the key is written onto the PIN-SMMC in advance before it is distributed to the sales clerks. The data is then sent from the headquarters server to servers in each store and on each floor, from where it can be successively downloaded over wireless LAN into the flash memory cards of the PDAs. The beauty of the system is that the sales personnel have the most up-to-date information at their fingertips at all times, and the PIN-SMMC ensures that data security will not be compromised even if the memory card or the PDA falls into the wrong hands.

CONCLUSIONS

Anticipating the advent of the ubiquitous information society, here we presented an overview of Hitachi's PIN-SMMC that provides a new level of security for protecting personal and corporate data on mobile handheld devices, and described several application examples.

Since content is protected by supporting an authentication security function, this not only permits expanded use of large-capacity memory on the same card, it also brings into being new value-added ways of use beyond simple storage. The size of the PIN-SMMC is smaller than that of an IC card, and can be accommodated in the expansion slot of compact mobile handheld devices, such as PDAs and cell phones. Users can store their most valuable confidential information on the card such as their address book, so all they have to do when they buy a new phone is switch the card over to the new phone.

Looking to expand mobile commerce applications for removable flash memory cards in compliance with the Mobile Commerce (MC) Extension Specification announced by Hitachi and four other companies in July 2002 (Ingentix, Matsushita Electric Industrial, SanDisk, and Toshiba), Hitachi will continue to push the security capabilities of removable flash memory cards and promote them as a key device for the now emerging age of ubiquitous information.

REFERENCE

(1) MMCA Technical Committee: The MultiMediaCard System Specification, Version 2.11, Official Release c (June 1999).

ABOUT THE AUTHORS

Akira Kanehira

Joined Hitachi, Ltd. in 1987, and now works at the Memory Application Department, the Memory Business Unit of the Semiconductor & Integrated Circuits. He is currently engaged in the development of next-generation flash card systems. Mr. Kanehira is a member of the Institute of Image Information and Television Engineers, and can be reached by e-mail at kanehira-akira@sic.hitachi.co.jp.

Jun Miyake

Joined Hitachi, Ltd. in 1984, and now works at the Memory Application Department, the Memory Business Unit of the Semiconductor & Integrated Circuits. He is currently engaged in the development of next-generation flash card systems. Mr. Miyake can be reached by e-mail at miyake-jun@sic.hitachi.co.jp.

Takashi Totsuka

Joined Hitachi, Ltd. in 1980, and now works at the Memory Application Department, the Memory Business Unit of the Semiconductor & Integrated Circuits. He is currently engaged in the development of next-generation applications for flash cards. Mr. Totsuka can be reached by e-mail at totsuka-takashi@sic.hitachi.co.jp.