Hitachi Releases PIN Secure MultiMediaCard as Industry's First Flash Card with User Authentication Function

— Personal Identification Number (PIN) reference is used to prevent data leaks to others and to protect personal information and confidential corporate data —

Tokyo, February 25, 2002— Hitachi, Ltd. (TSE: 6501) today announced the PIN Secure MultiMediaCard *[1] (PIN-SMMC) as industry's first Flash Card with user authentication function using a Personal Identification Number (PIN), as a recording media for confidential data that contains personal information or corporation information, and requires that leaks to others be prevented. As the first step, sample shipments of the 32 Mbyte HB28D032PSM2 will start in April 2002 in Japan.

This product has a content protection function, and is a flash card achieved by adding a user authentication function using a PIN to a Secure MultiMediaCard that achieves strong security. A PIN for getting the license key to decrypt the encrypted date is registered to data that has already been recorded, and that data can only be read when the PIN that is input corresponds to that PIN, thereby preventing data leaks to third parties. Consequently, when handling personal information or corporate confidential data on mobile devices such as PDAs, it is possible to protect the information even if the card or terminal is lost.

[Background]

In recent years, with the increasing market penetration of PDA and other mobile information devices, personal and corporate information is downloaded to these devices, and viewed and used away from the office with an increasing frequency. On the other hand, it is often the case that this personal information and corporate information is confidential, and under this usage environment, for example if a device is lost away from the office, there are fears about confidential information being leaked to a third party.

In response to this problem, data is generally encrypted or memory cards are locked using a password in an effort to protect the information. But using these methods the key to recover the encrypted data is on the same device as the information, resulting in fears that the key may be discovered by analysis of the software, or that if with the key, anyone may be able to view the data. In this way, the security of the data could not be described as infallible, and there is an increasing need for a system capable of achieving stronger security.

For these security systems it is also necessary that they do not require special hardware, but that instead can be achieved using general-purpose hardware.

To meet these needs, Hitachi has developed the PIN-SMMC, with the first product to be released the 32 Mbyte HB28D032PSM2.

[About this Product]

The main features of this product are as follows:

(1) First time in the world that a flash card has been equipped with a user authentication function using a PIN to protect personal information and corporate information
By registering a PIN, for getting the license key to decrypt the encrypted data, on data to be protected, it is only possible to read data when the correct PIN is input. This makes it impossible for anyone other than the authorized user to access the confidential data on the card.
The card is also equipped with the content protection function which has an established track record on conventional secure multimedia cards, and it is possible to handle the encrypted data and the license key required to restore the data separately. For example, by distributing license keys only to specific individuals or a specific rank within a company, it is possible to restrict the people who can access information. By combining user authentication with the copyright protection function, it is possible to create a stronger, more advanced data security system.

(2) Achieving PIN Authentication and Other Security Functions with Software
PIN authentication, data encryption and decryption, and other security functions can all be achieved with this card and device software. As long as it is a device with a MultiMediaCard *[2] slot, by installing this software it becomes possible to protect confidential data without requiring particular hardware changes to achieve security.

(3) Achieving Advanced Security through Tamper-resistant Hardware
With this product, PIN authentication, encryption/decryption and other security functions, and PINs and license keys and other security-related information is all stored in the hardware tamper-resistant module *[3], in the same way as conventional Secure MultiMediaCards. Advanced security is ensured against analysis by a third party in the event of loss of card or device.
By establishing a setting for the number of times a PIN is attempted, analysis of PIN code is rendered difficult, strengthening security from an application standpoint.

This card is upwardly compatible with standard MultiMediaCards, and external shape including thickness is the same compact size of 32 mm × 24 mm × 1.4 mm.

In the future, development into other capacities will be handled according to customer needs.

[Support Tools]

As support tools when designing PIN authentication application systems, reference software including encryption/decryption and authentication components, libraries and application interface specifications will be provided from April 2002.

Notes: 1. Secure MultiMediaCard is the collective name for MultiMediaCards which have been fitted with security functions such as content protection.

2. MultiMediaCard is a trademark of Infineon Technologies AG, Germany, and is licensed to MMCA (MultiMediaCard Association).
Hitachi is an MMCA Board Member. http://www.mmca.org/

3. Tamper Resistant Module (TRM): Tamper resistant technology physically and logically prevents internal analysis of or tampering with a semiconductor chip. TRM is the silicon module or card module which this technology is used to form.

< Typical Applications >

- Personal Applications
  All kinds of personal devices, such as PDAs and other portable information devices, PCs, mobile phones and digital cameras, etc.

- Business Applications
  - Corporate information network terminals
  - Business mobile devices

< Prices in Japan >(For Reference)

Product Code	Capacity	Price
HB28D032PSM2	32 Mbytes	Case by case

< Specifications >

Item	Specifications
Product code	HB28D032PSM2
Memory capacity	32 Mbytes
Interface	• MultiMediaCard • SPI (Serial Peripheral Interface)
Reading speed	1.7 Mbytes / sec
Writing speed*	1.0 Mbytes / sec
Operating voltage	2.7 V to 3.6 V
Operating current	When reading: 20mA (typ.) When writing: 35mA (typ.)
Operating temperature	- 25 to + 85 °C
Package dimensions	32 mm × 24 mm × 1.4 mm, 7 pins
Security functions	• PKI** encryption/decryption function • PIN authentication function

* Writing speed is the writing speed of the card itself, excluding the processing time on player side.

** PKI: Public Key Infrastructure technology