

Semiconductor Monthly

Flash Memory



Edited by Aimee Kalnoskas
Editor-in-Chief

Secure MultiMediaCard for Content Protection and E-Commerce



by Hank Ishihara, Hitachi, Ltd.

The distribution of the digital contents via networks has recently started on a large scale. Digital music distribution services have been especially popular. However, this has raised concerns over copyright infringement by means of illegal copying. SDMI (Secure Digital Music Initiative) defines the basic regulations for the content protection, which the participating companies must keep. In order to succeed in such distribution systems, it is necessary to protect digital contents with copyright protection technologies.

Focusing on the mobile phone market, Sanyo Electric, Fujitsu and Hitachi announced in December 1999 the "Keitai-Music" system that adopted "UDAC-MB (Universal Distribution with Access Control - Media Base)" and the CP-SMMC (Content Protection-Secure MultiMediaCard) as the DRM (Digital Right Management) to protect the digital music content.

shows how the encrypted content and the license are distributed in a mobile environment. First, the content is encrypted with a content key which is a symmetrical key and unique to the content. The encrypted content can be transferred to a CP-SMMC through any distribution channel including mobile network, Internet, CD-ROM, kiosk terminal, Bluetooth and wireless LAN, and stored in a plain area of a CP-SMMC. It is not necessary to be stored in a tamper resistant area since it is encrypted.

The charge to the encrypted content may not occur because the encrypted content cannot be played back without the content key. The content key and the access conditions (such as playable number) are combined as a license and stored in the license distribution server. The license is encrypted with a memory public key, and the encrypted license is downloaded from a license server to a CP-SMMC through a mobile network when it is purchased. Then, the encrypted license is decrypted with a memory private key, and the license is stored in a tamper-resistant area of a CP-SMMC. The right portion of Figure 1 shows how an encrypted content is played back at a portable player. First of all, the license in a CP-SMMC is encrypted with a player public key, and transferred to a player. The encrypted license is decrypted with a player private key and the content key to decrypt the encrypted content becomes available. The encrypted content is transferred from a CP-SMMC to a player and decrypted with the content key. Then, the content is played back with a player. This is the super-distribution concept. Having content makes no value but having license makes value. Therefore an encrypted content can be freely distributed without legal issue. A digital file can be shared between peers (peer-to-peer distribution).

Another benefit of UDAC-MB is that a cellular phone does not have to execute any ciphering operation since a CP-SMMC has a capability of ciphering operation. CP-SMMC also it executes a secure communication with a license server. A cellular phone, in general, does not have a powerful CPU to execute complicated ciphering operation. Therefore, UDAC-MB is suitable for digital music distribution, especially in a mobile environment.

Figure 2 shows a block diagram of a CP-SMMC. The security functions of a CP-SMMC were realized by the application specific commands (CMD55) on top of PKI. The representative examples of the content protection commands are READ_SECURE, WRITE_SECURE, ENCRYPT and DECRYPT. A ciphering engine is included in a CP-SMMC to execute encryption and decryption operation. The adopted ciphering algorithm for a symmetrical key is Triple DES and its key length is 112 bits. The Elliptic Curve has been chosen as an asymmetrical key algorithm and its key length is 163 bits. The robustness level of these ciphering algorithms is high enough to protect from attackers. The memory is divided into three areas: secure, semi-secure and plain. The secure area must be constructed by a

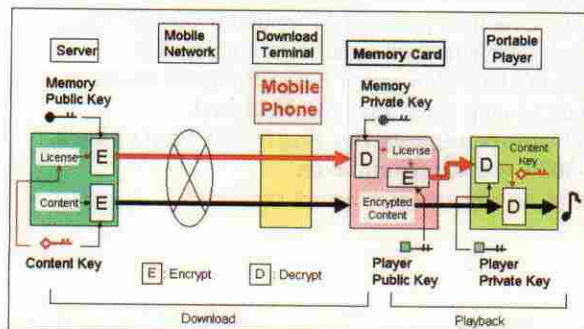


Figure 1. UDAC-MB content protection technology provides peer-to-peer distribution under PKI in mobile environments.

The UDAC-MB is based on the super-distribution system with PKI (Public Key Infrastructure), and allows both the encrypted content and its decryption key (the license) to be distributed separately. The left portion of Figure-1

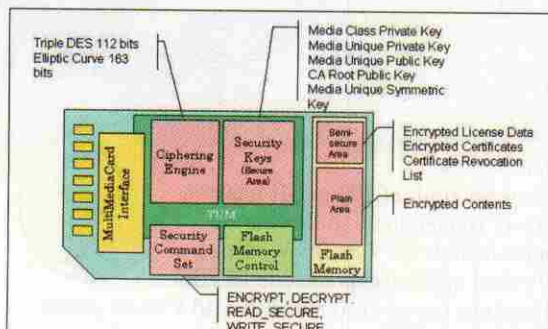


Figure 2. CP-SMMC contains security components such as a ciphering engine, security keys and a security command set.

Silicon Valley Direct

Edited by Chris Warner

North American Semiconductor Equipment Manufacturers' October 2001 Book-to-Bill Ratio Improves Slightly

Semiconductor Equipment and Materials International (SEMI) has reported that North American-based manufacturers of semiconductor equipment posted \$651.1 million in orders in October 2001 and a book-to-bill ratio of 0.71. Thus, \$71 worth of new orders were received for every \$100 of product shipped for the month.

The three-month average of worldwide bookings in October 2001 was \$651.1 million. The bookings figure is 5 percent above the revised September 2001 level of \$619.2 million and 78 percent below the \$2.99 billion in orders posted in October 2000. October 2000 marked the orders peak of the current cycle for North American-based manufacturers.

The three-month average of worldwide billings in October 2001 was \$916.2 million. The billings figure is 5 percent below the revised September 2001 level of \$967.4 billion and is 64 percent below the October 2000 billings level of \$2.57 billion. October 2000 also marked the billings peak of the current cycle.

"Excess capacity and weak end-market demand continue to beleaguer the semiconductor equipment industry," said Stanley Myers, president and CEO of SEMI. "While the decline in orders has abated, the average monthly shipment figure continues to weaken, and there is no appreciable indication of a near-term trend reversal."

The SEMI book-to-bill is a ratio of three-month moving average bookings to three-month moving average billings for the North American semiconductor equipment industry (not shipments and orders of the chips themselves).

Client and Access Point Chipsets

Resonext™

Communications, Inc. has announced the RN5200 family of 5 GHz Wi-Fi5 (802.11a) WLAN chipsets optimized for client and access point (AP) platforms. The Resonext RN5200 chipset family consists of two chipsets targeted at both WLAN clients and APs. Both chipsets incorporate True Zero-IF 5 GHz CMOS radio, flexible Media Access Control (MAC), Access Point on a Chip (APoC) architecture and AccuChannel™ equalization technology. These technologies, combined with full IEEE 802.11i compliant security features implemented into the chipsets, enable OEMs to reduce the cost of their client and AP products while offering differentiated features.

Both the RN5200 client and AP products consist of two chips — an integrated radio frequency (RF) chip and a baseband/MAC IC — each built on the standard 0.18 μ, 1.8 V CMOS process. The RN5200 client and AP chipsets are fully 802.11a compliant and support the 5.15 GHz to 5.35 GHz UNII bands and up to 54 Mbps data rate. The AP chipset, consisting of the RN5200R radio and the RN5200P baseband/MAC IC, enables the low-cost, high-performance and feature-rich AP platforms. The client chipset, comprised of the RN5200R radio and RN5200C baseband/MAC IC, delivers low power consumption and differentiable PC cards or mini-PCI cards.

Resonext's RN5200R single-chip RF transceiver reduces system design complexity, cost and power consumption while enabling high performance and small form factor platforms. The RN5200R incorporates the company's 5 GHz True Zero-IF CMOS radio, which directly converts 5 GHz to baseband frequencies without any intermediate frequency stages. This architecture is integrated with the required low noise amplifier (LNA) filters, phase lock loops (PLL) and voltage controlled oscillators (VCO) in the 0.18 μ, 1.8 V CMOS process.

For the AP systems, the RN5200 AP chipset adds the Access Point on a Chip (APoC) architecture in the RN5200P. This reduces



Two chipsets enable end-to-end wireless LAN for 5 GHz clients and access points.

continued on page 26

continued on page 27

Semiconductor Monthly

Flash Memory

tamper resistant module, and includes license data, key data, seed of random number, transaction log data and hash value of certificate revocation list. The pre-programmed key data at a card manufacturer are Media Class Private Key, Media Unique Private Key, Media Unique Public Key, Certificate Authority Root Public Key and Media Unique Symmetric Key.

The semi-secure area includes encrypted license data, encrypted certificates and a certificate revocation list. The certificate is generated based on the X.509 standard at a certificate authority and provided to a card manufacturer. It includes the information of the corresponding public key, the value of the public key, the name of the certificate authority and the digital signature encrypted by the certificate authority's root private key.

The plain area includes encrypted contents and non-secure data. A secure area and a semi-secure area cannot be accessed by normal MultiMediaCard commands.

In November 2000, DDI-Pocket, a mobile phone operator in Japan, became the first digital music distributor in the world to use the mobile phone. In this distribution service — so-called "Sound Market" — DDI-Pocket adopted the "Keitaide-Music" system and a CP-SMMC as a storage media for digital music. The Certificate Authority has been operated with RIAJ (Record Industry Association Japan), and approximately 30 content holders have been providing around 2000 contents with the "Sound Market" service. The "Sound Market" has been well accepted by mobile phone users, but this market is still under development.

Content protection does not only mean music distribution, but also personal and corporate data security. The CP-SMMC, based on the PKI technology, is also useful for these purposes. For example, a PDA can be a trusted device by a CP-SMMC to protect a personal secret data such as credit card information, and distrib-

uted corporate confidential data such as customer information.

E- and M-Commerce

In June 2001, the MultiMediaCard Association approved the Secure MultiMediaCard specification for the M-Commerce (Mobile Commerce) application based on the WIM (WAP Identity Module) functions defined at the WAP (Wireless Application Protocol) forum. It contains the same functions as the Smart Card, so a user downloads the digital content to his/her card and pays its fee by the same card under PKI. Moreover, it can be used as the electronic money. The third generation mobile phone with the M-Commerce Secure MultiMediaCard is expected to become the vital tool for mobile commerce.

The security functions were realized by the WIM and smart card commands. Therefore, the function of this card is variable depending on the application software within the EEPROM in the card. This card is generic enough for any security function related application including payment, ticketing and even content protection.

Conclusion

Secure MultiMediaCards, based on the Public Key Infrastructure, will provide seamless security for the personal data storage, corporate data storage, copyrighted data storage and mobile commerce. They will develop new businesses and new markets such as digital music distribution and financial transaction.

Haruji (Hank) Ishihara is the chief engineer at the Media Flash Memory Business Unit, Semiconductor and IC group of Hitachi, Ltd. Mr. Ishihara was born in 1952. He graduated from Akashi-Kosen College and joined Hitachi in 1972. He worked at Hitachi America Limited as memory product marketing manager from 1993 to 1997. He has been Chief Engineer responsible for Flash memory and Flash card products since 2001. He is located at Nippon Bldg., 6-2, Otemachi 2-chome, Chiyoda-ku, Tokyo, 100-0004 Japan; +81-3-5201-5021; www.hitachi.com. He can be reached via email at ishihara-haruji@sic.hitachi.co.jp.

Write in 138 or
www.ecnmag.com/info

EDITORIAL EVALUATION

Write in Number or Reply Online
I found this article:

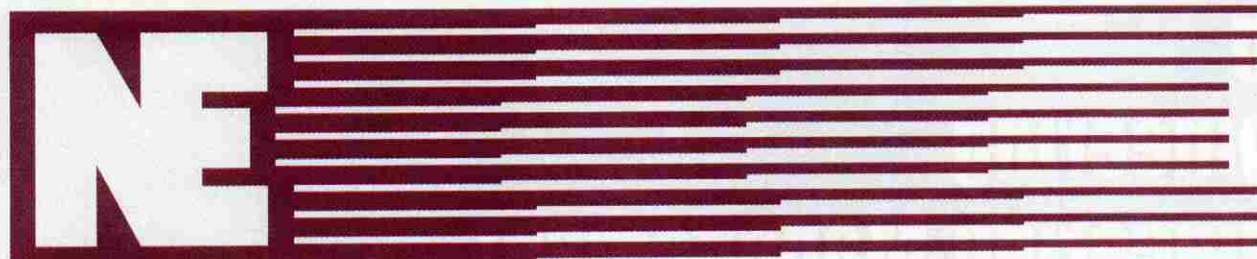
Very Useful	Useful	Not Useful
126	127	128

Say you saw
it in
ECN

Low Voltage Low Cost High Performance Device Programmers



Visit our website for complete product information
and the latest Windows software support.



NEEDHAM'S ELECTRONICS, INC.

www.needhams.com

4630 Beloit Drive, #20 • Sacramento, CA 95838 • (916) 924-8037 • FAX (916) 924-8065 (Mon. – Fri. 8 am – 5 pm, PST)

Write in 125 or www.ecnmag.com/info