Campus Smart Cards with Public-Key Infrastructure*

Chung-Huang Yang
Department of Information Management
National Kaohsiung First University of Science and Technology
Kaohsiung, Taiwan, R.O.C.
Email: chyang@ccms.nkfu.edu.tw
http://www.nkfu.edu.tw/~chyang/

ABSTRACT

The main objective of this research is to design campus-wide secure information systems using multi-purpose smartcards as the portable security devices. The security of our system is mainly based on public-key cryptography. In our campus card, we incorporate a Hitachi H8/3113 chip module into Philips Mifare contactless IC card to provide dual-interface campus applications, such as for physical access control, electronic mail, library book lending system... etc.

Keywords: smartcard, IC card, cryptography, public-key infrastructure, certificate, digital signature.

1. Introduction

The magnetic and IC cards [1-2] has a history of more than 20 years and these cards are more or less a part of the way that we live and do business. Systems utilizing these plastic cards are emerging in countries worldwide and the use of credit cards, ATM (automatic teller machine) cards, identification cards are a part of the way of life in most industrialized countries. With substantial cost reductions and the ability to handle multiple applications on a single card, the IC cards are about to enter a period of rapid growth. An individual bearing a single IC card will be able to electronically and securely interact with several servers or service provides. As a consequence, an entirely new type of commercial and educational landscape is being created.

The Taiwan government has been promoting the usage of IC cards, starting from early 1990s. The bank industry has issued over 2 million smart cards which have 56-bit DES [3] cryptographic function inside, but they also have limited applications on the fast growing Internet since these financial cards do not provide the internal generation of digital signature for non-repudiation. Such non-repudiation service protects against one party to a transaction or communication activity late falsely denying the transaction or activity occurred. Today huge number of telephones IC cards are in use, but these are simply proprietary memory IC cards, which have limited applications. Last year the "IC Card with Combined National ID and Health Insurance Card Functions (or Citizen's Card)" project was announced where government hope to find a private contractor to carry out the project [4]. Finally, the Freeway Electronic Toll Collection (ETC) Project was established last year, which uses contactless IC card to collect toll on the national Freeway. At present the ETC project is on filed trial at several tool station to pave the way for shorten the collecting time, save manpower, and decrease the energy consumption and air pollution [5].

We will design secure campus-wide information systems using multi-purpose smartcards as the main security devices. In our campus card system, the same smartcard will

* This research was supported in part by the National Science Council, Republic of China, under grant NSC 89-2213-E-327-002

have multiple applications, such as for the identification, door access control, electronic mail, electronic document interchange [6], library book lending system, transcript record and request... etc. Since the security of our system is based on the use of public-key cryptography [6] while currently the financial information in Taiwan is protected by the DES-based private-key cryptosystems, our main applications are for on-campus non-financial applications.

2. Campus Information Security

The college and university environment offers one of the best opportunities for the adoption of smart card technology. Faculty, staff, and students are generally willing to adopt new technologies and government is usually also willing to provide research funding for the research and development of highly evolved new systems. It is a trend that both bank cards and credit cards will evolve to smart cards and through the use of combination of magnetic stripe and smart card, the old existing systems could be kept to co-exist with new smartcard-based systems.

The information security services on campus shall include data confidentiality, authentication, access control, data integrity, and non-repudiation. However, mainly due to the impose of export controls, one could not implement a secure campus card system using off-the-shell email systems. And at the Department of Information Management (MIS), National Kaohsiung First University of Science and Technology, we had decided to develop the needed cryptographic functions by ourselves. An overview of our campus card system is shown in Figure 1.

We design such campus-wide multi-purpose smartcard systems use the XML (extensible markup language) [8] as the document standard, design the needed interface format between smart cards and the security management center, and provide non-repudiation, authentication, and confidentiality by using both public-key cryptography and private-key cryptography. Our system makes use of the idea of *digital envelope* and *digital signature* [9] of the public-key cryptography. Instead of using the commonly selected DES encryption algorithm, we decide to use the triple-DES encryption algorithm [10] since it was shown that the 56-bit DES encryption algorithm could be cracked within one-day [11].

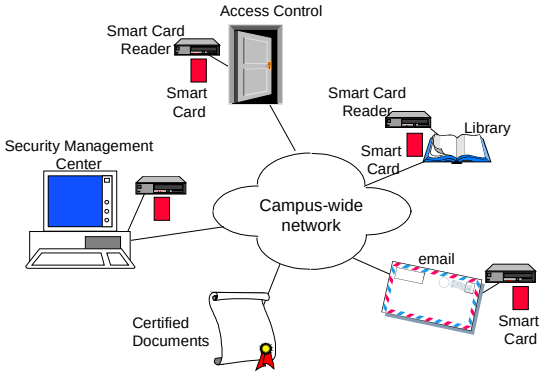

Figure 1: An overview diagram of the campus card system

A Sun's Ultra 10 Workstation running Solaris was setup as part of the security management center, which provides functions of a directory server (the CDC IntraStore) and will provide secure WWW service. On the other hand, an IBM Netfinity 5000 running Windows NT, isolated with the Internet by a firewall (the Checkpoint FireWall-1), serves as a self-developed certificate authority (CA). The certificate format is based on X.509 [12] and Figure 2 shows the client-side software where user interface is in traditional Chinese.

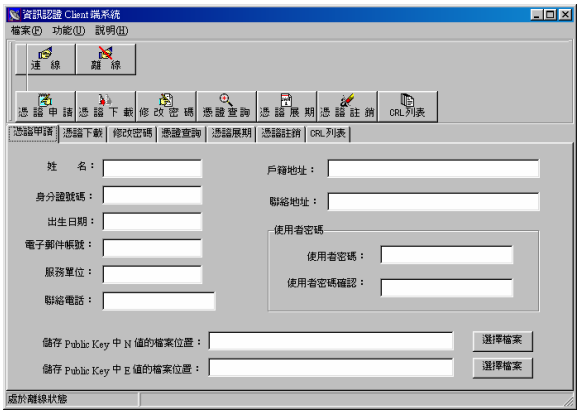

Figure 2: Certificate management at client

The developing schedule of our campus card system is given at Table 1. We had already completed the prototype development of a client and server CA and a smartcard-based secure email system (see Figure 3) on Phase I. Moreover, we developed a stand-alone file

protection system using smart card to store encryption/decryption key and digital signature key.

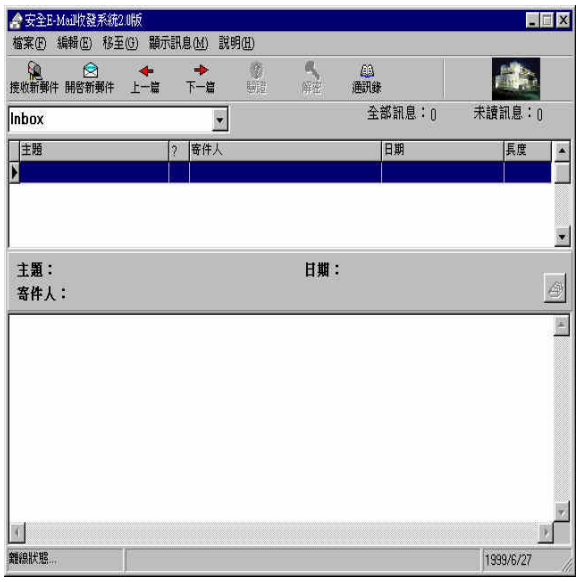

Figure 3: Smartcard-based secure email

Phase I (98/08~99/07)	● Certificate Authority ● Smartcard-based Secure Email System ● Smartcard-based File Protection System
Phase II (99/08~00/07)	● Smartcard Chip Operating System ● IC Card Door Access Control System ● Smartcard Issuing Management System ● Smartcard-based Secure File Transfer Protocol ● Smartcard-based Secure WWW

Table 1: Development schedule of the campus card system

We employ off-the-shelf smartcards (from the G&D) on Phase I and our application software had been integrated with the device driver of battery-powered Smarty (from the Fisher) smartcard reader that works directly from PC's floppy disk drive. On Phase II we will develop a chip operating system (COS) and then use our own smartcard to replace off-the-shelf card used in Phase I. The main functions of COS include data communication interface [13] between card and card reader, command interpretation, file management, cryptographic key management, and cryptographic algorithms. Our smartcard actually is a combination of both contactless memory IC card with contact smartcard and more details is given on the following section. We will also develop an IC-card door access system to provide secure access to major facilities.

3. The Smart Card

There are several types of IC cards, including memory, microcomputer, and contactless cards. The microcomputer-based IC cards (the smart cards) have always stimulated the fantasies of technology to require ever more sophisticated functionality. Several IC manufacturers, (such as Philips, Siemens, Hitachi, SGS-Thomson, etc.) offer family of chips to be integrated in smart cards. In Table 2 we summarize the specifications of lately announced smartcard chips.

Chip	P8WE5032	SLE 66CX160S	H8/ 3113
Manufacturer	Philips	Siemens	Hitachi
Process	0.35 ③m	0.6 ③m	0.5 ③m
CPU	80C51	8051	H8/300
ROM (bytes)	32K	31.5K	32K
EEPROM (bytes)	32K	16K	16K
RAM (bytes)	2.3K	2K	2.5K
Arithmetic Coprocessor	Yes	Yes	Yes
Random Number Generator	Yes	Yes	Yes

Table 2: Specifications of latest smartcard chips

The smartcard IC chip that we adopted is Hitachi 0.5-③m H8/3113 [14] microcomputer. It offers an 8-bit RISC-like H8/300 microprocessor, 32-Kbyte ROM, 16-Kbyte EEPROM, 2K-byte general-purpose RAM, an arithmetic coprocessor with special-purpose 512-byte RAM capable of performing 1024-bit ABR^{-1} *mod* N Montgomery modular multiplication, a random number generator, and a watchdog timer. Figure 4 shows the block diagram of the Hitachi H8/3113 chip.

The ROM area of the chip is used for chip

operating system while the EEPROM is used for personalized data and for storing cryptographic keys with data retention time of 10 years and rewrite endurance of 100,000 times. The chip also has many built-in protection measures to prevent physical attack. These measures include high/low frequency detector, high/low voltage detector, concealment of ROM code, scattered layout, multi-metal layer, removal of test pin, etc.

The Hitachi chip module will actually insert into milled hollows and mounting in the pre-molded Mifare [15] contactless IC card (from the Philips). In this way we provide two independent smart card interfaces, one is the contactless interface which uses memory IC for door access control system, and the other is the contact interface which uses Hitachi H8/3113 chip to provide high security needed in most applications.

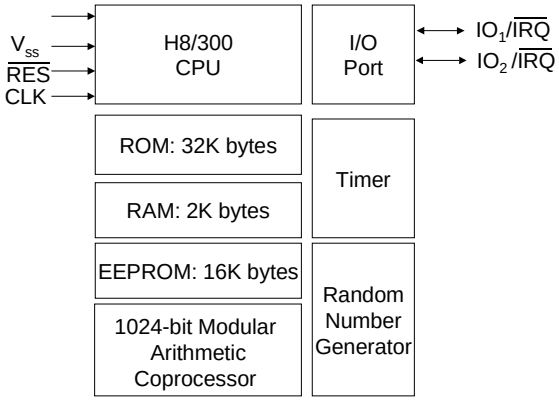

Figure 4: Block diagram of the Hitachi H8/3113 smartcard chip

4. Conclusions

As Internet grows in scale almost every year, security measures are expected to become all the more important on campus. We have presented a design of secure campus card system where communication security was made an integrated part within the system.

REFERENCES

[1] W. Rankl, W. Effing, R. Wolfgang, *Smart Card Handbook*, John Wiley & Sons, 1997.

[2] M. Hendry, *Smart Card Security and Applications*, Artech House, Inc., 1997.

[3] National Institute of Standards and Technology, “Data Encryption Standard,” Federal Information Processing Standard, FIPS PUB 46-2, December 1993.

[4] *Request for Proposal for IC Card with Combined National ID and Health Insurance Card Functions (Citizen's Card)*, R.O.C. Executive Yuan IC Card Planning &Promotion Task Force, June 1998, http://www.gsn.gov.tw/eng/iccard/erfp0610.html.

[5] *Request for Proposal On Board Unit-Related Technology Transfer for Freeway Electronic Toll Collection System*, Chunghwa Telecom Labs**,** May 1999, http://www.etc.com.tw/RFT-English-Final.doc.

[6] Chung-Huang Yang, Shy-Ming Ju, and T.R.N. Rao, "A Smartcard-based Framework for Secure Document Exchange, " *Proc. IEEE 32nd Annual 1998 International Carnahan Conf. On Security Technology*, October, 1998, pp. 93-96.

[7] Alfred J. Menezes, et al, *Handbook of Applied Cryptography*, (CRC Press Series on Discrete Mathematics and Its Applications), 1996.

[8] Extensible Markup Language (XML) 1.0, W3C Recommendation, February 10, 1998. http://www.w3.org/TR/ REC-xml.

[9] C. H. Yang, S. L. Yen, H. D. Liu, K. Liu , B. S. Jeng, K. Y. Chang, M. S. Chang, Y. L. Cheng, J. L. Liang, and D. M. Shien, “Secure Official Document Mail Systems for Office Automation,” *Proc. 31st Annual 1997 International Carnahan Conf. On Security Technology*, October, 1997, Australia, pp. 161-164.

[10] Announcing Draft Federal Information Processing Standard (FIPS) 46-3, Data Encryption Standard (DES), and Request for Comments, *Federal Register*, Volume 64, Number 10, January 15, 1999, http://csrc.nist.gov/cryptval/des/fr990115.htm.

[11] "Cracking DES code all in a day's work for security experts, " http://cnn.com/TECH/computing/9901/21/descrack.idg/index.html. See also " RSA Code-Breaking Contest Again Won by Distributed.Net and Electronic Frontier Foundation (EFF) - DES Challenge III Broken in Record 22

Hours," http://www.rsa.com/pressbox/ html/990119-1.html.

[12] ITU-T Recommendation X.509 “Information Technology - Open Systems Interconnection - The Directory: Authentication Framework,” 1993.

[13] ISO 7816 Part 1 to 6: Identification Cards – Integrated Circuit(s) Cards with Contacts, 1987 to 1996.

[14] Hitachi Single-Chip Microcomputer H8/3113 Hardware Manual, Hitachi Ltd., 1998. See also http://www.hitachi-eu.com/hel/ecg/products/smartcard/ h8_3113.htm.

[15] http://www-eu3.semiconductors.com/ identification/products/contactless/mifare/ ics50/.