

Embedded Electronic Smart Card for Financial and Healthcare Information Transaction

Lakshmisha Honnegowda, Syin Chan, and Chiew Tong Lau

Abstract—This paper gives a brief introduction to next generation electronic smartcard and its application in finance and healthcare sector to store and control the card holder’s account and personal sensitive information such as electronic medical record (EMR), respectively. The survey explains how the modern technology is being integrated, smart card and corresponding framework, to provide the portability to personal health care information in order to benefit patient, health care provider, and health insurer. This survey examines electronic smart card as an efficient solution to meet those crucial security requirements (privacy, confidentiality, Integrity and Authenticity) of health care information and e-commerce transactions. The discussion is extended to touch on research opportunities and future trends in electronic smart cards.

Index Terms—Electronic smartcard, electronic medical record (EMR), e-commerce, healthcare.

I. INTRODUCTION

Medicine and technology advancements are boosting the life expectancy to twice as long as 100 years ago. These advancements provide high quality of medical care, but with increase in cost.

The quality of medical care and health cost [1] increase in many developed, as well as developing, countries are triggering for an innovation in health care. In an emerging world of e-commerce, the healthcare can be improved by meeting the following essential requirements:

- Quick and secure personal information access without compromising the privacy
- Patient data access authentication
- Public/private key distribution
- Patient data integrity, confidentiality and security
- Digital signatures and certificates
- Provide portability for patient’s medical records and convenience
- Purchasing prescriptions through specific e-commerce transactions
- Reduction in medical fraud
- Improve communication and enhance quality

Advancement in miniaturization of battery operated electronic devices and semiconductor chips help to upgrade the existing medical systems. The smart card with an embedded crypto engine is cost effective, more reliable,

efficient, and secure solution to meet those crucial requirements of healthcare. The smartcard technology provides the unique solution that combine quick access to secure information and management of patient data mobility and privacy. Smart health cards with corresponding information technology framework help to improve health services and reduce costs [2] for both patients and service providers.

II. ELECTRONIC SMART CARD – AN OVERVIEW

Electronic smartcard is an embedded device contains secure microprocessors and standard peripheral components. Unlike normal smart cards, the next generation electronic smart cards [4], [5], [7] are standalone battery powered cards with communication port for external interface.

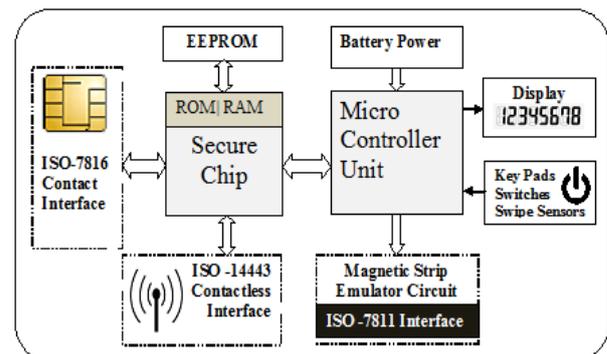


Fig. 1. Electronic smart card components

Secure Chip: Secure processor in the electronic card is responsible for contact (ISO/IEC-7816) or contactless (ISO/IEC – 14443) secure interfaces. The secure chip is powered either by these external interface (ISO- 7816 /14443) or an internal master controller. It is a power full chip that can be programmed for different application enables to store and access sensitive data. Applications securely exchange data with external interface. The primary requirement of this chip is to encrypt all sensitive information on the card, tamper proof, and securely communicate with Card Acceptance Device (CAD) or smart card readers.

Micro Controller Unit: This chip is directly powered by the battery and communicates with secure chip to get sensitive data securely to display [6] or to perform transaction via magnetic stripe emulator [3]. The chip interacts with an external entities, card user or readers, through peripheral devices.

Communication Ports: Communication port is a channel/medium through which the card interfaces with external smartcard or magnetic readers for sensitive data

Manuscript received November 10, 2012; revised December 24, 2012.

Lakshmisha Honnegowda, Syin Chan, and Chiew Tong Lau are all with the School of Computer Engineering, Nanyang Technological University, Singapore 639798 (e-mail: {honn002, asschan, asctlau}@ntu.edu.sg).

transactions. This includes EMV contact plate (ISO/IEC 7816), magnetic stripe emulator (ISO/IEC 7811), and radio frequency (RF) interface (ISO/IEC 14443) on the card to conform to international interface standards. This conformation enables the electronic smart cards to be interoperable.

III. ELECTRONIC SMART CARD APPLICATION

Smartcards with storage facility can typically be used to store data, to prove identity and as a key to access information. In healthcare application that translates to storing patient's sensitive personal information on the card, giving access to secured healthcare networks, and proving entitlement to healthcare benefits.

The smart card technology is an ideal choice for handling sensitive healthcare and e-commerce information transactions as it renders high level of security and privacy protection.

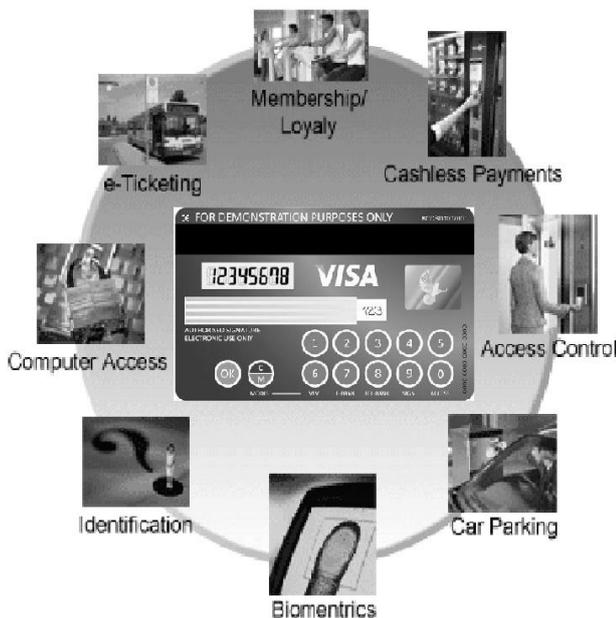


Fig. 2. Multiple application of electronic smart card

The capability of secure chip in electronic smart card to deploy multiple applications-like a pre-payment (e-ticketing), access control (network authentication), credit & debit cards (Visa card, MasterCard, and ATM cards), security token card (online and mobile banking) greatly reduces the bulk in one's wallet. The bulk here refers to average number of credit/debit/ATM cards [9] in card holder wallet.

IV. BENEFIT OF SMARTCARD IN HEALTHCARE

Mobility and maintenance of portable medical data are drawing attention in recent years. Accordingly, there has been a significant effort [10] to establish and refine corresponding healthcare standards for transaction of sensitive private information. Studies [11], [12] have demonstrated that ambulatory electronic health records (EHR) save billions of dollars due to reduction in repeated laboratory and radiology tests. As a proposed solution, the hybrid combination of 'centralized data repositories' and 'record locator services(RLS)' infrastructure with smartcard helps to achieve

a true interoperability among healthcare community.

Smartcard technology can enhance the privacy and confidentiality [8] of personal healthcare information. Healthcare cards work in a very similar manner to credit/debit cards and they are intuitively easy to use. This technology requires minimal infrastructure, reader and viewer software, to maintain portable sensitive data. Smart health card facilitates the portability of electronic medical records which renders benefits to healthcare stakeholders/entities, namely Patients, Healthcare Professionals/Providers and Health Insurer/Payers, involved in healthcare.

A. Benefits to Patients

- Positive identification to health professional and to system via self-service kiosks
- Expedite the registration/admissions process and reduces healthcare costs
- In emergencies, smartcard can enable immediate access to potentially lifesaving information.
- Expedites claims reimbursement
- Increases privacy and security
- Helps in management of chronic diseases
- Helps to track health information from all healthcare providers during the course of treatment
- Gain control over access to personal Electronic Medical Records
- A single integrated form factor with payment capability will give patients an ability to manage their expenses and services.
- Helps to provide easy and secure medical care.

B. Benefits to Healthcare Providers

- Accurate patient identification across health organizations
- Integration with health information exchange and locator systems
- Provides secure and convenient access to patient healthcare information
- Improves communication and medical records management
- Improves quality of care and administrative efficiency
- Improves emergency care with rapid availability of critical medical information
- Eases care of drug addicts
- Helps to review medication, diagnoses and allergies history in order to eliminate the conflict with the proposed course of treatment
- Prevents administrative errors and streamline the payment process
- Plays a key role in encouraging patients to participate in clinical research and studies with their control over personal data access
- Link or data pointers stored on the healthcare card can help physician to refer and review patient's complete health information located in remote database

C. Benefits to Health Insurer

- Helps to streamline paper-intensive health insurance claims system and eliminates delayed paper process.
- Save money from improper payments
- Authentication of the cardholder as the insured reduces medical fraud by eliminating card swapping, tampering, and cloning.

- Ensure treatment is restricted to covered services and prescriptions.
- Availability of a patient's up-to-date healthcare treatment record.
- Reduces incidence of fraud in healthcare benefit claims
- Improvement in claims processing which helps in reducing the reimbursement lengthy delays.
- Provides reliable data for patient's eligibility verification during their claims processing.

V. CONSTRAINTS IN ELECTRONIC SMARTCARD

As a battery-operated embedded device, the electronic smartcard faces numerous challenges to meet the security and lifespan requirements in both healthcare and financial applications.

A. Security

A study estimates that millions health care cardholders are victims of medical identity theft [13]. The same study found that 63% of the cases, forged cardholder name to obtain medical treatment or service, and in 43%, forged cardholder name to obtain government benefits, such as Medicare and Medicaid. The high-profile breaches of protected health information, in recent years, occur because sensitive personal information is stored on unsecured, unencrypted devices such as magnetic tapes, compact disks and USB flash drives, and also due to unauthorized access of medical records.

The smart card and corresponding infrastructure must implement security operations that guarantee cardholders authentication, data integrity, privacy and confidentiality of the patients' medical records. For example, to address electronic health record (EHR) privacy issues the smartcard frame work must be ensured that the Health Insurance Portability and Accountability Act [14] is observed. The key stipulated condition of the HIPAA privacy rule is to assure that the personal health information of an individual is properly protected and provide access and usage control to individual/patients.

The secure-chip technology adapts cryptographic encryption algorithms to secure the transaction of sensitive information. These secure algorithms design, public/private key based, must meet important requirements such as proper management of keys, computationally inexpensive and efficient (in terms of energy and memory space) code.

B. Lifespan

The lifetime of an electronic smartcard is a key performance metric. It can be estimated based on preliminary studies performed on simulations and real hardware specifications. These studies are usually based on assumptions:

- Power consumption at sleep and active states of the card
- Enable and disable of peripherals at different states of the electronic smartcard

Estimations based on assumptions usually fail to consider the non-linear behavior and large performance spread of real world batteries used in the electronic smartcard. The analysis [15] on battery characteristics shows that various parameters including discharge rate, the duty-cycling and the charge

pumps affect the usable battery capacity.

The automated battery life test, which simulates the actual functionality and usage of the card, performed on the branded electronic smartcard batteries (capacity 3V, 14mAh) shows, on the average, 77% of battery capacity shall be used up when the battery voltage drops to 2.5V.

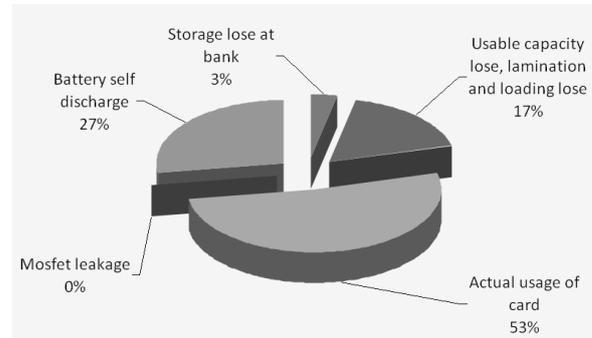


Fig. 3. Power distribution of battery capacity based on actual scenario

The power distribution analysis of the whole battery capacity, Figure 3, shows the actual usage of the card constitutes 53% of the total battery capacity which direct impact on the card lifespan.

VI. OPEN RESEARCH PROBLEMS AND FUTURE TREND

The next generation battery-operated electronic smartcards [4] [6] embed secure chip and magnetic stripes to initiates both EMV transaction as well as magnetic stripe data transaction, respectively. The smart secure-chip with multiple applications (healthcare, banking, entertainment, and transportation) provides contact (ISO/IEC- 7816) or contact less (ISO/IEC – 14443) secure interface with an EMV-compliant point-of-sale terminals. The magnetic stripe emulator in the card energizes and generates F2F data format, comply with ISO/IEC-7811 standard [39], only when the card is swiped across the POS terminal's magnetic read head. This novel feature of dynamic magnetic stripe, data disappear when the card is not being used, makes the card immune to fraud by skimming. And electronic smartcard's dual capability makes a bridging technology to support both EMV-compliant as well as magnetic stripe transaction.

Despite the advancement in credit/debit cards, three are many challenges that still need to be addressed, especially on readability of dynamic magnetic stripe data across all types of terminal readers in the market, energy efficient security algorithms to enhance the battery life time, and improvement to card manufacturing process to deliver reliable and robust electronic smartcards.

REFERENCES

- [1] S. Woolhandler, T. Campbell, and D. U. Himmelstein, "Costs of health care administration in the United States and Canada," *New England Journal of Medicine*, vol. 349, no. 8, pp. 768–775, 2003.
- [2] GAO, "Health and Human Services' Estimate of Health Care Cost Savings Resulting from the Use of Information Technology," GAO-05-309R, February 17, 2005.
- [3] H. Lakshmisha, W. C. Weng, C. Liu, and E. Foo, *Method for broadcasting a magnetic stripe data packet from an electronic smart card*, US Patent #8,226,001 B1, July 24, 2012.

- [4] E. Foo, J. Ziegler, Z. Alon, M. Poidomani, C. McGuire, and L. Rouhthenstein, *Electronic Card and Methods for Making Same*, US Patent #7,954,724 B2, June 7, 2011.
- [5] S. G. Narendra, P. Tadepalli, T. N. Spitzer, *Electronic Transaction Card Powered by Mobile Device*, US Patent Application Publication #7,954,716 B2, June 7, 2011.
- [6] J. D. Mullen and B. Cloutier, *Payment Cards and Devices with Display, Chips, RFIDs, Magnetic Emulators, Magnetic Decoders, and Other Components*, US Patent #7,784,687 B2, August 31, 2010.
- [7] S. G. Narendra, P. Tadepalli, and T. N. Spitzer, *Electronic Stripe Cards*, US Patent Application Publication #7,364,092 B2, April 29, 2008.
- [8] *Privacy and Security Framework Requirements and Guidance for the State Health Information Exchange Cooperative Agreement Program*, Department of Health & Human Services, Office of the National Coordinator for Health Information Technology, Public Information Notice, Document Number ONC-HIE-PIN-003, March 22, 2012.
- [9] Federal Reserve Bank of Boston. (2011). *The Survey of Consumer Payment Choice*. [Online]. Available: <http://www.creditcard.com>.
- [10] GAO, "Health Care: National Strategy Needed to Accelerate the Implementation of Information Technology," GAO-04-947T, Washington, D.C., July 14, 2004.
- [11] Center for Information Technology Leadership, "The Value of Healthcare Information Exchange and Interoperability," Boston, 2004, and "The Value of Computerized Provider Order Entry in Ambulatory Settings," Boston, 2003.
- [12] GAO, "Health and Human Services' Estimate of Health Care Cost Savings Resulting from the Use of Information Technology," GAO-05-309R, February 17, 2005.
- [13] Ponemon Institute© Research Report. (March 2011). *Second Annual Survey on Medical Identity Theft*. Available: http://www.protectmyid.com/images/education_center/pdf/050TypesofFraud/1_types%20of%20fraud_medical%20study.PDF
- [14] *Health Insurance Portability and Accountability Act (HIPAA) Privacy & Security Rule*, 45 CFR 160-164.
- [15] S. Park, A. Savvides, and M. Srivastava, "Battery Capacity Measurement and Analysis using Lithium Coin Cell Battery," in *Proc. International Symposium on Low Power Electronics and Design (ISLPED'01)*, Huntington Beach, CA, USA, Aug 2001.