JOURNAL OF OBJECT TECHNOLOGY

Online at http://www.jot.fm. Published by ETH Zurich, Chair of Software Engineering ©**JOT, 2004**

Vol. 3, No. 5, May-June 2004

Smart Cards: Status, Issues, and US Adoption

Won Kim, Cyber Database Solutions, Austin, Texas, U.S.A.
He-Joon Kim, Department of Computer Science, University of California, Los Angeles, U.S.A.

Abstract

The smart card has a microprocessor or a memory chip embedded in a plastic card. It has been in wide use in Europe and Japan for payment, entry into buildings and computer systems, and storage and access of special types of information. In the US, despite efforts by the credit card industry, the smart card has not been nearly as widely adopted as in Europe and Japan. In this article, we will review the status of the technology and applications of the smart card. Then we will summarize various issues that hinder a wider adoption of the smart card, particularly in the US, and discuss the trends and prognosis for the adoption of the smart card in the US in the foreseeable future.

1 STATUS

The concept of embedding microchips in plastic cards was first patented by two German inventors, Jurgen Dethloff and Helmut Grotrupp in 1968, and Motorola and Bull produced the first smart card microchip in 1977 [Shelfer and Procaccino 2001]. The smart card is distinguished into a memory card and a microprocessor card, on the basis of whether it contains only memory or a microprocessor and memory. The memory card contains read-only memory with a larger capacity than the magnetic stripe that comes with conventional credit cards and debit cards. The microprocessor card contains a smart chip or microprocessor, besides a read-only memory and a random-access memory. The first smart cards were prepaid phone cards that used memory cards in Europe in the middle of the 1980s [cardwerk]. The smart card is further distinguished into a contact card and a contactless card, on the basis of whether the reader has to make physical contact with the card. The contactless smart card has an antenna embedded along with the microchip, and communicates with the reader via radio frequency signal.

The architecture of the (microprocessor) smart card is fairly conventional. It includes a microprocessor, control logic, an interrupt controller, read-only memory (ROM), random-access memory (RAM), an EEPROM (electrically erasable programmable read-

Cite this column as follows: Won Kim: “Smart Cards: Status, Issues, and US Adoption”, in *Journal of Object Technology*, vol. 3, no. 5, May-June 2004, pp. 25-30.
http://www.jot.fm/issues/issue_2004_05/column3

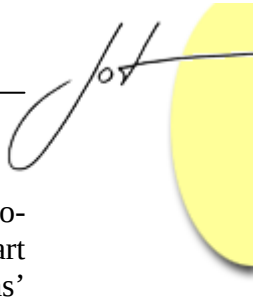
only memory) or a Flash EEPROM, a cryptographic co-processor, etc. [Bolchini et al. 2003]. The ROM is used to store the operating system, fixed data, lookup table, etc. The RAM is used to store executing programs and data temporarily. The EEPROM or Flash EEPROM is the non-volatile memory for storing a database, such as user's identification information, store coupons, user's historical information (e.g., purchase history, medical treatment history). Today, the processors are 8, 16, 32 bit architectures, and the RAM holds between 256 bytes to 1K bytes. The ROM capacity is largely 32K, but 64K and 128K (bytes) are also used to support multiple applications on one card. The EEPROM holds from 256 bytes to 64K bytes. Recently, Gemplus produced a prototype card with 256M bytes of flash memory on a card running six parallel processors [Briney 2002]. The average price of a microprocessor card is under $4, and a memory card is under 50 cents. Three major manufacturers are SchlumbergerSema, Gemplus and Oberthur.

The smart card is used in many applications, including mobile phone payment, building entry, computer logon, highway toll payment, personal identification, payment for small purchases such as lunch in the cafeteria, gas at the gas pump, vending machines, certain online purchases, etc. [cardwerk]. However, fundamentally, there are three types of uses. First is personal identification by storing personal identification data, such as password, private and public encryption and decryption keys, account number, etc. This includes even biometric data, such as fingerprints, iris scan data, and photographs. Second is electronic cash. The electronic cash is debited when a purchase is made, and the cardholder needs to replenish it by paying "real" money. Third is personal data (excluding identification data), such as purchase history in particular stores, medical treatment history, travel history, etc.

2 ISSUES

There are some important issues that have impeded a wider adoption of the smart card. These include the cost of infrastructure, standards for the multiapplication platform (operating system), and security and privacy.

A large-scale deployment of the smart card requires an extensive infrastructure. The infrastructure includes the readers and integration between the readers and the computer systems that support the smart cards. The smart card reader should be cheap, portable, easy-to-use, and secure. The cost of the smart card, the readers, and the infrastructure should be lower than the combined cost of supporting comparable functionality by alternate means. For example, for the purpose of user authentication alone, for a 1,000-user deployment, the smart card solution costs $60-65 per user, compared with $35-40 for USB tokens and $45-55 for password tokens. Further, the smart card programs initiated by US credit-card companies, such as Visa, American Express, Discover, and MasterCard, have all failed, because of the infrastructure cost. The cost of upgrading the computer system infrastructure of the credit-card companies, and the cost of having 5 million merchants upgrade 10 million magnetic stripe terminals to smart card terminals/readers is estimated at $12 to 15 billion [Chadwick 1999] [news 2003].



The smart card becomes more compelling when multiple applications can be co-located on the same card. Currently, there are three competing platforms for the smart card: Mondex's Multos, Microsoft's Windows for Smart Cards, and Sun Microsystems' Java Card [Briney 2002]. The Mondex Multos platform is widely used for financial smart cards in Asia and Latin America. While Microsoft is distancing itself from the smart card platform, the Java Card has gained momentum. The Java Card has been widely adopted for GSM (Global System for Mobile communications) and mobile-commerce applications and enterprise security applications (despite the fact that security is one area of concern with the Java Card). The loyal and large installation bases for Mondex Multos, Microsoft Windows for Smart Cards, and the Java Card, as well as the existence of a large number of proprietary platforms make standardization difficult, and interoperability among these different platforms remains a key issue.

One key benefit touted by proponents of the smart card is enhanced security. The microchip embedded in the smart card is tamper-resistant, critical information may be encrypted, and the bearer of the card needs to input PIN (personal identification number). However, as any computer system, the smart card cannot guarantee security. [securingjava 1999] and [hkstar 1997] summarize various ways in which the security of the microprocessor smart card can be compromised. The terminal (display) used to display interactions with the smart card cannot always be trusted, especially if a personal computer is used as the client-side terminal. The terminal may be compromised such that it steals the PIN, private key, etc., and saves it for later use. Further, the microprocessor can be removed from the plastic card. And an attacker may then subject the smart card to fluctuations in temperature, input voltage, or clock rate, or point a radiation source at the card, and even hit the card with a mallet. Such disturbances to the microprocessor can introduce computational errors into the smart card and cause the values of cryptographic keys to be deduced. Also, the fact that the microprocessor consumes different amounts of power to perform different operations can be used to discover information about the keys used during cryptographic computations. Of course, only the determined criminals would have the expertise and the equipment to penetrate the security of the smart card in such ways. [SINCE 2002] summarizes various ways in which the security of the contactless smart card may be compromised. Eavesdropping is the most common threat to the contactless smart card. An "active" adversary may insert blocks of data between the terminal and the reader, or cut or replace parts of the communication. An adversary may even destroy the card at a distance by sending electromagnetic waves to the card.

The fact that sensitive personal identification data and personal data, especially in multiapplication smart cards, are all kept in a single card makes many people uneasy. Further, the use of the smart card for building access control makes some employees uneasy because their whereabouts are known. Of course, it is important that the whereabouts of employees are precisely known at all times, when the employees work for certain types of employers, such as nuclear power plants, intelligence agencies, police, mines, etc.

3 US ADOPTION

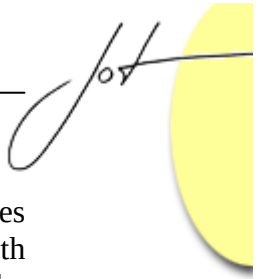
The issues summarized in the previous section are all reasons for the relative lack of adoption of the smart card in the US. However, there are a few additional reasons. One is the success that US credit-card companies and banks have had in authenticating and authorizing credit card and debit card uses at the point of sale. Intelligent networks and data mining software have been effectively deployed to combat fraud and theft involving credit cards and debit cards. One of the key reasons the smart card has been widely adopted elsewhere in the world is the high rate of fraud in the offline use of credit cards and debit cards. To combat fraud, banks there have migrated from magnetic-stripe cards to smart cards [gartner 2004].

Another reason is the culture. Americans appear to not get fascinated by technical gadgetry the way Japanese, South Koreans, and Western Europeans do. All the electronic gadgets in the Akihabara district of Tokyo, such as very small VCRs, very light and thin notebook computers, etc. came to market well before they did in the US. Japan, South Korea, and Western Europe widely adopted the cell phone and broadband Internet well before the US. Teenagers, and even elementary school children, in Japan and South Korea, have developed lightening fast fingers for typing messages on the cell phone. The downloading of the ring tones to the cell phone started there, too. In this respect, Americans appear to be relative laggards in adopting electronic gadgetry.

Of the $12 to 15 billion infrastructure cost estimated for the US credit card companies, banks and merchants to deploy the smart card, $8 billlion is the merchants' share. The credit card companies and banks had provided a strong financial incentive to the merchants to force them to migrate from paper sales slips to magnetic stripes. Currently, the merchants do not see any incentive to migrate from magnetic stripes to the smart card. It appears that until the credit-card companies and banks can offer a strong financial incentive to the merchants, the credit card industry is not going to adopt the smart card on a large scale.

The vision that everyone will move all cards in his wallet (credit cards, debit cards, store cards, personal identifications, etc.), in his brains or notes (passwords, private keys and public keys, building access codes, etc.), and in his computer or physical files (medical history, store coupons, list of friends to keep in contact, etc.) into a single smart card remains a far-fetched idea. Today, however, there are a few noticeable trends in the US that indicate that the adoption of the smart card in the US will accelerate in the near future. The trends include the adoption by the US federal government, advances in smart card technology, and the emergence of new application areas. These trends will force such issues as platform standards and multiapplication standards to be addressed.

After the September 11, 2001, terrorist attacks, various departments in the US federal government, including the Department of Homeland Security, the Department of State, the Department of Defense, the Department of the Treasury, and the Secret Service, have accelerated the adoption of the smart card as a means of secure authentication [news



2003]. The adoption of the smart card for integrated management of personal identities will have an impact on what the state governments and corporations that do business with the federal government will do. This is similar to what is currently happening with the RFID tags. The US Department of Defense and Wal Mart have demanded that their suppliers attach RFID tags on the pallets and containers they will receive from the suppliers. Other major retailers are now following suit and demanding that their suppliers use the RFID tags, too.

Advances in smart card technology have enabled the multiapplication smart card. The multiapplication smart card can help overcome the cost issue in deploying the smart card and can open up new application areas by combining several related or otherwise useful functions on one card. The Java Card has several multiapplication cards [java 2004]. The Java Travel Card combines electronic ticketing, air travel mileage, electronic cash, telephone call payment, hotel coupons for a particular trip, etc. The Java Internet Access Card combines email signatures, spam filter, Web gaming, tickets by the Web, payment for Web surfing, cybercoins, etc. The Java Student Card combines payment for cafeteria and vending machines, email identification, school computer access, phones, carpool roster, etc.

Advances in smart card technology have also given rise to the contactless smart card, which can open up new application areas. The contactless smart card avoids the need to swipe the card through the physical reader, and as such can deliver value to applications with high transaction throughput, such as highway toll collection, fast-food payment, etc. Motorists in Massachusetts and New York can zip through the toll gates by displaying EZpass contactless smart cards to the readers. ExxonMobil is experimenting with the contactless smart card on gas pumps [seattlepi 2003].

REFERENCES

[Bolchini, et al. 2003] C. Bolchini, F. Salice, F. Schreiber, and L. Tanca, “Logical and Physical Design Issues for Smart Card Databases”, *ACM Transactions on Information Systems*, July 2003, vol. 21, no. 3, pp. 254-285.

[Briney 2002] A. Briney, “A Smart Card for Everyone?”, http://infosecuritymag.techtarget.com/2002/mar/cover/shtml (March 2002)

[cardwerk] http://www.cardwerk.com/smartcards/smartcard_applications.aspx

[Chadwick1999] D. Chadwick, “Smart Cards Aren’t Always the Smart Choice”, *IEEE Computer*, December 1999, vol. 32, no. 12.

[entrepreneur 2002] http://www.entrepreneur.com/article/0,4621,297984,00.html (March 2002)

[gartner 2004] http://www4.gartner.com/DisplayDocument?doc_cd=119996 (March 2004)

[hkstar 1997] http://home.hkstar.com/~alanchan/papers/smartCardSecurity/ (1997)

[java 2004] http://java.sun.com/products/javacard/examples.html (2004)

[news 2003] http://news.com.com/2008-1082-1020807.html (June 2003)

[seattlepi 2003] http://seattlepi.nwsource.com/virgin/157549_virgin22.html (January 2003)

[securingjava 1999] http://www.securingjava.com/chapter-eight/chapter-eight-5.html (1999)

[Shelfer and Procaccino 2001] K. Shelfer and J.D. Procaccino, "Smart Card Evolution", *Communications of the ACM*, July 2002, vol. 45, no. 7, pp. 83-88.

[SINCE 2002] SINCE Security Group, *Open Smart Card Infrastructure for Europe: Security and Threat Evaluation Relating to Contactless Cards, eESC Common Specification v2*, November 2002, vol. 6, no. 2.

About the author

Won Kim is President and CEO of Cyber Database Solutions (http://www.cyberdb.com/) and MaxScan (www.maxscan.com) in Austin, Texas, USA. He is also Dean of Ewha Institute of Science and Technology, Ewha Women's University, Seoul. Korea. He is Editor-in-Chief of ACM Transactions on Internet Technology (http://www.acm.org/toit), and Chair of ACM Special Interest Group on Knowledge Discovery and Data Mining (http://www.acm.org/sigkdd). He is the recipient of the ACM 2001 Distinguished Service Award.

He-Joon Kim is a graduate student in the Department of Computer Science at UCLA. His research interests include database systems, data mining, intelligent systems, and multimedia systems.