Identity Protection and Smart Card Adoption in America

Stephen Irwin

Identity Protection and Smart Card Adoption in America

GSEC: Assignment Version 1.4b(August 2002)

Stephen T. Irwin

June, 2003

Identity Protection and Smart Card Adoption in America

Introduction

With the sudden rise in identity theft and on-line credit card fraud, there needs to be a correspondingly strong countermeasure from card issuers, banks and law enforcement to provide consumers with the tools to effectively fight this cyber crime epidemic. The low standard of security adopted so far (magnetic striped credit/debit cards) raises the public concern about other confidential and sensitive data breaches that may occur, especially as a result of e-commerce transactions. The combination of easy access to credit and identity information, no tangible solutions that have been proposed by card issuers, and the few attempted prosecutions of identity theft criminals, has created a precarious environment for consumers. Unknown to many U.S. consumers, the tools to combat this fraud are available, and are being used successfully in Europe and Asia on a regular basis. Smart cards have been used to validate users and make secure payments in Europe for nearly a decade, and have proven to be an effective method for preventing fraud, and positively identifying individuals, particularly in e-commerce transactions over the Internet. So why haven't card issuers rolled out similar programs in the United States? The answer is rather convoluted. Although the genesis of smart card development was in Europe, not America, and the "productization" evolution continued to develop on parallel paths between the continents; adoption has been slow to occur in America. In the meantime, The EU has standardized on EMV (Europay, MasterCard and Visa) standards for smart credit and debit cards, which will go into effect by the beginning of 2005. The U.S. marketplace has neither accepted EMV standards, nor has any plan to do so. In America, card issuers do not consider consumer fraud, as measured by a percentage of total card transactions, to have reached a level where they must voluntarily implement a technology that they had assisted the European Union to adopt. There is no federal legislation in the U.S. to get tough on identity fraud, and, as a result, no value proposition to follow the European course. America's slow evolution of integrating smart card technology is an enigma in the view of its perennial role as the world's leader in adopting high tech solutions for everyday problems. When those solutions combine security, computers, chips and communications, the U.S. should not be years behind.

This paper will address smart card technology as a viable alternative to present financial and identity standards, and why it will be woven into the American identity fabric over the next decade. The perceived security value, the increased emphasis on positive identification of U.S. citizens and non-citizens alike, by the federal and state governments (as a result of the tragedies of 9/11/2001), and the new business value propositions, will become compelling reasons to adopt smart cards as a standard part of identity for many applications in the future.

The Problem

Fraud is increasing for several reasons. First and foremost, it is easy to commit credit card fraud with a small chance of being caught. There is even a smaller chance of being prosecuted. Another factor is that more MOTO transactions are occurring via the Internet or telephone. Computers and the Internet have now made it possible to order merchandise without disclosing the physical location of the perpetrator, having to show an actual credit card or show an ID. A stolen or skimmed cards can be used in gas stations, grocery and retail stores with little or no hassle. The system is a comfort zone for dishonest people.

Why should we care so much about credit card fraud? It's because it is increasing at an alarming rate, and there doesn't seem to be much happening to prevent it, or remedies being recommended to those whose cards and identity have been stolen and resulting in their credit records being put into complete disarray. In other words, there doesn't seem to be any card issuing organization or institution doing anything to make it more difficult for the criminals to turn people's lives upside down. According to Celent Communications, a Boston, Massachusetts consultancy and research company, U.S. credit card fraud was a $1.8 billion problem in 2002[1]. That's an increase of $200 million in just two years. To make matters worse, Celent now estimates fraud will increase to around $2.3 billion during 2003.

What is a Smart Card?

Basically, a smart card is a plastic card with an integrated circuit that conforms to the International Standards Organization (ISO) standards 7816, series 1-10, for contact smart cards, and ISO 14443 for contactless cards. These cards fall into three major categories: Stored Value Cards, Microprocessor Cards, and Cryptographic Cards.

The simplest form, the Stored Value Card, is basically an integrated processing/storage capability card version of a magnetic stripe card that is able to perform basic counting operations. Phone cards are a typical use for these inexpensive, and frequently, throwaway cards. Businesses like these inexpensive cards, as they do not raise the total cost of the service or product offered.

Microprocessor Cards are significantly more complex from a functionality perspective. The architecture of these memory cards includes areas of ROM and RAM, as well as EEPROM (Electrically Erasable Read Only Memory) for the application data. These cards can enforce the use of PIN codes and other security features. These cards use 8 or 16-bit processors that can enable multiple applications, and have substantially more memory to store private crypto keys, digital certificates passwords and personal information about the employee, for example. These cards also incorporate some tamper-resistance features.

Cryptographic (Crypto) Cards are the most sophisticated cards in terms of function, and are subsequently, the most expensive. They offer feature support for digital signatures and other crypto operations. Their tamper-resistant features allow secure storage of private cryptographic keys (and other secret keys), which give it strong hacker-resistant qualities. Technically describing all of these architectural, electrical, mechanical and physical features are detailed in the ISO standards referenced above.

So How Do Smart Cards Function?

Briefly, they have either contact and/or contactless interfaces used to activate (read) them. There are smart card readers which function by using security software, network interfaces to banks accounts, e-mail accounts, and company servers, which validate the user to his/her application by using the users private key or digital certificate, which never leave the card. Only the card user can access the private key by using a two-factor authentication. This is accomplished very much like the use of an ATM card, by connecting the card into a card reader and inputting the users PIN or password. There is little difference in how we use ATM machines today and how we would authenticate ourselves to a device using a smart card. There are, however, not a lot of smart card readers in existence in the U.S., which is an infrastructure limitation, which I will address later.

Smart cards can provide non-repudiation, since the cards are designed to prevent the private key from being removed from the card, copied or replicated. It is portable, and when combined with a biometric such as finger scanning, the device becomes a very unique device that offers a substantially higher level of security and can still be transported in a wallet.

Smart cards offer the ability for personalization. This means that the artwork on the cards can be uniquely prepared for internal use as in an enterprise, hospital systems or universities as an ID, a bank credit or debit card, or as a card that also offers a limited stored value which can be used for miscellaneous fees such as parking permits, cafeteria areas, and for other small purchases. These cards would typically have the university logo artwork. Post issuance personalization can include a photo and personal data stored on the chip in addition to keys/certificates and other necessary access privileges for e-mail, physical access to buildings and rooms as well as network access.

So, with all of these security features, business and personal applications, and at least 15 years of experience in the real world environments, upgrades, improvements, flexibility, simplicity, and an ability to reduce credit card fraud, smart cards should being instituted by card issuing institutions all over America, right? You would be wrong.

Genesis and Evolution of Smart Card Technology

It is important to understand the genesis and evolution of the smart card. With that knowledge the reader will better understand how and why smart cards have developed independently on different continents.

The reasons that drove the value proposition for smart cards in Europe in the late 1980s had little to do with security and more to do with the French PTT's desire to reduce cash sitting around in phone booths. So, in Europe, it was the telephone monopoly (government owned) that was the principal driver of smart card technology and applications. Smart cards seemed to have lots of uses. Eventually, it was the French government, in conjunction with a bank, Gie Cartes Bancaires, and the PTT, France Telecom that used this technology for the first secure financial transactions. At the time, the problem was the cost of a telephone call charged to a merchant to contact a bank or credit card issuer to approve a credit card charge for sale of his merchandise. It took a few minutes, but it was very expensive relative to the average sale. In order to reduce their costs, the acquirers would agree to a "floor limit" with their merchants. All purchases under the limit would not be submitted for on-line authorization. Although this was much more cost effective than making calls each and every time someone used their charge card, criminals could use stolen or bogus cards unimpeded, as long as they charged below the

"floor limit"(in a shop that participated using "limits"). By the time the authorization was approved or denied, the shopper(s) were usually on his/her way. That process created a new set of problems…an artificially high rate of authorization failure and fraud.

A new system was devised where the chip card would contain a unique key that would be validated by the POS (point of sales) system using a cryptographic challenge/response session between the card and the terminal. Since the key was not externally visible to the system, it greatly reduced the amount of card skimming. The criminals could not clone the information on the chip. That tamper resistant achievement was key to reducing skimming crimes. This introduction of a chip card had reduced losses, transaction event-time requirements, as well as the average cost of the transaction that meant increased customer satisfaction. That happened because of the government and its monopoly, the phone company, worked together to solve a problem. In the late 1980s, the French parliament (government) passed a law that said that required all bankcards to include chip by 1994. The goal was designed to primarily reduce fraud. This is also the same year EMV commenced to supplant or remove magnetic stripes in favor of microchips.

The key difference that caused an independent and parallel evolution of smart cards during this same timeframe was a result of many factors. There was the lack of a relationship between the U.S. communications industry and the US government that would have provided the nucleus for joint development of products. Unlike the French PTT monopoly (and other European PTTs), the U.S. telecoms were competing head-to-head for business and market share. This, in turn, not only created a huge over-investment in high-speed infrastructure on the part of the U.S. telecom industry, but it effectively created enough new bandwidth to produce the lowest transaction cost/performance ratios ever. The cost of processing a transaction never became a business issue in the U.S markets

Also, during the 1980s and '90s,U.S. retail and commercial merchants had a substantially more sophisticated communications infrastructure in the back office. Combined with the low cost of phone calls, there was no need to take the authenticating processing off-line as they had in Europe. With no bandwidth limitations or authentication overhead costs to worry about, there was no corresponding incentive or value proposition to change the way transactions were processed in the U.S. In many respects, that is still true today, but it ignores newer issues and applications for and about security concerns. The business impact has been the dominance of European, and especially French companies, in the smart card markets today.

Smart Card Applications-

What exactly are the chances that smart cards will be used in the U.S.? Basically, to be successful, smart cards will have to offer an application value proposition that is capable of being ported to many operating platforms, use common criteria that can be utilized as a common international standard, and be adopted ubiquitously. Success will ultimately be universal adoption in spite of the evolution of the technology from different sides of the smart card family tree. In every case, independent of the application, security and identity verification/protection are key features integrated into the final functioning application. Even though credit card and identity fraud may play major roles in the adoption of smart card technology in the U.S., it is in conjunction with many other card applications that will ultimately drive decision makers to adopt the technology sooner rather than later.

We'll now look at chip card applications on various scales. Scalability is very important, especially when considering a national or international model. The following examples represent a few of the types of applications, the scale of the programs and where they will be/have been implemented.

Smart cards are used in many critical areas that support security applications. This is a list of a few of the most fundamental applications:

ID Cards

There are many types of identification used in our daily lives. The range runs from driver's licenses to passports, corporate access control, computer log on, and national IDs, which a few countries are considering, and China is implementing. China's adoption will be an enormous task to identify and issue cards to all 1.2 billion inhabitants. This will be the ultimate scaling feat.

Instead of describing all of the features of each application, this paper will focus on one area, medical smart cards, to illustrate the type of information stored on the cards, and their security features. This data is an example of what the German medical cards store.

Medical ID Cards- There will be nearly 80 million smart medical cards issued in Germany. The government believes the use of smart cards will reduce the incidences of fraud and disappearance of drugs. There is a clear audit trail that is assigned to doctors and patients by the use of these cards. Here is a list of six types of medical cards being issued to German citizens, with a brief description of their functions[2]:

- *Emergency Medical Cards* – Contain medical and contact information for EMS personnel.

- *Insurance Medical Cards*- Store insurance policy and ID information.

- *Hospital Admission Cards* – Detailed insurance information for hospital administration, including billing information.

- *Follow-Up Cards* - Store medical data for many specialties including: cardiology, maternity, oncology, and hospital pharmacies. This list can be easily expanded.

- *Universal Health Cards* - Offer health insurance ID information, patient's medical record links and demographic data.

- *Health Passport Cards* – Also contain comprehensive medical and insurance information.

If German medical cards are lost or stolen, it would be difficult to extract the personal data. The data is encrypted on the chip and two, four-digit numbers are required for the sensitive data to be displayed; one PIN by the patient, and the other by the doctor. These PINs are also used to encrypt any data on the card. Every medical card has a unique key. German medical cards are being deployed over a multi-year period. The German model addresses many of the security concerns of HIPAA, in America. There is a positive identity that can be made of each and every patient and healthcare worker associated with a patiently file/record (PIN for both patient and doctors), photo, an audit trail for hospital or insurance administration, and encrypted patient data. An optional choice could be a biometric card, which would produce an even higher patient validation criteria.

National ID cards-

Finland has a non-mandatory card that its citizens can buy and use. This might be a good option for countries attempting to facilitate national programs without creating as many possible privacy concerns

China is committed to issuing smart cards to every citizen. China does not have a large concern for citizens' privacy, but it will be interesting to see how this program is scaled and what additional privacy abuses (by Western standards) will be produced by the use of a national identity card.

Access Control (Physical and logical and serve as IDs too)

For physical entry to university dormitories and other classroom buildings; optionally, logging onto university networks and used as a stored value card in university vending machines - Penn State Univ., Univ. of Utah and Florida State Univ. and others.

Enterprise- Goldman Sachs for every employee (approx. 50,000), Microsoft Corp (25,000) has issued cards to its employees at its home office campus.

.

Set Top TV Boxes (pay-per-view) Adopted throughout Japan; the U.S. is just beginning to offer the same access control cards. Prepaid telephone cards-NDS is a leading supplier of open end-to-end digital systems and solutions for the secure delivery of entertainment and information to televisions and IP devices. Today, more than 30 million subscribers around the world depend on NDS smart cards to receive their pay TV services

Public Transit- The Los Angeles County Metropolitan Transportation Authority has begun installing contactless smart card systems on the balance of 1500 Metro buses. The benefits include a lower fraud rate, less cash held in the bus, and an improved fare reconciliation of the participating Los Angeles Metro agencies.

Smart cards are also currently being used on the Washington DC Metro system, The Bay Area Rapid Transit (BART) in the San Francisco Bay Area, and by the Chicago Transit Authority.

Credit Cards

Target Corp[3]**.,** with 1167 discount stores and 40,000 terminal locations has already issued over 9 million smart Visa cards designed to attract customers who will get loyalty points for each purchase. FleetBoston, Providian, American Express and First National Bank of Omaha are also actively marketing their Visa chip cards. Citibank, the largest card-issuing bank in the United States, has a small test market group to whom it has issued cards. The biggest interest is in contactless version of a MasterCard called PayPass. There have been about 15,000 cards issued in the Orlando, Florida area in conjunction with McDonalds, Chevron, Eckerd Drugstores, Loews Universal Cineplex, Ritz Camera, Friendlys, and Boater's World. Card issuers involved in this market test are some of the largest…MBNA, JP Morgan Chase, and Citibank.[4]

Government- There are currently 62 independent smart card projects within 18 different government agencies, to identify people or to control access to buildings, in the U.S. federal government, according to the Government Accounting Office (GAO)[5]. The largest program is the Common Access Card program (CAC), in which there are expected to be 4 million cards created and issued to DOD and the uniformed services personnel by the end of 2003.[6]

Reasons for implementing smart cards-

It's important to remember that while smart cards can offer significantly higher levels of protection against fraud, the value propositions and other economic factors that will drive this technology change are frequently not security related. In spite of that, here a few of the reasons for the U.S. to begin to seriously consider smart cards as an alternative:

- One needs only to compare the current use of magnetic stripes versus a microprocessor on a smart card for storing data (Any phase-in of smart cards would use both magnetic and chip media). Unlike magnetic stripe cards, smart cards can support multiple applications. Integrated circuitry makes smart cards more difficult to tamper with, especially its more complex file and data structure. Photos and fingerprints can be digitized and stored on the card, depending on the type of cards used. Finally, the ability to store key pairs allows the cards to sign digital certificates and encrypt the data on the card as well as send and receive s/mime e-mail. All of this makes smart cards more secure as a financial transaction tool. In fact, credit card fraud fell about 75%, after France fully replaced magnetic striped cards in 1992.[7]

- Timing- Forty to fifty percent of the point-of-sale systems and ATM terminals in the United States are due to be replaced over the next five years, according to the Smart Card Alliance. Some mass retailers have already begun to make the conversion.[8] **CVS**, a national pharmaceutical and health service retailer; **Virgin Megastore**, an entertainment retail chain; **Rite-Aid**, one of the largest drugstore chains in America, is incorporating smart card terminals in 4,000 stores; **ShopRite**, the largest retail supermarket cooperative in America, has decided to integrate smart card ready POS systems in 200 stores for a loyalty program.

Reasons Against Implementation

Opposition to adopting smart cards in America runs from uninterested parties to strong opposition on the part of privacy advocates. Somewhere in the middle are those who still have no solid business case to push for implementation.

· The cost of a fully loaded smart card is now $1.62; a magnetic stripe card costs around 50 cents. A bank wanting to enable 4 million cardholders pays a significant premium.

•The cost for banks to convert to smart cards in the U.S. would be in the area of $12 billion, according to Frost & Sullivan, the market research firm.[9]

•Fraud, as a percentage of total Visa card transactions, has decreased to .06% from about .15% in the early 1990s[10]. As cited earlier in this paper, total fraud in dollar terms is increasing at a rapid pace, but so is credit card issuance. The key point is that at this level of fraud, credit card companies have little motivation to make huge capital commitments to convert cards from magnetic stripes, for fraud reasons alone.

• Credit card companies are not required to pay for retail credit card fraud. The merchant is charged back for the fraudulently purchased goods, and in some cases, the card issuers also penalize the merchants monetarily. The cardholder has been accountable for up to $50 in fraudulent purchases in the past, but that's not even necessarily the case with Visa's Zero Liability program. As a result, the card issuers may actually financially benefit by each incident of fraud where they fine their merchants and incur none of the burden of the fraudulent card purchases.[11] There is no incentive to change.

•Smart card readers cost issuers about $15 by most estimates, present a hurdle to adoption if the issuers expect to charge users for them. "Consumers aren't going to go out and spend $25 or more on a device to read cards," says James Van Dyke, a research director with Jupiter Media Metrix. Van Dyke says he expects readers will be adopted in offline settings, such as stores and corporations, before many consumers have them.

•Privacy issues are central to opposing arguments regarding identity cards. Anything that simplifies the acquisition of an individual's personal information repository by corporate, government authorities, or potential identity thieves, will be challenged on loss-of-privacy grounds. In particular, medical knowledge which is acquired by insurance companies, employers, or governmental agencies is presumed to have a potentially adverse effect on the welfare of a given individual, is of concern. .

Conclusions

- Smart cards will ultimately be successfully implemented into the U.S. market over the next decade. There are many routes that it may take, but it will occur.
- Banks and credit card associations, like Visa and MasterCard, will not push for smart cards to lower credit and identity fraud. Since there is no compelling business reason, only new and stronger value propositions, class action litigation

or government legislation will motivate them (negatively) to spend billions to make the conversions in the near future. This is in spite of their successful smart card programs in Europe and Asia. The changes were legislated there.

- The acceptance by the U.S. government to study and implement smart cards for both physical and logical security will compel large resellers and integrators to standardize their solutions for similar applications in the commercial markets in order to comply with the standards set by the federal government, and to do business with the government. FIPS 140-x security standardization is a similar example.
- The acceptance and issuance of millions of smart cards by the federal government will also set new and lower card and reader price levels that will make the entry cost lower and less prohibitive in the commercial marketplace. All federal price schedules are publicly known. Most computer keyboard manufacturers will integrate card readers into keyboards, as a standard PC feature.
- As this paper has illustrated, the applications with smart cards are extensive. While most smart card applications can impede financial and identity fraud in some way, it will be the other pragmatic applications and features which will be the ultimate drivers of this technology. Those include accurate audit trails, reduced administrative costs (projected, at least), positive ID cards, improved medical and insurance processing and patient record administration compliant with HIPAA requirements, and digital signing of documents and secure e-mail.
- The many new features offered by smart cards, USB tokens, and similar fob devices for positive identification and data/financial security will eventually weave itself into our daily lives through integrated products and services (healthcare, retailers loyalty cards, public transit passes e.g.). Over the next decade, the integration will be complete.

GLOSSARY

EMV- EMV is named after Europay International, MasterCard International and Visa International, who created a joint industry working group which first met back in 1994 to facilitate the introduction of chip as the replacement technology for credit and debit cards, replacing the traditional magnetic stripe. More about EMV at URL: http://www.ecebs.com

EU- European **U**nion is an economic and political confederation of European nations. The fifteen members include: Austria, Belgium, Denmark, Finland, France, Germany (originally West Germany), Great Britain, Greece, Ireland, Italy, Luxembourg, the Netherlands, Portugal, Spain, and Sweden.

FIPS 140- (**F**ederal **I**nformation **P**rocessing **S**tandards) is a series of publications issued by the U.S. National Institute of Standards and Technology (NIST) that specifies information security guidelines for federal government departments and agencies. FIPS 140 –x series refers to tamper detection and tamper resistant design standards set by NIST.

IC- **I**ntegrated **C**ircuit

MOTO- Mail **O**rder **T**elephone **O**rder.

Non-Repudiation- The method by which the sender of data is provided with proof of delivery and the recipient is assured of the sender's identity, so that neither is able to deny (at a later date) that the data had been processed.

Post Issuance- Refers to data that is added to the smart card after all artwork and functional details have been designed for its use. The cardholder's personal information, PIN, rights and privileges are created.

PTT- stands for: **P**ostal, **T**elegraph & **T**elephone. It has been the acronym used for the governmental agency responsible for combined postal, telegraph and telephone services in many European countries

Skimming- The practice of copying the magnetic stripe information from a legitimate credit/debit card onto a facsimile card. These counterfeit cards can then be cloned several more times and used until the victim's credit line or bank account is completely depleted.

Value Proposition- A company's value proposition is its primary mission or goal (its reason for being). A good value proposition will be consistent with the company's business objectives, which also means an eventual return on investment (profit).

REFERENCES

[1]Beckett, Paul and Jathon Sapsford, "As Credit-Card Theft Grows, A Tussle Over Paying to Stop It", The Wall Street Journal, Page 1, May 1, 2003.

[2]"How Are Smart Cards Used in Healthcare?" Secure Information Medical Systems Home Page, Maxking, URL:http://www.maxking.co.uk/medsmartcard.htm

[3] "Smart Cards and Retail Payments Infrastructure: Status, Drivers, and Directions", Smart Card Alliance, October 2002, p.4. URL: http://www.smartcardalliance.org/

[4] Vanderhoof, Randy,"Catching the Wave", Intele-CardNews, May, 2003, Vol. 9, No. 5, p.31

[5] Hardy, Michael, "GAO Flags Smart Card Challenges", Federal Computer Week, February 5, 2003 URL: http://www.fcw.com/fcw/articles/2003/0203/web-smart-02-05-03.asp.

[6] Davis, Donald, "Building Blocks of the U.S. Smart Card Market", Card Technology, Vol. 8,No.6, May 2003, p.41

[7] "The Future Belongs to Smart Cards", Telecom Guide, May 12, 2002. URL: http://www.bsnl.in/Telecomguide.asp?intNewsId=4641&strNewsMore=more

[8]Smart Cards and Retail Payments Infrastructure: Status, Drivers, and Directions", *op.cit*. P.5

[9] "A Smart Card Day in Paris" CIO.com, May 1, 2003, URL: http://www.cio.com/archive/050103/tl_chip.html

[10]"Shop Safely With Visa", Visa USA, URL: http://www.usa.visa.com/personal/secure_with_visa/zero_liability.html?it=h2_/index.html , May 8, 2003.

[11] Beckett Paul and Jathon Sapsford, The Wall Street Journal, *op. cit*., p.1

3