

Evolving Smart Card and Biometric Technologies 2001

What's a Smart Card?

An intelligent Smart Card can be likened to a simple microcomputer. It can pick up, store, process, and secure data. The degree of its Smartness is also similar to a typical computer--it depends on its physical characteristics. It could have a magnetic strip or be processed by passing it over a plate using laser/optical technology. The amount of memory, the cryptography, whether it uses bar codes, or can respond to more than one type of application are all variables that describe each Smart Card. As Smart Card technology advances, adaptations are emerging based on needs. For example, the two different types of contact, either through a reader where there must be a direct interface between the chip and the reader, or indirect contact through antenna built into layers of the Cards are now being merged into hybrids. These newer Cards are designed to meet customer needs for multiple use, i.e., banking, mass transit, and medical information. Because of these variations and multiple asynchronous improvements in different technological components, there is still little agreement on which industry or standard will kick-start the U.S. versions of an ever-growing global Smart Card economy. Says John Dvorak in Forbes, "Currently there are about 2.75 billion old-fashioned magnetic-stripe payment Cards in circulation. Frost & Sullivan, a research firm, expects that SmartCards will be shipping at the rate of 5 billion Cards per year by 2004." [1]

There are two major reasons for deploying Smart Card technology – the first is security from a traditional perspective, i.e., fraud, theft, etc. How much less vulnerable assets are with good Smart Card technology is not yet determined. To date the major credit card corporations are just now deploying Smart Cards and cannot yet count the net savings on paper. The second reason is security from the growing use of e-business, m-business, and t-commerce [interactive television] technologies within the expanding global marketplace. Count all the ways you use a current ROM card today, along with access to the Internet via PDAs, cells, public kiosks, etc., and multiply that by the changes taking place in the presentation of personal [portal] Internet data. Then add the many membership enrollments and credit cards currently used; for example, there are cards for transit use, parking garages, library loans, building access, and so on. All of these current applications can be applied to [eventually] one personal Smart Card as this technology is improved with greater processing and storage capabilities.

There is less agreement on which technological innovation will make Smart Cards the preferred security technology. According to news reports up through the summer of 2000, the major problem with most types of current cards seems to be fraud that costs businesses large amounts of money. Says Ross J. Anderson, Cambridge University Computer Laboratory, (e-mail: ross.anderson@cl.cam.ac.uk), "There are two ways of attacking Smart Cards - destructive reverse engineering of the silicon circuit (including the contents of ROM), and discovering the memory contents by other means; a well equipped laboratory can do both. Persistent amateurs have often managed the latter, and may shortly be able to do the former as well."

That level of hacking, however, cannot compare to the current vulnerability of credit card users. The next steps toward generally improved security and highly improved economically advantageous uses of Smart Cards are now moving from the drafting boards to production. Jon Byous in, *The Java Cardtm Platform: Here, There And Everywhere*, quotes Philippe Tartavull, president and CEO of Oberthur Card Systems of America, as saying, Smart Cards using the public key infrastructure are a very powerful way to create this authentication. With a Smart Card, you have a very simple way to carry in your pocket an authentication tool that can plug into any web-enabled device. [He] "expects on-card fingerprint matching to be available soon. In this scenario, the fingerprint is not transmitted across the net, but instead processed locally by the card itself. The idea is to make instant identification easy and safe." [2]

Jumping ahead with huge implementation announcements, the focus seems to be on banking first. Recent news reports that, "Lloyds TSB is using Entrust's strong authentication and digital signature capabilities to implement the U.K.'s first large-scale, security infrastructure for a Smart Card Internet banking project. ... The systems incorporation of Smart Cards from Schlumbergers Test & Transactions are making Internet-based transactions possible and will provide added protection by securely storing the secret authentication and digital signature encryption keys." [3]

Another on-line paying service now on the market is SafeDebit. "SafeDebit allows consumers to make PIN-secured ATM like payments and holds consumer information in encrypted and embedded format. The data is passed via the Internet directly to existing secure online debit networks and financial institutions for authorization and settlement - the industry's most reliable and secure technology infrastructure. As transactions that are made each year.[4]

Looking into the future of multi-application Smart Cards with access to many personal data sources over the Internet, one must take a parallel look at security for this functionality. It seems that developers are thinking ahead, as evinced by the recent global competition sponsored by American Express and Sun. On May 23, 2001, via PRNewswire, "the winners of Code Blue -- a contest that challenged Java developers from around the world to create innovative, new Smart Card applications for potential use on the credit card Blue from American Express" were announced. "Igor Fisher, of Tuebingen, Germany, received \$50,000 as the first place winner, ... with his "Pass Keeper" application [designed to] enhance a user's Smart Card by storing a portable and securely locked list of Internet addresses ("bookmarks") together with a user's personal identification numbers (PINs), passwords, or account numbers that might be required for entering those sites." [5]

These newer Smart Cards that include digital credentials required for authentication and decryption are examples of cards that are multifunctional, capable of using multiple applications. The continuing expectation for the next generation is to embed the cards with tamper-proof biometric chips, and consequently, not only reduce fraud, but increase the trust of users.

Why Should We Keep a Keen Eye on Biometrics?

This technology is advancing rapidly today for several reasons. The first is that the cost of biometric technologies is becoming less to use than not to use, i.e., less than the costs associated with fraud. The second is the improved ease of integrating a high level of security by matching individual attributes such as fingerprints, facial structure, voice patterns, vein systems, eye tissues, signature patterns, and other physical identifiers to database fields. These changes, along with the ever-expanding e-commerce and business-to-business applications on the market today, may effectuate a sea change in the type of cards people will use to access and manipulate their personal information.

[6]

The Current Versus the Future

The typical university version of a Smart Card provides swipe access to resources such as libraries, food services, ATMs, residential halls, and various college businesses. Universities may begin to experience increased fraud and/or error as the use of Smart Cards against financial services increases. The 3/23/2000 Daily Report from The Chronicle of Higher Education states, the "University of Pittsburgh officials who want to expand their use of secure digital certificates for on-line transactions say they are not going to wait for the rest of the world to do the same. 'It's simply a much more secure way for us to do business than with the old swipe Cards and other things that we've used,' says Robert F. Pack, vice provost for academic planning and resource management at the university. ... that even if there is no agreement yet on the best way to secure online transactions, he is not going to let that stop the university from trying to achieve 'a level of security we think is appropriate.'"

USA Today reported on June 22, 2000, that the Army plans to use Biometrics in Arlington, Virginia starting in August. All soldiers' fingerprints, earlobes, and other characteristics will be stored in a database. The U.S. Army plans to be the first branch of the military to convert to biometric security. The Navy, Air Force and Marines are running pilot projects. While assaults on the Army's computer systems are a significant reason for the \$15 million [so far] dollar program, other obvious identification needs, such as on a battlefield have been taken into account.[7]

On May 03, 2000, in the article, Microsoft Buys Biometric Security Software for Windows, Juan Carlos Perez, IDG Ndw Service, wrote, "Microsoft announced today that it has bought biometrics technology from privately held I/O Software Inc. in Riverside, Calif., for an undisclosed sum and that the companies will collaborate to integrate the technology into Windows operating systems. ...When they're built into Windows, I/O Software's Biometric API technology and SecureSuite authentication product suite will offer alternative access control features, including iris, voice or fingerprint recognition, the companies said. ...Microsoft plans to include the technology with future versions of Windows, but it's not clear when, the companies said." [Microsoft]

How Does the Technology Compare to What We Already Know?

The good news is that some biometric software and devices such as cameras, microphones, and finger print readers can be attached to typical PC clients with the biometric software suites. Small set-ups can be accomplished relatively inexpensively. This type of application would be useful in a small Intranet where privacy and authentication are of the utmost importance. The evolution here is akin to all other desktop applications--small, relatively inexpensive (running anywhere from \$39 to \$199 typically, and occasionally an extremely broad suite as high as \$600 per workstation) and easy to use and install. [PC Magazine]

Not all biometric applications will require Cards or operate in the same way. Citadel GateKeeper uses a telephone for voice verification and a PIN number is used to set up a password. Once enrolled, the user can be limited to one logon and must change

the password when prompted. Even if another user tries to get in with the PIN number, if the user is not enrolled with a voice-print, access is denied. The Sony Fingerprint Identification Unit not only comes with the typical bundled software suite, but sophisticated hardware that can be used without a PC if needed. Network: Safink SAF/nt2.0 works with any type of biometric system, fingerprint scanner, camera face recognition, or microphone voice authentication. Digital Persona U.are.U Deluxe bundles in a fingerprint scanner with easy to use software that allows the user to secure individual files, create private or protected partitions on the hard drives and more. These are just a few ideas about different available features. And like many proprietary applications, these "evolving technologies" are subject to change frequently—assuring that products will be coming onto and going off the market fairly regularly. [8]

Colliding with Institutional Products and Services

From a teaching perspective, two significant security issues come to mind. Students, especially the math-computer science hacker variety, have been known to threaten systems, especially during finals' week. A larger issue than that, however, is the increased use of distance education and faculty concern about authenticating the person at the other end of the remote connection, as well as the assignments that are submitted through electronic conferencing programs. From the business side, student records and business transactions are enormously important to the survival of an institution. If a student financial system is corrupted, the loss of uncollected revenue can be staggering. If student records are compromised in a way that violates confidentiality, litigation on a large scale could be devastating. With the onset of Internet2 and increased live data sharing, the value associated with each research initiative is inestimable. Non-secure data is up for grabs. Sorting out the total costs of security against the loss-value of university data is not an easy analytical task.

If you are in the medical school business, you would be very interested in following an implementation by SmartMED. They are implementing a "Smart Card system at five Addiction Research and Treatment Centre (ARTC) methadone clinics located in New York City, USA. The system was first successfully implemented in an ARTC clinic in Brooklyn, NY during 1999 and represents the first widespread application of Smart Card technology in the US behavioural healthcare industry. ...The SmartMED Card, being rolled out to more than three thousand patients utilizing the six clinics will be "used for ID - through biometrics - storing clinical and dosage information, counselling records, amount of time patient spends at the clinic ...insuring accurate patient identification, tracking, co-ordinating, and recording at the point of service." [9]

For universities, the risk of losing certain kinds of data to corruption is an immeasurable liability, especially research data. But according to a report by Security @ The Millennium, through 1999, universities had still not put information asset protection on its priorities lists for existing data. In addition, they write that, "Undergraduate and graduate business schools still energetically resist adding asset protection and related curricula to heighten a student's awareness of future risks. Business students are entering the marketplace never having any studied appreciation for the many facets of future risk and their impact upon an organization's competitive position, profitability and yes, survivability."

Many more universities can be added to the Smart Card user-list. Penn State ID Smart Card gives students the choice of six banks and the Penn State Federal Credit Union. The University of Michigan, which has had a smart card program since 1995, has cards that can be used at 345 locations on campus and at 85 off-campus stores and restaurants. Florida State University now in its third year will add features that allow its smart card to use 68 pay phones around campus and wants to make student records available from any computer with Internet.[11] Many universities in Europe have implemented extensive smart card programs. [12]

But, from a more pragmatic perspective on governance, most enterprise-wide deployments require a high level of consensus and with biometrics, chances are the emotional level of interest will rise to record heights once images of surveillance are perceived in academia – not to mention the debates that will arise over the possibility of having physical identities in databases stolen. From a business perspective, imagine the problems that may occur in offices when computer hard drives are secretly partitioned and protected with biometrics. Even today, improperly secured PCs contain university owned records that are never retrieved when people leave an organization, and hard drive data is not recoverable.

When major security needs are planned, governance must balance appropriateness between academic freedom and civil liberties and protecting intellectual property, research data, and the personal records of faculty, staff, students, and patients.

For EduCause 2001 – Evolving Technologies Committee

By Laura Joyce Moriarty
Emory University ITD
Ljm@emory.edu – 404.727.7663

[1] John C. Dvorak, Forbes.com, SmartCards Get Smarter 06.01.01, 3:00 PM ET
<http://www.forbes.com/2001/06/01/0601dvorak.html?partner=yahoo&referrer=>

[2] The Java Cardtm Platform: Here, There And Everywhere by Jon Byous July 18, 2000 -- .
<http://java.sun.com/features/2000/07/javaCard.html>

[3] Lloyds Entrust
http://www.SmartCardcentral.com/news/pressrelease/may2001/entrust_052201.asp

[4] About SafeDebit
http://www.SmartCardcentral.com/news/pressrelease/may2001/globeid_053001.asp

[5] American Express Announces Winners of 'Code Blue' Contest - Global Competition Spurs Innovation in Java(TM) Technology-Based Smart Card Development
http://www.SmartCardcentral.com/news/pressrelease/may2001/amex_052301.asp

[6] Scottson & Michaels, Inc. has been in the business of Credit Card Fraud Verification Processing since 1994.
<http://www.scottson-michaels.com/ccfraudhistory.htm>

[7]"Army's New Password: 'Biometrics'", USA Today, Thursday, June 22, 2000, Section, "The Nation," page 3A.

Microsoft, Others Unveil Tools To Protect Online Privacy By Linda Rosencrance 06/21/2000
http://it.idg.net/crd_fraud_69160.html and

Microsoft buys biometric security software for Windows, Juan Carlos Perez, IDG Ndws Service, May 03, 2000
http://www.computerworld.com/cwi/story/0,1199,NAV47_STO44049,00.html

Smart Cards – The Future of Information” – Very interesting site from Purdue with real down to earth explanations - (includes universities using Smart Cards.)
<http://www.tech.purdue.edu/it/resources/aicd/smCard.htm>

[8] The following list of articles very nicely explains simple applications available. Although dated, if someone is looking for a quick solution, updated features and prices could be found at the vendor's sites.

PC Magazine: Biometrics American Biometric BioMouse Plus – By Stephen W. Plain, February 23, 1999

<http://www.zdnet.com/pcmag/features/biometrics/>

PC Magazine: American Biometric BioMouse Plus By Stephen W. Plain, February 23, 1999

<http://www.zdnet.com/pcmag/features/biometrics/387164.html>

PC Magazine: Compaq Fingerprint Identification Technology By Stephen W. Plain, February 23, 1999

<http://www.zdnet.com/pcmag/features/biometrics/387165.html>

PC Magazine: Digital Persona U.are.U Deluxe By Stephen W. Plain, February 23, 1999

<http://www.zdnet.com/pcmag/features/biometrics/387166.html>

PC Magazine: Identicator BioLogon By Stephen W. Plain, February 23, 1999

<http://www.zdnet.com/pcmag/features/biometrics/387167.html>

PC Magazine: Identix TouchSafe Personal By Stephen W. Plain, February 23, 1999

<http://www.zdnet.com/pcmag/features/biometrics/387168.html>

PC Magazine: Saflink SAF/nt 2.0 By Stephen W. Plain, February 23, 1999

<http://www.zdnet.com/pcmag/features/biometrics/387169.html>

PC Magazine: Sony Fingerprint Identification Unit By Stephen W. Plain, February 23, 1999

<http://www.zdnet.com/pcmag/features/biometrics/387170.html>

PC Magazine: Citadel GateKeeper By Stephen W. Plain, February 23, 1999

<http://www.zdnet.com/pcmag/features/biometrics/387171.html>

PC Magazine: voicecrypt 2.01 By Stephen W. Plain, February 23, 1999

<http://www.zdnet.com/pcmag/features/biometrics/387172.html>

PC Magazine: Facelt NT By Stephen W. Plain, February 23, 1999

<http://www.zdnet.com/pcmag/features/biometrics/387173.html>

PC Magazine: TrueFace Network By Stephen W. Plain, February 23, 1999

<http://www.zdnet.com/pcmag/features/biometrics/387174.html>

[9] Smart Card Use Expanded at Addiction Treatment Centres

E-mail: info@csmcorp.com or NetSmart Technologies

www.netSmartech.com

[10] Preface, By Ira S. Somerson, BCFE, CFE, CPP, President, Loss Management Consultants, Inc., Blue Bell, Pa.

<http://www.securitymagazine.com/whitepaper.htm>

[11] Some colleges are no dummies:

Smart cards have nearly unlimited possibilities

Last in a five-part series on college life and money

By Lucy Lazarony • Bankrate.com

<http://www.bankrate.com/ndaq/news/atm/19980807.asp>

[12] Below are multiple European smart card sites with explanations of the services they have incorporated.

http://winster.nottingham.ac.uk/smart_cards/homefrme.html

<http://www.cpa.ed.ac.uk/newsarchive/11.1998-smartcard.html>

http://www.hotecho.org/hotecho/archive/se31/online_news/online_news.html

<http://www.adelaide.edu.au/smartcard/uofacond.htm>

<http://www.pittsburghjournal.org/links/2cards.htm>

<http://www.aston.ac.uk/smartcard/newsletter/8-newlet.htm>

<http://www.ntu.ac.uk/cit/about/smrtdcard.htm>

General References

Lots of experimental integration projects using Smart Cards with laptops, Palms, etc., are going on at the CITI – University of Michigan.

<http://www.citi.umich.edu/projects/SmartCard/>

Interesting site on the degrees being offered in biometrics.

<http://www.hsc.colorado.edu/sm/pmb/biom/index.htm>