



View On-Line Articles

March 2002 - Second Feature Smartcards and Tokens Marching Onwards

Introduction

Illena Armstrong, U.S. Editor of SC Magazine.

Unlike the intimidating deck of cards that Lewis Carroll's little Alice so quickly beat back near the end of her trip in Wonderland, smartcards and their cousin tokens are not falling away to reveal themselves players in a mystifying dream. Far from the imaginings of a novelist's dreamscape such as that found in the tale of Alice in Wonderland, smartcards are marching onward and upward in today's corporate world.

While they may have seemed less than appealing to businesses because of high costs, lack of standardization, interoperability issues or potential manageability problems, smartcards are finally finding a place in today's cyber and physical security infrastructure. From network authentication and physical access to securing transactions taking place over the Internet, smartcard-based applications are predicted to continue their march on the global market. For instance, analyst firm IDC projects that by 2003 the worldwide smartcard market will reach \$5 billion. E-purse and cashless vending, PC secure log-on, all-in-one employee IDs, banking and medical authorization, and still other applications, are predicted to abound because of the smartcard.



Roland Fournier, RSA Security's product manager for RSA SecureID products, says that financial services, banks and credit card companies are only aiding in this growth. Also, because of the proliferation of Java card-based smartcards, the proprietary cards of the past are finding no place in today's increasingly interoperable market. With more open standards, high costs are no longer a roadblock to adoption, as prices have continuously come down, he notes.

Too, companies are looking to combine physical and network or PC access together in one smartcard. This combination of applications on one card offers a high-value proposition to corporations today that are more security-conscious than ever before, he notes.

Baltimore Technologies' Stephen Byrne, solutions product manager, agrees that smartcard and token applications are converging to a point that has made the technology more appealing to corporations and government entities alike. Access to networks, buildings, mobile phones and more, are revealing that smartcards have a place today. On top of this, their ability to store digital signatures or biometrics, and aid retailers, credit card institutions and other companies to build loyalty programs or roll out more services, will make smartcards an even more valuable tool for business success, both he and RSA's Fournier explain.

"There will be a lot more take up, as these things converge to make [smartcards] sufficient security tokens for people to easily use," says Byrne.

Securing networks is a top-of-mind issue for all types of organizations nowadays, from private enterprises to law enforcement agencies. These groups will "expect to be able to 'flex' their communications to embrace mobile workers, but without compromising security," says Barron McCann's X-Kryptor security specialist, Peter Alderson. "Smartcard authentication and network encryption guarantees all traffic is encrypted the instant a connection is made, so there's no gap between logging on and authenticating yourself."

David Braddock, managing director at smartcard developer Ecebs, expects the focus on smartcard security to grow as new applications are employed by businesses. "In some cases smartcard security has been heavily over engineered to ensure card holder confidence. What we will now see is security specifically tailored to the application," he says.

While many years in the past have been predicted to be the coming of the smartcard, industry pundits seem to believe that 2002 may be the true beginning of this technology's foray into global workings. In this feature, we get insight from experts as to where the smartcard is today and what its hopes are for tomorrow. We also find out about the pros and cons of this technology and learn what to truly expect from its march onward.

Ending Complications

Gilles Lisimaque, senior vice president and co-founder of Gemplus

How often do we find ourselves cursing the numerous cards we are forced to keep in our wallet in order to lead our daily lives? Minimizing the number of cards we carry on vacations and business trips becomes a complicated task when we carry a different card for payment, ID, social security, medical, dental and prescription insurance, airline and travel memberships, facility or corporate access the list goes on. Envision having all these functionalities locked into a few cards, which you could tailor or customize to fit all of your needs.

Smartcard technology could, quite easily, solve this dilemma through its multi-application capabilities. A smartcard's flexible storage capacity makes it possible not only to carry one card for a broad variety of applications and services both in web-based and physical environments, but also allow the user to customize the bundling of applications for each card. With this in mind, a business traveler could customize his or her card to hold all travel-related data, such as corporate credit accounts, frequent flyer, hotel and rental car memberships, etc. Another card could contain all Internet and online account passwords and credit card information.

Among the more obvious applications, smartcards are widely used for logical access to PCs and networks, while in the physical world they can authorize entry to home or office. For similar purposes government organizations require multi-application functionalities for national ID programs, in which smart ID cards will help governmental institutions elevate security standards and streamline services for citizens.

In the web-based world, smartcards make an ideal tool for secure B2B and B2C operations. Their compatibility with Java and public key technologies create a perfect platform for running several applications on the same card. Java card technology allows dynamic downloads of new or upgraded applications, such as monetary value or loyalty programs, while public key cards enable online authentication and signing of financial transactions and legal contracts.

They're Here

Donna Farmer, president and chief executive officer, Smart Card Alliance

The events of Sept. 11 have dramatically heightened interest in improving the ability to provide secure personal identification. Alliance member firms have spent years developing smartcard solutions that are used for secure ID applications that protect the individual's privacy. Public and private organizations are now issuing cards for both physical and logical identity and include such implementation programs as the U.S. Department of Defense and Department of State, SchlumbergerSema, Royal Dutch/Shell Group and the U.S. Federal Deposit Insurance Corporation (FDIC).

Smartcards provide the best technology platform for secure personal identification systems, delivering secure and accurate identification while also including features that help protect an individual's privacy. Smartcards have the unique ability to verify the authenticity and authority of the service request prior to allowing access to the cardholder's data and, through on-card computations, can verify identity without access to a central database of information. We are seeing a heightened awareness in the need for better identification processes and technologies from many sectors, and believe that multiple organizations will issue improved secure personal ID cards.

Financial institutions are also deploying smartcards on a large scale. The driving factors behind smartcard deployment are privacy and security. Smartcards' multi-application capability offers a strong business case for retailers due to their abilities to have improved online security and to support loyalty programs for users.

2001 has been a breakout year for smartcards and 2002 looks to be even stronger. They provide the most secure means for identification, protect users' privacy and also have the benefit of offering increasingly popular loyalty programs.

A Thing of the Future

Malcolm MacTaggart, president and CEO, CRYPTOCard Corp.

Today, network users require ubiquitous computing - access to anything, from anywhere, at anytime. The traditional static user-ID plus password paradigm, originally designed to secure large mainframes in secure terminal rooms, no longer provides adequate network access control. As the 'break-ins' to the Microsoft, SANS, and Yahoo networks illustrate, no amount of security will prevent hackers accessing the network if they can obtain a legitimate user-ID plus password.

Static user-ID plus passwords make it far too easy for potential hackers to 'shoulder-surf' an authorized user to obtain a legitimate password. Additionally, as the user has no way of knowing that their password has been compromised, they cannot inform network administrators.

In contrast, if a user's token or smartcard is stolen, the user simply informs a network administrator of the disappearance, and the token or smartcard is deactivated instantly. Higher security levels can be reached by utilizing a challenge-response system to provide a randomly generated one-time password. Analogous to the power-ball lottery, knowing all previous winning numbers (i.e. challenges) doesn't help predict the next winning number.

Smartcards Suddenly Make Sense

Dave Oshman, senior vice president of technology, Identrus

Smartcards face a familiar obstacle before they become an omnipresent fixture in Internet commerce: interoperability. The Internet doesn't work without it, and neither will smartcards.

For users, smartcard nirvana is being able to use any card in any reader to secure a transaction. The current reality of smartcards is far from nirvana, however. Smartcards manufactured by one vendor typically don't work in systems that use another vendor's smartcard. The other interoperability issue is that smartcard subsystems (the name given to the smartcard, reader and supporting software) usually only work with the application they were specifically designed for.

Smartcards haven't been more versatile because smartcard vendors haven't wanted them to be. They have been competing for the upper hand in the market and trying to push each other out. Unlike the operating system market, where Microsoft is the de facto desktop standard, no vendor has gained a dominant position. The result is a fragmented market that makes customers wary and stunts the smartcard market's growth.

However, leading security vendors like VeriSign, ValiCert and Baltimore Technologies are recognizing that customers will not buy into a system that makes them use three or four different systems to do business. They are signing on to interoperability initiatives that will offer the kind of smartcard portability users expect. Such interoperability projects are gaining momentum in several different quarters. The U.S. government's common access card (CAC) allows any smartcard that meets the CAC interface to communicate with any smartcard reader that also meets the interface.

Identrus LLC, a cooperative venture of 53 international financial institutions, has taken a different approach to interoperability. Identrus has defined interoperability at the system level and publishes open standards accessible to any vendor. Smartcard subsystems that meet the Identrus standard for the client side can then interoperate with any application (from potentially any vendor) that meets the complimentary standard on the server side.

The goal for these and any interoperability initiative is for users to operate across multiple email systems, purchasing applications, e-marketplaces, B2B web sites and more - anywhere on the Internet, regardless of the vendor providing the smartcard application.

Smarting from PKI Interoperability

George Gilka, senior product marketing manager, Kyberpass Corporation

The inception of public key infrastructure (PKI) had promises of a home run for the e-commerce world, touting the ability to secure messaging, e-commerce and virtual private networks (VPNs). But as the game plan unfolded, those three letters were fouled by functional inadequacies that left PKI vendors and smartcard providers struggling to interoperate. Lately, however the trend has shifted, demonstrating security vendors converging to a common baseline of interoperability, making PKI deployment more effortless and ROI more apparent.

The world is starting to appreciate the practicality of using smartcards. A smartcard can essentially replace the contents of a wallet, while providing ironclad security notarized by a recognized authority and verified by the PKI. If a smartcard is lost, it is useless to anyone finding it. PKI offers unparalleled security management of all the credentials stored on a smartcard.

However, just as a burglar alarm needs a property to protect before it is useful, smartcards and PKIs still lack general market appeal because of the complexity of integrating them with standard applications and services. The challenge is making all the players work as a team in a smooth and transparent way. The good news is that new vendor solutions are cropping up to bridge the gap between applications and the various security mechanisms that tie into PKI. Helping organizations deploy PKI-based security that integrates with new or existing applications, quickly, painlessly and at dramatically reduced costs, is crucial to helping them see the benefit of PKI-based smartcards. PKI and smartcard vendors are quickly realizing the value of ensuring that their mechanisms interoperate - and middleware solutions ensure that no one smarts from this convergence.

Ensuring the Security of Smartcards

Terry Fletcher, senior security engineer, and Bill Cullen, product line manager, Chrysalis-ITS

Smartcards help secure e-business transactions and electronic identities by storing the cardholder's sensitive data, like biometric information, personal medical history, cryptographic keys, or digital certificates for authentication. For smartcards to carry this data and ensure authenticity of users in online transactions, then the way the card's keys are generated and distributed must be trusted.

Each stage of smartcard production requires the use of sensitive encryption keys, which in turn need to be protected to make certain the process is secure. If these 'master' keys are compromised, then all smartcards issued or personalized using these keys are compromised, meaning counterfeit cards could be issued or credentials changed. For applications requiring the use of digital signatures, private signing keys also must be protected to ensure trusted signatures.

Specifications, such as Visa Open Platform and Identrus, call for key pair generation, and the protection and use of private keys within specialized hardware, to provide high security and ensure authenticity of

digital signatures used by these applications. Although it's possible to generate key pairs within smartcards, this proves costly for mass-user issuance, because expensive smartcards are required for on-card key generation. A viable, less expensive method of generating the key pairs for smartcards in wide distribution is to use separate hardware security modules (HSMs), in conjunction with smartcard management systems (SCMS) and less expensive smartcards.

Using an HSM for smartcard key issuance has more advantages than cost reduction alone. HSMs are much faster than smartcards in performing computationally intensive key pair generation. Additionally, using an HSM in conjunction with an SCMS allows the card issuance and PKI subscriber registration functions to be combined in a single entity. This enhances the speed and security of creating and distributing digital IDs to smartcards while simplifying the applications that must be hosted on the smartcard - the smartcard itself does not need to understand the protocols used for PKI registration and certificate issuance.

Smartcard design and security protocols for authentication and data confidentiality between smartcards and external entities provide the basis for securely transferring the private key generated in the HSM to the user's smartcard. The process ensures that private keys never exist in an unprotected form outside of secure hardware and that no unauthorized copy of private keys exist that could be later used to fraudulently sign transactions.

Smartcards as a Security Measure

Ken Greenwood, field marketing manager, SchlumbergerSema

While no one would suggest that smartcards offer a total solution to a company's security obstacles, a portable token with the ability to hold a person's identity both physically printed on the front and encrypted inside the chip is a big step forward. But is it secure?

Smartcards are already used for many applications that require a high level of security, ranging from access to paid television to securing a mobile telecom network. The fact is that while very few technologies can be classed as 100 percent secure, a smartcard comes closer than most. A smartcard is much less likely to be compromised than traditional network security, which is often subject to hackers and virus attacks.

A password typed into the keyboard has long been used as a means to secure a company's data. But the fact remains that intercepting keystrokes or even discovering secret keys stored on a computer's hard drive is relatively easy for most cybercriminals. How many people make every one of their many passwords the same? How many more write these passwords down inside a convenient desk drawer?

When used as a corporate badge, a smartcard can electronically allow or deny access to buildings as well as networks. It can store other passwords for internal applications, such as home banking. It can allow remote computer users to access secure company resources when on the road. It can offer other services such as payment in the staff cafeteria or vending machines. It can, when fastened to the belt, even act as a physical photo identification when walking around a site.

What is in the not too distant future for smartcards? The same card will allow access via a biometric, such as a fingerprint, to authorize the user, [which will enable] added security and convenience. It will allow access to personal digital assistants or other mobile devices, allowing the security to continue away from network connectivity.

Smartcard technology is available now and already is being used by many corporate enterprises, as well as government agencies. It is already legal in much of the world to sign a document with a digital signature encrypted onto a smartcard. With more and more organizations opting for this technology for its security and convenience, the smartcard will soon become an integral part of doing business in an increasingly technological world.

The Cost-Effective USB Token

By Eileen Angel

From a straight technology perspective, there isn't a lot of difference between a smartcard and a USB security token. Both offer users generally the same security footprint, the same measure of two-factor authentication, and much the same functionality when it comes to storing digital certificates or providing fine-grained access control to business critical data and applications.

Besides the obvious form factor look and feel, the largest difference in comparing these two popular forms of authentication comes down to cost. The cost of installing, deploying and managing a smartcard environment is much greater than a similar network using USB security tokens. The more an organization's size scales, the longer it takes to fully roll out a smartcard network to all users. With this, the more it costs the organization in terms of incremental user deployment, unsecured downtime, variable user training and added management costs for adds, moves and changes. All of these factors make a compelling argument for deploying USB authentication tokens as the more cost-effective and less costly authentication solution to fully deploy.

While prices certainly will vary based on which card or which key and how many purchased, the cost of a smartcard and smartcard reader is about 30 percent more than a USB token with an extension cable. Since readers have to be installed, this process can take up to 45 minutes per client, per installation. This makes the cost of installing a smartcard and card reader much more significant compared to configuring a

USB token. The installation cost per client for a smartcard solution is only about 68 percent greater than equipping the client machine with a USB authentication token. However, couple this with the fact that most users can handle installing the client software and configuration of the tokens entirely on their own, it not only saves valuable IT budget dollars, but changes the role of most stretched IT organizations, who at best, can install only about ten smartcard clients, per person, per day.

A USB token also offers some performance advantages over a smartcard, which lowers the cost of ownership. For example, a token can provide 67 percent faster response time over a smartcard using a standard reader with an external clock. In addition, the USB token is plug-and-play, while many smartcard readers will require additional configuration. Lastly, the USB token itself offers greater durability than a smartcard's magnetic strip, meaning it can handle more insertions.

For large enterprise organizations, full deployment of a smartcard solution can be both a costly and time-consuming endeavor. The same strong security footprint, but lower installation costs and no reader requirements makes a compelling argument for USB tokens.

Eileen Angel, strategic marketing manager, security components, Rainbow Technologies.

Hitting Asia Pacific

By Harold Lerner

As we face new challenges in this ever-changing 'digital age,' smartcards are rapidly becoming a hotbed for convenient, streamlined and highly secure information. Today, cardholders can make secure payments, provide personal information, and access a variety of accounts with the swipe of a chip-embedded card.

Smartcards are an ideal technology that offers a relatively low-cost, yet highly sophisticated method of storing and processing information that combines a variety of electronic networks with the traditional features of identification cards.

The Asia Pacific/Asia continental region has especially taken to this trend, as both governments and enterprises have recognized the importance of instant, yet secure, information. These cards serve as an ideal solution for Asia's growing secure identification and authentication needs as governments throughout the region are implementing initiatives, such as Singapore's national ID program and Malaysia's government multi-purpose card (GMPC). Now, governments can turn to a single card to access information from immigration background and passport authentication, to drivers' licenses, to social security and tax information. The list goes on and on.

In addition to various governments' adoption of smartcards for its citizens, Asia's vastly growing telecommunications industry is integrating smartcards into its business model through prepaid phone cards and GSM cards.

The banking industry has also adopted smartcards for payments for micro-payments and electronic purses, controlled access, and employee identification. Asia's mounting affluence and increased concern for security and fraud protection have also increased the surge of interest in smartcard usage.

As technology evolves and Internet usage continues to flourish throughout Asia, the ability to combine users' identification and authentication information while accessing electronic networks, ensures that smartcards will be a crucial facet of our daily lives.

Harold Lerner is director of implementation, TrustAsia.



[View On-Line Articles](#)

[Home](#)

[Articles](#)

[Advertising](#)

[Editorial](#)