FinSmart Security White Paper

Enabling E-Commerce with the FinSmart™ Smart Card Security Solution

To meet the demands of customers, merchants and financial institutions alike, FinSmart™ is a smart card-based, end-to-end solution securing financial transactions for e-commerce applications.

2001

The Market Potential of e-commerce Applications over the Internet

Over the recent past, not only has the Internet revolutionized the way we communicate, it has also transformed from simple electronic mail and Web publishing to a focus on advanced communications—connectivity via virtual means, personalized information, and possibly most important—a wide range of electronic commerce services. From approximately 130 million users worldwide at year-end 1999, New York based eStats Inc. predicts the number of users will grow to 350 million by 2003.

Another technology that has mirrored the speed of Internet adoption is mobile telephony. Many of today's mobile phones support the WAP (Wireless Application Protocol) standard that defines an Internet browser for access to information and commercial services. It also specifies how mobile phones will work with smart card technology to support banking services and electronic commerce applications. New mobile phones will have increasingly larger displays to support commerce, and many will be equipped to accommodate both a smart card and a second full-sized smart card for banking and e-commerce applications.

This white paper examines the security and privacy issues related to Internet e-commerce, with attention also given to Internet banking and other on-line transactions services—no matter which access device is used, including PCs, mobile phones, or set-top boxes. The benefits of smart card use for user authentication, and potential security breaches during and after an Internet-based transaction will be analyzed. Finally, a discussion of how smart card readers can be built specifically to address current security shortcomings, while providing key competitive advantages to the companies providing them.

E-commerce in the 21st Century—the Benefits and Challenges

Over the last few years, Web-based companies such as Amazon and e-Bay have demonstrated the potential of electronic commerce over the Internet. Today, it is easy to buy and sell shares of stock through an online broker, make travel reservations, and purchase a myriad of products and services. The benefits of doing so are considerable in terms of cost savings and convenience. However, two factors today limit the growth of consumer e-commerce:

- Concern about transaction security
- Protection of sensitive data

Armed with only credit card details, it is easy for criminals to order goods and services using any one of thousands of commercial Web sites on the Internet today. In a recent case, a California-based "adult services" company netted more than $40 million by legitimately purchasing lists of valid credit cards from a bank and fraudulently charging $19.95 to each cardholder's account. This type of incident is far from random, unfortunately, and as international press and media coverage of Internet-based criminal activity increases, the result is that potential users of e-commerce services are afraid to divulge credit card information online. Market analysts Ernst & Young report, "Ninety-seven percent of all households do not buy online because they do not feel comfortable sending credit card data across the Web, and 62 percent of online consumers have the same fear."

Despite these concerns, the number of Internet payments is increasing very rapidly largely due to the trust placed in the secure socket layer (SSL) protocol that provides secure (encrypted) communications over the Internet. Unfortunately, this trust is somewhat misplaced since many merchants use server computers with inadequate data security protection, and the weakest link is normally the user's PC and software applications resident on it.

Whenever a PC connects to the Internet, it is vulnerable to attack by many different types of computer virus. Such viruses are usually transmitted disguised as innocuous e-mail attachments. The most common replicate themselves via e-mail to all the addresses stored on the PC, and damage or alter the computer's operating system. It is also just as simple for a virus to remain undetected on a PC and undermine the security of the software handling Internet transactions, or extract sensitive data such as PINs and transmit them to an unauthorized user. And, as cryptographic protocol SSL runs entirely in software, hackers can easily determine session keys from PC memory during the encryption process.

There are considerable efforts to minimize customer concerns on the security of data. Security-sensitive merchants use server computers armed with hardware solutions that protect sensitive consumer data from prying eyes, combined with SSL to secure data transmission. The client PC remains the weak link featuring poor protection of credit card and personal data that is keyed in, stored and displayed. A real breakthrough in consumer e-commerce will only happen once there is an end-to-end system solution capable of authenticating the merchant and consumer identities and storing/sending confidential information in a highly secure manner.

Smart Commerce

To identify users attempting to conduct commerce over the Internet, the electronic equivalent of a passport—a digital certificate—is a standard and accepted authentication method. Merchant servers and PCs can both generate these certificates. For the client, they provide a high degree of assurance that the transaction is actually taking place with the required merchant's server computer and not a look-alike imposter system. However, they are insufficient for the merchant side as only the user's access device is identified—not the person conducting the transaction.

Passwords are the most common solutions to this problem. Unfortunately, passwords are often stored in the PC's memory where it is prone to attack by hackers, viruses, or unauthorized use. A far better solution, analogous to the keys we all carry to enter our homes, offices, and files, is the smart card.

Similar to a credit or bank card, a smart card houses both a microprocessor and memory, and is capable of providing cryptographic functions and a ‘personal’ digital certificated associated with PIN number. When initiating a transaction, a dialogue occurs between the server and smart card, using Public Key Infrastructure (PKI) keys. Only a correct response based on the PIN entry authenticates the user as a valid client.

The American Express “Blue Card” accompanied by a smart card reader connected to a PC, provides access to the American Express “electronic wallet” to pay for goods and services online. Although this solution is preferable to placing credit card details on numerous servers with questionable data security, it is still not completely secure. The smart card reader works with the PC, creating an insecure system that enables a hacker to determine the PIN entered on the PC keyboard and to potentially change the amount of the transaction.

Several schemes are under consideration such as handling micro-payments for online services via smart card-held electronic cash. However, the most optimal smart card application appears to be online user authentication. Smart cards allow a merchant, service provider, or government agency to verify consumer identity without physical checks such as matching a person’s face to photo identification. Smart cards meet the challenge by carrying secret codes unique to the cardholder. The most popular format is the Public Key Infrastructure (PKI) that quickly verifies cardholder and merchant identity. PKI also attaches a unique digital code—a signature—to every transaction and thus provides evidence for the merchant that the cardholder placed an order, or received services.

The use of a PIN code and bankcard (magnetic stripe or smart card) is a well-accepted and established method of withdrawing cash from an ATM. It is reasonable, therefore, to expect a similar level of consumer confidence in using a smart card/PIN combination to handle security for online commerce. Several major banks offer or have announced their intent to offer smart debit/bankcards and services based on this combination.

Securing Communications

Merchants, service providers and consumers must trust both the system security and the integrity of the data being communicated over the Internet for financial transactions. The challenge of using smart cards with a PC or other access device, connecting to the Internet, is how to secure the communication between the transaction server (Bank, Credit Card Company, etc.) and the smart card itself. In existing solutions, the communications path between the transaction server and the application running in a PC is secured using cryptographic protocols such as SET. Securing the communications in this way ensures data integrity—the transferred data cannot be changed by a hostile system without it becoming immediately evident that tampering occurred.

However, the application running inside a PC, because it is connected to the Internet, is the weak link in system security. Any one of a range of different viruses capable of retrieving sensitive data can penetrate and run on the PC. Further with the cryptographic protocol running completely in software, a hacker can determine the session keys that are available in PC memory during the encryption process.

It is relatively straightforward to breach system security through the connection between a PC and a smart card and via the application software running inside of a PC.

FinSmart™

To maintain system security at the PC level, it is clear a secure protocol must exist between the transaction server and a smart card reader. This protocol must ensure that keys and other critical data cannot be accessed from within a PC. Critical requirements to create a highly advanced security system for e-commerce applications include:

- High security and low cost implementation to ensure commercial acceptance
- An open system based on all types of smart cards and supporting different applications
- The capacity to download new firmware into a smart card reader
- A method to indicate that the reader is activated in secure mode
- A locally connected keypad for PIN entry
- A locally connected LCD to display transaction amount

To provide a solution and protect against hacker attacks and viruses, Securealink and Hagenuk CPS have developed a unique KeySmart™ technology as the key component of the Hagenuk FinSmart™ solution.

By using FinSmart technology, the communication between a smart card reader and the PC is protected against unauthorized use and attacks on the cryptographic protocol using PKI. Connected to the smart card reader are a keypad and liquid crystal display (LCD). The LCD allows for display of detailed information on the connection status and server identity. The LED indicates when the smart card reader is activated in secure mode.

KeySmart technology secures a PC-based communication by running a highly secure cryptographic protocol completely within a single chip KeySmart device; by generating true random numbers within the chip; and by performing all secure calculations within the chip, making tampering impossible.

FinSmart renders the following types of attacks impossible:

- Unauthorized PIN recovery
- Lock-up of smart card by entering invalid PINs
- Tampering with purchase amount
- Spoofing—where an attacker acts as an recognized application

- Sniffing—protected via a highly secure cryptographic protocol running within a single-chip KeySmart device
- False generation of random numbers in software
- Tampering with security protocols

FinSmart provides an e-payment solution for end-to-end security based on smartlets. Sensitive data is stored in encrypted form at merchant sites eliminating access by hackers. FinSmart supports an open platform, supporting multiple applications and varied smart card brands and schemes. In addition, up to five multiple certification authorities are supported. Users and merchants alike are provided an authentication and audit trail through certified smartlets. FinSmart, based on PKI, integrates easily with SET solutions.

A Technical Overview

The FinSmart solution is a highly secure smart card system capable of low-cost implementation that enables the creation of trusted devices. KeySmart technology, and specifically the PCC807 chip and downloadable (trusted on non-trusted) smartlets for multi-application compatibility provide the core of the security.

Certified or trusted smartlets are the key to the operation of the FinSmart concept and enable seamless operation with either Netscape Navigator or Internet Explorer browsers. From the browser interface, users select a function (pay, load, identify, etc.) for the brand of smart card required. This action prompts a trusted smartlet, which is secure, and a certified software script dedicated to the task.

The trusted smartlet can be loaded from a central site to guarantee uniformity and upgradeability. The smartlet performs the required function using an encrypted communication channel with the host (such as SSL). A FinSmart smart card reader contains a number of root keys. For each root key there are a freed certification of smartlets so that a nearly limitless number of smartlets are enabled.

FinSmart smartlets have a time-limited validation associated with their use. This forces an ensured upgrade inherent in a system approach. With Securealink's PCC807 chip, there is a size limit of 16KB for secured smartlets; however, secured overlays can also be supported. The PCC807 provides encryption security up to 2048-bit RSA, and can perform 1024-bit RSA verification in less than 100 ms.

Only certified merchants are able to use trusted smartlets. Smartlets are passed through the PC to the card reader chip as part of the communication chain and **cannot** run or have any action on the PC itself. The benefit of this method is that the smartlet corresponding to the required card type can be downloaded according to the consumer's choice of payment method.

FinSmart based smartlets can easily be encapsulated using Java with a small Java virtual machine (JVM) running inside the PCC807 IC. This system will be available during

2001, following he conclusion of the Finread Group (a consortium of European banks) with respect to the requirements of the JVM.

FinSmart Flexibility

FinSmart secure smart card reader technology can be used to secure communication between the server and smart card token. This highly secure solution is based on industry accepted cryptographic standards including RSA (asymmetric key exchange), 3DES (symmetric key exchange) and SHA-1 (hashing). These functions are implemented in one integrated circuit known as the KeySmart PCC807 that includes a true hardware-based random number generator.

Using state-of-the-art silicon technology and cryptographic implementation, Securealink has created a single chip architecture that incorporates all functions needed to create a low-cost smart card reader. The PCC807 chip is the first IC implementation using KeySmart technology that Securealink is supplying commercially. The device supports PC connection via an RS-232-C or USB interface.

The complete FinSmart solution is available under license to OEMs involved in creating devices ranging from low cost PC-connected smart card readers to future PDAs and Internet-capable WAP mobile phones. When used as a basis for smart card readers, it offers a myriad of benefits to OEMs, including:

- Designed for e-commerce and e-purse transactions
- Small footprint
- Simple operation based on PIN entry
- Explorer and Navigator browser interfaces
- KeySmart security
- Sensitive data stored encrypted at merchant sites
- Open platform supporting several smart card brands and schemes
- Easy installation under Windows™ 95, 98, NT, 2000

FinSmart gives banks and financial institutions an end-to-end user/merchant authentication system, providing secure data handling and the support of smart-card debit transactions. Sensitive data is stored encrypted at certified merchant sites and only the bank or clearing house is able to decrypt the data.

For more details on the FinSmart system solution, or for direct enquiries on Hagenuk's FinSafe™ smart card readers, please refer to www.hagenuk.com.

For more details on Securealink's KeySmart™ technology and the PCC807 chip, please refer to www.securealink.com.