

Expediting PIN Issuance

Revolutionizing PIN Issuance: How New Fully Automated Web-Based Technology Expedites and Secures the PIN Issuance Process

By Rene Bastien

SafeNet, Inc.

www.safenet-inc.com/financial

Revolutionizing PIN Issuance: How New Fully Automated Web-Based Technology Expedites and Secures the PIN Issuance Process

Introduction

Over time, methods of personal identification have evolved from simple name and face recognition to today's electronic-based techniques. Much of the impetus for this evolution has been the advancement of computer-based financial transactions, in particular the advent of the Automated Teller Machine (ATM), which provided consumers with access to their funds anywhere at any time. The Personal Identification Number (PIN) came into existence at the same time as the ATM as a means of authenticating the person executing the transaction. Today, the PIN is still most commonly used with ATM and credit cards.

Security is at the core of all PIN-based transactions. Two-factor authentication provides the basis for non-repudiation of financial transactions, which is an essential characteristic of card-based commerce. The person inserts or swipes the encoded card (something you have), and then enters the PIN (something you know). It is imperative that cardholders keep their PINs confidential and complex in order to maximize the security of their accounts. However, PIN privacy originates with the card issuer. The ability to securely deliver PINs to cardholders must be a priority of every card issuer and financial service provider.

Sending PINs through traditional mail is costly, time consuming, and highly insecure. Instead, why not look to the same technology used to provide customers with access to their financial accounts—the Internet. In the proper environment, PINs could be securely issued and managed over the Web, providing a wide range of benefits to both the

cardholder and the card issuer.

Traditional PIN Issuance Methods and Limitations

Traditionally, cardholders request a card by mail, Internet, or at their local branch office. In a few weeks, the card arrives, followed by a separate PIN mailer. Although a standard method of issuance, these tamper-evident, laser-printed PIN mailers are known to be vulnerable to attacks that reveal the PIN without tampering .

Some card issuers prefer to issue cards and PINs in the local bank branch, where the cardholder will be asked to select a PIN either through a dedicated terminal or at an ATM. Problems occur here when fraudsters place overlays on ATM PIN pads to register cardholder key strokes, or they switch out dedicated terminals with dummy terminals to gather the sensitive PIN and cardholder data, often unbeknownst to the ATM or terminal owners. Others perform PIN issuance through an Interactive Voice Response system that allows a computer to detect voice and touch tones through a phone call. Unfortunately, these systems cannot be secured in an effective manner.

A Study in PIN Management

With 3.2 million customers, Egg Banking, plc, a Citigroup company is the world's largest online bank. Several years ago, Egg began a search for a secure and convenient method of delivering cards and PINs to their customers. Most companies were doing this by mail, which is costly and insecure.

Egg wanted its customers to enjoy the best service experience possible by being able to use their cards immediately after they received them, rather than having to wait seven to ten days for their PIN to arrive by mail. Egg also wanted to lower the risk of PIN mailers being intercepted en route to customers, as well as decrease the costs associated with providing up to three million new PINs a year. Yet allowing customers to retrieve their PINs via the Internet seemed dangerous, even to some of the company's own IT people.

One of the biggest challenges of the project was ensuring that the customer was the only person able to view their PIN. Preventing disclosure of the PIN across the entire transaction would be difficult since typical SSL sessions meant encrypted data had to be decrypted on the Web server. The card issuer holding Egg's customer PIN data had doubts as to whether a technology actually existed to achieve this goal.

The solution was found through the implementation of a Web-based application security module, with an integrated hardware security module for secure key management, which allowed Egg to deploy a secure end-to-end encrypted tunnel between the cardholder and the card issuer. This provided cardholders with a safe and convenient way to retrieve their PIN over the Internet.

One major benefit of this solution was the tangible cost savings. For every million cardholders, Egg saves \$5,000,000 a year in postage and fulfillment costs, while providing the customer with a better service — a win-win situation for the bank and the customers. These savings will continue as new card customers come to Egg, or existing customers need new PINs or replacement cards.

Another major benefit was time savings. A PIN request through the Egg Web site is fulfilled instantly, allowing the customer to immediately use the card. In addition, the PIN change/request can be generated from a mobile device, adding increased convenience. In contrast, a PIN request that has to go through the mail can take up to ten days, assuming it is not subject to interception and does actually arrive.

"That's a week or more that the cardholder is either not purchasing or is doing so with a card from another issuer," said Stuart Horler, Lead Architect at Egg. "Multiplied by the number of credit card customers we have, that is a huge potential loss of revenue and an unnecessary inconvenience for our customers."

"Everyone understands that it's important that customers trust online banking while, at the same time, benefiting from its convenience, and this initiative will certainly improve the overall experience," said Dr. Rob Elliss, SafeNet's Director of Sales for Northern Europe.

In summing up the project, Tracy Willis, Head of Technology Security at Egg, comments: "PIN Browser provides a secure and highly convenient approach to PIN distribution for our customers. Our partnership with SafeNet has enabled another online banking breakthrough for Egg."

Securing the PIN Issuance Process

Egg realized a competitive advantage by offering the enhanced customer experience of instantly issuing PINs over a secure, easy-to-use Web session. With this solution, the hardware and software components are integrated into the card issuer's existing IT architecture and Web portal to facilitate the delivery of PINs across the Internet, or other communications network, to the customer. Using hardware-based cryptographic key management ensured that the keys and processes were stored and managed exclusively within FIPS-validated hardware. Using the existing Web site and user authentication system, this approach made use of standard Web security protocols without any requirement for applets or browser plug-ins on the customer side. By leveraging existing authentication and processing systems, no changes need to be made to the core architecture and, therefore, no potential vulnerabilities can be introduced to these sensitive areas.

Considering that the point of issuance can often be the weakest link in today's heavily mandated EFT (Electronic Funds Transfer) system, encryption has proven to be the most effective data security solution, ensuring that the storage and transfer of consumer card data is protected against manipulation and fraudulent card production.

It is vital that split security be maintained throughout the transaction so that a PIN number is never associated with a particular card number or customer, thus ensuring protection from both external and internal attackers. It is also imperative that management of the system is segregated from the operation of the product, such that even the security administrators are not able to gain access to critical data, such as PINs, at any time.

This solution saves card issuers millions of dollars each year, and is safe, fast, and environmentally responsible. The level of security provided by encryption far surpasses that of paper-based PIN mailers or voice-based interactive systems, thereby reducing fraud and theft. With customers retrieving their own PINs, they feel more in control. They no longer worry as to when their PINs will arrive and no longer have to wait for days or weeks before they can use their card.

Financial institutions realize tangible cost savings by replacing or reducing the number of physical PIN mailers that are issued, with the added benefit of preventing fraud by eliminating PIN mailer interception. They also achieve a competitive advantage by eliminating any delay between the time an account holder requests a new PIN and the time they receive it, thereby minimizing the opportunity for a customer to use a competitor's card during the waiting process. Financial service providers can be assured that sensitive financial transactions execute in a trusted environment that is immune to physical, logical, and operational threats.

About SafeNet

For more than 25 years, SafeNet has provided encryption technologies for the world's most important top financial services institutions. Trusted to protect more than 80 percent of the world's fund transfers—\$1 trillion per day,..

SafeNet, Inc. is a global leader in information security. UBS, Lloyds, Egg Banking plc, Bank of America, InstaPayment, First Data, Bank of Canada, Citibank, Barclays, the U.S. Federal Reserve, the U.S. Treasury, and many other financial institutions entrust their security needs to SafeNet. For more information, visit www.safenet-inc.com/financial.