ATMmarketplace.com

Increased automation may be key to PIN security

AS NETWORKS CRACK DOWN, REMOTE MANAGEMENT BECOMES AN ATTRACTIVE OPTION.

By Ann All, editor, ATMmarketplace.com

In an effort to improve PIN security, EFT networks require their members to use a unique encryption key for each ATM. While the requirement has been ignored by some ATM owners due to high implementation costs, a movement toward remote key distribution could improve compliance rates.

Using a unique key makes it more difficult for bad guys to compromise PINs at multiple ATMs. This concept is common in everyday security; few folks use the same key to secure their car, house and other valuables.

The use of unique keys was first required in a standard (X9.24 — Financial Services Retail Key Management) produced by the X9A3 committee in the early 1990s. Accredited by the American National Standards Institute (ANSI), X9 develops and publishes voluntary technical standards for the financial services industry. Card associations and networks adopt many of ANSI's standards, thus giving them considerable clout in the EFT industry.

How unique are we?

Yet despite the logic of using unique keys, many ATM owners have ignored the requirements. And until recently, networks didn't push the issue.

"Are we in better shape than we were five years ago? Yes. Before 1998, probably 90 percent of ATMs out there didn't have unique keys," said Darlene Kargel, a CPA with consulting firm DeLap White Caldwell & Croy. She has conducted compliance reviews for networks like Star and NYCE since 1991. "But are there still a lot of waivers out there today? Yes."

Jim Shaffer, senior product manager for security initiatives at ACI Worldwide, said, "If you really want to please the (network) auditor, re-keying an ATM network in the acceptable manner is an expensive and manually intensive process."

Indeed, one of ANSI's requirements for key management calls for the use of a security concept called dual control — having two people each manage and load separate components of a key into an ATM. A concept called split knowledge — no one person knowing any part of the key — is also required. These concepts obviously increase the cost for ATM owners, who must send two people to machines to load keys.

Kargel said that many ATM owners, particularly financial institutions with large networks, have postponed implementing unique keys to avoid this expense. "There was a business case for waiting," she said.

Now, all ATM deployers are faced with re-keying their networks to satisfy mandates for Triple DES encryption, which doubles the length of the keys to 32 hexadecimal characters. Because of this, Shaffer said, incidents of "fat finger syndrome," in which a service tech enters the wrong digits, could increase. (Most ATMs provide key check digits to ameliorate the fat finger problem, according to Dennis Abraham, president of Trusted Security Solutions and a member of the X9.24 committee.)

Kargel agreed, noting, "It's obviously more efficient if you have an HSM (host security module) rather than a human generating keys."

Abraham said that eliminating humans from the key-loading process at ATMs might also boost PIN security — if the system is properly implemented.

"What's protected most organizations to this point is the lack of knowledge of the people loading the keys. You had security through obscurity," he said. "Those of us that understand the technical details of the industry never participate in chat rooms where potential opponents discuss these systems and often swap incorrect information with each other. But what would happen if somebody didn't obey the unwritten code and said something they shouldn't in a chat room on the Internet?"

Prompted by ATM owners to simplify the key management process in time for Triple DES, an X9 working group (X9.F6 — Cardholder Authentication and ICC Cards) in March 2002 began reviewing a proposal that would create standards for remote key distribution.

Standards on the way

The move to Triple DES would have been simpler if remote key had been introduced earlier, said John Sheets, chairman of the X9.F6 working group and vice president and chief security officer for point-of-sale terminal manufacturer Ingenico Group.

"The unique key re-keying wouldn't have been necessary at all, since the remote key protocols all load a unique key into each ATM," Sheets said. "Triple DES re-keying would have been virtually as simple as a touch of a button."

Remote key capability will better position the industry to handle any future PIN security threats, Sheets believes. "What's coming down the road? No one knows for sure since we cannot predict where the weaknesses will be. But with remote key capability, the industry will be in a much better position to respond," he said.

The remote key proposal, written by security consultant Jeanne Fagan, president of Fagan & Associates, LLC, has undergone several revisions and will be voted on by the ANSI membership at its next meeting in March.

Shaffer hopes ANSI, which meets three times a year, will sign off on the proposal then. "I think the Triple DES deployment is really fueling this, and the ATM manufacturers are eager to support it," he said.

Fagan said an ANSI blessing would "open the door for networks to add approved methods for remote key to their operating rules" and, perhaps more importantly, add them to the Technical Guideline 3 (TG3), a document which network auditors use to assess ATM owners' compliance with network requirements.

> "ARE WE IN BETTER SHAPE THAN WE WERE FIVE YEARS AGO? YES. ... BUT ARE THERE STILL A LOT OF WAIVERS OUT THERE TODAY? YES."
>
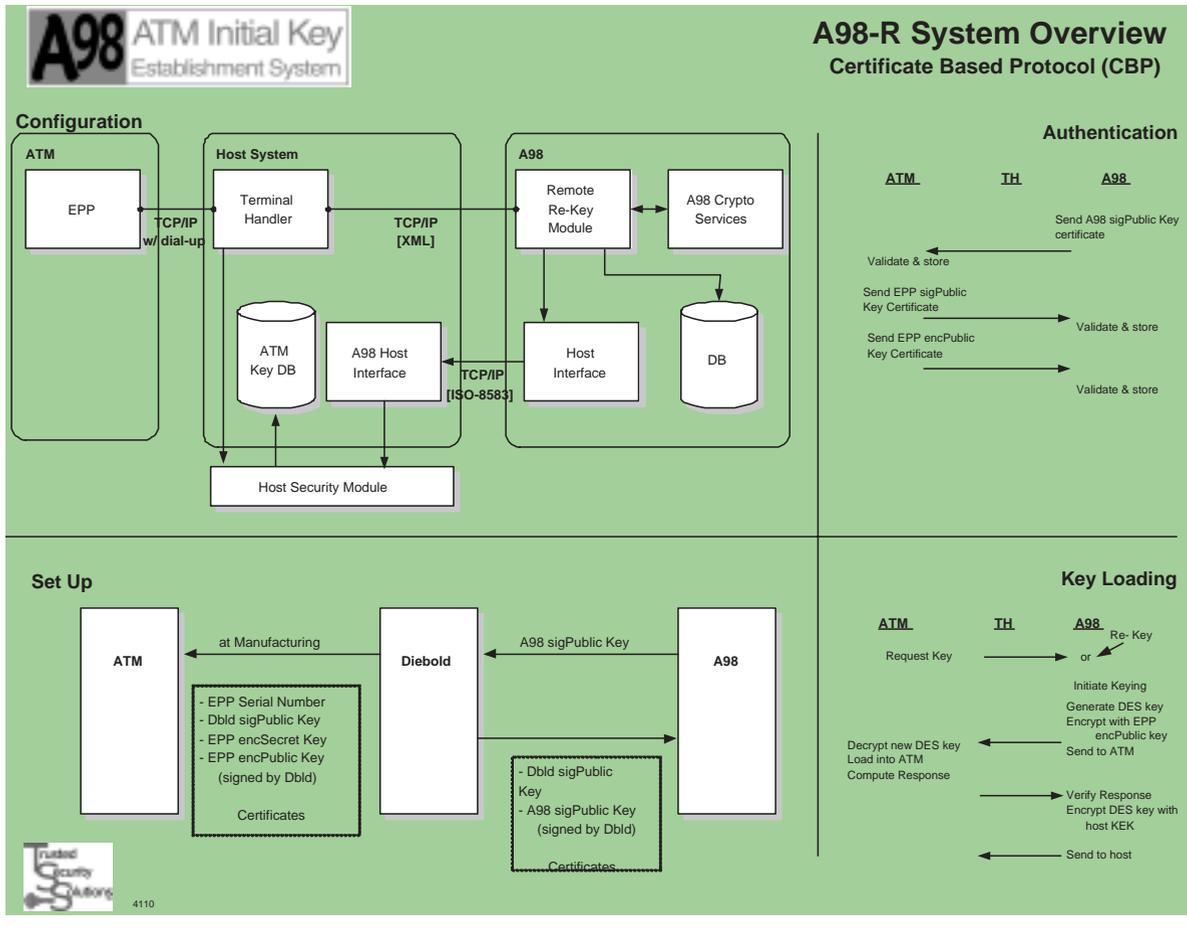> — DARLENE KARGEL, CPA, DELAP WHITE CALDWELL & CROY

Shaffer said ACI already has several customers in beta implementations of remote key and hopes to bring a customer "live" soon. However, Fagan said, "it might cause some grief for networks or auditors" if ATM owners rush to implement remote key before it can be added to the TG3.

Two of the largest ATM vendors, Diebold and NCR, have already equipped their EPPs (encryption PIN pads) with the components necessary to support remote key distribution and outlined their own methods for doing so. Because both vendors' methodologies are included as reference implementations in the X9.F6 draft, Fagan said, they are likely to be included in future standards.

Going public/private

Both are based on public/private key cryptography, in which keys used for encryption are different than ones used for decryption. In public/private (or asymmetric) cryptography, both sender and receiver (the host and the ATM) have their own respective pair of keys. Each pair includes one public and one private key.

A98-R SYSTEM OVERVIEW CERTIFICATE BASED PROTOCOL (CBP)

A98 ATM Initial Key Establishment System

A98-R System Overview
Certificate Based Protocol (CBP)

Configuration

ATM — EPP
TCP/IP w/ dial-up
Host System — Terminal Handler
TCP/IP [XML]
A98 — Remote Re-Key Module — A98 Crypto Services
ATM Key DB — A98 Host Interface
TCP/IP [ISO-8583]
Host Interface — DB
Host Security Module

Authentication
ATM   TH   A98
Send A98 sigPublic Key certificate
Validate & store
Send EPP sigPublic Key Certificate
Validate & store
Send EPP encPublic Key Certificate
Validate & store

Set Up
ATM — at Manufacturing — Diebold — A98 sigPublic Key — A98
- EPP Serial Number
- Dbld sigPublic Key
- EPP encSecret Key
- EPP encPublic Key
 (signed by Dbld)
Certificates
- Dbld sigPublic Key
- A98 sigPublic Key
 (signed by Dbld)
Certificates

Key Loading
ATM   TH   A98 Re- Key
Request Key   or
Initiate Keying
Generate DES key Encrypt with EPP encPublic key Send to ATM
Decrypt new DES key Load into ATM Compute Response
Verify Response Encrypt DES key with host KEK
Send to host

Trusted Security Solutions
4110

According to Fagan, data encrypted with a public key can only be decrypted with its corresponding private key (and vice versa). Only public keys are exchanged in the clear, so the need for secrecy is greatly reduced.

This contrasts with the current private (or symmetric) cryptography used for ATMs, in which both the sender and receiver of a message use the same secret key to encrypt and decrypt, respectively. Because of the need to maintain secrecy at all times, secure key management is crucial — thus the ANSI standards and the move to Triple DES, which makes it more difficult for interlopers to decrypt a key.

Under the proposed standards for remote key, the emphasis shifts from maintaining secrecy to mutual authentication of sender and receiver, Fagan said.

"If (remote key) is not implemented properly, you may introduce a new security risk," she said. "You have to make sure the keys you receive belong to who you think they do. The whole crux of it becomes: does the public key I'm using really belong to who I think it does?"

According to Abraham, under the NCR, or Signature Based Protocol (SBP), method all trust is vested in the NCR root key. NCR installs a unique identifier and unique public encryption key signed by the NCR root key — along with corresponding digital signatures — in the ATM.

The host generates a private-public signature key pair and has the public key signed by the NCR root key. The ATM sends its NCR-signed unique identifier to the host, which verifies the signature to authenticate the ATM. The host sends its NCR-signed public signature key to the ATM, and the ATM verifies the signature. The ATM sends its signed public encryption key to the host. The host then generates a new Terminal Master Key (TMK), encrypts it using the public key of the ATM, signs it using its public signature key and sends it to the ATM. The ATM completes the keying process by verifying the signature and decrypting the new TMK using its private encryption key.

With the Diebold, or Certificate Based Protocol (CBP) method, trust is placed in a certificate authority and keys are stored and transported using digital certificates. Mutual authentication between the ATM and host is accomplished by the exchange of digital certificates. When an ATM comes online, it requests a new TMK by sending a message to the host. The host generates a new TMK, encrypts it using the public encryption key of the ATM, signs it using its Diebold signed signature key and sends it to the ATM. The ATM uses the Diebold root key to verify the host-applied signature on the TMK transport message, and decrypts the new TMK using its private key.

With the latter method, Fagan said, "It's important to ensure that you don't have a compromise at the certificate authority level."

Diebold product manager Ernest Chapman said the vendor plans to use Identrus, a third party digital identification authentication firm, to issue its certificates to minimize the possibility of a compromise. "We are very confident the process will be done correctly," he said.

Chapman, Shaffer and others say it would be simpler if the industry adopted only one method of remote key distribution. However, Sheets said, "Security standards are not necessarily interoperability standards. Many of the standards we write exist to establish the security requirements for a particular set of functionality."

> "GOING FROM DES TO TRIPLE DES IS LIKE ADDING MORE NUMBERS TO AN EXISTING COMBINATION. WITH REMOTE KEY, YOU'VE GOT TO CHANGE THE LOCK MECHANISM ITSELF."
>
> — DENNIS ABRAHAM, PRESIDENT, TRUSTED SECURITY SOLUTIONS AND A MEMBER OF THE X9.24 COMMITTEE
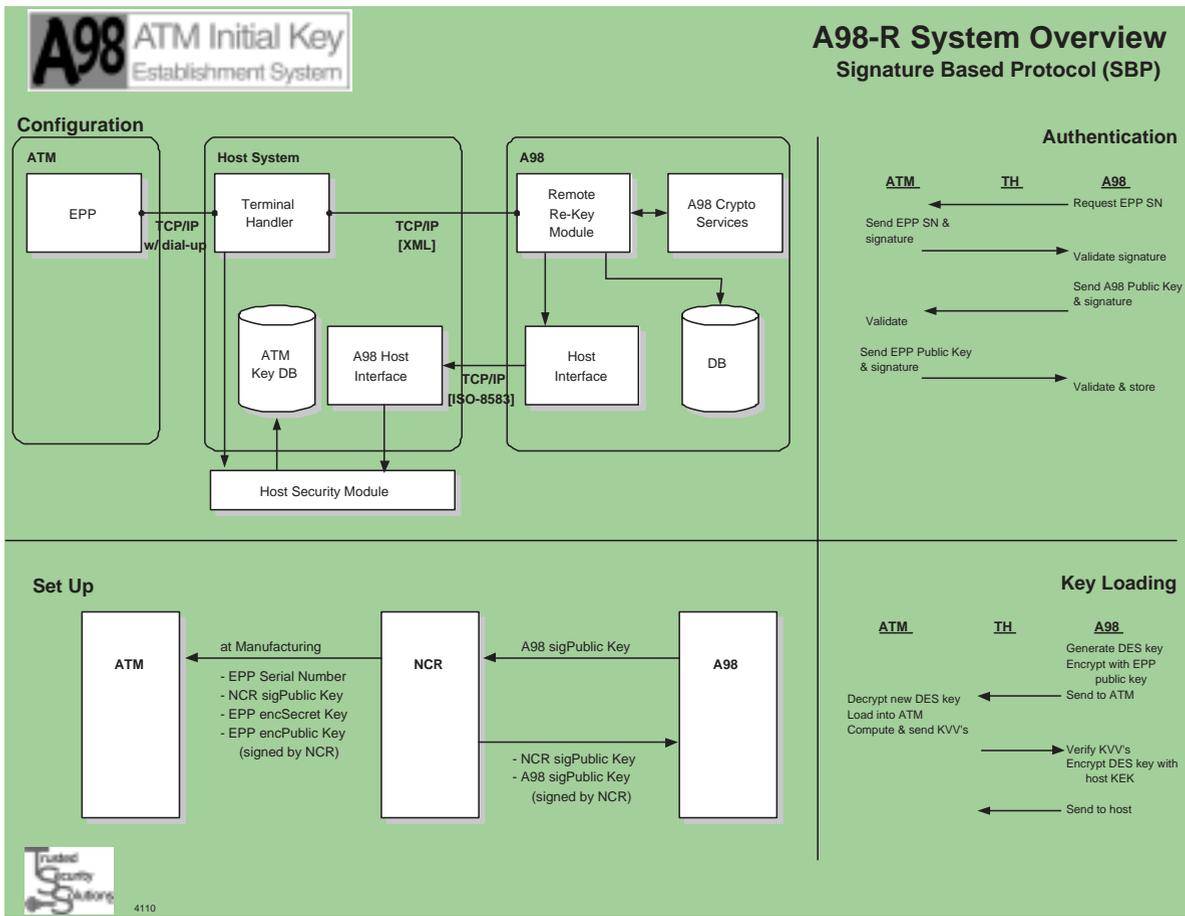
He added, "When there is no single preferred solution, it is usually best to support several to allow for as much innovation as possible. If we were to select a single method, then there wouldn't have been much opportunity for innovation by the various vendors. Of course having a single standardized method simplifies things, but over time it can stifle innovation."

Rush to remote key?

Trusted Security has added Remote Re-Key functionality that supports both vendors' methods to its A98 Initial Key Establishment System, Abraham said. However, he is not certain that ATM owners will rush to implement remote key even after it meets with ANSI approval.

Because public/private key cryptography introduces an entirely new algorithm — unlike Triple DES, which simply doubles the length of the existing DES key — it will require a more involved upgrade, Abraham said.

A98-R SYSTEM OVERVIEW SIGNATURE BASED PROTOCOL (SBP)

A98 ATM Initial Key Establishment System

A98-R System Overview
Signature Based Protocol (SBP)

Configuration

ATM: EPP

TCP/IP w/ dial-up

Host System: Terminal Handler

TCP/IP [XML]

A98: Remote Re-Key Module ↔ A98 Crypto Services

ATM Key DB — A98 Host Interface

TCP/IP [ISO-8583]

Host Interface — DB

Host Security Module

Authentication

ATM	TH	A98
		Request EPP SN
Send EPP SN & signature		
		Validate signature
		Send A98 Public Key & signature
Validate		
Send EPP Public Key & signature		
		Validate & store

Set Up

ATM

at Manufacturing
- EPP Serial Number
- NCR sigPublic Key
- EPP encSecret Key
- EPP encPublic Key
(signed by NCR)

NCR

A98 sigPublic Key

A98

- NCR sigPublic Key
- A98 sigPublic Key
(signed by NCR)

Trusted Security Solutions
4110

Key Loading

ATM	TH	A98
		Generate DES key Encrypt with EPP public key
		Send to ATM
Decrypt new DES key Load into ATM Compute & send KVV's		
		Verify KVV's Encrypt DES key with host KEK
		Send to host

"Going from DES to Triple DES is like adding more numbers to an existing combination. With remote key, you've got to change the lock mechanism itself," he said.

While Diebold and NCR machines have included EPPs with remote key support for nearly two years, most other manufacturers have not yet begun doing so. Hardware upgrades will be required for machines without support for remote key built into EPPs, Abraham said.

In addition, a hardware upgrade of the HSM may be required at the host end, and new software is required at both the host and the ATM.

Using Trusted Security's A98 method will remove some of the complexity, Abraham said. The A98 system's XML-based Remote Re-Key Module will exchange keys, signatures and certificates with the ATM's terminal handler or device driver via a TCP/IP link.

This approach confines modifications to the ATM device driver and eliminates any additional changes at the host, including the need to add public key capability to the HSM, Abraham said.

ATM owners with small networks, particularly those located at branches, may prefer to manage their own unique keys. "If you're a small shop and you don't have that many ATMs, the easiest and least expensive way may be for you to do it yourself," Fagan said.

Kargel agreed that those with only a few ATMs may prefer to manually load keys into machines, particularly if they drive their own terminals. "But if they're using a large processor and the processor can provide the technology, why wouldn't they want to do (remote key)?" she said.

Shaffer said that manual entry of keys is by its nature a more involved process than remote distribution, even for branch personnel. "If you're going to abide by the rules, you're still going to have to have a key custodian go to the HSM, generate a new key and securely transport it to the ATM. With remote key, you don't need a key custodian."

According to Abraham, his A98 system, used by clients including Navy Federal Credit Union, Compass Bank, M&T Bank, eFunds, Concord EFS and NYCE Corporation, simplifies the manual entry process. PIN mailer-type documents called Comvelopes are randomly distributed to field technicians. Each Comvelope contains random numbers and key check values that become key components only after they are loaded into the ATM and the key is established at the host.

Specific Comvelopes are not assigned to specific keys until technicians visit an ATM, randomly select them and the A98 establishes the key at the host. Until that time, the Comvelopes merely contain random numbers and are of no value to a bad guy.

It's also important for ATM owners to realize there are ways of re-keying machines other than those advocated by the major vendors, said Abraham, who holds a patent on a method called Persistent Key Component (PKC).

With PKC, Abraham explained, a key custodian loads the first component and the ATM holds it in secure tamper-resistant storage. Later, a single technician — rather than the two required for dual control — enters a second component that is combined with the first persistent component to form the unique key. Employing PKC will allow a single technician to compliantly re-key an ATM, Abraham said.

Each time the ATM needs to be re-keyed, only the second component needs to be entered. Most machines that need to be re-keyed also need to be repaired, Abraham said, which entails a visit from a technician who can enter the second component.

PKC technology was designed into the A98 system from the beginning, said Abraham, who urged ATM vendors to give it serious consideration as a cost effective and compliant alternative to remote keying using public key cryptography.

About Trusted Security Solutions Inc.

Abraham & Associates, Inc. of Concord, NC and J.S. Walker and Co., Inc. of Charlotte, NC created Trusted Security Solutions, Inc. in 1998 for the purpose of bringing unique security solutions to the transaction processing industry. Abraham & Associates specializes in consulting services for the financial transaction processing industry with an emphasis on PIN based transactions. J.S. Walker & Company specializes in providing consulting services and the development of custom software applications for financial institutions, insurance companies and related businesses. TSS is privately owned.

TSS markets directly and through several established resellers.
For more information, visit www.trustedsecurity.com or call 704-849-0036.