1st Annual ATM Key Management Report

The Current State of Remote Key Loading for ATM Networks

March 2008

Trusted
Security
Solutions

www.trustedsecurity.com

Table of Contents

Introduction

Financial institutions around the globe are constantly looking to streamline their ATM management processes. Though their challenges and specific needs vary, all must address seemingly daunting technical challenges in order to ensure security while still keeping a balance on operational costs.

After much anticipation, the practical use of public key cryptography in loading initial keys into ATMs has arrived. Trusted Security Solutions' 1st Annual ATM Key Management Report serves as a truly comprehensive look at the issues surrounding remote key. The report includes varied perspectives from industry users and technical experts from ATM manufacturers, banks, credit unions, processors and auditors.

1st Annual ATM Key Management Report:

The industry's first comprehensive look at the benefits and challenges of ATM remote key loading technology

Future editions of the TSS ATM Key Management Report will provide updates on remote key implementations while also addressing broader issues surrounding ATM key management – including strategy, costs, technology and regulations. All readers are encouraged to email comments and suggested topics for future reports to info@trustedsecurity.com.

Throughout the report, ATM administrators and others provided their personal perspective based on first-hand experiences surrounding remote key technology. All persons volunteered to participate in this report and in no way received incentives to do so from Trusted Security Solutions.

ATM Remote Key Loading: The Answer for Security & Efficiency

To deter ATM fraud and protect card user PINs, ATM owners have been required, among other things, to establish all encrypting keys in a compliant manner. In the simplest of terms, the primary security challenge of establishing the initial key in an ATM is keeping a secret a secret. If you know where to look, there is ample documentation with procedures on how to compliantly create, safeguard, transport and utilize key components to create the initial master key. Unfortunately, many ATM owners and service organizations find the implementation and maintenance of a key management process that is compliant with network mandated operating rules and industry standards difficult to achieve, resulting in gaps in the overall security of the payments infrastructure.

Remote key essentially eliminates the arduous nature of manual key loading and the associated compliance tracking. Asymmetric cryptography (public key cryptography), employed in remote key protocols, much like what is used to secure internet traffic on sensitive Web sites, replaces the manual methods of symmetric cryptography in the ATM world for establishment of the initial cryptographic key. The result is dramatically reduced cost and increased security.

Dennis (Abe) Abraham, President of Trusted Security Solutions, remarked, "Across the board, from banks and credit unions, to auditors and ATM manufacturers, industry leaders tell us it's clear that all stages of ATM deployment and maintenance benefit from the security enabled through ATM remote key technology."

So why hasn't remote key taken off more rapidly? If it is this good, why hasn't everyone taken advantage of remote key?

The reasons for relatively slow adoption are similar to reasons why the world has not completely converted from copper wire to fiber optics. There is much to do from point A (the ATM) to point B (the Host). Many contemporary ATMs are being sent to the field "remote key ready," but the vast majority of ATMs in the field require significant upgrades. And not only do ATMs need upgrading, but the same applies to network infrastructure, host software, and security modules. Cost is a major factor in remote key's slow growth.

THE EVOLUTION OF STANDARDS GOVERNANCE

ATM owners look to the Payment Networks for the operating rules they must implement and enforce. The Payment Networks look to the standards groups such as ANSI X9 committees and the Payment Card Industry Security Standards Council for security guidance and requirements.

At a minimum, owners of PIN entry devices and those who deploy them must submit to a bi-annual TG-3 Review by a certified TG-3 auditor. A copy of the most recent TG-3 Compliance Guideline can be downloaded from the X9 Financial Industry Standards Web site (www.x9.org). Additionally, the Payment Card Industry Security Standards Council and their member brands produce procedural requirements that participating members must follow. Examples of the requirement documents pertinent to ATM deployment are VISA's PCI PIN Security Requirements and MasterCard's' PCI Data Security Standard. These standards are monitored closely by issuers and acquirers alike. Periodic audits by these and other networks serve as effective enforcement for the written standards. Internal policies must be written – and it must be proven during an audit that procedures are followed that comply with the current written industry standards. As proof that the written procedures are followed, sufficient evidential material must exist in the form of key management logs, vault activity logs, courier records etc. It is the generation and maintenance of such logs that causes much of the non-compliance found during TG-3 reviews.

> “ATM manufacturers that do not have remote key capabilities today in their terminals now have serious motivation to secure a remote key protocol for their ATMs.”
>
> *Dennis (Abe) Abraham*
> *President*
> ***Trusted Security Solutions, Inc.***

REMOTE KEY MANDATE

Remote key has an inherent security advantage over all other manual or semi-manual methods for key management. With remote key, human beings are virtually removed from the key management process. Compromise of a key through collusion of two key custodians or field technicians is eliminated. Since no components are generated, stored, transported, distributed, loaded or destroyed, the steps that manual key management requires humans to perform, no humans are required – resulting in an immediate reduction in risk level as well as costs.

Acknowledging the increased security with the use of remote key, networks in certain countries are mandating the use of remote key for keying ATMs. Much like the days of the Triple DES upgrade, banks and processors not able to comply with the remote key mandate early on will likely have to justify why they are not able to implement remote key and make plans as soon as possible to implement the new technology.

A major financial network in the UK has requirements in place whereby all new ATMs being deployed after March 31, 2008 must use remote key. Deployment of remote key in all other ATMs has a deadline in 2009 to use remote key. “Due to the wide acceptance of remote key,” remarked Dennis (Abe) Abraham, “ATM manufacturers that do not have remote key capabilities today in their terminals now have serious motivation to secure a remote key protocol for their ATMs.”

ATM Manufacturer Perspective

Rupali Patel, Software Product Manager at Diebold, and Charlie Harrow, Product Manager for Cardholder Authentication at NCR, report their companies do expect to see a trend toward increased adoption of remote key loading for ATMs – despite initial hesitation by many organizations.

Patel said, “I think that the very early discussions by the card associations on what they would consider an approved method of DES key entry was a major factor in several banks’ decisions to initially hold off on implementing remote key transport. Now that PCI has produced some standards around remote key, I believe the implementation of remote key loading will start to pick up.”

> “Now that PCI has produced some standards around remote key, I believe the implementation of remote key loading will start to pick up.”
>
> *Rupali Patel*
> *Software Product Manager*
> ***Diebold***

Patel said that Diebold sees public key cryptography as a relatively new issue facing the ATM industry, and that the associated learning curve is one notable obstacle for firms looking at remote key. Specifically, Patel noted, “For new organizations implementing remote key support, most of the difficulty is centered on understanding what parameters need to be encrypted/signed.”

Security stands as remote key’s most valuable contribution in the eyes of manufactures, as it not only adds an unmatched level of protection and efficiency, but also allows companies such as Diebold to engage their customers and share their expertise in this and other areas. Patel said remote key loading is clearly more secure than traditional ATM key transport, as it involves fewer human beings and, therefore, fewer procedures exist as potential points of compromise.

“No part of the secret DES keys ever has to be seen by a human being in order to get them to a remote key enabled ATM,” Patel said. According to Patel, despite the relative newness of remote key transport, it has had a significant impact on Diebold, giving the company the opportunity to consult with customers and work closely with them to help further reduce their costs.

Currently, Diebold offers remote key technology on Diebold ATMs. The company does believe, however, that its industry standard approach is the best way to perform remote key regardless of the hardware involved. Patel noted that the different vendor implementations of remote key are sometimes challenging, and if one, unified and secure protocol was developed, it may ease some of the burden of implementation for financial institutions.

As one Midwest-based bank, which opted to remain anonymous, stated, “It’d be much better if even more manufacturers supported remote key for ATMs – as any technology that reduces trip costs will likely be adopted rapidly.”

Harrow adds that NCR has seen a steady migration of remote key implementation now that the wave of Triple DES adoption is largely complete – noting that organizations were less likely to embrace remote key and Triple DES at the same time. Harrow also indicated that once an organization begins to evaluate remote key technology, it's often the actual testing that raises best practices issues. He said, "Typically the test stages can sometimes trip people up, especially over when to use a Test EPP and when it's valid to test on a production EPP."

However, Harrow notes the overall benefits of remote key. "Yes, remote key technology largely removes the human element from the key loading process, which removes the main cause of bad practice and corner cutting that can occur with manual processes," he said. "Whenever you can eliminate hassle from a security process, often it can lead to an increase in security."

Harrow's personal experiences at NCR also unveil other significant issues organizations continue to face with key management. "They (our customers) are also looking at ANSI key block vs. AES," Harrow said. "Current methods of Triple DES key encryption with Triple DES have issues, and resolving them will take industry-wide migration. Organizations are asking themselves which is the most sensible option: invest money and resources on R&D surrounding AKB integration, or wait for AES?"

Note: Advanced Encryption Standard (AES) is a symmetric key algorithm that, unlike DEA that uses a fixed key length of 56 bits (112 bits for Triple DEA), uses a variable length key. The claim is that it permits the user to select the strength of protection desired for each class of asset being protected. It has been advanced by certain U.S. government bodies for use in the payments network, but has not been well received by some due in part to the huge financial investment the industry currently has in Triple DES equipment, and continues to make in Remote Key Transport equipment that supports Triple DEA devices.

Addressing other technical hurdles, Harrow said NCR developed an advanced version of remote key which locks the host public key to the EPP. He added the NCR innovation is being adopted as a solution to the 'rogue host' scenario, but without the management overhead of using CRLs (Certificate Revocation Lists). NCR calls this Enhanced RKM. The basic idea is that when the initial host establishes a trusted relationship with an EPP, the EPP will only accept key management messages from that host. Only that initial host can cause the EPP to unlock. It's a simple solution to what could have been a complex key management problem.

Note: CRL's are issued by the Trust Authority that issued the certificate to inform users of a particular public key that the certificate for that key has been deemed to be not longer trusted due to compromise or for some other non-specified reason.

At least two other ATM manufacturers, Wincor/Nixdorf and Triton are known to either have or will soon have remote key loading for their ATMs.

ELECTRONIC PIN PADS ARE CHANGING

The PIN Entry Device (PED) on ATMs must be certified by financial networks. Each ATM manufacturer must go through an expensive certification process whenever they introduce a new, or make changes to, an existing EPP design. Certifications also have an expiration date. The existing VISA PED certification that most current day PIN Entry Devices operate under expired December 31, 2007. Diebold and NCR have recently launched new EPPs that have been approved under inspection of the most current PCI EPP standards. This certification has an expiration date of March 2014. One of the central requirements in the new certification standards mandates that newer EPPs contain more sensors to make the EPP more secure.

Fortunately, the rollout of new EPPs allows for backward compatibility to the earlier versioned EPPs. Below is a list of some of the potential changes with the use of the new EPPs:

- Earlier versions of Diebold's EPPs allowed for a remote key load from a new acquiring host – as long as the signed certificates of the new host passed inspection when processed by the EPP during remote key authentication. For security reasons, Diebold has deemed that its new EPP5 will "lock on" to its initial acquiring host. If the ATM is moved to another host, a trip to the ATM is required to decommission or unlock the relationship of the previous host and allow for a new host trust relationship.

- NCR's newest EPP was launched in January 2008 as part of NCR's new SelfServ ATM family. "The new EPP was designed to meet the forthcoming PCI EPP 2.0 requirements, and it supports NCR Enhanced Remote Key Management as standard." In addition to a whole new ATM family, NCR also released a PCI compliant EPP for their existing product family. This EPP can also support Enhanced Remote Key Management with a firmware upgrade, which can be deployed in the field.

> "Organizations are asking themselves which is the most sensible option: invest money and resources on R&D surrounding AKB integration, or wait for AES?"
>
> *Charlie Harrow*
> *Product Manager for Cardholder Authentication*
> ***NCR***

User Perspectives

ONCE IMPLEMENTED, KEYING THE ENTIRE ATM FLEET CAN BE QUICK

As San Diego's largest locally owned financial institution with more than $4 billion dollars in assets, the San Diego County Credit Union (SDCCU) fully implemented remote key technology throughout 2004. Eric Stone, SDCCU's ATM Network Manager, is responsible for managing its ATMs that serve more than 190,000 members in three California counties. He reports that remote key loading was not only fast to deploy, but also significantly reduces expenses.

"Remote key technology has proven to be safe and reliable, and it performs well within our network," Stone said. "We used remote key to re-key practically all of our ATMs in two days. Sending keys is very fast and efficient. There's no need to schedule dual entities to manually enter keys. Policies and procedures are easier to follow and maintain."

SDCCU faces the challenge of minimizing ATM management costs while maximizing services for residents of the counties it directly serves. Stone said his operations continue to see dramatic cost savings by utilizing remote key technology.

"We do not have to pay for two people to go out to a new installation, or to an existing installation to install a new pin pad or DES keys into an ATM," Stone continued. "Furthermore, it's a time saver as well because of the time saved not having to document and destroy keys as they go through the key management lifecycle."

> "Processors have a mission to control costs. If you don't have to send two people to the ATM (by using remote key loading), it costs less, which ultimately saves the financial institution money."
>
> *Kevin Gregoire*
> *Executive VP, Product Development*
> ***FISERV***

INSTITUTIONS WITH LARGE ATM NETWORKS EMBRACE REMOTE KEY TECHNOLOGY

Mary Bland, director of information technology for FISERV, one of the world's largest service providers to banks, credit unions, lending institutions, and investment advisors, said remote key loading has been very popular and her company has seen a wide adoption rate among institutions with a high number of ATMs – as they see the most immediate reduction in cost and time.

FISERV also sees remote key loading as the clear answer to security and compliance requirements. Alongside ensured compliance comes convenience never before available for financial institutions. As Bland noted, “It eliminates the need to have clear key components, two servicers on site to load keys, and compliantly storing or destroying keys.”

Implementing remote key wherever possible is in the customer’s best interest. As Kevin Gregoire form FISERV said, “Processors have a mission to control costs. If you don’t have to send two people to the ATM (by using remote key loading), it costs less, which ultimately saves the financial institution money.”

Due to remote key’s greatly simplified, yet secure method of key transport, FISERV is looking at offering their clients the option of changing their Triple DES Terminal Master Keys (TMK’s) more frequently – further enhancing security. However, Bland reports that at this relatively early stage, her company has not yet set a timeline for offering automatic periodic TMK changes at the ATM.

John Sandridge, Vice President of Systems and Operations at Elan Financial Services, said he sees the lack of a directive to periodically change keys at certain intervals as another possible barrier to adoption. “There is no mandate from the major interchanges to change keys at the ATM on an annual, monthly, or other basis,” Sandridge said. “So, essentially, once the terminal is compliant there is no requirement to change the keys.”

Additionally, Sandridge said that since all device types and communication methods need to be supported for remote key to be implemented, a slower adoption rate may remain until full support is more readily available. “Remote key technology has been slow to adapt over the last several years, as there are still questions as to which devices (Diebold, NCR, Triton, etc.) do indeed support remote key in both the dedicated and dialup modes.”

REMOTE KEY: A BLESSING FOR GEOGRAPHICAL CHALLENGES

Jeff Rath of the Navy Federal Credit Union, one of the largest credit unions in the world with ATMs across the United States and throughout Navy bases worldwide, firmly states his organization’s support for remote key technology.

Rath told TSS, "Remote key management's main benefit is that it's much more secure -- people are out of the loop and that's its primary value.”

With security as one of a financial institution’s utmost responsibilities, Rath said that the absence of a manual process greatly enhances reliability and consistent compliance. “People aren't meant to handle encryption keys. Period,” Rath added. “Organizations want to use remote key."

Using remote key has advantages beyond security and efficiency. "Having the ability to offer remote key loading does have its financial rewards," said Toby Salsman, Vice President of Information Technology for Columbus Data Systems. "Recently we were able to pick up a sizeable piece of business due to the fact that we could offer remote key loading while others could not offer it. Having RKL allows you to more easily roll out a large number of ATMs – and that is an advantage for all of us."

> "Clients will be more comfortable adopting the technology when they truly have a better understanding of the technology itself."
>
> *Joseph O'Connor*
> *President*
> ***The Point Consulting Group***

When Salsman was asked why remote key loading has been slow to be adopted by ISO's, he said, "ISO's are more than willing to adopt a new technology that would help them save money and time. However, the ATM manufactures that the ISO's usually purchase from have not rolled out this functionality yet. The manufactures are currently in development and are working on a remote key solution, but it has not made it to market."

Auditor Perspective

TG-3 Reviews are required once every two years. Section 5 of the latest version of the TG-3 document deals entirely with the use of asymmetric cryptography, hence, remote key loading techniques. Careful reading of Section 5 finds that many of the questions are not pertinent to an ATM network owner, but rather apply to the Trust Authority where certificates and key pairs are signed, certificates issued, and transmitted to end users.

ATM manufacturers, along with the host security module supplier or host remote key software supplier, should be fully aware of Section 5 and be able to assist in answering the questions surrounding that particular section of the audit. Azie Amini, Sr. IT Data Security Consultant and Sr. IT/TG3 Auditor and Instructor, said, "The most challenging topic that concerns me is that TG3 audit requirements in Section 5 are very difficult for users to comply with. Banks or Credit Unions now must be proactive to determine how the ATM vendor has implemented this new remote key technology in advance of purchasing new ATMs."

Joseph O'Connor, President of The Pointe Consulting Group, offered his viewpoint as a respected industry auditor. "Cost, familiarity with the technology, as well as an organization's natural aversion to change, could be considered potential barriers to remote key adoption," he said. "But I also think some individual's may be averse to adopting RKT simply because it would eliminate some of their responsibility."

But nonetheless, O'Connor reiterates that remote key technology remains the next step in further securing ATM operations – with proper training being instrumental to a wider adoption of remote key throughout 2008 and beyond.

"By design, remote key technology is more secure than traditional key loading for initial keys," he said. "Assuming the remote key infrastructure is implemented in compliance with ANSI standards, it's certainly more secure because it eliminates the greatest area of risk with the Key Management Lifecycle – human involvement. In regards to actual implementation, education is the key. Clients will be more comfortable adopting the technology when they truly have a better understanding of the technology itself."

Additionally, education on the auditor side can be very important to the growth of remote key, as pointed out by Amini. "From an auditor's end, I believe there is a huge lack of understanding on how to perform sound and thorough audits of remote key loading operations covering all third parties involved; e.g. ATM vendor, HSM vendor, Certificate Authority operations, etc. – creating a need for proper training on our end as well."

Once training at both the auditor and user levels is completed, organizations will see an enormous benefit in efficiency, Amini said. "The benefit of remote key is saving the time and cost of sending two staff to various sites etc., but also keep in mind that the majority of previously required key management functions, policies and procedures will no longer be needed – another significant advantage."

With efficiency gained and a nearly automated system in place, replacing keys is recommended from an auditor perspective.

"Changing the initial key in ATMs is not mandatory, but it is a good practice," Amini said. "With new remote key loading technology, it is far easier and time efficient to remotely load new keys into ATMs. There are no standards mandating a lifetime for keys, but I would say as a matter of good practice it would be beneficial to change keys frequently."

Amini also noted, "There are concerns over key compromise and recovery process where keys are the public/private keys and need authentication in advance of real-time use. There are also concerns on how a list of revoked certificates (CRL) can be given to ATMs/HSMs so they would be aware of bad keys (i.e. compromised keys) in a timely and periodic manner."

PRACTICAL CONSIDERATIONS FOR IMPLEMENTING ATM REMOTE KEY

One of the most common oversights for banks or credit unions considering the use of remote key is not having one of two items:

- Either the FI does not have an adequate inventory of the hardware, firmware, and software construct of their fleet of ATMs; or

- The FI is unaware of what levels of hardware, firmware, and software is required at ATMs in order to be "remote key ready"

Those planning for remote key in the near future should conduct a detailed assessment of their ATMs and ask their ATM manufacturer exactly what it will take to make sure their ATMs are remote key capable. TSS maintains a short list of what it takes to become remote key ready for all ATMs currently known to support remote key loading. Visit www.trustedsecurity.com.

Remote key loading can be accomplished on any remote key capable ATM – whether or not it is connected to the host via TCP/IP or dial up. Generally, Dial up ATMs face more challenges in implementing remote key over IP connected ATMs. However, with a thorough understanding of the process and good planning, issues that may arise in a dial up environment can be minimized.

Keeping compliance at the forefront of all key management decisions, Sandridge concluded, "It's simply crucial to make sure all procedures at both ends (from the processor to the ATM) are fully compliant with all audits (CISP, PCI, etc.), keeping in mind that the storage of any data must comply with audit rules."

About Trusted Security Solutions

Trusted Security Solutions, Inc. (TSS) is a leading provider of secure financial transaction processing solutions for ATMs. For more than 10 years, TSS technology has led the industry in innovatively addressing ever-growing ATM security and compliance demands through its secure ATM key management solutions. Serving institutions that manage cryptographic keys for ATMs, Trusted Security Solutions' A98 ATM Initial Key Establishment System ensures compliance with ANSI, ISO, and network standards. A98's patented technology has established itself as the de facto industry standard for symmetric ATM key generation and distribution. TSS provides a module for remote key loading to accompany its patented automated symmetric key loading process so that all ATMs on a network are keyed in the most efficient and compliant means possible. TSS also provides outsourcing, consulting and training services to selected clients. Privately held, TSS is headquartered in Charlotte, North Carolina.

Trusted Security Solutions, Inc.
1500 Orchard Lake Drive
Charlotte, NC 28270
Tel: (704) 849-0036
info@trustedsecurity.com

www.trustedsecurity.com