WHITE PAPER

ATMmarketplace.com

Security Advantages of Remote Key Loading

By Richard Slawsky
Contributing writer

Changes in the way data encryption keys are loaded into ATMs can mean increased security for network operators.

The adoption of stricter standards for data encryption in recent years has meant that ensuring ATM security has become more complicated.

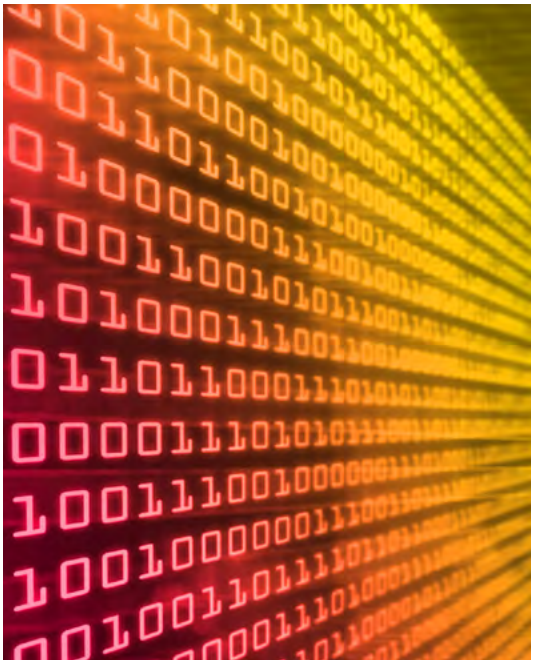
The latest Payment Card Industry Council Data Security Standards dictate that ATM deployers incorporate encrypting PIN pads and the more secure Triple Data Encryption Standard.

DES keys encrypt the information being sent back and forth between the ATM and the central processing center. Best practices had normally called for financial institutions or independent sales organizations to send two-person teams to the ATMs when keys must be loaded.

For the operator of a large network, though, that could be a costly and time-consuming process. Technicians might not get to a far-away ATM for days, depriving the operator of revenue and the customer of convenience, while leaving the ATM potentially vulnerable to tampering.

Manual key loading increases the potential for errors. In addition, the more human hands are involved in any process, the less secure it becomes.

Those factors are encouraging ATM manufacturers to start marketing remote key loading as part of their overall ATM offering. Remote key loading involves loading DES keys to ATMs from a central administrative site via a network connection rather than physically loading the keys at the ATM itself.



Without the benefit of remote key loading, changing encryption keys can be a costly and time-consuming process.

While financial institutions and ISOs have expressed interest in remote key loading, not many have adopted the solution, primarily because of the initial investment required.

Those who haven't adopted remote key loading may be missing out on several advantages, however. And the investment in a remote key loading solution may pay off in the long run by eliminating the need to have human hands involved in the process, reducing labor costs and enhancing security.

"The business case for ISOs is simple: less key handling," Chuck Hayes, product development manager for Long Beach, Miss.-based Triton Systems of Delaware, told ATMMarketplace.com. "That's an advantage. If an ATM key was corrupted, the host could rekey that ATM within minutes, rather than having to go through the manual process of sending someone out, which takes time and expense."

The process of RKL

Remote key loading can be handled in one of two ways: either through a signature-based protocol or a certificate-based protocol. Companies including NCR and Wincor Nixdorf International rely on the signature-based method. Diebold uses certificate-based protocol.

With signature-based protocol, the data structure is simple. It's a structure of information that has a digital signature attached to it, such as a public key.

With certificate-based protocol, the data structure is much more complex. The amount of data being transmitted is much larger, so it's not easily transported over dial-up networks. And the certificates themselves contain much more information.

Key information is transmitted online using secure cryptographic methods.

"Because of that complexity, implementation for Diebold CBP (certificate-based protocol) would not work on a Triton CBP," said Dennis Abraham, president of Concord, N.C.-based Trusted Security Solutions Inc. "They each have differences; so consequently, we end up implementing different protocols."

Trusted Security Solutions is the developer of the A98 remote key loading system. Some manufacturers, like Triton, are working with third parties like Trusted Security.

Others, such as BBS Denmark, have developed their own key loading solutions. Copenhagen, Denmark-based BBS Denmark, formerly Sagem Denmark, launched its Remote Key Load solution in 2008.

Basic requirements for BBS Denmark's solution include: The ATM's EPP and the

host's HSM must all support RKL. The host must have a host key pair and a suitable certificate on the public key, and the EPP must have two key pairs with corresponding certificates.

"As long as a system meets some basic requirements, installing the first Triple DES master key is a matter of connecting the ATM to the host via regular channels and running the Remote Key Load protocol," said Michael Larsen, product manager with BBS Denmark. "The installation takes place in about 10 seconds — without the need for human involvement."

RKL adoption is definitely picking up, Abraham says, both from the FI and the ISO side of the business.

"In today's economy, the price of labor is going up and the number of people is diminishing," Abraham said. "Everybody is looking for more efficient ways of doing things."

Eliminating the human factor

Remote key loading offers a number of security advantages for financial institutions and independent sales organizations.

Though complicated by complex algorithms and multiple levels of encryption, the function of remote key loading is simple. The bottom line is that remote key loading eliminates the need for ATM technicians to physically visit ATMs for manual key changes — thus eliminating expense and the possibility for human error.

"All information is safely transmitted online using secure cryptographic methods, which leads to a cost reduction because of the practical issues where two persons had to go to the ATM," said Torben Elgaard, product manager with BBS Denmark. "Anyone can see how that can be a costly procedure."

Remote key loading eliminates the need for ATM technicians to physically visit ATMs for manual key changes — thus eliminating expense and the possibility for human error.

Elgaard presented the benefits of remote key loading in an ATMMarketplace.com webinar titled "Remote key loading for ATMs: Enhancing security, unlocking efficiency."

Beyond cutting costs and simplifying key management, RKL incorporates several security features such as mutual authentication, meaning the host and the EPP can verify each other in a single operation. Other advantages include protection from inadvertently reinstalling old key values, an encrypted transport of the master key and a cryptographically signed message after a successful key transfer.

"The key management becomes more cost effective, more secure, more efficient and more simple," Elgaard said. "In other words, more intelligent."

About the sponsor: *BBS Denmark is one of the world's leading providers of high-security payment solutions. The company specializes in encrypting pin pads for ATMs and kiosks, unattended payment solutions for self-service applications and EMV compliant POS terminals.*