WHITE PAPER

Understanding Remote Key Loading

RKL is inevitable for ATMs, so understanding the basics can help ATM operators improve efficiency and enhance security.

By Gary Wollenhaupt
Contributing writer,
ATMmarketplace.com

By using remote key loading (RKL), ATM operators have the opportunity to improve operating efficiency while at the same time enhancing security. In some locations around the world, RKL already is a standard; in others, it's coming.

Simply put, RKL is the process of distributing the terminal master key from a central administration point to the EPP (Encrypted PIN Pad) or PED (PIN Entry Device). The code keys encrypt the information being sent back and forth between the ATM and the central processing center.

Prior to the introduction of remote key loading, typical practice called for financial institutions or independent sales organizations to send two-person teams to each ATM when a new key was loaded. Manual key loading increases the potential for errors and fraud.

For the operator of a large network, this was a costly and time-consuming process. ATM operations were at the mercy of service technicians' schedule, depriving the deployer of revenue, the customer of convenience and leaving the ATM potentially vulnerable to tampering.

Remote key loading is the process of distributing the terminal master key from a central administration point to the EPP (Encrypted PIN Pad) or PED (PIN Entry Device).

In recent years, many ATM manufacturers have offered RKL capability. But the owner of an existing fleet may have to deal with machines from a wide range of manufacturers and even varying vintages from the same manufacturer. Financial institutions that have undergone mergers and acquisitions face the challenge of efficiently managing fleets not of their choosing.

Global opportunity

Remote key loading has spread across the globe as individual countries adopt unique security schemes. For instance, financial transaction networks in the United Kingdom require ATMs to change cryptographic keys on an annual basis, making RKL technology a cost-effective solution. Payment card standards in many countries, Australia and Germany among them, allow for RKL.

In response to compliance standards set by the "Superintendencia de Bancos de

Venezuela" (SUDEBANK), Banco Guayana installed the A98 ATM Remote Key System from Trusted Security Solutions Inc.

"With the SUDEBANK's directive to increase security standards in placing encrypting keys in ATMs, we wanted to implement not only a compliant solution, but one that was the most advanced and secure available today," said Bernardo Kabche, executive president of Banco Guayana. "The A98 Remote Key System met these requirements, and we are pleased that it is now installed and operational."

As the concept has spread, differing technologies have developed, making it difficult to adapt the solutions to other countries. A more global approach, based on the card brand and ANSI standards, will drive more widespread adoption.

Fortunately, RKL capability resides in the encrypted PIN pad and the network's host security module. That means ATM deployers may have more options than they thought to implement the enhanced security and lower costs from RKL.

For instance, off-premise ATM leader Triton deployed RKL in the United Kingdom, and will roll it out in other locations, including Canada, the United States, Australia and South Africa.

Essentially, most RKL solutions are platform independent. The capability for RKL is embedded within the encrypting PIN pad and the host, not with the ATM.

Differing protocols

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

Nenyedi

Most RKL solutions are platform independent, because the capability for RKL is embedded within the encrypting PIN pad and the host, not with the ATM.

The signature-based protocol has a digital signature attached to it, such as a public key. With public-key encryption, a code key is used to encrypt the digital key, which is sent to the ATM's encrypted PIN pad. A suitably equipped PIN pad contains a secret key that decodes the encrypted information, and uses security checks to block fraud attempts.

The certificate-based protocol has a much more complex data structure. The certificates contain more information than the signature-based protocol, so the amount of data being transmitted is much larger, making this solution difficult to use via dial-up connections.

Various solutions are on the market to implement the different protocols. Glostrup, Denmark-based Cryptera, a manufacturer of

encrypted PIN pads, launched its Remote Key Load solution in 2008.

Cryptera's solution employs an RSA signature-based protocol that uses an encryption algorithm to safeguard the information. At each end of the communication, the software decodes the message, and checks the signature to verify that the message is authentic.

System needs

Because an ATM's capability for RKL is embedded in the encrypting PIN pad, the decision to replace or upgrade a fleet to RKL depends on the age of the machines. With software upgrades, some EPPs may be RKL capable. If not, then an upgrade to an RKL-capable PIN pad may be necessary. In the case of much older machines, replacement of the entire unit ultimately may be required.

"The EPP has to be modern enough to handle the RKL process, because you have to have key handling and key generation within the EPP," said Torben Ellgaard, product manager for Cryptera.

The RKL-capable EPPs can be used in a standard or manual mode until the system is ready to support the RKL protocols. The host security module and host software must be RKL-capable as well. An ATM owner can begin implementing RKL capability with replacement EPPs, and when the host security module is capable, the system can transition to using RKL.

"An ATM owner could have several brands in a network and they could provide some kind of subset they could control using the manufacturer's RKL system," Ellgaard said.

Understanding the different protocols

- **Signature-based:** Has a digital signature, such as a public key. The data structure is simpler, involving a code key that encrypts the digital key, and then the digital key is sent to an encrypted PIN pad. The PIN pad decodes the encrypted key, and uses security checks to block fraud attempts.
- **Certificate-based:** Certificates are transmitted, rather than keys. Because the certificates contain more information than the signature-based protocol, more data is sent at a given time, making it difficult to use with a dial-up network.

RKL has been implemented in a variety of the most popular ATMs used in off-premisesinstallations, such as Nautilaus Hyosung, Triton and Tranax. The EPP hardware has to be able to support the software for RKL. If the hardware is capable, the upgrade path is a simple one. It can be as easy as installing new software.

To ensure security for upgrading EPPs, Cryptera generates the initial encryption key while the EPP is inside its secure production facility. That way, the EPP is prepared for remote key loading in a secure environment.

Cryptera's method of preparing its RKL-capable EPPs while they're still secure gives the ATM owner flexibility for the future. Deployers can decide whether to continue to use the traditional manual key loading method, preparing the host system and only then switching into full RKL usage.

About the sponsor: *Cryptera 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.*