WHITE PAPER

Remote Key Loading Revitalizes Legacy Terminals

To secure a legacy ATM portfolio, it's important to consider hardware, software and connectivity requirements, as well as scalability.

By Gary Wollenhaupt
Contributing writer,
ATMmarketplace.com

For years, ATM owners have relied on expensive and risky manual installation of encryption keys. The traditional method relies on two technicians, each carrying a portion of the secret code, to enter the code into each and every machine in a portfolio.

Susceptibility to fraud and error are two of the drawbacks to this method, not to mention the cost. Of course, regulatory mandates for remote key loading (RKL) are on the horizon as well. Version 1.2 of the Payment Card Industry Council Data Security Standard requires keys to be changed every 12 months. Updating keys manually every year could turn into an expensive, time-consuming proposition.

Remote key loading allows a deployer to use an encrypted PIN pad and digital keys to update keys without investing a lot of time or money in the process.

The industry has responded with RKL, the future of ATM security. This method uses public-key encryption to upload encryption keys without the intervention of technicians. 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.

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.

Fortunately, RKL capability resides in the encrypted PIN pad and the network's host security module. That means

ATM owners may have more options than they thought to implement the enhanced security and lower costs from RKL. This paper will answer some basic questions about upgrading an existing ATM fleet to incorporate RKL capability.

Hardware and software requirements

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

"The ATM is just a transport layer between the host and the encrypted PIN pad," said Michael Larsen, product manager for Cryptera, a Glostrup, Denmark-based manufacturer of encrypted PIN pads.

The host and the encrypted PIN pad each use an RSA 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.

An ATM's capability for RKL is embedded in the encrypting PIN pad, so for an ATM owner the decision to replace or upgrade a fleet to being RKL capable depends on the age of the machine. 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. "It's a matter of the generation and version of the EPP in the ATM."

An ATM's capability for RKL is embedded in the encrypting PIN pad, so for an ATM owner the decision to replace or upgrade a fleet to RKL depends on the age of the machine.

Flexible upgrade path

Implementing RKL in an ATM fleet does not require an all-or-nothing approach. Cryptera's Ellgaard said that RKL-capable ATMs can be mixed in a network with non-capable units.

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.

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's a matter of changing the software to achieve it," Ellgaard said.

RKL has been implemented in a variety of the most popular ATMs used in off-premise installations, such as Nautilaus Hyosung, Triton and Tranax.

To ensure security for upgrading EPPs, Cryptera will generate the initial encryption key while the EPP is inside its secure

production facility. That way, the EPP is prepared for RKL 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.

"The customer can decide whether to use the traditional manual key loading method, prepare the host system and only then switch into full remote-key loading usage," Larsen said.

If an EPP is installed without the initial encryption key loading, that process has to be performed in the field, leaving the EPP open to fraud, most likely a man-in-the-middle attack.

"It puts some constraints on the upgrading of EPPs in the field if they are not already prepared for RKL," Ellgaard said.

Connectivity requirements

Fortunately for operators of off-premise ATM networks, RKL capability does not rely on a particular type of network connectivity. The typical bandwidth requirements are accommodated by standard dial-up connection. Of course, TCP/IP connectivity easily handles the communication between the EPP and the host.

"There is no notion of the transport mechanism that is used to convey the message," Ellgaard said.

The EPP uses whatever form of connectivity is built into the ATM to communicate with the host security module or the switch. There is no need for a secondary communications channel solely for RKL communications.

Implementing RKL

When implementing RKL, a deployer has choices. He can:

- Use RKL-capable EPPs in a standard or manual mode until the system is ready to support RKL protocols.
- Implement RKL capability with replacement EPPs, until the entire fleet is RKL ready.
- Overhaul the entire fleet at one time.

The ATM can use the main channel between the host and the ATM. The RKL message is basically the same as transporting the PIN transaction from the ATM to the host.

"The physical design and security measures in the EPP to protect the encryption keys are the same regardless of the method used to transport the keys," Ellgaard said. "It is solely a matter of the software in the EPP that makes it possible to pass information between the host and the ATM to change the keys."

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.*