



Decoding the Encryption Enigma

With no clear standard and shifting technology, ISOs weigh their options

By Richard H. Gamble

As the industry tries to stay ahead of clever thieves with tactical fixes and a safer infrastructure, some companies are turning to end-to-end encryption to safeguard data. But the solution is not only highly complicated and expensive, it also forces ISOs to decide how to deliver to merchants without compromising the all-important encryption keys.

“We’re in the very early days of end-to-end encryption,” notes Doug Klotnia, general manager of the compliance division for Chicago-based Trustwave, a data security and compliance provider. “There are many challenges due to all the platforms and organizations that need to touch a transaction from one end to the other.” It will take a comprehensive methodology to make it happen, he indicates. So far, end-to-end encryption has occurred largely in proprietary environments, implemented and controlled by one organization.

Even for just the merchant-to-processor leg of the journey, security is not uniformly robust, Klotnia points out. Although triple data encryption standard (TDES) has become the benchmark, it is not required between merchants and processors and isn’t widely used. PCI DSS does require encryption, but not all small merchants (Level 4) are PCI DSS compliant. “Encryption doesn’t guarantee security, especially if the keys are not securely maintained, but if done correctly, it’s a valuable security tool,” he adds.

Beyond PCI

TDES has already been compromised in the laboratory, reports Steve Elefant, chief information officer at Heartland Payment Systems in Princeton, New Jersey. Data security issues have pushed Heartland to the edge of encryption technology. Its trademarked E3 solution is in production with dozens of merchants carrying thousands of transactions a month, and Heartland plans a general roll-out this year.



In E3, the swipe of the mag stripe puts the sensitive data directly into a tamper-resistant security module that is part of a terminal that Heartland is manufacturing in house so that it meets its tough security standards. That module completely encrypts Tracks 1 and 2 (including the card number) and only passes the first six and last four digits to the terminal application, leaving the digits needed for routing and reporting accessible, Elefant explains. The encrypted information is pushed from the POS equipment to Heartland for processing, and it goes from Heartland to the brands securely. Further, the company and the card brands have worked out a solution that allows the brands to accept and process these transactions without needing special equipment.

The standard favored by government intelligence agencies, however, is advanced encryption security (AES), which is more complex, harder-to-break encryption coding than TDES. The special Heartland front-end hardware solutions have public encryption keys inserted during

manufacturing, and strong cryptography in the hardware allows other crypto keys to be generated at least daily, Elefant explains. All terminal applications have to be signed and certified before they can be installed, he adds.

Early implementations of encryption that goes beyond PIN debits and PCI compliance have begun, reports Chuck Fillinger, a consultant based in Boca Raton, Florida, and an associate of The Strawhecker Group. Heartland is encrypting transmitted data between the point of sale and the host; RBSWorldPay has announced a partnership with Verifone for its VeriShield Protect solution; and First Data just announced a deal with RSA that provides encryption from the merchants’ POS to the First Data host and then creates a token, he notes.

Some solutions currently on the market allow a large merchant to encrypt cardholder data traveling between the POS device and the merchant’s host, where transaction data for that merchant would be aggregated, Fillinger explains. In the online world, where cards are not present, tokenization has been used to replace and securely store the personal account number (PAN) in a form that makes it hard to steal the important cardholder data, he adds.

Encryption, even with tokenization, is no silver bullet that can eliminate the need for PCI compliance, notes Brad Caldwell, CEO of SecurityMetrics in Orem, Utah. The two most common forms of security compromise—the insertion of malware and SQL injections—won’t be prevented by encryption, he points out. “Encryption is exciting technology that can strengthen data security, but it won’t really prevent the majority of compromises.”

But it can streamline PCI compliance. Knowing what kind of encrypting hardware is in place allows fields in the merchants’ self-assessment to be pre-populated automatically, speeding up the self-assessment process, Caldwell says.

PCI COMPLIANCE? NO PROBLEM.



Simplify PCI

Wondering how to help your merchants become PCI compliant and keep them happy? SecurityMetrics can help. As a leader in PCI-DSS we handle more than 100,000 merchant PCI calls every month. Our Simple approach works.

Call today to receive a free PCI consultation for your business. 801-724-9600

www.securitymetrics.com

securityMETRICS®

Securing the Pathway

Once the technology is settled, the huge challenge will be updating the myriad merchant locations with the chosen encryption standard, which requires the right software to be embedded or injected into the right hardware.

Encryption and decryption are performed by software, so the cardholder data comes off the mag stripe unencrypted and needs a secure pathway to the encryption application, Fillinger explains. If the software is in the terminal or POS system, the path is short. If the transaction must travel to encryption software in a merchant's host system, vulnerability could be greater.

Placing encryption software in terminals and POS systems can happen in two ways, Fillinger explains: It can be physically injected, one terminal or system at a time; or it can be remotely injected, telecommunicated to many terminals from one remote site in one secure process. Obviously, a single process from a single remote location that could fix many terminals would be easier, cheaper, and probably safer, but significant obstacles remain.

One business opportunity for ISOs is to swap out hardware that doesn't encrypt for hardware that does, earning additional revenue in the process. ISOs should go to all their processors and find out where each stands on end-to-end encryption. They also need to learn about the latest terminals and the kinds of encryption they provide, he advises.

Major Challenge

The lack of consensus about the path to end-to-end encryption is wreaking havoc with some solution providers. A host of vendors were working on ways to safely provide remote key injection (RKI) when MasterCard threw a wrench into the works in July, notes consultant Bob Hughes, senior vice president at Speer & Associates.

If vendors can't use RKI, the TDES encryption will have to be done physically, terminal by terminal. ISOs will have to either send service reps into each merchant site with a black box containing the keys and inject the software into the hardware on site; send a rep to pick up

the hardware and take it to a secure site for the encryption software injection; or assign a rep to bring encrypted hardware to the merchant site and swap it for the noncompliant hardware. All are cumbersome processes that entail real risk, Hughes says.

"A few companies like Semtek and MagTek were building systems for remote management of encryption keys," Hughes says. "It would make life easier for ISOs and terminal providers if keys could be pushed out to merchant hardware through a network from a secure remote location," he says. With the deadline for compliance with TDES coming in less than a year, the prospect of losing RKI options is causing frustration and uncertainty, he explains.

"This is pretty late in the game to be learning that your plans will have to change," he says.

To handle installation of security software, typically a large ISO will have an office site and a person responsible for getting new devices ready, Hughes explains. That person would inject the encryption keys into the hardware at that secure site—if the manufacturer has not already embedded them—and then a sales or customer service person might carry the loaded device out to the merchant site and simply plug it in. But when merchants won't agree to buy new terminals, and when they can't afford to have their terminals down for a while, the keys might have to be injected right at the merchant site, he notes.

No Job for Small ISOs

The manner in which PIN debit transactions currently are encrypted will probably serve as a rough prototype for cardholder data encryption, says Greg Cohen, president of Moneris Solutions in Chicago.

"When end-to-end encryption becomes a reality in the U.S.—if it does—it will follow the pattern we've seen with PIN debits. The processors, mega-ISOs, and bank acquirers will maintain the encryption procedures, and the smaller ISOs and processors will leverage the work of the large players."

The critical security pieces are the keys that convert in-the-clear data into elaborately coded data and then decode

it as needed for processing. The experts agree that key management is not something small ISOs should attempt. The encryption key should be built into the terminal, so the merchant or ISO would not have access to it or responsibility for its security, Klotnia explains.

Actually handling and installing encryption keys isn't for small ISOs either, Fillinger agrees. A super ISO that does its own processing could be involved in key management, but smaller ISOs are well advised to find a competent processor and leave the key management up to the processor, he suggests. "ISOs should stay out of key management altogether," he insists. "It just opens them up to a lot of problems." Instead, small ISOs should review the hardware being used by their merchants to determine which ones can provide encryption and which cannot, and then start to systematically upgrade merchants to hardware that can encrypt, he advises.

"Transactional latency" also is an issue, says consultant Paul Martaus, president of Martaus & Associates in Mountain Home, Arkansas. Latency is the time it takes to apply the encryption, send the transaction to the authorization site, decrypt the transaction into plain text, process it, re-encrypt it, and send it back. Some vendors are offering solutions that take as long as one minute; others have got it down to three milliseconds. Obviously, the longer the merchant's point of sale is tied up waiting for authorization, and the longer the shopper has to wait, the greater the burden imposed by encryption, he explains.

While the solution is ultimately likely to come from hardware vendors, "there is no standard yet," Martaus concludes. The terminal or POS system vendor that can build the chosen standard encryption applications directly into the terminal or system so that the merchant and the ISO don't have to deal with encryption keys and routines will score big, he predicts. That will make it simple plug-and-play for the merchant and ISO, he notes. **TT**

Richard H. Gamble is a contributing writer for Transaction Trends. Reach him at gamble10@earthblink.net.

*If you want to grow **BIGGER** and **SMARTER**, stay **WELL** **CONNECTED***

Make the most of your **ETA membership!** Get connected to the people, issues, education, information, and resources that can help take your organization and your career to the next level.



Publications & Resources

- *Transaction Trends Magazine*
- *ETA Currents E-Newsletter*
- US Economic Indicators Report
- Industry White Papers

Advocacy & Issues

ETA monitors every piece of legislation that could impact the payments industry in a positive or negative way. We advocate for our members and promote the value of the payments industry to Washington officials.

Education

ETA's educational programming, ETA University (ETAU), provides crucial payments education in a variety of delivery formats, all designed to increase your skills and competencies. Attend live, instructor-led classes, bring our classes to your location, or learn 24/7 in a self-paced, online format.

Signature Events

Find the perfect supplier or partner.

ETA Annual Meeting & Expo

April 13-15, 2010, Las Vegas, Mandalay Bay Hotel

Strategic Leadership Forum

October 27-29, 2010, Palm Beach, The Breakers

Follow us on: 


ETA 20

celebrating 20 years 1990-2010

www.electran.org