



PCI COMPLIANCE AND THE HOSPITALITY INDUSTRY

EVALUATING P2PE IN THE WORLD OF HOSPITALITY PAYMENTS

By Christian McMahon

Point-to-point encryption and tokenization are still evolving, so understand how to identify the technology with the right fit by understanding all your business processes, asking the right questions, choosing trusted partners and keeping yourself updated.

As every business owner now knows, credit card security is an ongoing struggle and PCI Compliance is only the starting point for data theft prevention strategies. Just like in an arms race, merchants as well as the rest of the players in the payments industry are trying to keep up with the hackers and thieves. Point-to-point encryption (P2PE) and tokenization solutions are responses to the escalating and evolving threats in the payment security landscape. As a merchant you need to understand how these technologies will affect your cardholder data environment and fit into your overall risk management and compliance strategy.

Though P2PE technology has been around for years, it is still early in its genesis in the hospitality payments world. What makes P2PE in our industry so complex are the numerous points where payment card data can enter the merchant environment, the unique lifespan of the payment cards and the number of interfacing systems that make up the merchant environment. For example, a hotel merchant may have front desk terminals, call center reservationists, back office accounting systems, multiple point-of-sale systems and retail/booking web sites. Each of these systems may have different methods of capturing, transmitting and storing payment card data. P2PE solutions will have to be flexible enough to support each point of entry and business process and will no doubt encompass both hardware and software components. (See the *Point-of-Entry diagram on page 33*).

Multiple Points of Destination

Not only are there multiple points of entry to consider, there are also multiple end points, or points of destination. The term “end-to-end encryption” or E2EE is often confused with point-to-point encryption. E2EE often is thought of on a grand scale and defined as encryption between the local entry point and the merchant’s bank. In reality though, there is no vendor today that covers this entire path. P2PE can be described as encryption from a beginning point to an end point that is connected securely to the back end banking networks. These end points can be interfaced with gateways, processing agents, banks or even the card associations. Because P2PE more accurately describes the solutions in the marketplace today, it has become the standard way of describing encryption services and is the term advocated and used by the PCI Council.

P2PE technologies work to protect and secure payment card data as it is being transmitted through and from the merchant environment. This is commonly referred to as “data in motion.” P2PE places this data in a wrapper

In This Issue:

- Introduction
- Myths and Rumors
- **Point-to-Point Encryption**

Christian McMahon is product manager for lodging and security solutions at Merchant Link, LLC in Silver Spring, Md. and a member of the PCI Compliance Task Force. He can be reached at Christian.McMahon@merchantlink.com.

Reprinted with permission from the October/November 2011, Volume 26 Number 6 issue of *The Bottomline*, the journal of Hospitality Financial and Technology Professionals. Learn more at www.hftp.org.



that can only be decrypted by an endpoint that has the requisite key. The merchant should never possess or have access to the cryptographic keys or a decryption function that would allow encrypted data to be decrypted. This was pointed out in the “Initial Roadmap: Point-to-Point Encryption Technology and PCI DSS Compliance” document issued by the PCI Council in October 2010.

The goal of P2PE technologies is to encrypt as close to the point of entry as possible and guard against thieves who attempt to install sniffing/hacking software on a merchant’s network. For example, in an online transaction, where a software-based P2PE solution is typical, the encryption should occur from the point the payment data is manually entered or received from a third party system. If the payment card data is entered from a call center or a card swipe, a hardware-based solution is typically employed. The encryption should occur as close to or within the device as possible. The encrypted payment data is transmitted to a third party vendor who hosts the decrypting mechanism, otherwise known as the host security module (HSM). At that point, the data goes out to the banking networks for authorization and payment.

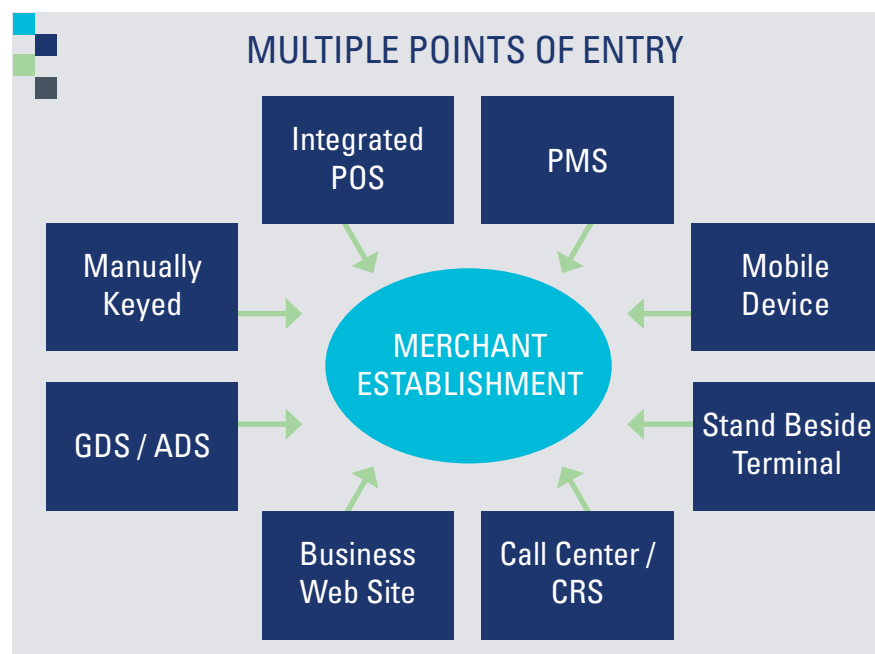
P2PE VS. Tokenization

When evaluating the implementation of a point-to-point encryption solution, merchants need to think about whether encryption alone is sufficient, not only from a security standpoint, but also from a practical standpoint — especially in a hospitality environment.

If P2PE protects data in motion, tokenization is its counterpart and protects data at rest by completely replacing the payment card numbers with tokens that are meaningless if stolen. Tokenization has been defined by VISA as “a process through which Primary Account Number (PAN) data is replaced with a surrogate value known as a “token.” The security of an individual token relies on properties of uniqueness and the infeasibility to determine the original PAN knowing only the surrogate value. As a reference or surrogate value for the original PAN, a token can be used freely by systems and applications.”¹ Layering P2PE and tokenization technologies can appreciably increase overall security while significantly reducing PCI scope.

Determining Your Needs

The PCI Security Standards Council has repeatedly acknowledged the ability of these two emerging technologies to protect cardholder data and reduce PCI





burden and recently released guidelines on both tokenization and point-to-point encryption. Not surprisingly, P2PE vendors are offering a wide array of solutions until standards are agreed upon. Solution types include both hardware and software-based solutions, and are being offered by POS/PMS vendors, payment gateways, bank processors and even acquiring banks. A small, independent retail merchant that has limited credit card entry points may have their needs met by a simple, bank-issued, stand-alone encrypting terminal; whereas, a restaurant with both an online ordering site and POS hardware on-site may require one or more solutions. Examining your own environment and creating detailed use cases that outline data flow from initial capture to final payment can arm you with a better understanding of what you need so you can make an informed choice.

Finding a Solution

Shopping for a solution can be intimidating, and there is much to consider. The first step a merchant should take after examining the data flow in their own environment is to educate themselves on the various methods and technologies that are available. A good place to begin is by reading “Initial Roadmap: Point-to-Point Encryption Technology and PCI DSS Compliance v 1.0” published by the PCI Security Standards Council in October 2010¹. It describes in detail what to look for in a P2PE system.

As a second step, merchants should ask their POS/PMS vendor if they are working with any companies to provide P2PE and tokenization and if those solutions are integrated or non-integrated into their POS or PMS system. Integrated solutions may require extra steps at set-up and installation, but offer greater functionality; whereas non-integrated solutions may be easier to install, but restrict choice and ease-of-use. Yet another factor to consider is device

Examining your own environment and creating detailed use cases that outline data flow from initial capture to final payment can arm you with a better understanding of what you need so you can make an informed choice.



functionality, i.e. whether or not the device encompasses swiped cards, manually entered cards, etc. and whether or not the device is tamper resistant, all of which impacts the ultimate price tag.

When evaluating vendor P2PE solutions, ask probing questions such as:

- Is the P2PE solution a hardware or software solution or both?
- Is the vendor well established in the payments industry?
- Does the solution encrypt both swiped cards and manually entered cards?
- Does the solution encrypt online transactions, as well as on-site or card-present transactions?
- Has the vendor solution been evaluated by a trusted Qualified Security Assessor (QSA)?
- Is the P2PE solution integrated with the property management or point-of-sale system or is the encrypting device standalone?
- What happens if the encrypting device fails? What is the fall back scenario?
- Where is the HSM located in the solution? Where is the data decrypted exactly?
- Does the P2PE solution integrate with a tokenization system?
- Can the solution function effectively without tokenization?
- How does the encrypting device handle non-payment cards such as employee cards, gift cards and airline/membership cards?
- How does the vendor secure communication between their network and the merchant’s systems?
- Is the solution tamper resistant? What happens if an attempted breach occurs?
- Does the solution support format-preserving encryption?
(Format-preserving encryption refers to encrypting in such a way that the output is in the same format as the input, i.e. encrypting a 16-digit credit card number that outputs another 16-digit number. This method will more easily fit with into existing reporting, receipts, and databases.)

In the end, the purpose of both point-to-point encryption and tokenization is security, not PCI compliance. Until there is standardization across technologies to accommodate both encrypting and tokenization technologies, there will be a myriad of solutions and flavors to choose from. Even so, waiting for standardization is not an option for merchants. Thieves won’t wait for a unified approach and specification. They are looking for your data now and you need to enter into the technology arena as soon as you can. Doing something is much better than doing nothing. By understanding all your business processes, asking the right questions, choosing trusted partners and keeping yourself updated, you can identify which technologies are right for your business. ■

¹ VISA Best Practices, Tokenization Version 1.0, July 14, 2010, pg. 1