PCI BLOG

THE UNOFFICIAL PCI COMPLIANCE & IT SECURITY BLOG

HOME PCI IN THE NEWS PCI TOOLS IT SEC. JOB BOARD DOCUMENTS

CONTACT US FORUM

P2PE, EMV, Tokenization, Oh My!

June 14, 2016 PCI Blog Cardholder Data Environment (CDE), E2EE, Encryption, Guidance, Ingenico, P2PE, Payments Industry, PCI Blog, Point to Point Encryption (P2PE), PTS, SRED, Tokenization 2

"I'm sure there are better ways to disguise sensitive information, but we don't have a big budget."

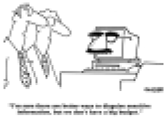
Unless you're an industry expert, understanding the many industry technologies such as Point-to-Point Encryption (P2PE), EMV and Tokenization – and their confusing acronyms – can be

TRENDING ARTICLES

Security Alert: EMV Skimmers Now Available for Purchase [Video]
October 20, 2016 0

Part I: Understanding the SAQ P2PE for PCI SSC Validated P2PE Solutions
September 5, 2016 0

Security Alert: Oracle Micros POS Breach
August 8, 2016 0



P2PE, EMV, Tokenization, Oh My!
June 14, 2016 2

extremely difficult. For most merchants, payments security focuses on three major goals:

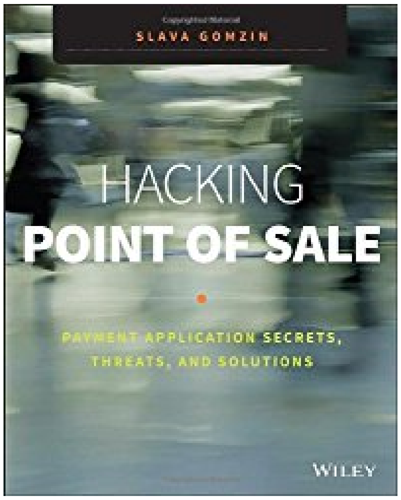
1. Prevent a data breach by limiting or removing sensitive credit card data from their environment, and
2. Prevent acquirer charge backs as a result of credit card fraud
3. Simplify PCI Data Security Standards (DSS) compliance

What is Point-to-Point Encryption (P2PE)?

Point-to-Point Encryption, also known as P2PE, is a payments industry standard which encrypts sensitive cardholder data upon swipe, dip or other payment method, such as NFC mobile wallets like Apple Pay or manual/hand-keyed transactions. The payment method does not matter, and all data, regardless of whether accepted through the magnetic stripe, EMV reader or NFC module, is encrypted within the payment terminal. In the case of PCI Validated P2PE solutions, the devices are what's known as SRED certified, which stands for Secure Read and Exchange of data. The SRED module within the device is a requirement for PCI Validated P2PE solution, and is a segmented processor within the device used specifically for encryption processes. In the United States, Ingenico (side image) or Verifone are the leading payment terminal providers in the U.S., and are both the leaders in SRED-approved devices. In most cases, Ingenico or Verifone devices are implemented with PCI Validated P2PE solutions.

Payment Processing
Payment Processing Made Easy. Free
Get Yours Today. Go to mybillingtree

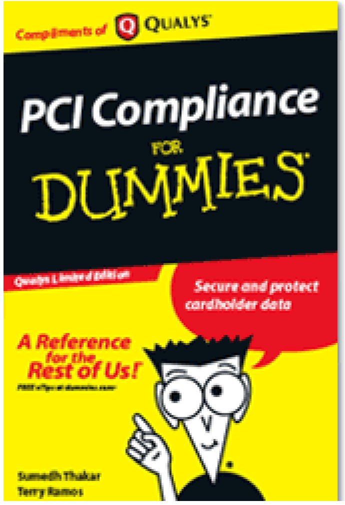
BOOK RECOMMENDATION



4.5 Stars on Amazon

CONSIDER SUPPORTING OUR SPONSORS

Free App + Reader
Download the free Phone Swipe app from your app store and we'll send you a free card reader upon approval.



P2PE solutions come in many flavors, such as non-integrated or semi-integrated, but that is a discussion for another post. It is important to note that the PCI Security Standards Council has an official standard for point-to-point encryption solutions, which was released in 2012. This is what we refer to as PCI Validated P2PE or, simply, PCI P2PE. Although P2PE and E2EE solutions are not required to validate to the PCI P2PE standard, most merchants are moving towards only those solutions that have been independently validated by a QSA and meet the PCI P2PE security standards. The full list of PCI Validated P2PE solution providers can be found at the link below:

https://www.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions

The purpose of point-to-point encryption is to render sensitive cardholder and Personally Identifiable Information (PII) useless. As most security experts tell you, it's not a question of "if" you will get hacked, it's a question of "when." With that, the purpose of Point-to-Point Encryption (P2PE) is to ensure that the cardholder data is encrypted before it enters the merchant network or systems in any way, transforming a once-sensitive payment environment to a non-sensitive environment (at least as it relates to credit card data). Once the payment data is encrypted within the payment terminal, the data is protected throughout transit to the backend solution provider, where the data is then decrypted for processing. Depending on the solution provider, the data may be decryped at a payment gateway and then sent over SSL/TLS or direct circuit to the processor, or the data is decrypted at the backend processor. To date, though, no backend processor (e.g., First Data, TSYS, etc.) has a PCI Validated P2PE solution, although this is likely in the works by many of the major backend credit card processing providers. To learn more about the differences of scope reduction between encryption solutions, such as an E2EE or P2PE solution, versus a PCI Validated P2PE solution, view our post on PCI Validated P2PE: PCI Validated P2PE Explained

P2PE Summary: Point-to-Point Encryption (P2PE) makes data unusable and protects merchants from a potential data breach.

What is EMV?

The EMV acronym stands for Europay, MasterCard and Visa, the organizations who initially built the EMV technical standard, which is managed and overseen by EMVCo (click to visit their website). EMV is the integrated chip that consumers are now finding embedded in their newly issued credit cards. Unlike Point-to-Point Encryption (P2PE), the purpose of EMV is two-fold:

1. Validate consumer identity
2. Prevent fraud

Notice from the above, that encryption is not a purpose of EMV. Once again, protecting data in transit. or within your POS or other systems, is not a purpose of EMV. It's important to understand this point, as EMV became the focal point following the major breaches of 2014. Once again, EMV is not a data security solution and it would not have prevented the breaches like Target, Home Depot and others – point-to-point encryption likely would have, however.

That being said, our purpose is not to undermine the importance of EMV as a fraud prevention technology. EMV is a crucial technology in payments security, which aims to validate a consumer's identity in real-time at the point-of-sale and to also prevent fraud by making chips nearly impossible to duplicate. Unlike magnetic strip cards, the EMV chip cannot be duplicated. When consumers complain about fraudulent credit card charges, it's often the result of their data being stolen due to a data breach within the merchant environment

(Prevention: Point-to-Point Encryption) and then a criminal utilizing a tool to write that stolen credit card information to a magnetic strip (Prevention: EMV). These tools are cheap, and combined with a simple software program can be easily utilized to write stolen credit card information to a blank magnetic strip card. A quick Google search demonstrates how easy and affordable it is for criminals to obtain the hardware to create fraudulent magnetic stripe cards:

https://www.google.com/search?q=magentic+stripe+card+reader#tbm=shop&q=%22magnetic+stripe%22+%22card+writer%22

There is no such technology (at least yet) that can be used to duplicate the chip in EMV cards. So, in cases where a data breach occurs and credit card data is stolen, criminals are only able to duplicate that card data onto magnetic stripe card. This is usually what occurred when you see three charges at a gas station for $75, four states away. As a result, in geographic regions where EMV is the primary acceptance type, such as Europe, card present fraud with duplicated cards is extremely low.

EMV Summary: EMV works to prevent fraud by verifying the identity of the consumer in real time, and disallows the copying and duplication of chip cards.

What is Tokenization?

Tokenization is often confused with point-to-point encryption (P2PE), as both solutions involve once-sensitive data being converted into non-sensitive data that is useless to hackers. Tokenization and P2PE are very different however, and solve two very different purposes within a merchant environment.

Where P2PE utilizes an encryption algorithm (e.g., TDES-DUKPT, AES, RSA, etc.) to encrypt the sensitive payment data within the payment terminal, tokenization only occurs after the transaction has already traversed through the POS system and network, and is sent out to the processor for an authorization. On the way back from the processor, a "token" is sent back to the point-of-sale with the approved authorization. This "token" is simply a numerical value that represents the actual card number within the payment system, but is not considered sensitive. The token is usually provided by the payment gateway (e.g. Merchant Link) or processor (e.g. Vantiv), and that same provider holds the "token vault," which is where each token is mapped to the real card number. The token allows for a merchant to store a number that represents a card number within their environment. The merchant can then treat that token as if it were a real card number, allowing them to run additional sales, refunds, voids, etc., without the burden of maintaining true cardholder data which would be subject to PCI DSS restrictions.

Tokenization Summary: Tokenization replaces real credit card numbers with non-sensitive numbers within a merchant's POS environment, after an authorization occurs.

Have questions about P2PE vs. EMV vs. Tokenization? Head over to our Q & A section to ask a question. We will do our best to answer it within 24 hours!

Share this:

Related

PCI Validated P2PE
In 2012, the PCI Council released a standard for point-to-point encryption, known
In "E2EE"

Credit Card Processing, Encryption and EMV Explained
In "E2EE"

Security Alert: EMV Skimmers Now Available for Purchase [Video]
In "Awareness"

EMV VS TOKENIZATION P2PE VS EMV

P2PE VS TOKENIZATION

□

About PCI Blog › 14 Articles

PCI Blog is the most trusted PCI Compliance and IT Security blog on the web. Authored by industry experts within the payments and IT security industries, PCI Blog provides insight on the complex world behind modern compliance and security standards. As a wholly independent source of news within the payments industry, PCI Blog focuses on the ever-changing responsibilities of merchants who accept credit cards. PCI Blog also provides reviews on PCI compliance tools and enterprise security solutions to offer a fair, independent critique of product offerings within the payments industry.

PREVIOUS ARTICLE NEXT ARTICLE

2 TRACKBACKS & PINGBACKS

Security Alert: EMV Skimmers Being Sold Online [Video] – PCI Blog

Security Alert: EMV Skimmers Now Available for Purchase Online [Video] – PCI Blog

Leave a Reply

Enter your comment here...

PCIBlog.org - The Unofficial PCI Blog | Copyright 2016