PSC
part of nccgroup

Payments
Security
Compliance

TrustCommerce, a Sphere Company TC Safe® PCI Validated Point to Point Encryption

Written by: Paul Guthrie, CISSP, QSA, PA- QSA, P2PE QSA, P2PE PA-QSA, PFI, PCIP, CTGA
Vice President

Table of Contents

Table of Contents 1
Executive Summary 2
Overview of P2PE Programs 3
How P2PE Works 3
History of P2PE 3
PCI Validated P2PE 4
Benefits of Validated P2PE 6
Risk Reduction 6
PCI DSS Scope Reduction 6
Use of Validated P2PE with Tokenization 7
Use of Validated P2PE with EMV 8
Validated P2PE Deployment Scenarios 9
Retail Stores 9
Kiosks or Unattended Devices 9
Telephone Order (Call Centers) 9
E-Commerce 10
TrustCommerce TC Safe® PCI Validated P2PE 11
Overview of Solution 11
Devices and Software 11
Use Case - Healthcare 12
Challenges 12
Use of P2PE 12
Summary 14
Who is PSC? 15

Executive Summary

Point-to-Point Encryption (P2PE) is a critical technology used to protect credit card data from being breached. While P2PE has been around for many years, including at TrustCommerce, only PCI Validated P2PE technologies such as TrustCommerce's TC Safe® have been tested to rigorous standards and should be trusted to reduce risk, and PCI DSS scope at a merchant.

In this whitepaper, we explore PCI Validated P2PE in detail, including how P2PE works within several environments and with other technologies, and how the TC Safe® solution may be used to reduce both risk and scope at retail environments and call centers. We present a challenging use case (healthcare) and demonstrate how P2PE provides an exceptional solution to PCI DSS and credit card security issues within that environment.

PSC obtained permission from TrustCommerce to utilize information gathered during their P2PE Validation process to prepare this whitepaper, including technical support and guidance.

Overview of P2PE Programs

How P2PE Works

Point-to-Point Encryption systems protect cardholder data such as the primary account number (PAN) from the Point-of-Interaction (POI) terminal within a merchant's retail store, to a payment gateway that may decrypt the data, such as TrustCommerce. A merchant will never have access to unencrypted credit card data, removing entirely this critically sensitive data element from their environment, and eliminating the largest source of credit card data breaches.

In a credit card data breach, an attacker gains access to a store or corporate headquarters and targets any storage or processing of credit cards by using special tools to monitor memory or to scan disks. In a P2PE system, there is no unencrypted credit card data, and therefore the only data items that might be available to an attacker would be truncated data (e.g. the first six and last four digits of a credit card), encrypted credit card data, or tokenized credit card data. In each of these cases, there is little the criminal can do with this data.

As such, P2PE is one of the best methods a merchant can use to protect their customers, themselves and prevent a credit card breach.

History of P2PE

P2PE has been around in many forms for over 20 years, with varying approaches and degrees of security. There have been many terms or names applied, some commercial, and some generic, such as "end-to-end encryption." There have also been deviations from the principal that data should be encrypted from the POI device to the payment gateway. Some solutions only protect data in transit, and other solutions do not encrypt within the POI device, but rather a connected workstation, leaving cardholder data vulnerable to memory sniffing attacks. Then there are solutions that decrypt somewhere on the merchant network to re-encrypt the data before sending on for processing, providing a point of weakness.

Some of the less secure solutions have led to significant credit card breaches, and in those cases, the merchant mistakenly believed that they were secure because they were running some form of P2PE; but indeed they were not. To counter this problem, the Payment Card Industry Security Standards Council (PCI SSC) produced a program to provide standards for P2PE solutions, and a high bar that must be met by solution providers to call their P2PE products "validated".

PCI Validated P2PE

The PCI SSC is a standards organization created and supported by Visa, MasterCard, American Express, Discover and JCB. Its role for any of the security standards it supports is to develop and publish the standard, educate and certify third party assessment companies (such as PSC), and in some cases to approve and list solutions based on those standards.

In the case of P2PE, the council maintains a list of validated P2PE solutions on their website[1] and each of these solutions has been tested and validated to meet an exceptionally high bar. Some of the required security features include:

- Usage of approved hardware devices with approved encryption methods
- Using or developing secure applications that have had their source code reviewed by a security specialist
- Creation of a hardened decryption service that uses hardware security modules to manage keys and decrypt card data.

While each of these areas is beyond the scope of this whitepaper, it is important to convey that there is a lengthy and challenging audit that validated P2PE solutions have successfully passed. Conversely, solutions that are not listed with the council have not had that same level of rigorous testing applied to them and may not reduce a merchant's risk in the same way – in fact they may leave the merchant with a false sense of security.

In recognition of the status of using a listed P2PE solution, the PCI SSC has allowed the scope of a PCI Data Security Standard (DSS) assessment to be greatly reduced, something that is not possible using a non-listed solution.

Benefits of Validated P2PE

Risk Reduction

As discussed earlier, there is significant risk reduction for a merchant using a validated P2PE solution. There is no unencrypted cardholder data in a merchant environment, and attackers cannot steal what does not exist. It is critical; however, that a merchant keep their retail environments clean and do not accept credit card data through non-P2PE interfaces, e.g. maintaining a spreadsheet of their "best customers'" credit cards for easy purchasing. That type of information is best kept using tokens as discussed later in this paper.

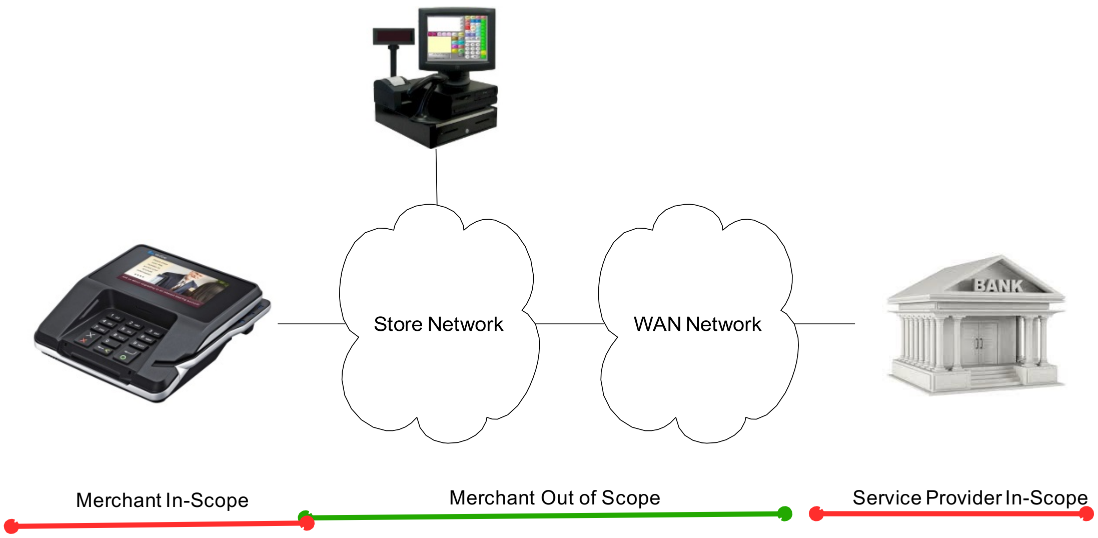
The costs of a data breach are extremely significant, and the damage to the reputation of a merchant severe. In a recent report[1], the Ponemon Institute estimated the cost per card of breached credit card data at $141. This includes fines from the card associations through the merchant's acquiring bank, as well as administrative costs, legal costs and potentially fraud costs on the cards.

PCI DSS Scope Reduction

For a validated P2PE solution, the scope of the merchant's PCI DSS assessment is adjusted accordingly[2]. The rule of thumb is that nothing between the encryption environment (i.e. the POI device) and the decryption environment (TrustCommerce) is considered in scope for PCI DSS. Assuming a retail store has no other means of credit card acceptance that are non P2PE (e.g. a kiosk, linebusters, etc.) then the store network may be considered out of scope:

[1] https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN

[2] https://www.pcisecuritystandards.org/faqs FAQ numbers 1158 and 1247



It is important to note that the store itself is not considered out of scope, because either the merchant or the PCI DSS assessor must consider a set of controls around management of the POI device itself (PCI DSS §9.9) as well as ensuring the validated P2PE solution is properly implemented within the store.

This scope reduction is significant as it removes from scope the management of both POS workstations and network infrastructure – which due to rigorous requirements for hardening, patching, anti-virus and logging are a challenge to maintain in a large, distributed environment such as a chain of retail stores.

For merchants working with a PCI QSA (Qualified Security Auditor), the auditor will validate the scope, and provide appropriate scope reductions. Other merchants performing self-assessments may be able to use the minimal SAQ- P2PE, providing they meet all of the eligibility requirements.

Use of Validated P2PE with Tokenization

Validated P2PE is especially effective when combined with tokenization of credit card information. The token replaces the credit card PAN with a random number, a globally unique identifier (GUID) or some other data element that is known only to a payment service provider such as TrustCommerce. Tokens are not considered in-scope for PCI DSS and cannot be stolen by an attacker and reused at another merchant and as such are extremely secure.

Tokens are useful to merchants in many use cases that require repeated use of a credit card number, where the token may be used as a proxy for the credit card. Some of these include:

- Refund back to the original card without the card present
- Routine (e.g. monthly) or installment charges
- Correlation with the e-commerce channel to link purchases to the correct customer

Use of Validated P2PE with EMV

EMV is the standard for use of chip cards at the point-of-sale, instead of swiping the magstripe on the card. EMV can take the form of a "dip" of the card into the card reader, or a "tap" of the card when using a Near-Field-Communication (NFC) interface. It is a common misconception that EMV encrypts credit card data and can replace P2PE. It does not. As such, EMV and P2PE technologies complement each other, and in many cases, as merchants upgrade terminals to allow EMV to work in their stores, they are implementing P2PE at the same time. Almost all modern POI devices support both P2PE and EMV technologies at this time, but not all merchant providers and/or gateways.

P2PE Deployment Scenarios

Retail Stores

Retail stores are the primary focus of the P2PE standard. By selecting a POI device supported by the TC Safe® P2PE solution and listed within TrustCommerce's P2PE Instruction Manual (PIM) , such as the Ingenico Group iSC250, the merchant may implement the TC Safe® solution in their environment. The PIM provides instructions as to how to receive, set up and manage the POI devices, and other details surrounding the P2PE solution. It is important that the merchant follow all of the applicable instructions within the PIM.

The scope reduction for the merchant would generally be the entire store network. As all TC Safe® supported devices currently only support USB interfaces, it is important to note that the Windows workstations that the POI devices are connected to are not considered in-scope for PCI DSS, unless they receive cardholder data from a non-P2PE input mechanism such as manual entry on the keyboard.

Kiosks or Unattended Devices

Kiosks or unattended devices (gas pumps, self-checkout stations, etc.) may also utilize validated P2PE solutions as long as they are utilizing a card swipe, encrypting PIN PAD or other POI technology that is supported by the TC Safe® Validated P2PE solution. TrustCommerce maintains a current list of supported devices within their PIM, and the PCI SSC maintains a current list on their website, provided earlier.

Telephone Order (Call Centers)

It is also possible to utilize TC Safe® in call center environments, reducing or eliminating from scope the entire network and all call center workstations. This requires that all cardholder data entry is performed not on the keyboard of the call center workstation, but instead on an attached POI device such as the ID Tech SREDKey. The customer's name, order information, address, etc., may be entered on the primary keyboard, but when the time comes to receive the credit card information including Primary Account

Number, Expiration Date and CVV2, these must be entered on the POI device which will then encrypt the data and fill out the form with encrypted data. At that point, the TrustCommerce TC Link API as either a component or full solution may be used to submit the payment to TrustCommerce and (optionally) tokenize the cardholder data for future use.

E-Commerce

At this point, there are no validated P2PE technologies in use that support e-commerce channels. The PCI P2PE standard requires hardware encryption of cardholder data and the point-of-interaction, and is targeted at card-present transactions, rather than card-not-present such as in e-commerce. There are other security technologies in use to support security of e-commerce transactions or having the gateway host the payment page, like TrustCommerce's TC Trustee Premier, to keep the PAN data out of the merchants' environment, but these are outside of the scope of this document.

TrustCommerce TC Safe™ P2PE

TrustCommerce has been providing encrypted credit card transactions for over 10 years and has supported encryption of credit card data in transit and storage since the company's inception. Validating their solution to the P2PE standard was the obvious next step in providing assurances to their customer base that the security measures already in place met the stringent standards of the payment card industry.

Overview of Solution

Any validated P2PE solution is roughly divided into an encryption environment, which exists at a merchant, as well as a decryption environment, which exists at TrustCommerce. The decryption environment is out of scope for this whitepaper but has been subject to audit through both the PCI DSS and PCI P2PE standards as is the merchant's interface to its acquiring bank's payment services.

The encryption environment includes a POI device supported by TC Safe®, as well as optionally the TC IPA® software, which is not considered in scope for PCI DSS when used as part of the TC Safe™ solution. The TC IPA software is used to interact with the POI device, and instruct the device to take payment, which it returns in encrypted form.

The other means of use of TC Safe® is via the TC Link® API. A merchant that uses TC Link can integrate a supported POI device and send encrypted data to the API. Note that the API has always supported transport encryption using TLS, but the validated P2PE encryption is required for any scope reduction.

Devices and Software

The current list of supported devices can be provided by TrustCommerce as part of their P2PE implementation manual or referenced on the PCI SSC website.

Use Case - Healthcare

Challenges

Healthcare organizations have unique challenges when considering cardholder data security and PCI DSS. Take, for example, a large hospital complex which may be accepting cards at nurses' stations, patient intake, cafeterias, parking garages, gift shops, opticians, and even third parties such as on-site physician practices. All of these acceptance channels likely share the same network. As such, without additional segmentation controls, this may bring the entirety of the hospital complex network into PCI DSS scope.

PCI DSS requires significant security controls around in-scope networks and systems including hardening, patching, logging, but most importantly, scanning and penetration testing. Running a penetration test, or even a scan on a network segment that can include medical equipment is an extremely dangerous proposition.

Up to this time, the primary alternative for a healthcare organization is to identify all channels of card acceptance and segment all of the workstations and supporting services to a separate network. This is a significant undertaking and costly to perform and maintain. It is greatly preferred that healthcare organizations do not require segmenting of their networks to "payment acceptance" and "nonpayment" – after all, the role of the organization is to provide health services, not payment services.

Use of Validated P2PE

P2PE solves this dilemma. Use of a P2PE device connected to a workstation or network does not bring that workstation or network into scope for PCI DSS. Additional endpoint controls, mandated by PCI DSS, are not required, reducing the amount of overhead that an already burdened IT department may have to support.

The P2PE devices may safely share the network segments with medical hardware or other support devices requiring additional security controls. This brings flexibility and convenience to network design and allows for rapid changes on the network.

The TC Safe® solution supports this model and is an ideal solution for the healthcare market.

Summary

Validated P2PE solutions represent the most effective way of protecting card-present and agent-entered credit card transactions. By performing encryption in hardware at a POI device and decryption using hardware devices at TrustCommerce, card data is protected between these two points. This allows a merchant using TC Safe® to receive scope reduction from their PCI DSS QSA, or to use the PCI SAQ-P2PE should they be eligible.

The TC Safe® solution, supporting both a Windows-based payment software package, TC IPA® or an API to the TrustCommerce gateway, TC Link®, allows merchants the flexibility of interfaces, as well as a number of POI devices to choose from.

TrustCommerce has raised the bar on their long-standing encrypted payment service by validating to the PCI P2PE standard and providing their customers both the means to reduce their risk as well as their PCI DSS scope.

Who is PSC?

With offices in the USA, Canada, UK and Australia, PSC is a leading PCI Assessor and Forensics Investigator Company. We are one of an elite few companies qualified globally to provide expert services and solutions to organizations that require specialist compliance or consulting support in the areas of Payments, Security or Compliance.

Our focus is exclusively on clients that accept or process payments or technology companies in the payment industry. All staff at PSC have either worked within large merchant/retail organizations or services providers. Each partner at PSC has held executive management positions with responsibilities for payments and security.

Our approach includes a high-touch, hands-on methodology, that helps guide our clients from consideration of strategic alternatives all the way through implementation and sustaining activities. The partners at PSC work closely with Clients to understand their objectives produce pragmatic and actionable plans and aid in execution as required.

- PSC is certified globally as a Qualified Security Assessor Company ("QSAC"); Payment Applications Qualified Security Assessor Company ("PA-QSA") and an Approved Scanning Vendor ("ASV") for the PCI Security Standards Council.
- PSC is certified as a Point to Point Encryption Qualified Security Assessor Company ("P2PE QSAC") and Point to Point Encryption Payment Applications Qualified Security Assessor Company ("P2PE PA-QSA") for the PCI Security Standards Council.
- PSC is certified as a PCI Forensics Investigator Company ("PFI") for the PCI Security Standards Council.
- PSC is certified to perform Visa/PCI PIN and TG-3 assessment services in accordance with the TG-3 Retail Financial Services Compliance Guideline (X9 TR-39-2009).
- PSC is certified as a Verified by Visa (VbV) Assessor Company for Visa Inc.
- PSC is certified as a Card Production Logical Security, Physical Security and Over the Air Assessor Company for Visa, Inc.

To ensure Independence, PSC does not represent, resell or receive commissions from any third party hardware, software or solutions vendors.

www.paysw.com

+1 (408) 228 0961

info@paysw.com

591 W. Hamilton Ave, Suite 200, Campbell, CA 95008