COALFIRE

IMPACT OF PCI P2PE

PCI DSS COMPLIANCE, SCOPE REDUCTION, AND COST-BENEFIT ANALYSIS FOR PCI-LISTED P2PE

Bluefin Payment Systems

Prepared For:

Bluefin Payment Systems
www.bluefin.com
800-675-6573

Prepared by:

Dan Fritsche
CISSP, PA-QSA(P2PE), QSA(P2PE)
VP, Solution Architecture
Coalfire Systems, Inc.

Tim Winston
CISSP, CISA, QSA(P2PE)
Product Director, P2PE
Coalfire Systems, Inc.

Date:

January 24, 2017

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The purpose of this white paper is to assist merchants in making cost and compliance decisions related to the use of the Bluefin P2PE solution. To do this, Coalfire Systems, Inc. ("Coalfire") has conducted an independent review of publicly available PCI Data Security Standards (PCI DSS) compliance tools, as well as a review of the Payment Card Industry (PCI) Security Standard Council's (SSC) Point-to-Point Encryption (P2PE) program and how it fits into the modern payments security and compliance ecosystem. Using this information, this white paper demonstrates how P2PE aligns with the PCI DSS compliance framework in order to simplify merchant compliance effort and how the associated cost savings may be measured from this scope reduction. Finally, this document proposes ways in which a merchant may model its own compliance costs in order to evaluate the total cost of ownership (TCO) and return on investment (ROI) for the Bluefin P2PE solution PCI compliance scope reduction.

AUDIENCE

The intended audience for this document is merchants who are considering or have already implemented Bluefin P2PE within their card-present or mail order/telephone order (MOTO) processing environment. The impacts on compliance and risk discussed herein are tailored for merchant organizations, and therefore the term "merchant" is used throughout. Many of the concepts may also apply to service providers; however, the specific impact on PCI DSS compliance may vary. Please consult with a qualified security assessor (QSA) for further clarification on how Bluefin P2PE may impact your organization's risk and compliance.

BACKGROUND

PCI SECURITY STANDARDS COUNCIL AND COMPLIANCE

The PCI SSC was founded by the major card brands Visa, MasterCard, American Express, Discover, and JCB. The PCI SSC maintains the PCI DSS and oversees additional standards that are used to validate devices, software, services, and solutions that aid merchants in meeting those standards. Among them are the Payment Application Data Security Standard (PA-DSS), which may be used to validate software applications; the PIN Transaction Security standard (PCI PTS), which may be used in the approval of transaction devices; and the PCI Point-to-Point Encryption standard (PCI P2PE), which may be used to validate solution providers and components that are used to perform terminal-based encryption, key management, and decryption operations.

Within the payments ecosystem, there are also devices, software, and services that have not been assessed under these standards. For instance, software applications may be ineligible for PA-DSS validation if they are custom-built ("bespoke") or do not affect security of cardholder data. Certain acceptance devices (particularly magnetic stripe readers) may be in use that are not approved under the PCI PTS standard. There are also encryption solutions (often called either unlisted P2PE, non-validated P2PE, or end-to-end encryption (E2EE) solutions) that provide additional encryption security but have not been validated to the PCI P2PE standard. While such non-validated solutions currently exist, and many have built-in security features, PCI SSC does not approve scope reduction as they have not been assessed in conjunction with the appropriate program. Since each solution varies in how effectively they manage transaction encryption, the use of a QSA (P2PE) is recommended to perform a risk assessment and assess the appropriate compliance impact and/or compensating controls. The ultimate authority rests with the merchant's acquirer to accept that risk and approve the recommended approach.

REVIEW OF CURRENT SECURITY THREATS

In the past few years, the rate of merchant data breaches has grown dramatically. In many cases—from high-profile merchant breaches such as Target[1] and Home Depot[2] to much smaller merchants—forensic investigations have confirmed that the preferred method for extracting account data from point-of-sale (POS) systems has been the use of RAM-scraping malware[3]. This breed of malicious software is able to access clear-text card data as it is processed within system memory, even if the system uses encryption to receive and re-transmit this sensitive data. While card data may be received by the POS system in encrypted form, encrypted when stored, and encrypted when transmitted, it is unencrypted while in memory and therefore is highly vulnerable to this type of attack.

Hackers have used a number of methods to gain access to POS systems in order to install malware and extract the data. Common delivery methods include phishing, compromising remote weak or known account credentials, exploitation of software and OS vulnerabilities on the POS system, or exploitation of auxiliary system and elevation of privileges.

In order to protect sensitive data from exfiltration, industry security experts recommend a variety of preventative actions. Verizon's 2016 Data Breach Investigation Report specifically recommends malware defense (SANS CSC-8) and controlled access based on need-to-know (SANS CSC-14) to help mitigate this specific threat[4]. SANS expounds on this approach by recommending depth in security and implementation of 20 critical security controls that would often prevent the chain of events associated with this attack vector[5]. Similarly, there are 329 applicable controls within the PCI DSS version 3.2, such as installing strong perimeter and network segmentation controls, changing default passwords and settings, patching for known vulnerabilities, developing secure software, enforcing strict user access controls to limit exposure to data based on need-to-know, preventing unauthorized elevation of privileges, restricting physical access to sensitive areas, training employees to prevent access to user credentials through phishing attacks, scanning for malware, logging key functions, and monitoring for suspicious activities.[6]

DAMAGE IF YOU DO; DAMAGE IF YOU DON'T

Every security control has a direct or indirect financial impact to the bottom line: whether an employee must divert attention from other revenue-generating activities; whether a third-party contractor must be hired to perform the task; or whether a tool must be purchased to automate the process. Since so many controls are necessary to protect account data as it passes through a merchant network, a thorough cost accounting is necessary to identify the total cost of any chosen approach.

However, stolen credit card account data is also very costly—to the consumer, the card networks, and to the compromised merchant. These costs include fines, penalties, consumer notification and credit monitoring for those affected, forensic investigation, remediation, loss of business, damage to relationships, and damage to consumer reputation and trust.[7] Recent studies of retail data breaches have attempted to estimate this cost, with results ranging from an average cost of $172 per record[8] to volume-specific average costs, ranging from $67,480 for 1,000 records to $8.8 million for 100 million records.[9]

1 https://www.sans.org/reading-room/whitepapers/casestudies/case-study-critical-controls-prevented-target-breach-35412
2 https://www.sans.org/reading-room/whitepapers/breaches/case-study-home-depot-data-breach-36367
3 http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/
4 Ibid.
5 https://www.sans.org/reading-room/whitepapers/casestudies/case-study-critical-controls-prevented-target-breach-35412
6 https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss
7 http://www.verizonenterprise.com/resources/report/rp_pci-report-2015_en_xg.pdf
8 http://www-03.ibm.com/security/data-breach/
9 http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report_2015_en_xg.pdf

Fortunately, there are certain tools that have a significant impact on cost. In the following section, we will review three widely recognized payment tools, EMV, P2PE, and Tokenization, and their purpose.

COMMON TOOLS FOR SECURING TRANSACTIONS

In today's credit card transaction environment, there are three valuable technologies that are sometimes misunderstood. Here we discuss EMV, P2PE and Tokenization, where they may add value to a merchant's security program, and common misconceptions about their impact on a merchant's security and risk profile.

ROLE OF EMV – SECURING AGAINST COUNTERFEIT CARDS

EMVCo, which was founded by (and named after) Europay, MasterCard, and Visa in 1994, manages the EMV standards. The most widely used of these standards is the current EMV 4.3 specification[10]. The payment industry around the world has begun adopting EMV for production and transaction support for credit cards issued with integrated chips in order to provide new card fraud protections for consumers. To facilitate this transition in the United States, the major card brands have instituted phased liability shifts, where card present merchants or credit card issuers who fail to support these cards may be liable for counterfeit card fraud. As credit card issuers move to offer cardholder verification methods such as PIN, support for EMV may also help merchants shift liability for fraud resulting from lost or stolen cards[11]. Important liability shift dates include October 2015, which affected most credit card networks and industries; October 2016 for ATMs accepting MasterCard; October 2017 for other ATM cards; and the upcoming liability shift in October 2020 for automated fuel dispensers[12,13].

The EMV chip embedded within the new chip cards is capable of using advanced cryptography to generate a unique code (iCVV) that is then sent to the card networks with each transaction to confirm that the physical card is legitimate. This process has been demonstrated to be effective at preventing fraudsters from creating counterfeit cards. However, the EMV chip does not provide any encryption for the credit card primary account number (PAN), expiration date, or cardholder name: three sensitive data elements classified as cardholder data and required to be protected according to PCI DSS. Threat actors that steal this information can use this data to conduct fraud through other channels such as online (e-commerce) or MOTO transactions.

Therefore, support for EMV does not reduce a merchant's PCI responsibilities for protecting account data, nor has recent movement throughout the industry to adopt EMV had any measurable impact on the number of cardholder data breaches. In summary, EMV is primarily effective for reducing card-present fraud by **securing against counterfeit cards**.

ROLE OF P2PE – SECURING CARD DATA IN FLIGHT

P2PE is the term used by the PCI SSC to refer to its terminal-based encryption standard, where transactions are encrypted within specific PTS-approved hardware using encryption keys that reasonably protect the account data so that it can be transferred through the merchant environment safely, reducing risk of compromise.

The role of P2PE is to immediately and fully encrypt all cardholder data and sensitive authentication. By using strong encryption, device management practices, and key management, P2PE is effective at

10 https://www.emvco.com/specifications.aspx?id=223
11 http://www.emv-connection.com/downloads/2015/05/EMF-Liability-Shift-Document-FINAL5-052715.pdf
12 http://www.emv-connection.com/best-practices/what-is-the-fraud-liability-shift-and-when-is-it/
13 https://usa.visa.com/visa-everywhere/security/emv-at-the-pump.html

addressing the risk of card data compromise for card data in transit out of the merchant network as it is transmitted to the gateway or acquirer for decryption and processing.

There are two types of terminal encryption – PCI-listed P2PE solutions and unlisted solutions (sometimes called end-to-end encryption or E2EE). While there are many nuanced differences, which we will explore in the next section, there are three high-level requirements that every P2PE/E2EE solution must offer:

- The card data must be encrypted using strong cryptography
- The encryption must be performed within a secure hardware device
- It must not be feasible to decrypt the data within the merchant environment

As a result of these requirements, it becomes physically improbable to access card data prior to encryption; it becomes computationally infeasible to derive captured card data using brute-force methods; and it becomes logically unattainable to access the decryption keys in order to decrypt directly[14].

Through this process, P2PE performs the function of devaluing the cardholder data in the eyes of any hacker who may otherwise seek to access this information within the merchant's software, systems, and network, therefore **securing card data in-flight**.

ROLE OF TOKENIZATION – SECURING CARD DATA AT REST

Finally, there are merchants who must perform certain customer billing functions such as delayed charges, subscriptions, refunds, or credits, which require credit card information. Some merchants may have also used cardholder data as a means to track consumer behavior (although this practice is generally prohibited). Traditionally, these operations require the merchant to store sensitive credit card information so that it can be accessible for future use. Unfortunately, this also leaves a "treasure trove" of stored credit card data that may be stolen. For that reason, the efforts required to fully protect stored card data (PCI DSS Requirement 3) can be quite extensive and expensive.

Tokenization is the technology where secure card data storage is centralized and a different value is used to represent the original cardholder data. When ready to be re-used, the token must generally be passed to the tokenization provider, where the original cardholder data is retrieved, decrypted, and utilized.

Similar to P2PE, a compliant third-party service provider may perform this service on behalf of the merchant, including portions of the data security that rely on cryptography (in this case, storage encryption). However, unlike P2PE, the value that the merchant receives is not commonly a reversible encrypted form of the original PAN, but is uniquely designed to be stored safely. The token value may resemble a credit card number or even retain certain non-sensitive portions of the card data, or it may look entirely different. In some cases, the token may be an encrypted form of the cardholder data, but in most cases it is merely an arbitrary or random reference number used to access the stored information in the token vault. The entity performing the tokenization may be the gateway or another service provider, the acquirer, the card brand, or even the issuing bank.

To take full advantage of the benefits of tokenization, PCI SSC recommends that merchants tokenize sensitive data as quickly as possible, replace cardholder data with tokens wherever it is stored, and use services that do not provide a mechanism to "detokenize" data, as this presents another avenue that may be exploited.[15] In each case, the merchant must still observe PCI compliance requirements for systems that

14 https://www.pcisecuritystandards.org/documents/P2PE_At_a_Glance_v2.pdf
15 https://www.pcisecuritystandards.org/documents/Tokenization_Guidelines_Info_Supplement.pdf

store, transmit, or process card data before the data has been tokenized. When properly implemented, use of tokenization instead of storing actual cardholder data is valuable for **securing card data at rest**.

DIFFERENCE BETWEEN PCI-LISTED AND UNLISTED P2PE SOLUTIONS

HOW THE PCI P2PE STANDARD APPLIES TO PCI DSS

Before considering the specific impact of P2PE on a merchant's environment, it is important to understand how encryption fits into the larger context of a merchant's compliance with the PCI DSS. Since its first version released in 2004, the PCI DSS security framework has set forth a list of controls that are required to address the evolving landscape of security threats that could compromise cardholder data within a merchant environment. Each security control—whether through physical security, technical controls, or organizational policies and procedures—is associated with one or more identified threats that may jeopardize the security of credit card data.

Throughout the PCI DSS, different forms of encryption are required in conjunction with other technical, physical, and procedural controls within the cardholder data environment (CDE). For example:

- Secure protocols for services provided within the CDE (2.2.3)
- Encryption for all non-console access (2.3)
- Encryption of stored cardholder data (3.4)
- Encryption of file systems (3.4.1)
- Encrypted data transmission across public networks (4.1)
- Encryption across wireless networks (4.1.1)
- Use of encryption by software applications (6.5.3, 6.5.4)
- Strong authentication for administrative access (8.2.1)
- Key management practices and policies (2.3, 3.4, 3.5, 3.6, 4.1, 8.2.2)

Taking a piece-meal approach to encryption, the framework provides merchants the flexibility to access the PAN or other account data—as long as they ensure that each system and process is well-protected from the many possible attacks. For merchants that have the business need to access PAN, track data, or other account data, this ability to decrypt and encrypt again at each "hop" may be important.

It is Coalfire's experience that a significant majority of merchants do not have a legitimate business need to access this sensitive account data at all. In most cases, it is much preferred to trade this "flexibility" to view card data as it passes through each system in favor of ensuring the data is sufficiently secured through encryption and remains encrypted. This approach of voluntarily restricting the ability to view card data devalues the data, and the best vehicle for doing this is through P2PE.

INTENT OF THE PCI P2PE STANDARD

Since these terminal-based encryption services help protect data from "end-to-end"—across all segments of a merchant's network including wireless connections, processing servers, and open networks—it is reasonable to expect there to be significant mitigation of the risks associated with the system- or network-specific threats addressed through the numerous PCI DSS controls. It also stands to reason that any such broad reduction in risk should correlate with a reduction in the scope of the PCI DSS for merchants using such a solution. However, without clear guidance from the PCI SSC, it is difficult to know which exact

controls are still applicable and which systems that encounter this encrypted cardholder data must still be included in the CDE and therefore subject to these controls.

Recognizing the presence of existing solutions and the growing need for guidance on their proper implementation, the PCI SSC sought to identify the specific impact of transaction encryption within its standards framework and provide a structure for receiving that scope reduction. It was very important for the PCI SSC to clearly identify which risks could be fully addressed and the associated controls which might be reasonably omitted in order to adequately protect the card data. It was also important that the encryption itself would not be defeated by a malicious user by disabling terminal encryption or accessing sensitive encryption keys. How strong must the encryption be to safely courier data without being vulnerable to brute-force decryption? What key management practices are adequate to protect the private key from compromise? What controls are necessary at the point of encryption to protect sensitive encryption keys? How can a merchant trust the integrity of the decryption environment to be free from vulnerabilities? How will these controls be validated? [16]

In 2012, the PCI SSC released the first version of the PCI P2PE standard, the P2PE program guide, and special P2PE self-assessment questionnaire (SAQ) for these merchants. [17] Updated in 2015, PCI P2PE version 2.0 establishes a specific list of controls that encryption providers must enact in order to be listed as an approved P2PE solution or component. [18]

This PCI P2PE standard does not replace PCI DSS for merchants or service providers. Instead, service providers that choose to be validated must comply with both the DSS and the *additional* requirements of PCI P2PE (see Table 3). In return, merchants using these solutions may receive a sizable reduction in both the *size* of their CDE, and up to a 90% reduction in the *number* of applicable PCI DSS requirements that apply to the CDE that remains.

There are many ways in which to perform transaction encryption, and each has its own advantage. For the purposes of this review, terminal-based encryption solutions fall under two distinct categories: listed P2PE solutions and unlisted encryption solutions (sometimes called E2EE solutions).

UNLISTED SOLUTIONS

Solutions that have not been validated, but still provide functions such as encrypting within the POI terminal and decrypting outside the merchant environment, are generally called unlisted P2PE solutions, or E2EE. The trouble with unlisted solutions is that there may be no way for a merchant to know whether the provider has fully addressed the controls identified by PCI SSC as necessary to properly protect the account data. Many of the unlisted solution providers Coalfire has reviewed do use very secure processes; however, since unlisted solutions have not been assessed under the standardized PCI P2PE framework by qualified assessors, merchants using these solutions may still need to implement additional security countermeasures to ensure threats associated with the absence of these controls.

Since there is no PCI-approved assessment framework for unlisted solutions, merchants using these solutions that wish to reduce the scope of their compliance assessment must be able to determine how thoroughly the E2EE solution has addressed the threats identified by PCI P2PE and use this risk assessment to identify any controls that are adequately addressed and therefore inapplicable. Unlisted solutions do not qualify for the reduced SAQ P2PE, so merchants using these solutions should use the SAQ D (or ROC template if applicable), mark these controls as “NA,” provide full justification for these assertions within the “Appendix C: Explanation of Non-Applicability,” and receive special approval from the

16 https://www.pcisecuritystandards.org/pdfs/pci_ptp_encryption.pdf
17 https://www.pcisecuritystandards.org/documents/P2PE_Program_Guide_June_2012_v1.pdf
18 https://www.pcisecuritystandards.org/documents/P2PE_v2.pdf

acquirer for any control reductions. Coalfire highly recommends engaging a QSA (P2PE) to evaluate the E2EE solution, review the merchant's implementation of the solution, and request approval for the reduction of applicable controls prior to performing the assessment.

PCI-LISTED P2PE SOLUTIONS (PCI P2PE)

The second category is so named because these solutions have been assessed by a QSA (P2PE) as having met the PCI P2PE standard and are therefore listed on the PCI website under Approved P2PE Solutions.[19] It is worth noting that, in addition to meeting the P2PE standard, the decryption component of the solution must operate within a secure environment that has been assessed to the full PCI DSS standard.

Other requirements include assessment of the key management practices and cipher strength; key injection facilities; use and configuration of PTS-approved POI devices with encryption performed in the SRED (secure reading and exchange of data) tamper resistant security module (TRSM); positive device identification prior to decryption; and key management/decryption in hardware security modules (HSMs) that have been validated by PCI and/or FIPS 140-2 Level 3.

Since 2013, 25 P2PE solutions have been assessed as being compliant with this standard.[20] These solutions should have many security features in common, because they have all been assessed to comply with the same PCI P2PE standard. However, functionally these solutions may be very diverse, supporting different POI terminal devices, terminal payment applications, POS software systems, and processing networks. A list of current P2PE solutions may be viewed at any time on the PCI website.

DIFFERENCES BETWEEN VALIDATED AND NON-VALIDATED P2PE

It is impossible to generalize and say that all non-validated solutions are missing any specific security control(s), because every solution is different. While it is true that all validated solutions have been assessed as meeting the criteria for the PCI P2PE program, the only general statement that can be made about non-validated solutions is that they have not yet been validated to actually meet the same standard. For some, it may simply be a matter of completing the assessment process. For others, non-validated solutions may be lacking important security controls that prevent them from becoming validated, such as performing key management functions without the use of an approved HSM or using PTS devices that lack the SRED-certified TRSM.

There are numerous tangible benefits merchants may receive from using a solution that has been through the validation process, which are discussed in the next section.

19 https://www.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions
20 Ibid.

THE BENEFITS OF PCI P2PE VALIDATION FOR MERCHANTS

PCI-AUTHORIZED SCOPE REDUCTION

Merchants who use a validated solution within their environment and keep this environment segmented from any card data from other channels (e.g., e-commerce) may be eligible to complete the authorized self-assessment questionnaire SAQ P2PE that is known and accepted by all acquirers. Under PCI DSS v3.2, this represents a significant reduction of controls, reducing the number of questions by nearly 90% for merchants moving from the SAQ D (329 questions) to SAQ P2PE (33 questions).[21, 22]

Another aspect of scope reduction is the impact of PCI P2PE on the definition of the CDE itself. Since merchant systems can no longer access the cardholder data once it is properly encrypted, P2PE effectively reduces the number of networks and systems considered to be within the scope of the PCI DSS assessment.[23] This scoping guidance is endorsed by PCI and commonly followed by assessors, but only for solutions that have been through the validation process.

CARD BRAND PROGRAMS

Visa Technology Innovation Program (TIP)

Merchants who accept at least 75% of their transactions through a PCI-validated P2PE service may qualify to apply through their acquirer for the Visa TIP program, which allows approved merchants the ability to discontinue their annual assessment process to revalidate PCI DSS compliance. While available for merchants of any size, this program is especially valuable for high-volume or geographically dispersed merchants who may otherwise undergo a more strenuous and costly assessment process.[24]

Visa Secure Acceptance Incentive Program

This program incentivizes acquirers by providing safe harbor for fees in the event of a compromise for Level 3 and 4 card-present merchants who use a PCI-validated P2PE solution. There is no application process, although a merchant should still strive for full PCI DSS compliance and have documentation showing that 100% of transactions were accepted via a listed solution.[25]

SOLUTION FOR CHALLENGING COMPLIANCE ISSUES

Mobile Acceptance

Securing mobile card present payments today can be problematic. Mobile point-of-sale (mPOS) apps available for download for consumer mobile devices (like Android, iOS and Windows Mobile) do not qualify for PA-DSS, making it very difficult for merchants to assess the compliance of these software applications. PCI guidance recommending non-payment capabilities be disabled inhibits the use of mobile devices or tablets for ancillary functions, limiting the device's value as part of a unified solution for the mobile workforce.[26] Mobile device management systems capable of performing remote wipes, ensuring timely updates, and enforcing access policies may be incompatible with bring-your-own-device (BYOD)

21 https://www.pcisecuritystandards.org/documents/PCI-DSS-v3_2-SAQ-D_Merchant.pdf
22 https://www.pcisecuritystandards.org/documents/PCI-DSS-v3_2-SAQ-P2PE.pdf
23 https://www.pcisecuritystandards.org/documents/pci_ptp_encryption.pdf
24 https://www.visa-asia.com/ap/sg/merchants/stayingsecuremerchants/accountsecurity_merchant_req_tip.html
25 http://www.greensheet.com/emagazine.php?story_id=4056
26 https://www.pcisecuritystandards.org/documents/Mobile_Payment_Security_Guidelines_Merchants_v1.pdf

environments. Performing quarterly network vulnerability scans of mobile workforce devices via individual cellular network connections represents another significant logistical challenge.

PCI P2PE is perfectly suited to address these issues. By encrypting all card data within a validated card reader before it passes through the mobile device, the consumer mobile device is rendered out of scope for PCI DSS compliance (so long as it is not used for any other payment function), ensuring compliant card acceptance via a consumer mobile device. MasterCard's singular guidance for merchants pertaining to securing transaction data on the mPOS is through the use of a PCI P2PE solution.[27]

Foreign Networks

Because systems and networks between the encryption point and the decryption environment are no longer in scope due to the P2PE encryption, this unique advantage can address complex network responsibility challenges for some merchants. Store-within-a-store retail concepts often use their host store's network to provide Internet connectivity, but cannot treat the host network as a true "open, public network" (as defined in Requirement 4). Therefore, no conventional method can descope the host network for PCI DSS. PCI P2PE, on the other hand, does provide the desired effect. For instance, in a case study published by PCI, The Hillman Group discusses this specific challenge and their use of Bluefin P2PE to transmit P2PE-encrypted account data over their host's network without bringing it into scope.[28]

27 http://arm-pdf-directory.s3.amazonaws.com/MasterCard_Mobile_Point_Of_Sale_Best_Practices.pdf
28 https://www.pcisecuritystandards.org/pdfs/PCI_SSC_P2PE_Bluefin-Hillman_Case_Study.pdf

ASSESSING TCO AND ROI OF PCI-LISTED P2PE

TOTAL COST OF OWNERSHIP (TCO)

TCO analysis is a means of calculating the costs of an asset, service, or initiative over its lifespan. Originally, TCO was used for the evaluation of asset purchases, but the application of this concept has been extended to intangible assets and services as well, allowing comparison of dissimilar solutions to the same problem (e.g., buying a widget vs. using a service to perform the widget's function). While TCO formulas may vary depending on the solution being reviewed, an effective calculation must include all visible costs directly related to the project, as well as a reasonable and consistent measure of hidden or indirect costs. Common visible costs include the acquisition cost, setup cost, operating cost, maintenance cost, security cost, regulatory cost, repair cost, disposal cost, financing cost, and depreciation savings. Hidden costs may include opportunity cost, cost of impact to corporate culture or processes, or other costs associated with business risk such as downtime or weighted costs due to impact of new risks.

For example, consider a security project that requires $6,000 in up-front asset costs, $3,000 in one-time configuration and training, and $1,000 in hidden HR costs due to having to replace personnel who are not capable of supporting the new system. The useful life of the asset is ten years, during which there is a $1,000 per year direct cost to maintain the solution. The TCO for such a solution over its ten-year lifespan is calculated as follows:

TCO = Visible Costs + Hidden Costs

TCO = [$6,000 + $3,000 + ($1,000 x 10)] + $1,000

TCO = $19,000 + $1,000 = **$20,000**

In the example above, let's assume that the implementation of the security project is projected to improve compliance efficiencies, with annual savings estimated at $3,000 per year. What is the best way to represent this in TCO? While there are conflicting views on how to account for savings, it comes down to representing the savings in such a way as to best visualize the impact of each respective project. Where discrete compliance efficiencies can be associated to a single asset, the savings is generally reflected as a reduction of the TCO for that project. But when evaluating larger initiatives that affect an entire compliance program, it may be more effective to calculate the total associated compliance cost as a hidden cost for each option being evaluated. This will lead to a higher TCO *dollar amount* (since compliance cost is now associated with each program option), but the more efficient program will have a lower *relative* TCO when compared to other projects. For P2PE, we recommend using the latter approach, as it represents a comprehensive paradigm for compliance, and cost-efficiencies may be recognized in many areas of the organization. However, as long as the methodology is consistent, the end result is the same. This is a distinction from ROI analysis, where net savings are associated with the proposed project itself as its return.

Comparing TCOs is a common way to decide between multiple competing solutions based on their respective costs. However, while this approach only identifies which solution is expected to have the lowest overall cost, it does not directly identify how quickly these efficiencies will justify the new investment.

RETURN ON INVESTMENT (ROI)

An alternate approach is to perform an ROI analysis. The ROI (also known as Rate of Return or ROR) is an expected gain that may be realized through the investment over a specific time period and is expressed as a net gain (or loss) associated with a project over the designated period of time.

Like TCO, in order to calculate ROI, an organization must quantify the direct costs related to an initial project or asset cost. However, net annual savings (due to improved efficiencies or reduced compliance

requirements) is calculated against that investment and used to identify the annual rate of return. Consider the previous example for the project that initially costs $10,000 and also costs $1,000 per year to maintain, but produces $3,000 in new annual savings. The net annual gain is $2,000 -- or $10,000 in five years. Thus, it may be said that the ROI is 100% in five years.

ROI = [(Return - Cost of Investment) / Cost of Investment] x 100

ROI = [($10,000 - $10,000) / $10,000] x 100 = **100% ROI over five years**

Sometimes ROI is expressed as simply the length of time to reach the 100% ROI break-even point, where the net savings equals the initial investment So in the above example, it may be stated that this solution has a **five-year ROI**.

Alternatively, if a solution has an expected life span of 10 years, it may also be expressed as having an **ROI of 200% over the ten-year expected life of the solution**.

ROI = [($20,000 - $10,000) / $10,000] x 100 = **200% ROI over ten years**

The value of the ROI metric better conveys the long-term benefits of a solution, but does so without respect to the initial cash flow impact of an investment. Therefore, measuring TCO and ROI together provides an organization with a holistic view of the impacts to cash reserves as well as the long term return for competing solutions.

IMPORTANT NOTE ON SECURITY VS. PCI COMPLIANCE

PCI DSS is a compliance framework that is designed to protect only the credit card account data that a merchant may encounter. It is not a security standard, per se, as the controls dictated by PCI are a bare minimum necessary to protect one sensitive data type. However, many of the controls required under PCI can also be necessary to support an organization's overall security program.

One of the remaining requirements for PCI DSS v3.2 (even for merchants who use a PCI P2PE solution and qualify to complete the vastly reduced SAQ P2PE) is to conduct annual risk assessments to identify assets, threats, vulnerabilities, risks, and impact (Requirement 12.2). This exercise is imperative to inform security-related decisions, including the use of security controls to protect *other* sources of cyber risk, such as protecting confidentiality of personally identifiable information (PII), patient health information (PHI), intellectual property (IP), or ensuring the availability of critical business services.

In this section, we reviewed two common metrics used by management to inform strategic IT and security investment decisions. The purpose of this section was to propose a common framework for these calculations and provide perspective into the financial benefits of meeting PCI compliance requirements through devaluing of card data through PCI-listed P2PE, thereby providing organizations the flexibility to allocate these resources elsewhere (e.g., providing additional security for other types of data or business risk). It is very important to understand that the purpose of this exercise was not to endorse the arbitrary elimination of security controls where those controls are still necessary to protect sensitive business functions or data.

SAMPLE TCO AND ROI ANALYSIS FOR PCI P2PE SOLUTIONS

Every merchant is different, and costs vary by environment, device, provider, and innumerable other factors. To illustrate the process of reviewing the cost impact for PCI P2PE, we will consider a hypothetical small merchant with eight mobile sales representatives, a retail storefront office with a point-of-sale, a dozen or so non-payment related workstations, and WiFi. For simplicity, we will assume that the merchant does not develop custom software or store cardholder data electronically or physically. In the tables below, the merchant has identified their costs to implement a hypothetical P2PE solution with eight mobile and two

countertop devices, including initial setup costs, recurring costs, program investment, and ongoing compliance costs.

Note: This pricing below does not reflect Bluefin's pricing or any specific hardware products or other services, but has been gathered from publicly available pricing information as an example of one possible TCO / ROI analysis. This information is provided for illustrative purposes only.

TABLE 1: SAMPLE P2PE INVESTMENT

INVESTMENT:	DESCRIPTION	ONE TIME COST:	ANNUAL COST:
Hardware			
POI Devices	In this example, the merchant must purchase approved customer-facing POI devices rather than use the integrated magstripe reader within the POS.	$5,000	$0
POI Injection and Shipping	Injection of P2PE data encryption keys and shipment to or from an approved key injection facility may incur an additional cost.	$400	$0
Service Fees			
Setup Fee	Solution providers may charge an account setup fee or other up-front costs.	$1,000	$0
Monthly Fees	Solution providers may charge a monthly fee for gateway services, licensing, or device management.	$0	$2,400
Per Transaction Fees	Gateway providers may charge a recurring fee per transaction for services including decryption, tokenization, switching, and reporting.	$0	$600
Other Costs			
Employee Training	Implementing new devices and services will require training and an initial period of diminished productivity. P2PE also requires employee to review the P2PE Instruction Manual (PIM).	$800	$0
New Inspection Processes	While inspection of acceptance devices to identify evidence of tampering is a requirement under PCI DSS, the inspection process for P2PE solutions may be governed by the PIM or tools specific to the P2PE provider. Bluefin, for instance, provides the P2PE Manager, an online reporting tool, to facilitate this purpose.	$0	$1,200
	Total	**$7,200**	**$4,200**

In this example, the merchant has also performed an analysis of their PCI DSS compliance costs, noting which costs will no longer be required due to the implementation of a PCI P2PE solution.

TABLE 2: SAMPLE COMPLIANCE COSTS

REQUIREMENTS:	PCI REQ (IF APPLICABLE)	INITIAL COST	ANNUAL COST	INITIAL COST	ANNUAL COST
		Without P2PE		With P2PE	
Hardware					
Firewall for Office Internet with antispoofing, NAT, SPI and IPS	1.1, 1.2, 1.3	$2,000	$100	$1,200*	$50*
Firewall for Wireless LAN	1.2.3	$1,000	$50	$0*	$0*
Layer 3 Switch with VLAN segmentation	1.3, 11.3	$1,000	$50	$750*	$50
Physical Security	9.3	$2,000	$0	$1,000*	$0
Video Surveillance	9.1.1,	$5,000	$500	$3,000*	$250*
Software					
Antivirus	5.1, 5.2	$200	$200	$100*	$100*
Personal Firewalls on laptops and other mobile devices, including initial setup	1.4	$200	$200	$100*	$100*
Security Information/Event Mgmt Use of a SIEM can streamline logging, file integrity monitoring, reporting, and incident response	10.5.5, 10.6, 10.7, 11.5	$4,000	$400	$0*	$0*
Activity Costs These costs represent outsourcing or hourly wage costs to perform required activities					
Network Admin Functions including reviewing default security, firewall rules, scanning for rogue WiFi	1.1, 2.1, 4.1.1, 11.1	$1,000	$500	$1,000	$500
Systems Admin Functions including default security, access privileges, multifactor authentication, audit logs, monitoring systems	2.1, 2.2, 2.3, 2.4, 5.3, 6.1, 6.2, 6.4, 7.1, 7.2, 8.1, 8.2, 8.3, 8.5, 10, 11, 10.6	$0	$20,000	$0	$10,000
Device Management Functions	9.9	$0	$0	$1,000	$1,000
Policies & Procedures including drafting, review, update, and dissemination of policies	1.5, 2.5, 4.3, 5.4, 6.7, 7.3, 8.8, 9.10, 10.9, 11.6, 12	$2,000	$400	$500*	$100*
Training and Hiring Employee security training, tamper detection, and background checks	4.2, 8.4, 9.9.3, 12.6, 12.7	$4,000	$2,000	$1,000*	$500*
SAQ Compliance Assessment	All	$0	$1,000	$0	$0*

REQUIREMENTS:	PCI REQ (IF APPLICABLE)	INITIAL COST	ANNUAL COST	INITIAL COST	ANNUAL COST
Services					
ASV Vulnerability Scans	11.2	$0	$400	$0	$200*
Penetration Testing to confirm segmentation controls	11.3	$0	$2,000	$0	$600*
	Total:	**$22,400**	**$27,800**	**$9,650**	**$13,450**

* These controls may no longer be required, or effort may otherwise be reduced when using PCI P2PE; however, they may still be needed to protect other sensitive data or functions. While not always recommended, some businesses may choose to use free or lower-cost alternatives (such as freeware antivirus and personal firewall products) to address these remaining risks instead of more expensive commercial off-the-shelf (COTS) products.

Sample Calculations

Assuming a ten-year life span, the TCO for the current state and P2PE solutions are shown below:

TCO = Visible Costs + Hidden Costs

$\mathbf{TCO_{current}}$ = $22,400 + ($27,800 x 10)
$\mathbf{TCO_{current}}$ = $22,400 + $278,000
$\mathbf{TCO_{current}}$ = **$300,400**

$\mathbf{TCO_{P2PE}}$ = ($7,200 + $9,650) + [($4,200 + $13,450) x 10]
$\mathbf{TCO_{P2PE}}$ = $16,850 + $176,500
$\mathbf{TCO_{P2PE}}$ = **$193,350**

The TCO of the P2PE solution in this example is less than 2/3 that of the current state and should therefore be selected.

Similarly, calculating the ROI for the same solution over the same period would be performed as shown below. First, the return must be calculated, which is the total savings realized over ten years:

$\mathbf{Return_{P2PE}}$ = (Initial Cost Savings) + (Annual Cost Savings x 10)
$\mathbf{Return_{P2PE}}$ = ($22,400 - $9,650) + [($27,800 - $13,450 - $4,200) x 10]
$\mathbf{Return_{P2PE}}$ = ($12,750) + [($10,150) x 10]
$\mathbf{Return_{P2PE}}$ = ($12,750) + ($101,500)
$\mathbf{Return_{P2PE}}$ = **$114,250**

The return is then plugged into the ROI formula to determine the rate of return:

$\mathbf{ROI_{P2PE}}$ = [(Return - Cost of Investment) / Cost of Investment] x 100
$\mathbf{ROI_{P2PE}}$ = [($114,250 - $7,200) / $7,200] x 100
$\mathbf{ROI_{P2PE}}$ = **1,487% ROI over ten years**

At this rate, the organization should expect to recoup their investment nearly 15x over the life of the solution.

Of course, this is just an example to demonstrate the calculations, and again we remind management that it is imperative to perform a full assessment pertaining to the impact of reduced controls on the security of critical systems and data. Keep in mind that the primary cost savings is through the flexibility gained by returning security decisions to the organization, but that those decisions must be made with full knowledge of the risks they incur.

BLUEFIN P2PE

HISTORY

Bluefin Payment Systems provides financial technology solutions for merchant security, compliance, and payment processing. Among their suite of products is Bluefin P2PE, which operates both within their proprietary omnichannel payment gateway, PayConex, and also as a stand-alone decryption service, Decryptx, which enables non-validated processors, acquirers, and gateways to provide the Bluefin PCI-validated P2PE solution through their own platforms

PCI P2PE

In March 2014, Bluefin became the first P2PE solution provider in North America to be validated to the P2PE standard and listed by the PCI SSC.[29] At that time, there were only two other solutions available in the world. At the time of this publication,[30] the Bluefin P2PE solution is one of 25 validated solutions available worldwide and one of only 15 validated solutions that are marked as available within North America. Bluefin holds four issued patents related to its P2PE Decryption as a Service (Daas) solution, including "Systems and Methods for Creating Fingerprints of Encryption Devices,"[31] "Systems and Methods for Decryption as a Service,"[32] "Systems and Methods for Decryption as a Service via a Message Queuing Protocol,"[33] and "Systems and Methods for Decryption as a Service via a Configuration of Read-Only Databases."[34]

As Bluefin's QSA (P2PE), Coalfire has performed Bluefin's PCI DSS Report on Compliance (ROC) and PCI P2PE Report on Validation (P-ROV), including interviews, observation, documentation review, log review, technical data discovery and analysis, and on-site physical audit of all relevant technical, physical, and procedural security controls. It is the assessment of Coalfire that Bluefin is a fully-compliant PCI DSS service provider and PCI P2PE solution provider.

Bluefin's P2PE solution is also unique in that they offer encryption devices for multiple channels, addressing specific business needs for a number of customer verticals:

- The ID TECH SecuRED and SREDKey are encrypting magnetic stripe readers (MSR) that connect via USB keyboard emulation, allowing them to interoperate with Bluefin's PayConex virtual terminal and hosted payment pages for secure processing without the use of software. The SREDKey also adds support for keyed entry of card data, which is required for P2PE in MOTO environments such as contact centers.
- In 2014, Bluefin was the first P2PE solution provider in the world to validate a mobile secure card reader. In 2016, they also validated the BBPOS WisePad, Anywhere Commerce Nomad 2.0, and Ingenico iCMP, providing more mobile devices vendor support than any other PCI P2PE solution provider,[35] including support for iOS and Android apps and mobile SDKs.
- Bluefin offers support for leading Ingenico RBA devices, such as the versatile iPP320 and iPP350; the multilane touchscreen devices iSC250, iSC Touch 250, and iSC Touch 480; the unattended iUC285; and the mobile iCMP.

29 https://www.bluefin.com/bluefin-news/pci-validated-p2pe-mean/
30 https://www.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions
31 U.S. Patent 9,355,374
32 U.S. Patent 9,461,973
33 U.S. Patent 9,531,712
34 U.S. Patent 9,531,684
35 https://www.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions

- Bluefin’s P2PE solution includes the P2PE Manager, a cloud-based device management platform that assists merchants with complying with device management, device inspection, and chain of custody functions. When used in conjunction with the PIM, P2PE Manager supports the merchant’s efforts to comply with PCI DSS requirements 9.9, 9.9.1, and 9.9.2.
- Bluefin's patented PCI-validated P2PE Decryption as a Service (DaaS) product, Decryptx, enables non-validated processors, acquirers, and gateways to integrate to Bluefin’s PCI-validated P2PE solution and provide the solution on the organization’s own platform and direct to their clients.
- Through Bluefin’s Independent Software Vendor (ISV) program, software and service providers may integrate to Bluefin’s PayConex payment platform, adding the value of PCI P2PE to their transaction capabilities.

The PCI P2PE version 2.0 standard is divided into six major domains and two additional annexes, each of which comprises a number of controls that are relevant to entities that provide a component of a fully-functioning P2PE solution. Below is a breakdown of the standard and how each domain applies to Bluefin's solution:

TABLE 3: BLUEFIN P2PE COMPLIANCE REQUIREMENTS

Domain/Annex	Description	Controls	Applicable
Domain 1: Encryption Device and Application Management	Domain 1 must be met by entities providing POI devices that will be used for the initial acceptance of a credit card transaction. These devices may be card present terminals or card-not-present data entry devices. This domain also applies to the installation of any software onto the device (subject to Domain 2 validation) and use of any terminal management system that may impact the secure configuration of these devices. **Bluefin has validated 12 PTS POI devices to Domain 1, representing one of the largest device selections among current listed solutions.**	44	**Yes**
Domain 2: Application Security	These requirements are applicable for use of POI software application (other than the approved PTS firmware) that may have access to account data. **Bluefin's Solution includes validation of Ingenico Retail Base Application v12.0 and v14.0.**	61	No
Domain 3: P2PE Solution Management	Certain controls are applicable to the solution provider for managing the solution and govern the relationships and communications with any third-party providing other components of the solution.	20	**Yes**
Domain 4: Merchant-managed Solutions	These requirements only apply to merchants, who wish to utilize a PCI P2PE solution, but require access to the decryption environment. **Bluefin does not offer a Merchant-Managed Solution at this time.**	15	No
Domain 5: Decryption Environment	The decryption environment must have mechanisms in place to control physical and logical access and policies that govern custody and operation of approved HSMs. **Bluefin operates multiple redundant decryption environments.**	89	**Yes**
Domain 6: P2PE Cryptographic Key Operations and Device Management	Key management practices for P2PE solutions are governed by Domain 6, associated with the creation, transfer, injection, and destruction of keys, as well as their use in encryption and decryption of data. **Bluefin P2PE has been validated to support two key injection facilities in conjunction with its Domain 6 requirements.**	145	**Yes**
Domain 6 Normative Annex A: Symmetric-Key Distribution using Asymmetric Techniques	Solutions that use remote key injection must ensure that keys are properly protected and that remote injection processes are secured to protect sensitive keys from interception. **Bluefin does not provide remote key injection at this time.**	110	No
Domain 6 Normative Annex B: Key-Injection Facilities	Key injection facilities (KIFs) that handle sensitive key material that wish to validate as component providers must undergo additional validation to controls that protect the encryption keys from compromise. **Bluefin is not a KIF component provider.**	175	No
PCI P2PE Requirements Applicable to Bluefin P2PE Solution:		**298**	

While Bluefin is not the author or manufacturer of the software or hardware itself, they are responsible for validating the compliance of these elements and that the service delivered through them complies with the relevant standards.

The following PTS POI devices with certified SRED support have been validated by Coalfire for use with Bluefin's PCI P2PE solution:

TABLE 4: BLUEFIN P2PE VALIDATED DEVICES

PTS #	Make	Model	Features	Primary Industries
4-10144	ID Tech	SecuRED	MSR, USB	Retail, Unattended
4-10156	ID Tech	SREDKey	MSR, Keypad, USB	MOTO, Retail
4-30123	Infinite Peripherals	Prima M	MSR, Audio Jack	Mobile, Retail
4-20142, 4-20184	Ingenico	iPP310, iPP320, iPP350	MSR, ICCR, CTLS, PIN, Keypad, USB, RS-232, Ethernet	Retail, MOTO, Unattended
4-30062, 4-30135	Ingenico	iSC250, iSC Touch 250	Touchscreen, MSR, ICCR, CTLS, PIN, Keypad, USB, RS-232, Ethernet	Retail, Unattended
4-30098	Ingenico	ISC Touch 480	Touchscreen, MSR, ICCR, CTLS, PIN, Keypad, USB, RS-232, Ethernet	Retail, Unattended
4-30161	Ingenico	iUC 285	MSR, ICCR, CTLS, USB, RS-232, Ethernet	Unattended
4-20235	Ingenico	iCM 122 (iCMP)	MSR, ICCR, CTLS, PIN, Keypad, Bluetooth, WiFi	Mobile, Restaurant
4-10146	BBPOS	WisePad, WisePad W300	MSR, ICCR, CTLS, PIN, Bluetooth, WiFi	Mobile, Restaurant
4-10149	Anywhere Commerce	Nomad 2.0	MSR, ICCR, CTLS, PIN, Bluetooth, WiFi	Mobile, Restaurant

METHODOLOGY OVERVIEW

As Bluefin's QSA (P2PE), Coalfire has performed Bluefin's PCI DSS v3.1 Report on Compliance (ROC) and Bluefin's PCI P2PE v2.0 Report on Validation (P-ROV) and reviewed the specific security controls, systems, networks, audit logs, policies, documentation, and cryptographic methodology used to deliver its PCI-compliant services.

Within the scope of these engagements, Coalfire has also worked directly with Bluefin's vendors including Ingenico, Verifone, Spencer Technologies, and CDE Services to assess their responsibilities and security measures to meet the relevant compliance requirements.

Tools used to perform evidence capture specific to this white paper include:

- Wireshark
- Ekahau Wireless HeatMapper
- Netsparker
- Direct observation of systems and data stores using native and third-party console and admin tools

ABOUT THE AUTHORS

Dan Fritsche CISSP, PA-QSA(P2PE), QSA(P2PE) | VP, Solution Architecture, Coalfire Systems, Inc.

Dan Fritsche has two decades of experience in application and network security architecture. As the Vice President of Solution Architecture at Coalfire, Dan and his team are responsible for translating requirements created by IT risk and compliance mandates into business-centric cyber solutions strategies. His experience covers a broad spectrum of security disciplines including payment security, vulnerability scanning, application security, penetration testing, mobile security, software development, encryption, compliance, anti-virus, and IDS/IPS.

Tim Winston CISSP, CISA, QSA(P2PE) | Product Director, P2PE, Coalfire Systems, Inc.

As the Practice Director for Coalfire's P2PE program, Tim Winston leverages his experience advising and assessing cryptographic security, identity management, cloud platforms, e-commerce payments, and retail systems to assist solution providers and merchants maximize the benefit of their PCI P2PE strategy.

ABOUT COALFIRE

As a trusted advisor and leader in cybersecurity, Coalfire has more than 15 years in IT security services. We empower organizations to reduce risk and simplify compliance, while minimizing business disruptions. Our professionals are renowned for their technical expertise and unbiased assessments and advice. We recommend solutions to meet each client's specific challenges and build long-term strategies that can help them identify, prevent, respond, and recover from security breaches and data theft. Coalfire has offices throughout the United States and Europe. www.coalfire.com