Guidance on Improving Security in the Interim to a Point to Point Encryption Implementation

January 26, 2021

Version 1.0

CONEXXUS
solve forward

Document Summary

Deploying and managing a resilient cybersecurity infrastructure is the first line of defense against criminal elements who may be looking to compromise an electronic payments system that has not yet moved to a point to point encryption (P2PE) infrastructure. If you are a merchant concerned about the security of your payment information, kept up at night by what the cyber criminals are planning next, feel P2PE is someone else's responsibility, or is just a project for next year this document will provide some insight into steps toward P2PE and explain why P2PE is an ongoing effort. This document will discuss the devices, technology, and areas of focus that a convenience or retail fueling merchant should understand to provide that line of defense until a full P2PE implementation is available and fully implemented.

Contributors

Alan Thiemann, Conexxus

Brian Russell, Verifone

Charles Aschenbeck, Shell

Chuck Young, Impact 21

Clerley Silveira, Conexxus

Dan Harrell, Invenco

Donna Perkins, Conexxus

Jim Shepard, Phillips 66

Kevin Eckelkamp, Comdata

Kim Seufer, Conexxus

Sam Pfanstiel, ControlScan

Sharon Scace, WEX

Sue Chan, W Capra

Revision History

Revision Date	Revision Number	Revision Editor(s)	Revision Changes
January 26, 2021	Version 1.0	Kim Seufer, Conexxus	Final Release Version
January 14, 2021	Draft 0.13	Kim Seufer, Conexxus	Updated copyright date and responded to comments from public comment period
November 17, 2020	Draft 0.12	Kim Seufer, Conexxus	Clean ups for review
October 13, 2020	Draft 0.11	Kim Seufer, Conexxus	Created Glossary
September 1, 2020	Draft 0.10	Sharon Scace, WEX	Changes during Group meeting
August 27, 2020	Draft 0.9	Kim Seufer, Conexxus	Clean up from legal review
August 23, 2020	Draft 0.8	Alan Thiemann, Conexxus	Legal Review

		Allie Russell, Conexxus	
July 7, 2020	Draft 0.7	Kim Seufer, Conexxus	Clean up comments and add contributors list
June 30, 2020	Draft 0.6	Dan Harrell, Invenco Sharon Scace, WEX Kim Seufer, Conexxus James T. Shepard, Phillips 66 Chuck Young, Impact21	Review and Updates
May 17, 2020	Draft 0.5	Dan Harrell, Invenco	Review and Updates
April 21, 2020	Draft 0.4	Sharon Scace, WEX	Updates during meeting
April 12, 2020	Draft 0.3	Jim Shepard, Phillips 66 Sharon Scace, WEX	Updates sent in after meeting
March 18, 2020	Draft 0.2	Sharon Scace, WEX	Updates during meeting on March 10, 2020
March 4, 2020	Draft 0.1	Sharon Scace, WEX Kim Seufer, Conexxus	Initial Draft

Copyright Statement

Disclaimers

Conexxus makes no warranty, express or implied, about, nor does it assume any legal liability or responsibility for, the accuracy, completeness, or usefulness of any information, product, or process described in these materials. Although Conexxus uses reasonable best efforts to ensure this work product is free of any encumbrances resulting from third party intellectual property rights (IPR), it cannot guarantee that such IPR does not exist now or in the future. Conexxus further notifies all users of this standard that their individual method of implementation may result in infringement of the IPR of others. Accordingly, each user is encouraged to carefully review its implementation of this standard and obtain appropriate licenses where needed.

Table of Contents

1 Introduction

With the introduction of PCI and the migration of payments to EMV, including outdoor EMV, the retail fuel market has seen many changes related to security technologies and processes. Various iterations of PCI requirements govern elements of how payment devices are designed and manufactured, as well as the security processes that surround a retailer's IT infrastructure. These control improvements are implemented in order to secure the cardholder data environment which is the basis of PCI scope. PCI is largely focused on providing a means to keep cardholder data and other related payment information secret. EMV, on the other hand, provides a new tokenization/encryption security tool which limits an attacker's ability to produce and use fraudulent cards.

P2PE provides a mechanism to encrypt data at the point of card entry and is intended to keep data protected until it reaches the payment processor host for authorization. Keeping data encrypted is fundamental to limiting PCI scope at a retail location, because if that is accomplished, no card data is accessible at the retail location. This helps to keep point of sale (POS) and other systems out of scope because they will not have access to cardholder data.

While processors and technology providers seek to complete their certifications and upgrades to EMV, and ultimately to a certified P2PE infrastructure, merchants need to continue to invest in technology and processes that contribute to a strong cybersecurity strategy. Cybersecurity is not a "once and done" project or initiative. Operating cybersecure infrastructures requires never-ending maintenance and continuous improvements to keep up with evolving security objectives for ensuring the confidentiality, integrity, and availability of data, networks, and information systems.

The remainder of this document will focus on various areas of the retail system and related processes:

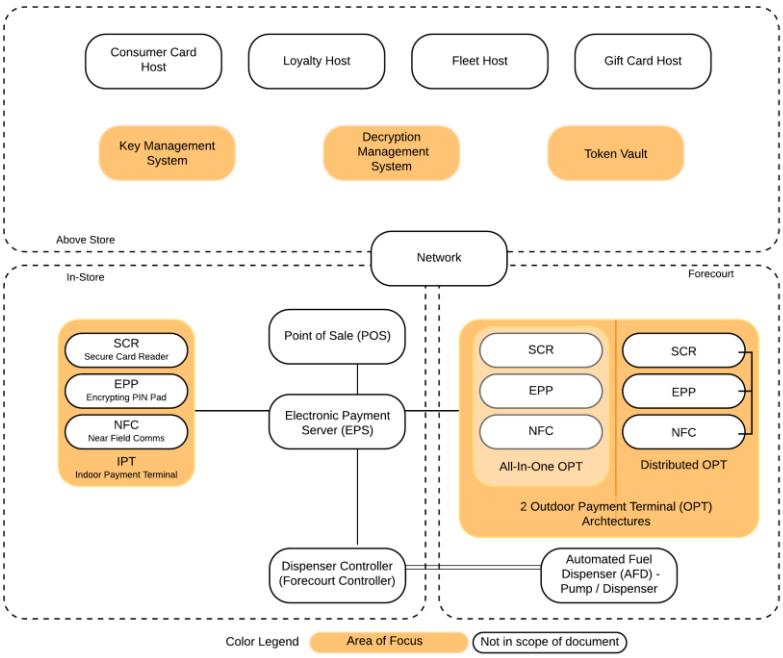
- Where we are today;
- Working with vendors;
- New considerations and strategies; and
- Developing a comprehensive interim strategy.

2 Where We Are Today

2.1 Current Architecture

The convenience or retail fueling site is made up of Automated Fueling Dispensers (AFDs), a Dispenser Controller (also known as a Forecourt Controller), POS, Point of

Interaction (POI), and a Network Communication Connection. Optionally, the site may include an Electronic Payment Server (EPS). The site may connect to one or more of the following: loyalty host, gift card host, fleet card issuer host, or consumer card host.



This document will focus on the elements of this system which participate in the process of securing card or personally identifiable information (PII) data which include the POI, Key Management System/Strategy, Decryption Management System (DMS), and optionally a Token Vault System.

2.1.1 Point of Interaction (POI)

A POI requires focus because it represents the part of the system where the payment data, and potentially PII, are entered by the customer. There are two categories of POI in the convenience and retail fueling industry:

- Indoor Payment Terminal (IPT) - typically found in attended environments. In this case, the components that make up the POI are usually a single physical unit.
- Outdoor Payment Terminal (OPT) - typically for unattended environments (e.g., pay at the pump, pay at the carwash). In an OPT, the components are more likely to be separate.

A POI is typically made up of:

- Secure Card Readers (SCR);
- Encrypting PIN Pad (EPP);

- Near Field Communication (NFC) (RFID/Tap/Contactless) Reader;
- Secure Display or Screen – this is required for secure prompting such as PIN;
- Non-secure screen (optional);
- A PCI-PTS certification; and
- A Secure Read and Exchange of Data (SRED) certification.

POI – Integrated (all one unit) or Separate devices (requires integration)

	Integrate (Single Unit)	**Separate Devices**
Benefits	• Able to provide tamper resistant and tamper evident housing to contain cryptographic functions • Simplified serviceability	• Can be built to fit the space (retrofits into existing form factors) • If a part is compromised other parts may still function
Drawbacks	• Adequate space for single unit • Less modular • When compromised all elements are compromised	• Integration requirements • Service complexity

The POI is an important component to the cybersecurity strategy as it is almost always the place where the data that needs to be protected is entered into the system. Now that most of the new EMV POIs are running over the Transmission Control Protocol/Internet Protocol (TCP/IP), new considerations around network security need to be understood.

2.1.2 IP-Enabled Outdoor POIs (Installed in Fuel Dispensers) Are Introducing New Cybersecurity Risks

IP-enabled POIs that are being installed with the move to outdoor EMV utilize TCP/IP for communication. Adoption of the TCP/IP protocol has made it easier to get information to and from the fuel dispenser. This protocol is more widely understood by cyber- criminals, who are looking to steal electronic payment card data (known as a harvesting attack); therefore, additional network security measures are needed to keep electronic payment data safe and secure.

2.1.3 Wireless on the Forecourt

One of the big disadvantages of using Wi-Fi, or other wireless communications, on a forecourt is that a malicious actor can sit close by and monitor those communications

without being detected. In such a case, the hacker could have infinite time to inspect the traffic and find a way to get to the parts of it that they want. A retailer who is looking to include Wi-Fi (or any wireless communication) to the payment components on a forecourt, must make sure that they are using strong cryptographic elements and consider frequent cryptographic key rotation so that it will not be easy for criminal actors to gain access to the data flowing over the network.

2.2 Evolving Payment Mechanisms

This section looks at the various methods that are currently available to pay for goods at a site. This is not to suggest that one is better than the other, rather it is intended to provide options for review based on meeting business needs.

Some key points to keep in mind:

- What is the impact on the customer? Will the use of a particular technology create a practical burden on and thus alienate some customers?
- Is my customer willing to pay inside rather than at the pump?
- Impact on international tourism (i.e., payments from outside the US)
    - If I turn on Address Verification Service (AVS), will this confuse some or many of my customers?
    - If I do not install EMV readers, will my customers be able to buy fuel?
- How does my customer want to pay? Some customers prefer mobile payments options via a smart device. This method of payment may negate the need for accepting full account numbers via a POI device, offsetting the value of a P2PE investment.
- Does this payment solution lead to better security?

2.2.1 Payment Device Considerations at the Site

Each electronic payment terminal is the point of entry of customer data at a site. Skimmers and other listening devices are easily installed and difficult to detect in some payment terminals. Regular monitoring of all POIs is a critical line of defense and a Payment Card Industry Data Security Standard (PCI DSS) compliance obligation.

2.2.2 Chip Readers (EMV) Rather Than Magstripe Readers

EMV is intended to help with counterfeit/white plastic fraud. EMV does NOT provide security for the payment card data as it travels from the card reader to the network for authorization by the processing host. As such, each merchant must make sure that it has the right security strategy in place to protect data as it migrates over the various network segments to obtain an authorization with the host.

As the U.S. migrates to EMV, there is also likely to be some consumer training on how to use these new devices and the processes that they may require, such as leaving the card inserted for a period of time. Signage, graphics, instructional banners, and even on-device videos can help customers make this transition with less frustration.

The implementation of P2PE along with EMV provides retailers a stronger mechanism for keeping card data safe from the initial point of entry to the payment processor.

2.2.3 EMV Contactless (Tap)

When implemented correctly, contactless payments, via card or mobile phone, provide a great user experience for customers. EMV contactless payments use similar authentication mechanisms as EMV contact payments and so they are better at preventing counterfeit fraud than their magstripe equivalents. The technology needed for P2PE can work equally well for contactless payments, and so a retailer's investment in P2PE should also cover this method.

When used with a mobile device (e.g., smartphone), contactless payments can offer some built in advantages. For instance, tokenization is largely built into products like ApplePay and SamsungPay. This means that the consumer and the retailer benefit from the use of a one-time use token (which means it cannot be used in another transaction) without having to implement any of the security themselves. Another benefit of contactless on a mobile device is the implementation of a Cardholder Verification Method' data element (CVM) that is built into the phone. When implemented completely, this means the consumer does not have to touch the payment device to enter postal code, which feature might be especially important in a post COVID-19 world.

2.2.4 Mobile Payments with Mobile Payment Processing Application (MPPA)

The Conexxus/IFSF Mobile Standard includes MPPA as an alternative to NFC "tap and go" mobile phone payments that has been evolving over the last few years. In mobile data payment, meaning it is using the consumer's mobile network connection instead of the local network for the authorization, the mobile app generally is using a token to get the card details from a token vault stored in a secure facility. These card details are used to obtain authorization of the transaction from within the secure host facility. Once an authorization is received, the mobile app cloud services sends an authorization to the forecourt controller of the store and updates the mobile application with progress. All of these authorization processes happen outside of the physical retail store and keeps the store out of PCI scope as to that transaction. Using mobile payments with tokens and

strong encryption mechanisms provides a more secure infrastructure for customer and payment data.

There are a few disadvantages to mobile browser payment. For one, they do not appeal to all customers, and it does require the customer to have a smartphone with an app that works at the retail location. Additionally, there are a few customer experience problems that can emerge if there is a problem with the mobile network, the site network, or any of the application interfaces in between. One bad customer experience can turn a reluctant customer into one who will never use the app again. Finally, some card brands view a mobile app payment as a card not present (CNP) transaction, which will likely increase the interchange fee. Over time, it is likely that mobile payment solution providers will overcome these hurdles and open a new world of opportunities regarding retail payments.

An advantage of the mobile data is that a consumer is able to associate a number of other payment methods (other than card brands) to the token stored by the phone. This opens up avenues for providing non-branded payment cards, ACH, and even cryptocurrency transactions in the future. There are significant hurdles to open up such a future, but by offering these additional avenues for payment, retailers have a means to look for lower transaction fees associated with these other payment methods.

2.3 Emerging Technologies That Have Moved the Forefront

Over the last 10 years, there have been many advances in security technologies that have been made available. Not only do these technologies provide better methods to secure data, but they have been simplified and made more cost effective so that retailers can more easily include them in their cybersecurity strategy.

Many of these technologies are integrated as a part of other elements of a cybersecurity strategy, including P2PE. They are mentioned here because their usage can be applied to an overall cybersecurity strategy, with or without P2PE.

2.3.1 Key Management System

When data is encrypted in between two points, it is necessary for each side to have the proper information to encrypt and decrypt data. This usually breaks into two important components: the algorithm with which to encrypt data and the key to decrypt it. The algorithm is the mathematical routine that is performed on data to encrypt it. An algorithm establishes a “lock” which makes the derived data output of the algorithm unique and only understandable by a system that has the necessary key to decipher data.

Generally, there are two types of keys and algorithms in use today: symmetric and asymmetric. Using symmetric keys means that both parties in the system are using the same keys. In this case, the keys need to be kept in a secure place on both sides of the encryption/decryption process. This can be very challenging if one of those sides is not equipped with the technology and processes to keep the key safe. Asymmetric keys and algorithm techniques usually use key pairs, one private and one public. In this case, only the private keys need to be kept in a secure location, and thus the additional security is only required on one side of the encryption/decryption process.

Keeping keys secure is the fundamental purpose of the Key Management System. In the US, the management of keys is governed by a national standard (X9.24-Parts 1 and 2). There are many concepts embedded in the concept of Key Management (e.g., key generation, activation, deactivation, changes). For purposes of this Guide, it is sufficient to know that any good encryption system is going to have a Key Management System at its core.

Here are some examples of the keys used in a convenience store transaction:

Key	**Brief Explanation**	**In scope?**
Data Encryption Keys	Key used to encrypt from POI to DMS; also, the fundamental keys used for P2PE	Yes
Debit Encryption Keys	DUKPT Keys for accepting debit (injected into the EPP)	No
EMV Keys	EMV keys do not relate to cardholder data encryption, but to the verification of digital signatures confirming the integrity of the chip itself and issuer communications for data verification during EMV (insert and contactless) transactions.	No
Remote Key Loading Keys	Signed public private key pairs used for authentication and remote loading of data encryption keys. Each of these functions needs a unique key pair (it is not appropriate to use the same key pair for both functions).	Yes

The entries marked as in scope 'Yes' are included in this document as they relate to P2PE. The entries marked 'No' are included to emphasize other keys which, while critical to security, are not used in P2PE.

2.3.2 Decryption Management System

After data is encrypted by a POI, that data is sent to a Secure Cryptographic Device (SCD) that can decrypt data and either use the exposed data in a secure location or sometimes it is re-encrypted with another key and sent to the next decryption point in the chain (hence point to point encryption). The intermediate decryption point may be needed to inspect site-level encrypted data for fleet information (such as prompting) or primary account number (PAN) information for routing. Wherever the decryption points are maintained, they should be in a secure environment in conjunction with an SCD such as a hardware security module (HSM) to ensure the security of the keys that are being used.

2.3.3 Tokenization Vault

A tokenization vault is a system for leveraging and storing a token (any bit of information used in lieu of original information so that the original information such as a customer ID, loyalty ID, hash or other data, is protected) to "look up" other information such as associated card or loyalty data. Typically, a token vault is highly secured and would fall under strict PCI scope if it contains "sensitive card data" associated with any of the card schemes (See X9.119 – Part 1). This means that all of the security around this sensitive card data is focused in this one, controlled place, rather than distributed amongst all the retail locations.

Typical implementations of a token vault include mobile payments, proprietary RFID, and barcode loyalty schemes. When a token is used, it means that no card data is exposed at the store, only the token and the associated authorization information – and means that anyone able to obtain this information would NOT have access to a consumer's sensitive card information.

2.4 Where We Are Today

There have been a number of security developments that have evolved since the migration to EMV began. It is important for retailers to understand these product concepts and technology introductions to know what tools are at their disposal to protect critical data at their stores and throughout their network. While P2PE offers a proven mechanism to protect data, it may be some time before all retailers implement this technology. With the other technologies around encryption, evolving payment methods, and the processes to go with them, retailers have tools that can become part of

their cybersecurity strategy to protect their data and networks in the meantime. Before discussing future strategies, this Guide will examine some of the circulated myths that have evolved around the responsibility of securing data at retail locations.

3 Working with Vendors

As a retailer, both a cybersecurity strategy and a P2pE implementation have many facets to be considered. It is important that retailers be informed on all elements of the solutions and strategies that can protect the information in their businesses. In most cases P2PE solutions are provided by vendors such as host POS, POS provider, Managed Network Service Providers (MNSP); this section discusses the relevant questions to keep in mind.

3.1 Ask the Vendor

P2PE has many components to it and involves some of the technology already mentioned in previous sections. It also affects many points in a retailer's overall technology strategy, and each point must work with other points to provide a complete P2PE solution. As a retailer, make sure that you have considered all these points when making a final choice on your overall P2PE strategy. P2PE is not a "one and done" project. In reviewing a solution, a retailer should ask the following questions:

- What is the cost to obtain P2PE services from my vendor, compared to traditional vendor services?
- Is it a one-time cost, or is it a recurring cost?
- How easy is it to change/update P2PE implementations?
- Does it only support the major card brands or will it apply to all mobile payment apps?
- Does it impact the ability to accept gift cards?
- Does it impact the ability to accept any local cards?
- Does it impact the ability to accept fleet cards? (Branded or 3rd Party)
- Does it impact the loyalty program(s) used at the site?
- How will my Acquirer/Processor view this P2PE service from a compliance perspective?
- Will the acquirer/auditor reduce PCI scope if I implement this solution?
- Is it a solution approved by PCI P2PE? Is it a solution implemented consistent with X.9.119 – Part 1? (both questions can be asked in a request for proposal (RFP).
- Does it improve my overall cybersecurity plan?
- What is the degree of difficulty for me to manage this P2PE solution?
- Am I merely trading PCI compliance/assessment expense for P2PE management expense?

P2PE provides an effective means for the future to secure the cardholder data within the stores. However, there are many complex questions that need to be evaluated to ensure that a truly secure and cost-effective solution. There are likely to be multiple vendors associated with your P2PE solution: Host/processor, POS/EPS, POI, and maybe others. Thing about the aspects above as it relates how all of these elements will come together and whether it provides the security desired and a roadmap to meet future needs.

3.2 Retailer Responsibility

Choosing an effective cybersecurity strategy and P2PE solution is the responsibility of the retailer and the retailer's IT team.

- Operating cyber-secure and within PCI compliance is the responsibility of all merchants who accept a major card brand's payment card (i.e., Visa, MasterCard, American Express, Discover) as a method of payment.
- If your merchant ID is on it, it's your responsibility.
- A payment card data breach can quickly translate to loss of revenue and loss of livelihood.

4 New Considerations / Strategies

This section will review some new technologies, strategies, and processes that should be consider as part of an overall cybersecurity strategy. Adding layers of security to the approach will strengthen defenses against any kind of attack and, when implemented correctly, complement a retailer's implementation of P2PE.

With all the new features that can be offered at a site (e.g., loyalty, marketing, mobile payments) come new challenges related to the security of this data.

What if there is no desire to change anything? What if a retailer took a stance of "if it ain't broke, don't fix it"? The risk here is that inaction exposes a retailer to a loss of data that is nearly undetectable, until the eventual greater damage is done. There have already been well publicized examples where criminals have found ways to get to critical data, and they will continue to exploit the easiest targets first.

New technology does have its own issues, risks, and maintenance requirements. Therefore, it is important to understand what those risks are as you pursue upgrades to your cybersecurity strategy. To protect the retail brand and customer information, retailers must leverage the latest tools and processes that are available to them. This section will discuss various considerations and processes that retailers should consider in the implementation of a cybersecurity defense or when selecting a vendor who provides various components of the system that a retailer uses.

4.1 Encryption Key Management

In a previous section, we discussed the importance of the management and distribution of encryption keys. While this system provides a tool for performing these operations, a retailer should be considering all the processes that it needs to have in place to manage keys appropriately, including the following considerations:

- How to manage the full lifecycle of cryptographic keys, including generating, using, storing, archiving, and deleting keys;
- Important players in this system are the registration authority (RA), certificate authority (CA) and possibly a third-party validation authority (also a CA); and
- In order to ensure PCI DSS compliance scope reduction, it is critical that the Merchant does not have access to cryptographic keys capable of decrypting sensitive authentication data (SAD).

A best practices way to "keep secrets secret" is using Public Key Infrastructure (PKI). In the simplest of terms, PKI uses a system of certificates and keys to authenticate endpoints and encrypt data in a methodical and maintainable way. Used appropriately, each endpoint can ensure that all the data it receives is only meant for it.

The implementation of a good key management system is the heart of good cryptography. This system can be used as the foundation to authenticate and encrypt network connections using Transport Layer Security and Authentication (TLS), encrypting critical data in-flight or at-rest, and any other place in the system where the foundation is keeping secrets in a very secure place.

4.2 Cryptographic Strength

When sending data from one point to another, the system should ensure that if the data is intercepted (i.e., it is traveling across public networks), that it is encrypted in a manner and strength that is appropriate for the type or data it is protecting.

- This is an evolving issue, which involves looking at key lengths and strength of the encryption algorithm used (DES, AES to ECC and beyond).
- Key length: the longer, the better -- but as with algorithm there is a tradeoff for speed
- Algorithm: the more processor time it takes, the better – however, this needs to be balanced against the lifetime of the POI and available computing "horsepower" available at any given point in time for decrypting data (i.e., advances in quantum computing may eventually reducing the time to decrypt).
- As computing power increases, these systems are likely in need of updating to better combat attempts to compromise the system.

Making these transitions in the future can be a complicated, synchronized task. It is important when making major changes to the system to consider the timeframe that a

chosen cryptographic strength level will exist before the next "big" change. Generally, a retailer should choose whatever the currently accepted best practice is with an eye on what is coming next, and when that change (to what is next) is likely to impact their system.

4.3 Tokenization of Data

As defined earlier, tokenization is a process to substitute sensitive data with a non-sensitive equivalent and make the data unusable if it does happen to be captured by someone/some system. This is a critical component of P2PE, but is also useful technology in other processes to keep sensitive data safe.

A tokenization strategy should be part of the overall cybersecurity roadmap, and at a minimum will be realized with a retailer's implementation of P2PE. Here are some considerations for a tokenization strategy:

- With traditional card, or chip, based payments, there is still a need to protect the data as it is read. This is why the PCI SRED is an important requirement for devices to meet. It ensures that the card data is encrypted in a secure place in the device and bad actors will not have access to it before it is encrypted. After the data is tokenized it is no longer useful to foreign systems.
- Storage tokens prevent clear data from being accessed by other systems.
- Payment tokens are generated in real-time and are specific to the merchant/environment.
- Data tokenization is also a critical way to keep any PII private.

Format preserving tokens can be used to alleviate any changes needed to any other parts of the system, like the EPS. This method ensures that the token must match the original data for format and length. This allows other systems like the POS/EPS to continue operating as they are, even though a payment token is being used rather than a payment card. The US national standard for format preserving encryption is X9.124 – Parts 1-5.

4.4 Decryption Management System

In a previous section, this Guide discussed the role of the Decryption Management System. There are many policies that must be in place to ensure the integrity of this service point in the system. There are many governing processes that a retailer can look to in order to implement and operate a secure environment for a DMS:

- PCI PIN: https://www.pcisecuritystandards.org/documents/PCI_PIN_Security_Requirements_v2__Dec2014_b.pdf?agreement=true&time=1593271800740; and
- Federal Information Processing Standards (FIPS): https://csrc.nist.gov/projects/fips-140-3-development.

Keep in mind that an area for decryption is a weak point in the overall solution. Ensuring the merchant does not have access to cryptographic keys capable of decrypting SAD is necessary for effective PCI de-scoping.

The DMS is critical whether it is an endpoint on a TLS network connection or a point/node in the P2PE network. Providing the right level of protection and processes is critical to the overall integrity of a retailer's cybersecurity strategy. Look to best in practice bodies like PCI and FIPS for guidance on best implementation practices.

4.5 Protecting Communications

One of the most important considerations in evaluating your options for securing data over the network is the balance between cryptographic methods/costs and the value of the data that is being protected. There are various levels of encryption that can be applied between encryption points and having a multi-layered encryption approach provides many layers of security of the data that is traveling between those two points.

This section of the Guide will explore three different levels of encryption: Application; Transport; and Line.

- Application level encryption means that the application is encrypting the data, and this level of encryption will not be resolved until the data is received by an intended receiving application.
- TLS is generally accepted as one PCI method for encrypting to network connections. When implemented properly, TLS provides a strong mechanism for authenticating both sides of a connection, which provides the added benefit of making sure that the two things that are talking to each other are actually authorized to do so.
- Line Level Encryption. Many network devices (including the ones that repurpose the twisted pair in the ground as an Ethernet network) also provide a level of encryption between the two boxes. This can provide an additional layer of protection to data that historically is often transmitted in the clear.

4.6 VLAN and VLAN Tagging

In addition to encrypting data flowing over the network, retailers should restrict network traffic and protocols on their networks to ensure that only the required network traffic is allowed. This is especially true now that the network traffic flows to the forecourt.

Separating forecourt LAN from site LAN and tightly managing the rules between them is fundamental to securing the network communications. Make sure that vendors are specific about the protocols that are being used and the direction in which they flow. Then assign rules between VLANs that only allow this traffic.

4.7 Semi-Integrated Payments: Terminal direct to HOST

One method for simplifying the site architecture for addressing security concerns is to have each POI manage the transaction directly with the processor. This is more commonly known as a "semi-integrated" solution where the EPS actually runs on each POI device. This approach is commonly used in general retail and even in fuel retail in various parts of the world. The advantage of this approach is that all systems in the store outside of the POIs, as well as their communication path to the host, are rendered out of scope because they are not exposed to the card data of the system. The in-store systems simply request an authorization for an amount, and the terminal responds with whether the transaction is authorized or not.

Unfortunately, most current fuel retail systems in the U.S. do not support this capability. Rather, US retail systems are integrated, with the centralized EPS, into the payment transaction.

4.8 Device Lifecycle Management

This is an important consideration as the devices like POIs and SCDs/HSMs iterate through installation, service stock, and eventually are taken out of service. During each step of this process, these devices need to be maintained appropriately to make sure that they do not fall into the wrong hands and become compromised. Many of the POI devices have an associated security policy (which you can download from the PCI website). These security policies explain how a device should be managed while in the custody of a retailer or service location. These policies must be followed for the device to maintain the PCI security levels that the merchant expects and they cover topics such as:

- Supply Change Management (chain of custody is part of the device lifecycle management);
- Physical security of the device; and
- Merchant having full knowledge related to each piece of equipment (every step of the device through the supply chain, and merchant knows its location).

As a part of a retailer's cybersecurity strategy, you must ensure that store and service personnel are aware of these policies and follow them to maintain the security of these devices.

4.9 Additional Risk Mitigation Techniques

Outside of all of the technology elements that have been discussed in this Guide, it is also pragmatic for a retailer to consider some simple physical controls and process that can help to prevent and detect malicious activity. These can include use of the following:

- Security (tamper-evident) tape on devices and areas that have sensitive access;

- Security switches that detect door opening;
- Enhanced AFD door locks with unique keys to ensure only appropriate people have access; and
- Regular security screening and inspections of the forecourt and back office.

While these methods do not require a degree in cybersecurity, they certainly can provide deterrents and detection that can keep a site from being an easy target of cybersecurity fraud. Additionally, they add to the overall "defense in depth" strategy needed to ensure cohesive and unified controls are in place and working effectively together.

4.10 Care and Feeding

There is so much to consider from a technology and processes perspective related to securing the sensitive data on store systems. Keep in mind this is an ongoing battle to keep ahead of the criminals. When evaluating one's cybersecurity strategy, retailers should consider the following questions when building coordinated processes to protect critical data:

- How do you validate that the processes are in place and being followed?
- How do you ensure that certificates are properly managed?
- What is a reasonable lifetime of the certificates?
- Do you have a way to revoke certificates?
- How will certificates be changed if necessary, in the lifetime of the equipment?
- How can keys be changed/revoked?
- How do you manage authentication?
- How do you validate certifications given that their generation makes it difficult to validate – use a list of CA or certificate pinning (no way at the host side in real time to tell if authentication is being done)? How do you test when certificates are being renewed?

Being regimented about the implementation and effectiveness of the processes that retailer puts in place is paramount to keeping ahead of criminals who are intent on compromising the security of retail locations. When a compromise occurs, retailers must have plans in place to investigate security incidents/breaches and to remediate any vulnerabilities that have been discovered utilizing any of the technologies listed above or through new processes that they put in place.

5 Conclusion

This Guide discusses many elements of existing technology and processes that are currently available to build a cybersecurity strategy. This information gives retailers options for improving their security until they have a complete P2PE implementation in place.

Ideally, retailers will implement a P2PE system where consumer information is not easily available or useable by any unknown third parties—so it is important to render the all consumer data useless once it is captured by the site, which process is often referred to as encryption at point of entry[1]. This approach may have negative drawbacks for site operations or other retail strategy elements:

- Identifying customers of loyalty programs;
- Identifying co-branded or other special use payment cards that need more than the first 6/last 4 digits of the account number;
- Processing Fleet transactions; and
- Routing debit transactions.

Choosing a P2PE solution gives rise to many detailed decisions that have to be made that will impact both the effectiveness and cost of that solution over the life of its implementation. As such, the degree of difficulty migrating to P2PE is likely to create considerable challenges for retailers.

Many of the basic technologies that are mentioned in this Guide are utilized in P2PE solutions but can also be leveraged to protect a retailer's infrastructure and data even before they have completed a P2PE implementation. Many of these technologies are ones being used by large retail chains to comply with PCI DSS requirements, so they are proven to be effective.

To enhance a cybersecurity strategy, retailers should use a combination of the following techniques and layer their overall approach to security:

- Evaluate new payment methods;
- Segment network traffic, isolate payments traffic from store ops traffic
- Encrypt data everywhere – at rest, in motion, and in processing;
- Use strong cryptographic algorithms, leveraging good key management techniques and best practices;
- Properly secure decryption management service locations;
- Ensure that third party service providers and vendors have implemented effective cybersecurity strategies. Ask vendors for certifications demonstrating proof of cybersecurity maturity;
- Adopt good physical security practices, designed to protect equipment, cabling, hardware, and facilities; and
- Monitor the effectiveness of processes and technology and modify those processes when needed.

[1] Note that encryption is not required, security controls are also permissible. It is very difficult to implement perfect security controls.

A layered approach to security provides both extra avenues of protection and provides checks and balances between systems and departments of an organization. The benefits of investing in good overall cybersecurity practices can keep cyber thieves away from your doorstep both now and in the future.

A.Glossary

Term	Definition
AES	Advanced Encryption Standard
AFD	Automated Fuel Dispenser
AVS	Address Verification Service
CA	Certification Authority
CNP	Card Not Present
CVM	Cardholder Verification Method
DES	Data Encryption Standard
DMS	Decryption Management System
DUKPT	Derived Unique Key Per Transaction
ECC	Elliptic Curve Cryptography
EMV	Europay, Mastercard, Visa
EPP	Encrypting PIN Pad
EPS	Electronic Payment Server
FIPS	Federal Information Processing Standards
HSM	Hardware Security Module
IPT	Indoor Payment Terminal
LAN	Local Area Network
MNSP	Managed Network Service Provider
MPPA	Mobile Payment Processing Application
NFC	Near Field Communication
OPT	Outdoor Payment Terminal
P2PE	Point to Point Encryption
PAN	Primary Account Number
PCI	Payment Card Industry
PCI DSS	Payment Card Industry Data Security Standard
PCI-PTS	Payment Card Industry PIN Transaction Security

Term	Definition
PII	Personally Identifiable Information
PIN	Personal Identification Number
PKI	Public Key Infrastructure
POI	Point of Interaction
POS	Point of Sale
RA	Registration Authority
RFID	Radio Frequency Identification
SAD	Sensitive Authentication Data
SCD	Secure Cryptographic Device
SCR	Secure Card Reader
SRED	Secure Read and Exchange of Data
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security and Authentication
VLAN	Virtual Local Area Network