mzeropay™

USER GUIDE

mzerosoftware

MERIDIAN

Table of Contents

MzeroPay Explained

MzeroPay provides a collection of managed, semi-integrated EMV payment solutions as middleware.

The PCI-PA (Payment Application) solution handles all aspects of electronic payment card transactions at the point of sale. Technologies utilized to make this happen are End-to-End encryption (E2E) or PCI-validated Peer to Peer Encryption (P2PE). The solution encapsulates the transaction, providing a PCI-scope reduction, and removes both the kiosk developer (mzeroCreate SDK) and the operator (Merchant) by blocking access to the storage, processing and transmitting of PCI-cardholder data and personally identifiable information (PII). This protects all parties involved, including Meridian as the solution provider, the Application Vendor (Kiosk Developer or Reseller) and the Kiosk Operator (Merchant) from compliance risk and associated liability.

The solution is targeted to kiosks where there are card-present retail transactions. It’s already approved by major providers such as BB&T, Chase, Elavon, Electronic Payment Systems, EvoPayments, First Data, Global payments, Heartland, TSYS, Worldpay with a variety of hardware offerings from Ingenico and Paymentech.

ADVANTAGES

The use of the PCI-PA solution greatly reduces the PCI-Software Quality Assurance (SQA) requirements for the kiosk solution provider. The technologies listed below encapsulate the transaction preventing the access to sensitive cardholder, thus ensuring removing the kiosk software application using it PCI-Scope.

- PA-DSS certified
- End-to-End encryption (PCI-Validated P2PE or E2E)
- EMV-Certified (Chip card)
- Injected pin-tokens in the terminal

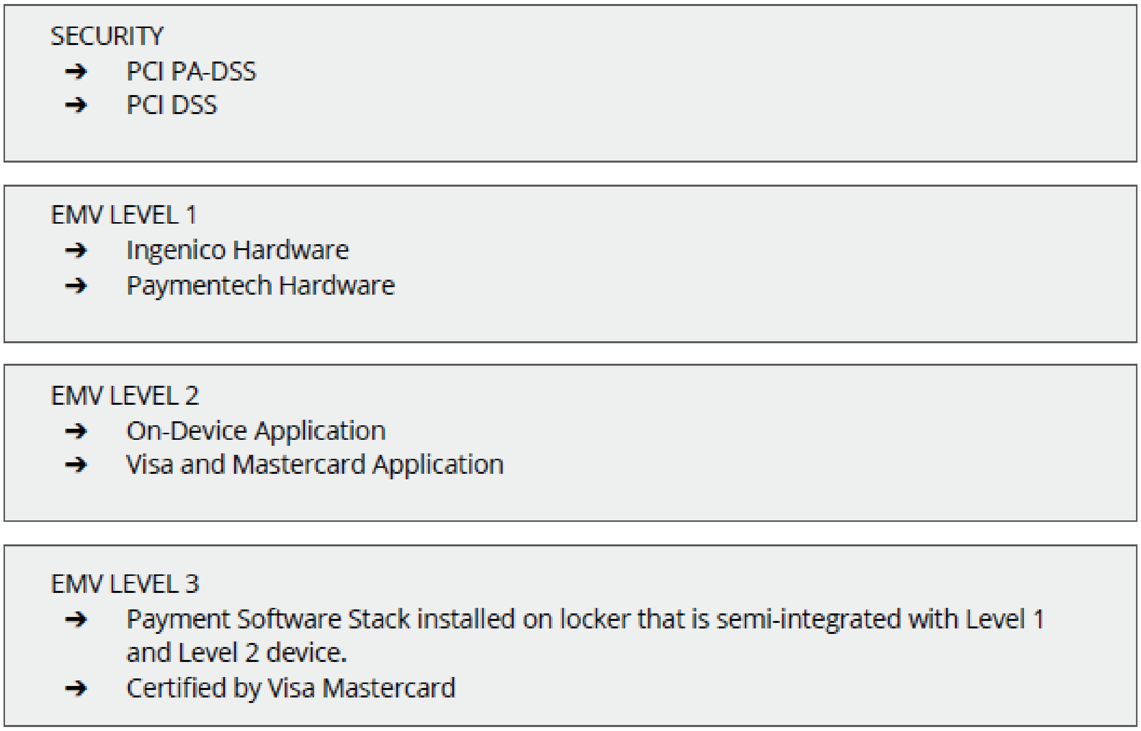
Access to the middleware for Kiosk Developers is made possible by Meridian's MzeroCreate SDK. A programming interface provides a kiosk developer simple-to-use methods to start a card transaction and print the receipt. MzeroPlatform manages the middleware and transmits payment reports and state-of-health information to our MzeroManage central management server. MzeroPlatform also enables you to swap out middleware solutions depending on the region and specific features required, without changing your kiosk application.

ADDITIONAL ADVANTAGES

- Ability to select and change your payment processors to take advantage of features and values from other providers, while keeping the software APIs and SDKs the same.
- Supports all manager payment types: including credit, debit.
- Unattended cardholder verification methods of pin entry.
- Operates in either attended and unattended (semi-attended scenarios) where supported.
- Simplify management of compliance and updates (subscription based customers only).
- Remote upgrades are available

PAYMENT STACKS

MzeroPay contains Level 3 payment stacks which are PA-DSS certified and in some cases P2PE certified.



SECURITY
- ➔ PCI PA-DSS
- ➔ PCI DSS

EMV LEVEL 1
- ➔ Ingenico Hardware
- ➔ Paymentech Hardware

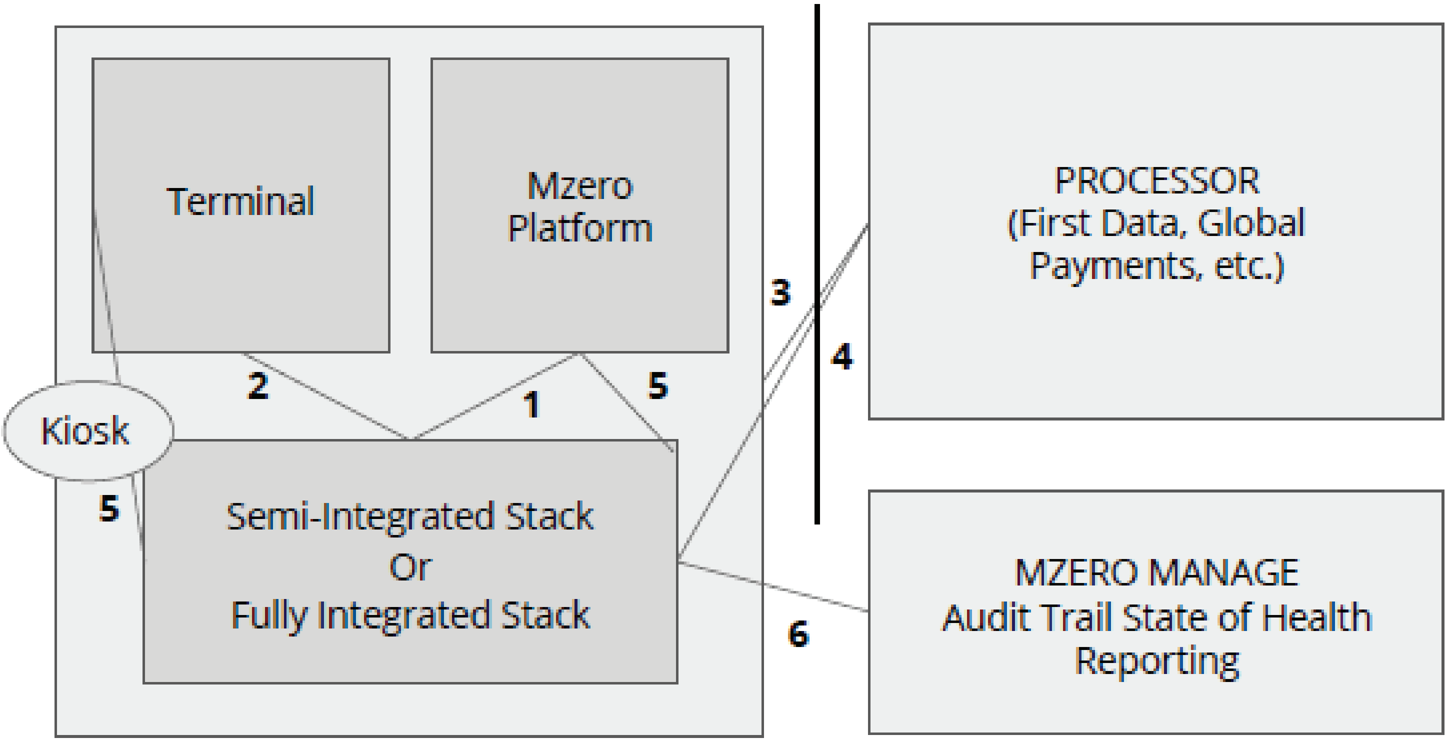
EMV LEVEL 2
- ➔ On-Device Application
- ➔ Visa and Mastercard Application

EMV LEVEL 3
- ➔ Payment Software Stack installed on locker that is semi-integrated with Level 1 and Level 2 device.
- ➔ Certified by Visa Mastercard

HOW IT WORKS

There are two methods based on the merchant selected: Direct End-to-End or PCI-Validated P2PE Hosted.

OPTION 1: DIRECT END-TO-END (PERPETUAL LICENSE ONLY)


Terminal
Mzero Platform
PROCESSOR (First Data, Global Payments, etc.)
Kiosk
Semi-Integrated Stack Or Fully Integrated Stack
MZERO MANAGE Audit Trail State of Health Reporting
1
2
3
4
5
5
6

The following steps occur during a transaction: [Corresponds with above chart]

1. The Kiosk application through MzeroCreate requests a payment to start.

2. The MzeroPlatform forwards the request to the semi-integrated payment stack which initiates a connection to the payment terminal to the EMV-enabled pin pad.

3. Encrypted data from inside the hardware of the payment terminal is transmitted through the certified semi-integrated middleware to the processor. In some cases, a supporting gateway is required depending on the processor network used (see PCI-Validated P2PE solutions).

4. The response from the payment processor is forwarded back to the semi-integrated stack.

5. The approve or decline arrives at the platform and ultimately the kiosk application. A receipt is automatically printed with region-specific requirements provided.

How It Works

OPTION 2: PCI-VALIDATED P2PE SOLUTIONS WITH HOSTED GATEWAY (SaaS ONLY)

In cases where a P2PE certification is held, a PCI-Level 1 service provider gateway is leveraged by the semi-integrated solution to manage the transaction flow.

The following steps occur during a transaction: [Corresponds with below chart]

1. The Kiosk application through MzeroCreate requests a payment to start.

2. The MzeroPlatform forwards the request to the semi-integrated payment stack which initiates a connection to the payment terminal to the EMV-enabled pin pad.

3. Encrypted data from inside the hardware of the payment terminal is transmitted through the certified semi-integrated middleware to the processor. There is a gateway provider specific E2E encryption key that is injected into the payment terminal that facilitates the communication securely to the gateway. Meridian utilizes many payment gateways in the solution, so the E2E keys vary depending on the hardware, merchant, and country for which the solution is deployed.

4. The data is processed from the gateway to the processor's network, which has been certified and pre-approved for this purpose in advance. This goes directly to the Merchant account.

5. The response from the processor is passed back to the gateway.

6. It then E2E encrypts the data and passes it back to the semi-integrated stack.

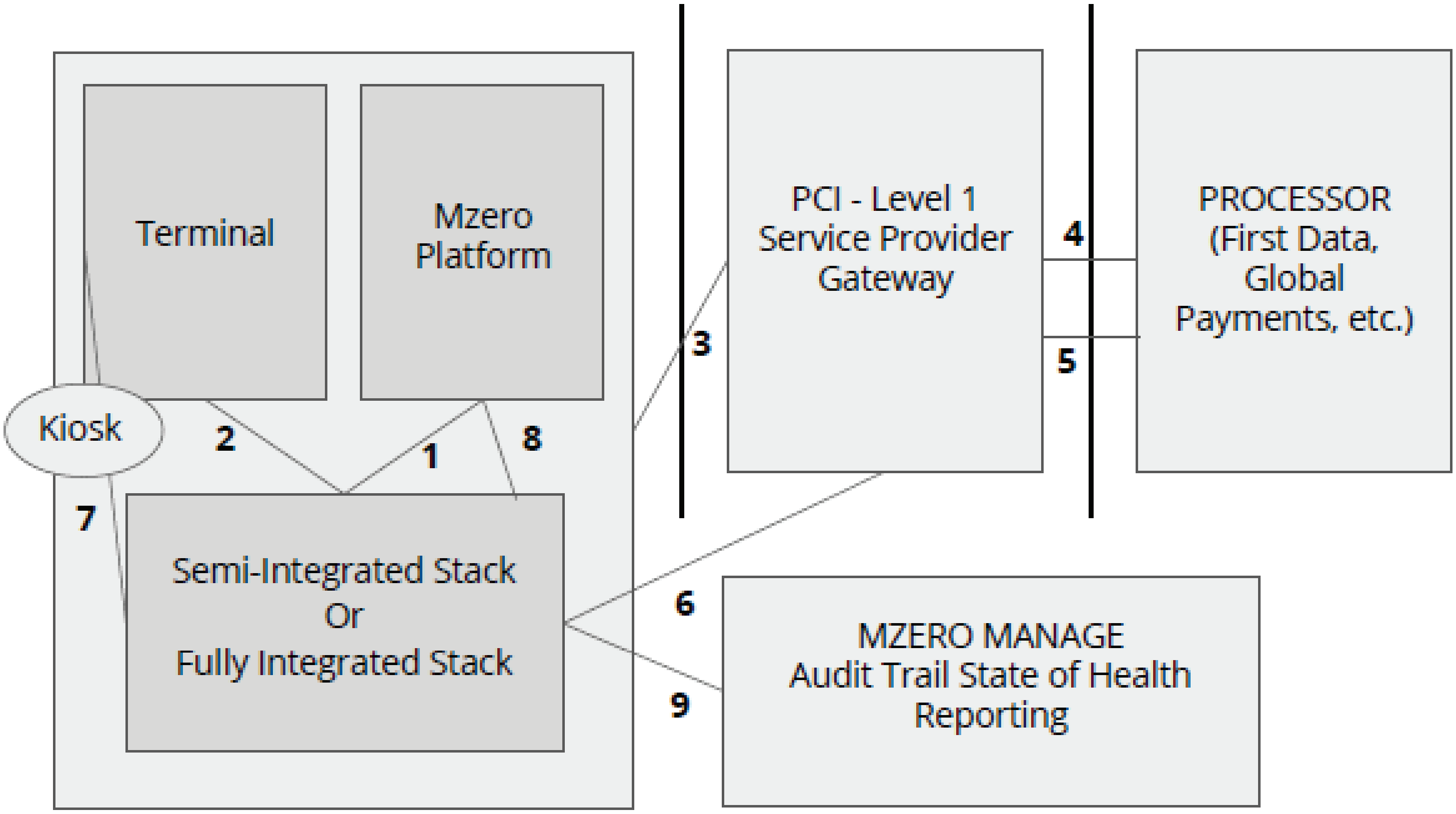
7. The payment terminal displays a decline or approved message.

8. The Application is informed of the response and transaction references are provided.

9. The approve or decline arrives at the platform and ultimately the kiosk application. A receipt is automatically printed with region specific requirements provided.

10. The PCI-Level 1 Service Provider Gateway provides additional value adds: the ability to create scheduled recurring charges through tokenization, the provision of a payment terminal which can be used to review daily transactions and batch, manage and void transactions before they are posted. The user can also refund transactions already posted or create new manual authorizations.

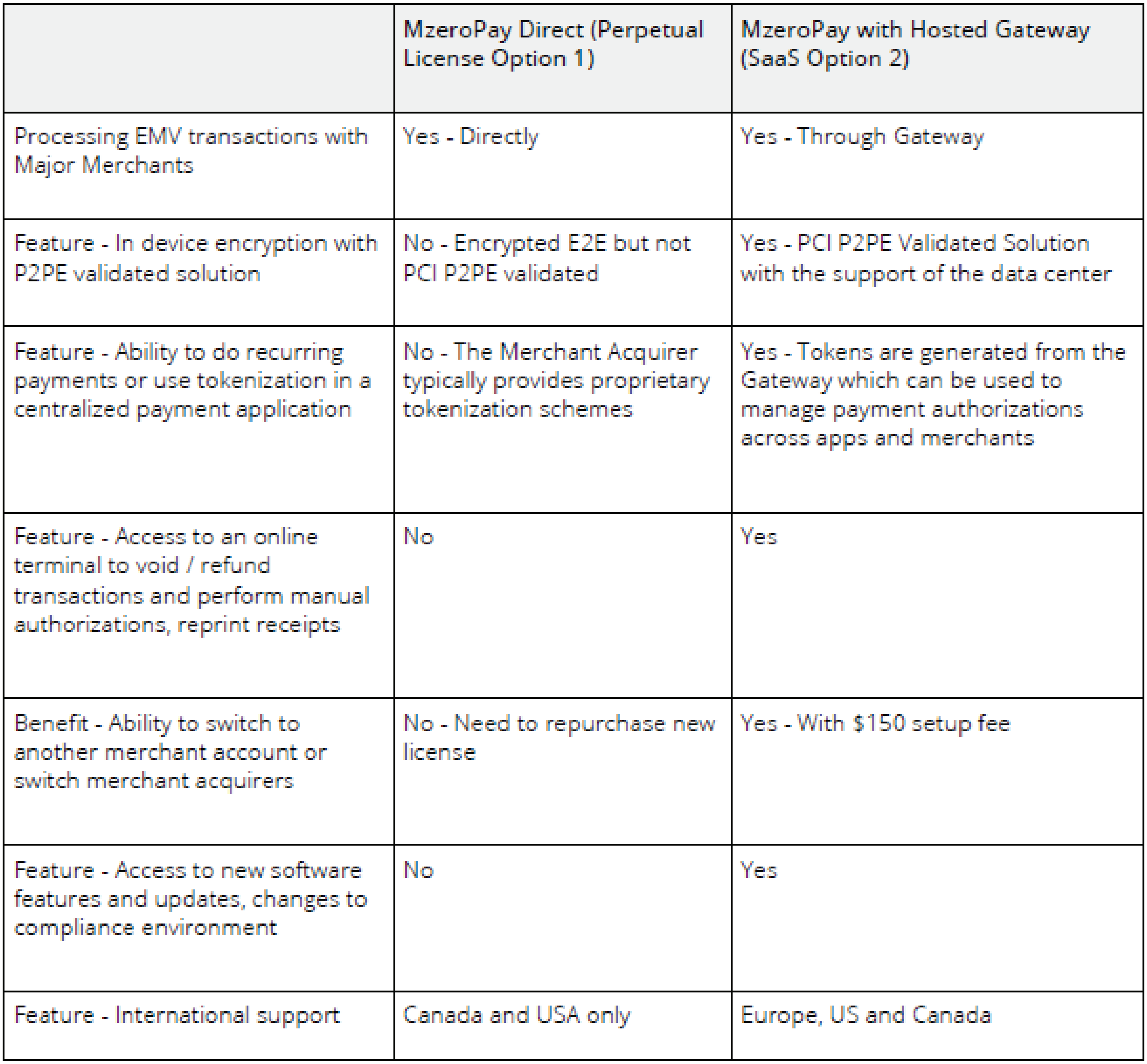
How It Works


Terminal
Mzero Platform
Kiosk
2
1
8
7
Semi-Integrated Stack Or Fully Integrated Stack
3
PCI - Level 1 Service Provider Gateway
4
5
PROCESSOR (First Data, Global Payments, etc.)
6
9
MZERO MANAGE Audit Trail State of Health Reporting

What is PCI Level 1 Service Provider and why is this required regardless of how you are processing retail transactions?

Level 1 Service Provider are service providers that store, process, or transmit more than 300,000 credit card transactions annually you must pass PCI Requirements validated such as Annual Report on Compliance (ROC). The data center in this solution has the required approvals and maintains this annually. The subscription is paying to access this ongoing certification and recertification.

FEATURES AND BENEFITS



	MzeroPay Direct (Perpetual License Option 1)	MzeroPay with Hosted Gateway (SaaS Option 2)
Processing EMV transactions with Major Merchants	Yes - Directly	Yes - Through Gateway
Feature - In device encryption with P2PE validated solution	No - Encrypted E2E but not PCI P2PE validated	Yes - PCI P2PE Validated Solution with the support of the data center
Feature - Ability to do recurring payments or use tokenization in a centralized payment application	No - The Merchant Acquirer typically provides proprietary tokenization schemes	Yes - Tokens are generated from the Gateway which can be used to manage payment authorizations across apps and merchants
Feature - Access to an online terminal to void / refund transactions and perform manual authorizations, reprint receipts	No	Yes
Benefit - Ability to switch to another merchant account or switch merchant acquirers	No - Need to repurchase new license	Yes - With $150 setup fee
Feature - Access to new software features and updates, changes to compliance environment	No	Yes
Feature - International support	Canada and USA only	Europe, US and Canada

DEFINITIONS

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

Point-to-Point Encryption (P2PE) is an encryption standard established by the Payment Card Industry (PCI) Security Standards Council. It requires that payment card data be encrypted immediately upon use with the merchant's point-of-sale terminal and cannot be decrypted until securely transported to and processed by the payment processor. Reference:bluefin.com

What is a PCI-validated P2PE solution?

A PCI-validated P2PE solution is a combination of secure devices, applications, and processes that encrypt credit card data immediately upon swipe or dip in the payment terminal (also called the Point of Interaction, or POI). The data remains encrypted until it reaches the Solution Provider's secure decryption environment.

In order for a P2PE solution to receive validation from PCI, the solution, the Solution Provider, and associated players in the overall P2PE solution must undergo assessment and audit by a P2PE Qualified Security Assessor (QSA), prior to being brought before the council for approval. Reference: bluefin.com

What does a PCI-validated P2PE solution have to include?

A PCI-validated P2PE solution is required to have all of the following:

- Secure encryption of payment card data at the POI / i.e. the payment terminal.
- P2PE-validated application(s) at the POI.
- Secure management of encryption and decryption devices.
- Management of the decryption environment and all decrypted account data.
- Use of secure encryption methodologies and cryptographic key operations, including key generation, distribution, loading/injection and administration

DEFINITIONS

What are the benefits of a PCI-validated P2PE solution for merchants?

There are many benefits for merchants who use a PCI-validated P2PE solution. Some of these benefits include reducing your risk in protecting customer's payment data as well as various incentive programs for merchants using a PCI-validated P2PE solution.

- **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) are 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).

- **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 re-validate PCI DSS compliance.
  - Visa Secure Acceptance 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.

- **Solution for Challenging Compliance Issues**
  - Remote Acceptance: 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.
  - 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.

DEFINITIONS

EMV introduction

As U.S. merchants, acquirers, and processors plan for the migration to EMV® contact and contactless chip, many stakeholders ask: “What are Visa’s minimum requirements for a chip terminal in the U.S.?” Visa’s U.S. market strategy is to focus on online only acceptance, leveraging existing online magnetic-stripe infrastructure which is robust, real-time, and always online for authorization and authentication. Reference: usa.visa.com

Merchants are encouraged to work directly with their acquirer and/or terminal provider to determine the approved EMVCo terminal configurations offered that satisfy Visa’s U.S. Online Only terminal requirements. Approved EMVCo terminal configurations (chip reader and chip software) are a global industry requirement, and the U.S. is no exception. Site: usa.visa.com

EMV - Fraud protection

When you upgrade to chip technology, you continue to be protected from counterfeit fraud losses. As of October 1, 2015, businesses that don’t accept Visa chip card transactions may be responsible for any resulting counterfeit fraud. Similarly, effective October 1, 2017 [October 1, 2020 for U.S. domestic Automated Fuel Dispensers (AFDs)], Visa transactions made at ATMs and AFDs will be included in the Liability Shift Policy. Reference:usa.visa.com

If you haven’t yet adopted Visa chip technology, there are a few things to keep in mind: customers can still swipe their chip-enabled card at your terminals using the magnetic stripe on the back of the card and use their cards over-the-phone or online just as always. Whether your customers insert, swipe or use their card online, they’re protected from unauthorized transactions with Visa’s Zero Liability Policy. Reference:usa.visa.com

EMV Configuration

EMV terminal providers will be intimately familiar with the configuration options associated with their particular device and will provide guidance on satisfying Visa’s Online Only requirements.

Corporate Headquarters

312 S. Pine Street,
Aberdeen, NC 28315

+1 910-944-1751 Ext. 2
Help@mzero.com

Meridiankiosks.com

MERIDIAN
CONCEPT TO COMPLETION