PREPARED BY | CONEXXUS Quick Reference Guide

GETTING STARTED WITH P2PE

Part 1 - Three Main Tenets of P2PE

P2PE

Point-to-Point Encryption (P2PE) is an essential security measure that can significantly reduce the risk of data breaches and cyber-attacks at card readers (e.g., AFDs and PIN Pads at the counter) Every POI with cardholder data presents a unique challenge for P2PE technology due to the variety of communication options and protocols that are available.

When selecting a P2PE solution, it is essential to ensure that the chosen solution meets industry standards for security and compliance, such as the PCI DSS. It is also important to consider several factors (data elements, integration, and cost) to ensure that the chosen solution is the right fit for the merchant's specific needs.

By carefully considering these factors, the merchant can select a P2PE solution that provides the necessary security, flexibility, and affordability for it's business.

Data Elements

The merchant should work with a qualified PCI Assessor or Processor to identify which data elements need to be protected and the level of encryption required. Some solutions may only encrypt payment card data, while others can encrypt additional data.

Considerations:

> Compliance Requirements - Evaluate if the P2PE solution is listed and in good standing with PCI and review the supported devices, applications, and components.

> Security Features - Consider the overall P2PE solution for security and ease of implementation. Look for features such as an encryption methodology, device chain of custody, remote key loading capabilities, etc.

Integration

The merchant must determine the level of integration required with existing payment systems and equipment. Some P2PE solutions may require significant changes to payment processing systems, while others may be more easily integrated.

Considerations:

> Scalability and Future-Proofing - Ensure that your chosen P2PE solution can accommodate your organization's growth and evolving payment needs.

> Integration Complexity - Consider the ease of integration with your existing payment infrastructure and POS solutions.

> Vendor Reputation and Support - Evaluate the reputation and track record of the solution vendor by considering factors such as its experience, certifications, reviews, and quality/availability of its support services.

> Training and Education - Evaluate the training and educational resources provided by the P2PE solution vendor to ensure that your staff is adequately trained to understand and utilize the solution effectively and securely.

Cost

The merchant should consider the total cost of ownership, including hardware, software, implementation, maintenance, ongoing support, upgrades and associated fees.

Considerations:

> Scope Reduction - Verify all cardholder data flows in your environment to understand how a P2PE solution could impact your PCI DSS scope by significantly reducing the number of systems and controls requiring validation.

> Audit and Reporting Capabilities - Consider the reporting capabilities of the P2PE solution such as centralized management consoles, device tracking, transaction audit logs, and monitoring tools.

- **Note:** Transaction monitoring is required to be performed by PCI P2PE solution providers.

GETTING STARTED WITH P2PE

Relevant Acronyms

AES	Advanced Encryption Standard
AFD	Automatic Fuel Dispenser
BIN	Bank Identification Number
CVM	Cardholder Verification Method
E2EE	End to End Encryption
EPS	Electronic Payment Server
FEP	Front End Processor
IPT	Indoor Payment Terminal
MNSP	Managed Network Service Provider
OPT	Outdoor Payment Terminal
P2PE	Point to Point Encryption
PAN	Primary Account Number
PCI DSS	Payment Card Industry Data Security Standard
PII	Personally Identifiable Information
PIN	Personal Identification Number
POI	Point of Interaction
POS	Point of Sale
PTS	PIN Transaction Security
QSA	Qualified Security Assessor
SCD	Secure Cryptographic Device
SCR	Secure Card Reader
SRED	Secure Read and Exchange of Data
UPM	Universal Payment Module