GETTING STARTED WITH P2PE

Part 2 - Pros and Cons of PCI Validated and Non-Validated Solutions

In the last part, we talked about the three tenets of a P2PE solution. This part is a continuation of part 1 and shows not only the pros and cons of validated and non-validated P2PE solutions, but how that choice would also impact the data, integration, and cost.

PCI Validated P2PE Solutions

Pros:

> Security Assurance: PCI-validated P2PE solutions have undergone rigorous testing and validation processes, assuring merchants that they meet the highest industry-standard security requirements. This can enhance trust with customers and payment processors.

> Compliance Simplification: Using a validated solution can simplify PCI DSS compliance for the merchant. Compliance requirements may be reduced, potentially lowering audit and assessment costs significantly.

> Reduced Liability: Should a breach occur, merchants using a PCI-validated P2PE solution may have reduced costs, liability, and exposure.

Cons:

> Cost: Store hardware and software upgrades may be required to support a validated P2PE solution. Costs should be taken into consideration.

> Implementation Complexity: Implementing a PCI-validated P2PE solution can be more complex and time-consuming due to the stringent security measures and validation requirements.

> Limited Vendor Options: The pool of vendors offering PCI-validated P2PE solutions may be smaller, limiting the merchant's choices and potentially leading to higher costs.

Non-Validated P2PE Solutions

Pros:

> Cost Savings: Non-validated P2PE solutions typically come with lower upfront costs, making them more accessible for smaller businesses with budget constraints.

> Flexibility: Merchants have greater flexibility in choosing from a wider range of vendors and solutions, allowing them to tailor the solution to their specific needs.

> Simplified Implementation: Non-validated solutions may be easier and quicker to implement.

> Improves Security: A non-validated P2PE solution can provide increased security.

Cons:

> Security Risks: Non-validated solutions may not meet the same security standards as PCI-validated solutions.

> Limited Compliance Benefits: Merchants using non-validated solutions may still need to meet full PCI DSS compliance requirements, which can be more onerous and costly. The reduction in PCI scope, for your specific P2PE implementation, might require the approval of your processor and it is strongly advised to have the implementation validated by a QSA.

> Higher Liability: In the event of a data breach, merchants using non-validated solutions may face higher fines, penalties, and liabilities.

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