GETTING STARTED WITH P2PE

Part 3 - Additional Considerations

In parts 1 and 2, we discussed the three main tenets of a P2PE solution, the pros and cons of both validated and non-validated solutions, and how those two topics impact the data, integration, and cost of this decision. In this part, we detail some additional considerations to ask yourself as you are evaluating solutions.

Do you need to upgrade your POI?

> Do you have an accurate inventory of all POI devices that interact with cardholder data? (E.g., PIN Pads, SCDs, UPMs)
>> Are they PTS 4.X and above listed and support the SRED standard?
>> Is the device firmware only or does it require a P2PE payment application?
>> Is there a P2PE payment application for the device already listed on the PCI Council website?
>> Is your personal PIN Pad stand-alone or semi-integrated?
> What is your POS system?
>> Does it support P2PE message formats?
>> What PAN information do you require to maintain your existing infrastructure?
>> Do you accept non-branded gift, private label, or non-PCI compliant fleet cards?

Does your processor have a P2PE solution?

> Can it support all of your POI device types with P2PE?

Project management and resources

> Do you have a deployment plan?
> Do you have a deployment team?
> Who will be leading compliance?
> What type of testing will be required? (E.g., hardware testing, card testing, BIN whitelists)
>> Acquirer/Processor Testing – There may be multiple certifications and testing that might be required
> Do you have an asset management system to manage your PTS device inventory?
>> Can your PCI P2PE Solution Provider integrate with it?

Do you have a payment switch?

> Is the switch cloud-based or on-premise?
> Who will be managing compliance on the switch?

Are you using a vendor-managed network provider?

> Are they PCI P2PE listed?
> Do they support your devices?

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