

PCI

Compliance Tool

Eligibility to Complete SAQ's A-EP, B-IP, and P2PE

PCI 3.2.1 PART 1

AGENDA

- What do I do about mobile merchants?
- Review of PCI SAQ Selection criteria
- Questions

What Do I Do About Mobile Merchants?

- No Official SAQ Exists
- PCI SSC has published Best Practices
 - Industry validation best practices
 - Cellular connection = SAQ B
 - WiFi = SAQ C or higher

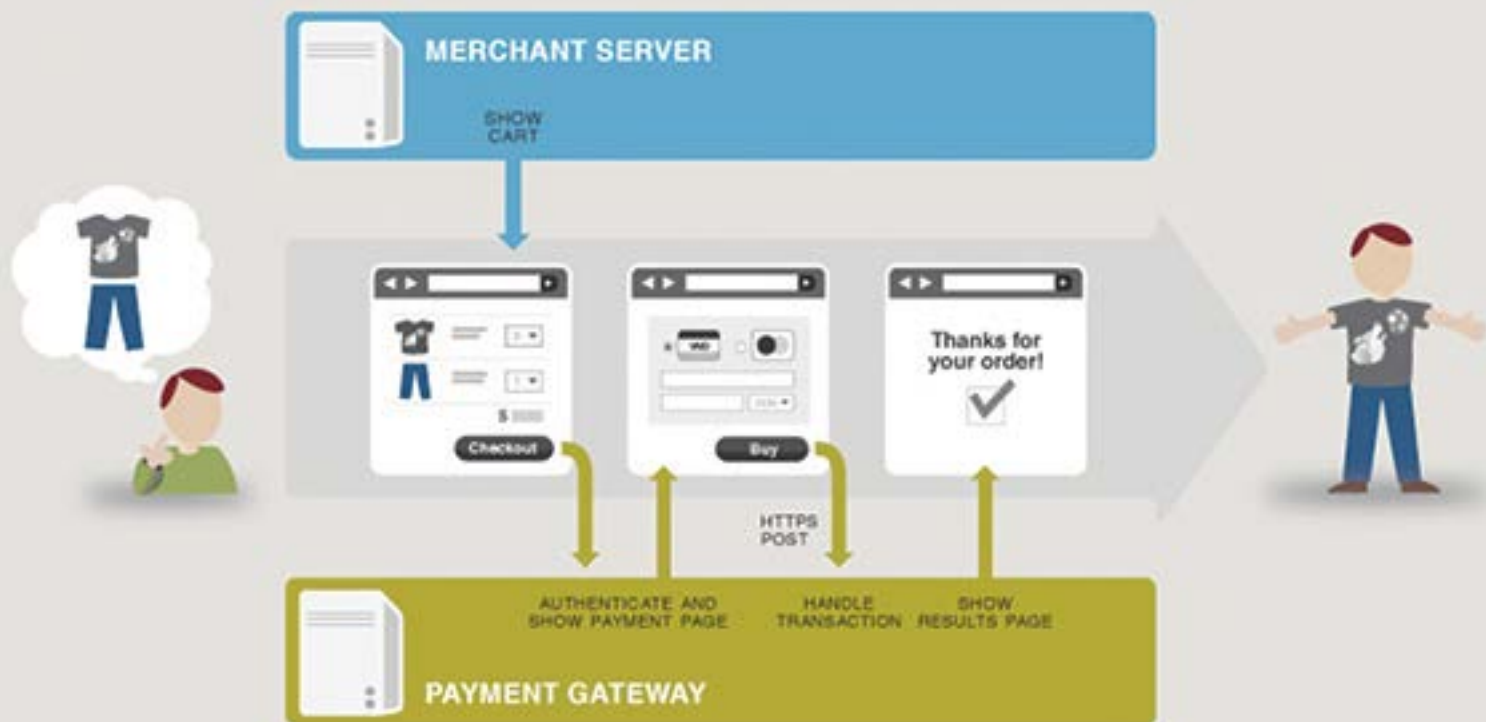


PCI DSS SAQ Selection

- SAQ A
- SAQ A-EP (New)
- SAQ B
- SAQ B-IP (New)
- SAQ C
- SAQ C-VT
- SAQ P2PE-HW
- SAQ D

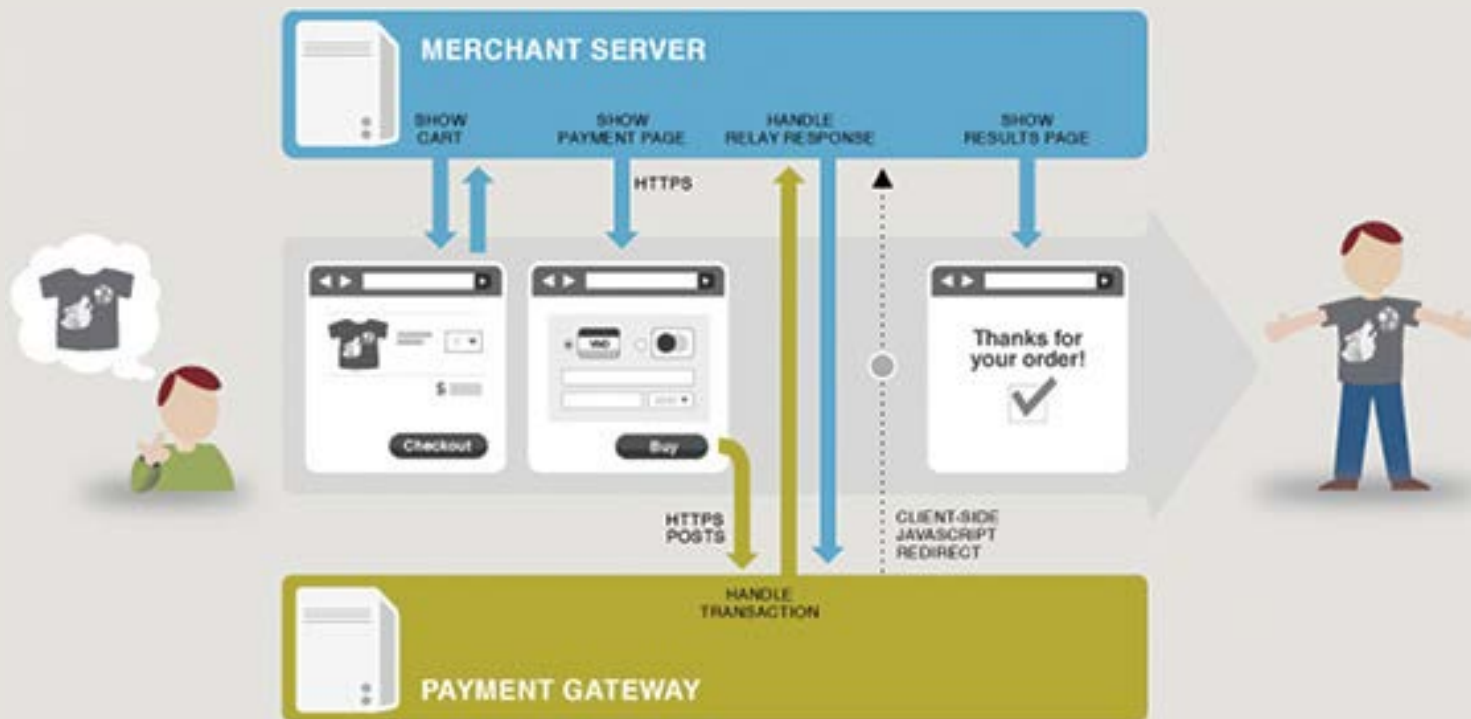
SAQ A

- Applies to CNP Only
 - e-commerce
 - MOTO
- Card acceptance completely outsourced
- Payment page originates *directly* from service provider
- No cardholder data is stored in electronic format
- A PCI DSS compliant service provider is used



SAQ A-EP (NEW)

- Applies to only to e-commerce merchants
- No electronic cardholder data enters merchant environment
- Merchant controls how consumer is redirected to third party payment provider
- Merchant website does not connect to any other systems with in the merchant environment
- If website is hosted, it is hosted at a PCI DSS compliant hosting company
- Merchant must select a PCI DSS compliant service provider

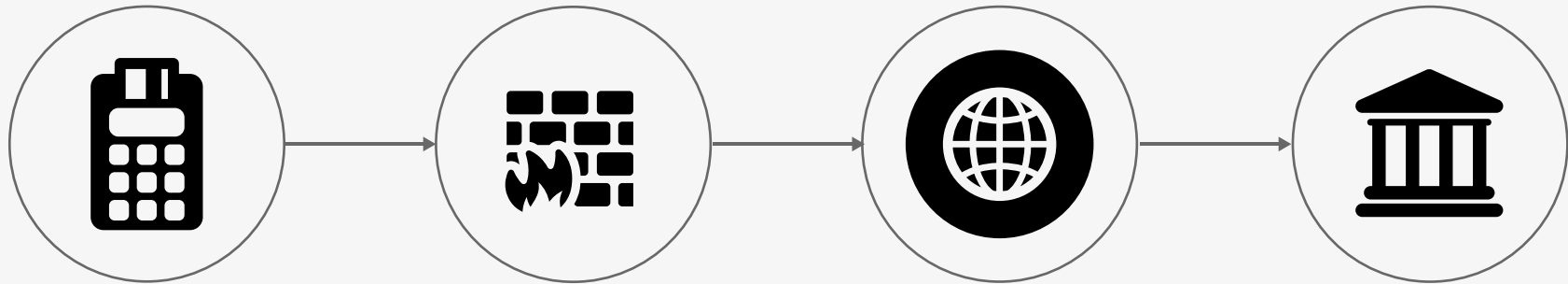


SAQ B



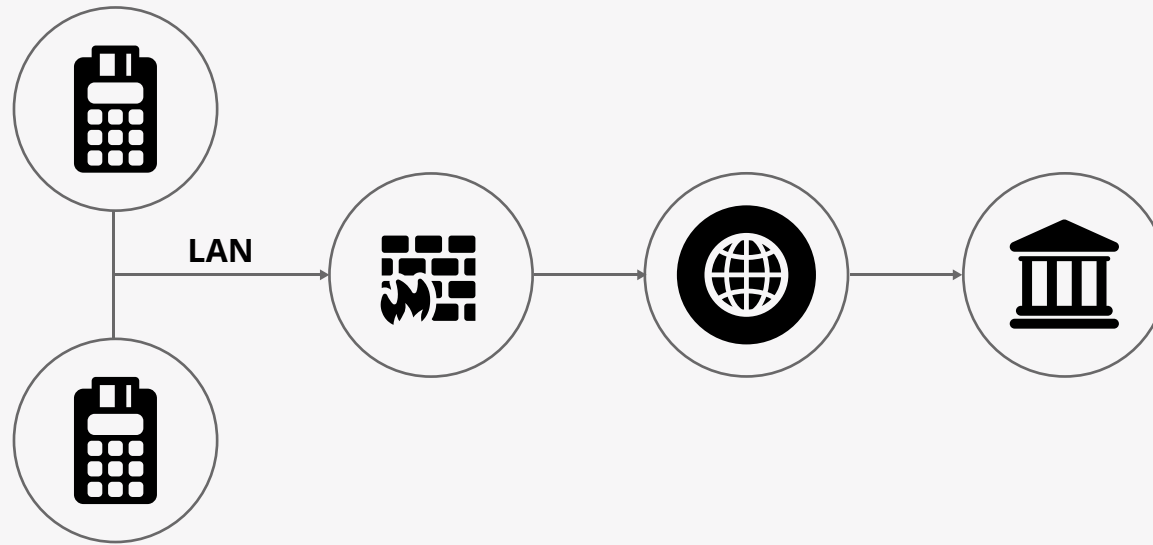
- Merchant only uses imprint machine or stand alone dial out (analog) terminal
- If dual interface terminal (IP and analog), only analog is used
- No electronic cardholder data is stored
- Terminal is not connected to any other systems in merchant environment

SAQ B-IP (NEW)



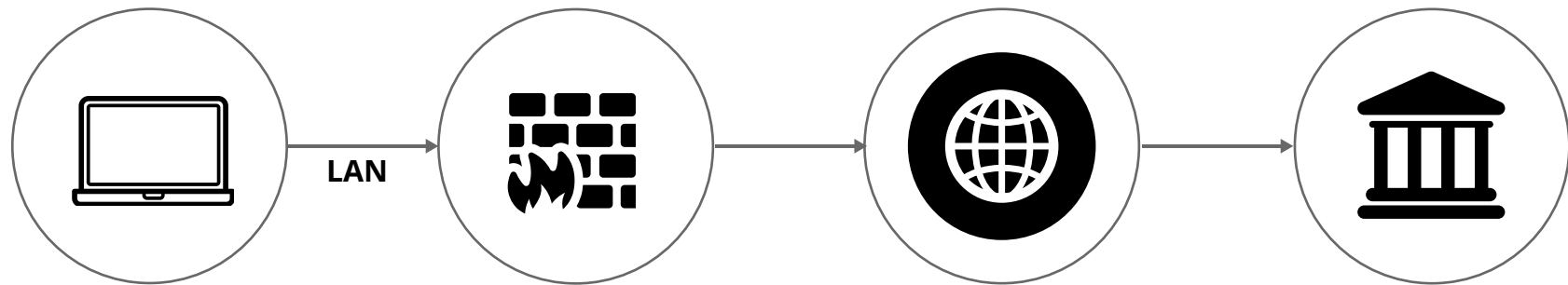
- Merchant only uses a stand alone IP based PTS approved POI device
- Terminal is not connected to any other systems in merchant environment
- Device does not rely on any other device to connect to payment processor
- No electronic cardholder data is stored

SAQ C



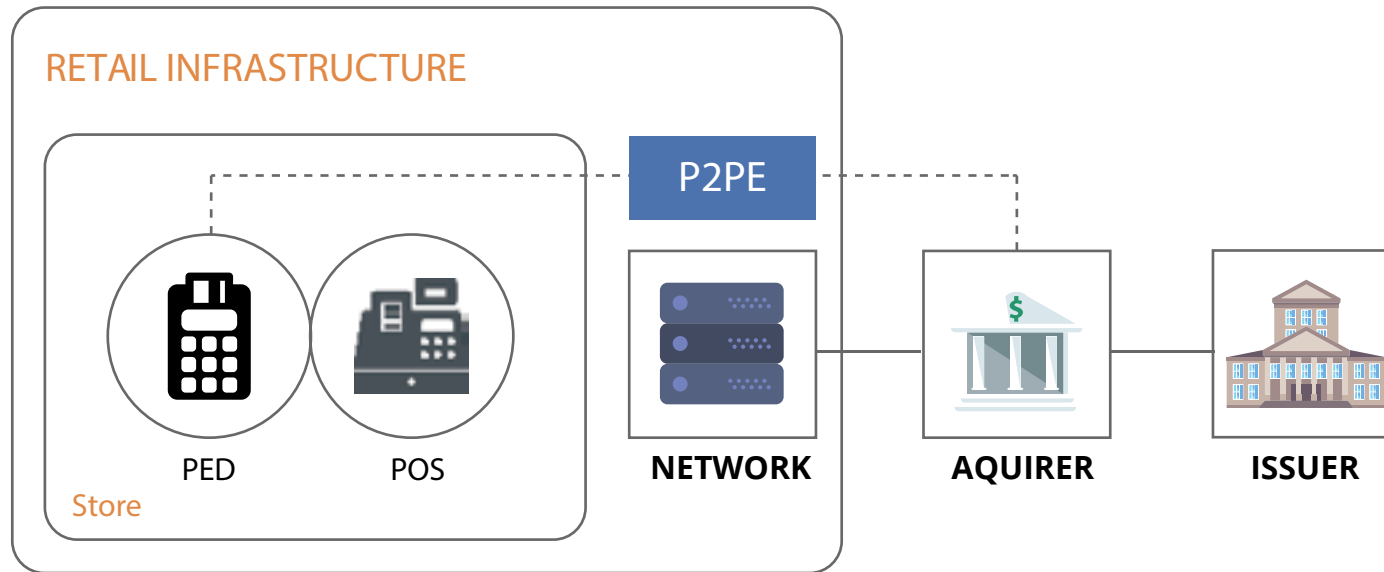
- Merchant payment application system and internet connection are on the same device or local area network
- The application system/ internet device is not connected to any other systems within your environment
- The physical location of the POS is not connected to other premises or locations and LAN is for single location only
- No electronic cardholder data is stored

SAQ C-VT



- Merchant's only payment processing is via virtual terminal
- The virtual terminal solution is provided and hosted by a PCI validated third party service provider
- No cardholder data is captured or stored during the transaction process and there is no hardware installed to electronically capture data **(NO CARD READERS!)**
- No other channel is used within the organization to receive or transmit cardholder data
- No electronic cardholder data is stored

Point to Point Encryption (P2PE)



Point to Point Encryption (P2PE)

If a merchant does not fit into any of the SAQ's previously covered, they are an **SAQ D**



Question?

