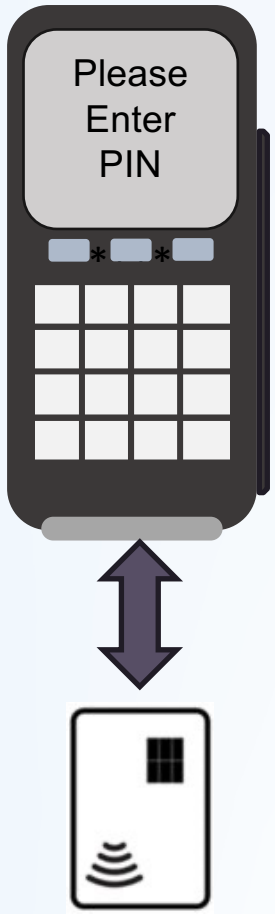
PCI Security Standards Council

Mobile Security and Standards Update

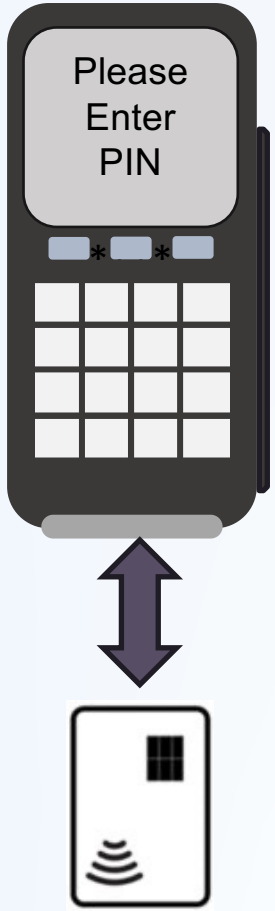
Andrew Jamieson, *VP, Solutions*
PCI Security Standards Council

EMVCo & PCI SSC Securing Payments Together



EMVCo & PCI SSC Securing Payments Together

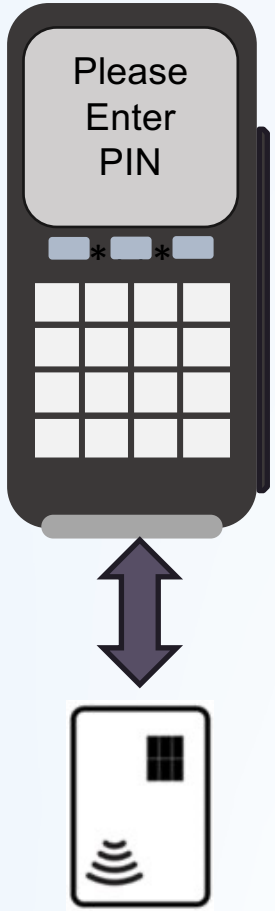
Security of the POI / payment processing environments
Security of PIN entry and encryption
Security of account data during and after processing
Associated terminal / acquirer key management



EMVCo & PCI SSC Securing Payments Together

Security of the POI / payment processing environments
Security of PIN entry and encryption
Security of account data during and after processing
Associated terminal / acquirer key management

Physical properties and security of payment instruments
Protocol for how the card and terminal communicate
Security of payment card ‘chips’ and software
Security of authentication on payment instruments (CDCVM)



Cardholder Authentication

Offline PIN

PIN sent to card
for validation

PCI Security Standards Council

Cardholder Authentication

Offline PIN

PIN sent to card
for validation

Online PIN

PIN sent to Issuer
for validation

PCI Security Standards Council

Cardholder Authentication

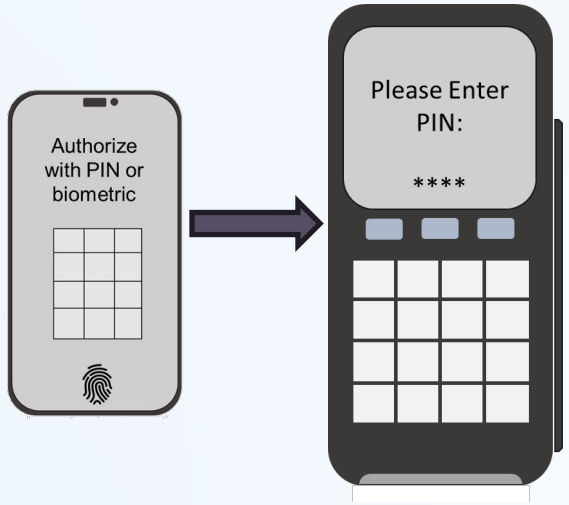
Offline PIN

PIN sent to card
for validation

Online PIN

PIN sent to Issuer
for validation

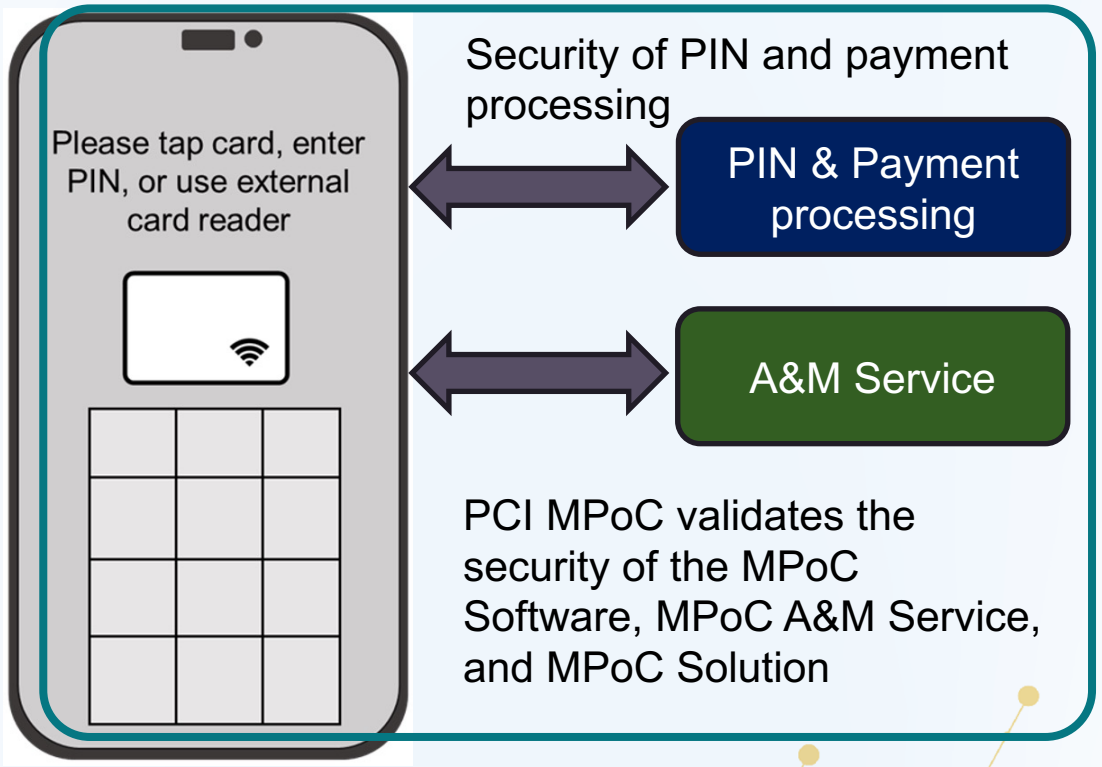
CDCVM



Cardholder authenticates
on COTS device

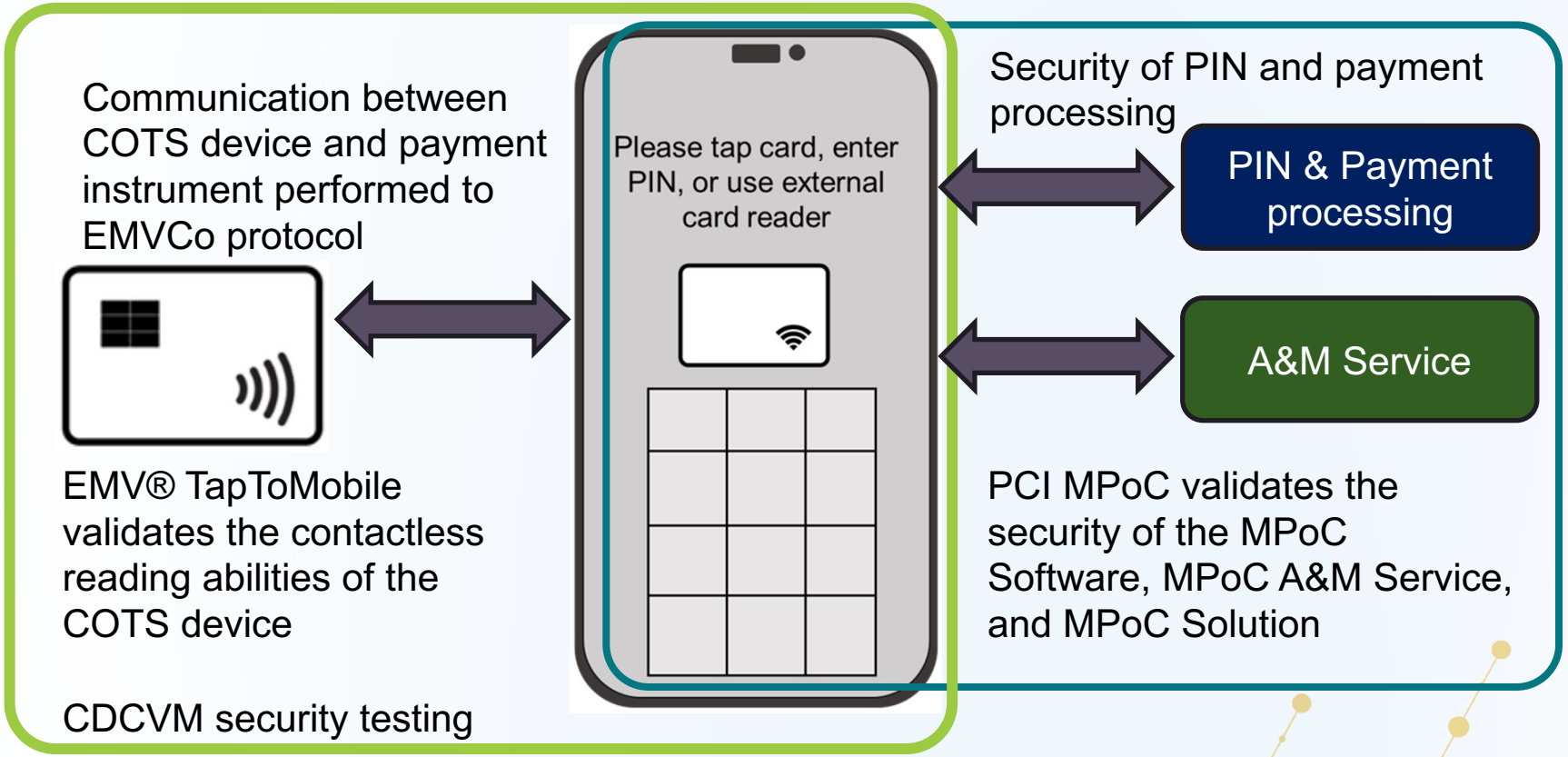
PCI Security Standards Council

Improving Mobile Payment Acceptance Security And Interpretability



PCI Security Standards Council

Improving Mobile Payment Acceptance Security And Interpretability

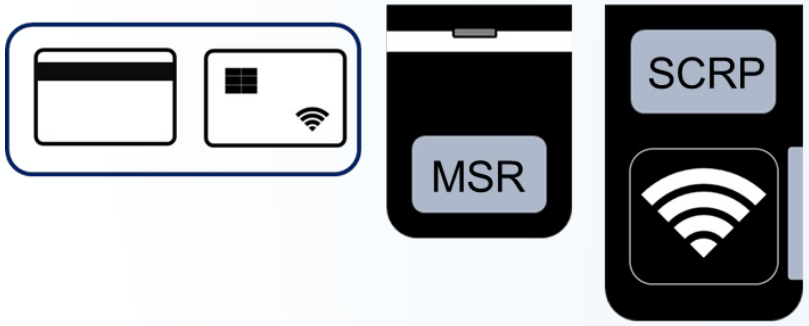


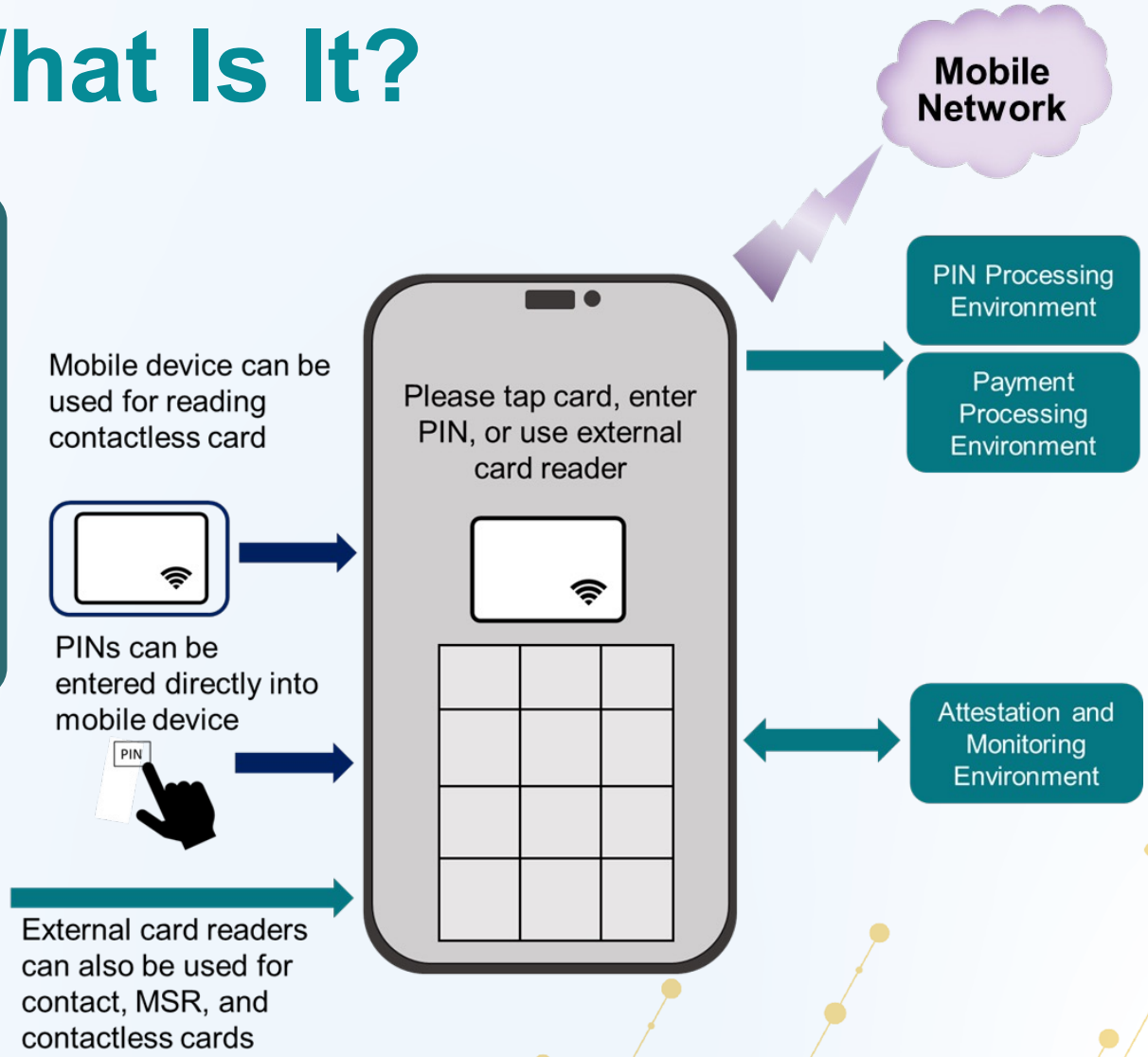
PCI Security Standards Council

PCI MPoC – What Is It?

MPoC Software / MPoC Solutions
must support one form of COTS-native account data entry (PIN or contactless)
AND
must support at least one form of EMV-based card entry

So; no PIN entry only, no MSR only*, no use of external SCRP with no account data input on the COTS device*





* 'No MSR only', 'No account data on COTS' exclusions are on an MPoC SDK or MPoC App basis, not a per-transaction basis

PCI MPoC – COTS Device Examples

COTS examples suitable for consideration under MPoC:

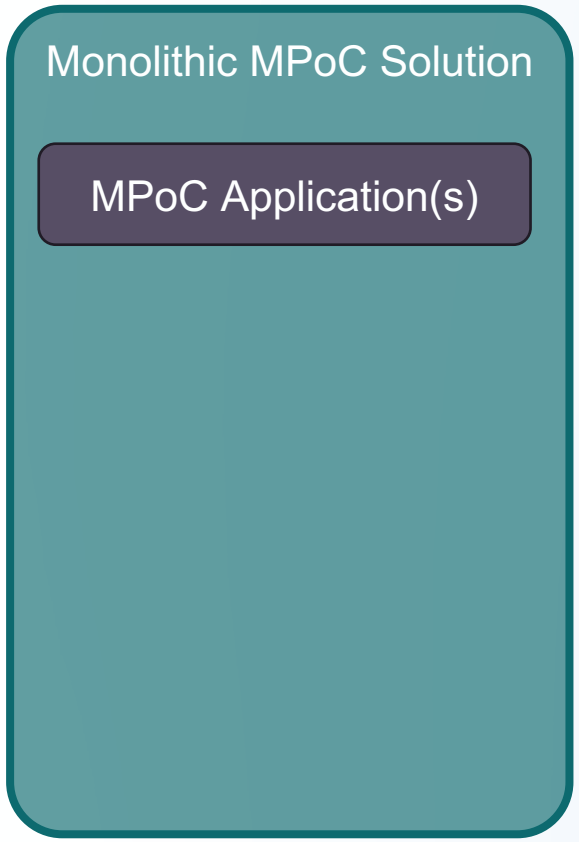
- A mobile/tablet device running Android/iOS
- A mobile/tablet device not running Android/iOS
- A non-consumer / commercial device, if it meets all other criteria (such as not designed solely for payments)
- A device which does not implement 'Google Play' store/services

COTS examples **NOT** suitable for consideration under MPoC:

- A 'bare board' device (such as a Raspberry Pi or BeagleBoard)
- A device which integrates an SCRP into a single formfactor/device
- A device which uses an external NFC antenna (physically separate, not an SCRP)
- A multi-part device (e.g. a device with a touch screen coupled with another device that does most of the processing)

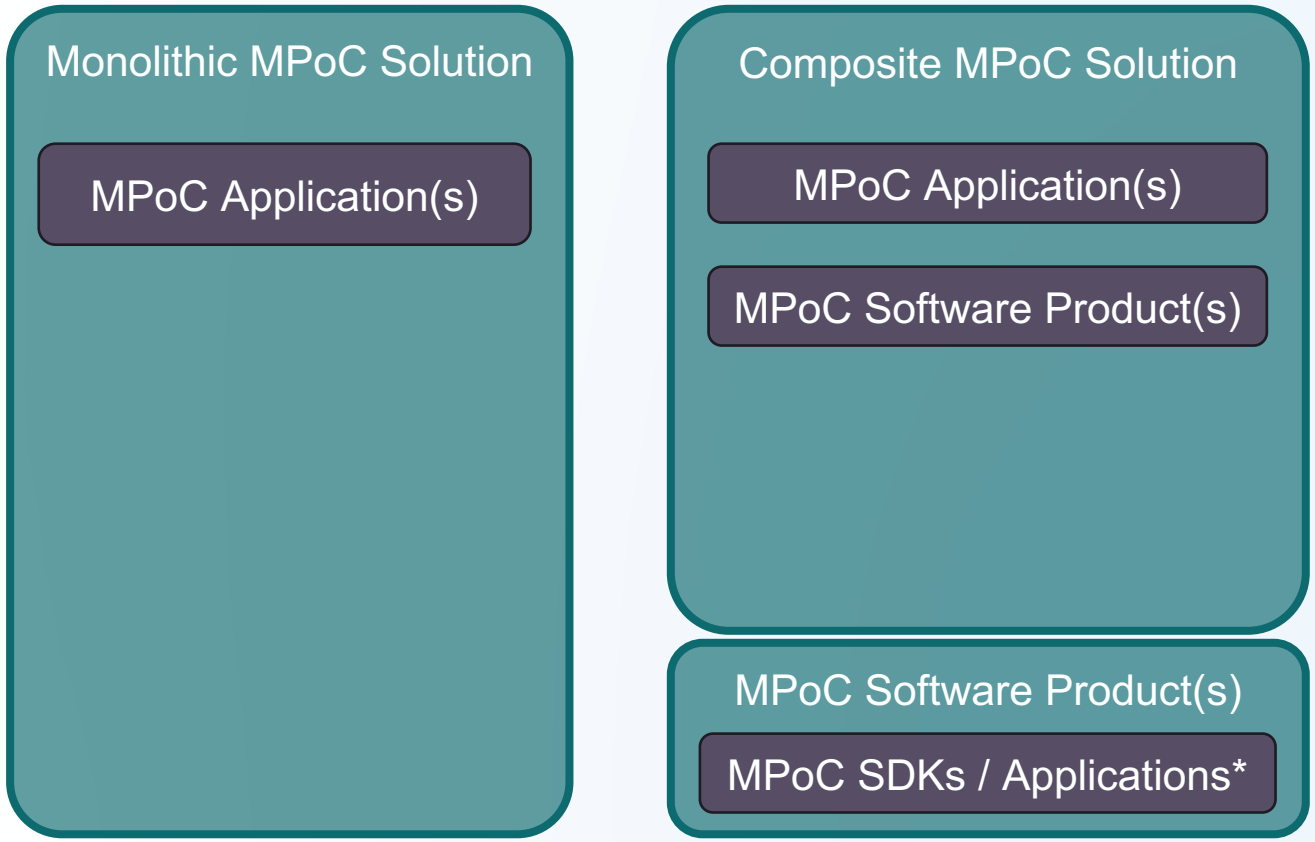
PCI Security Standards Council

MPoC Products Interaction

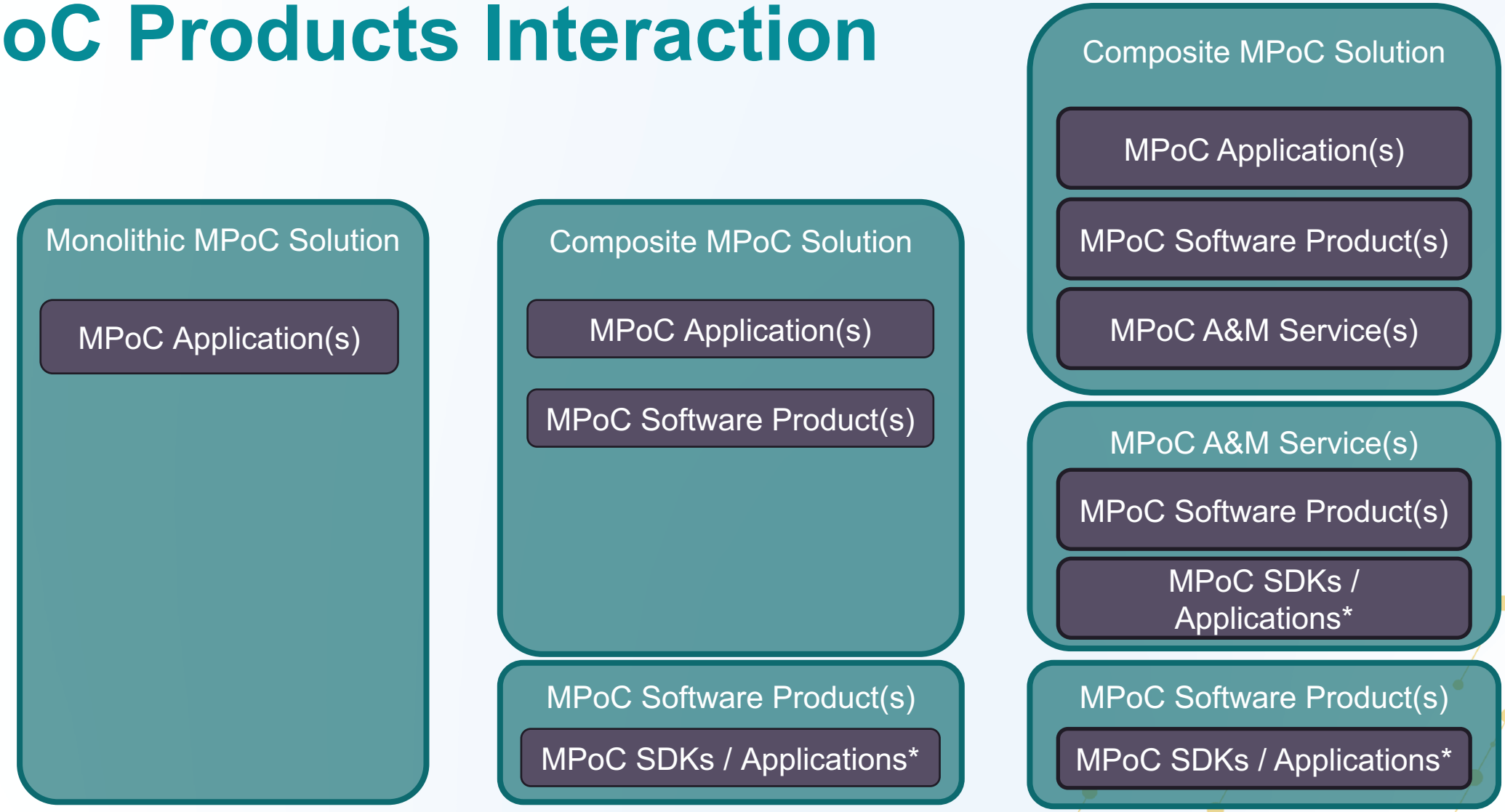


PCI Security Standards Council

MPoC Products Interaction

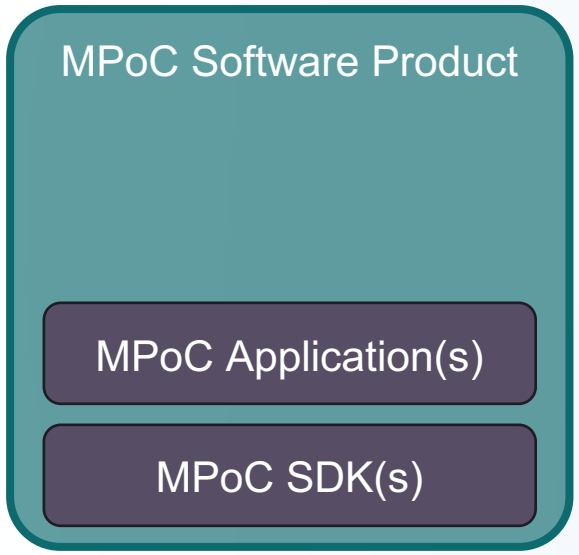


MPoC Products Interaction



PCI Security Standards Council

MPoC Applications and MPoC Software Products



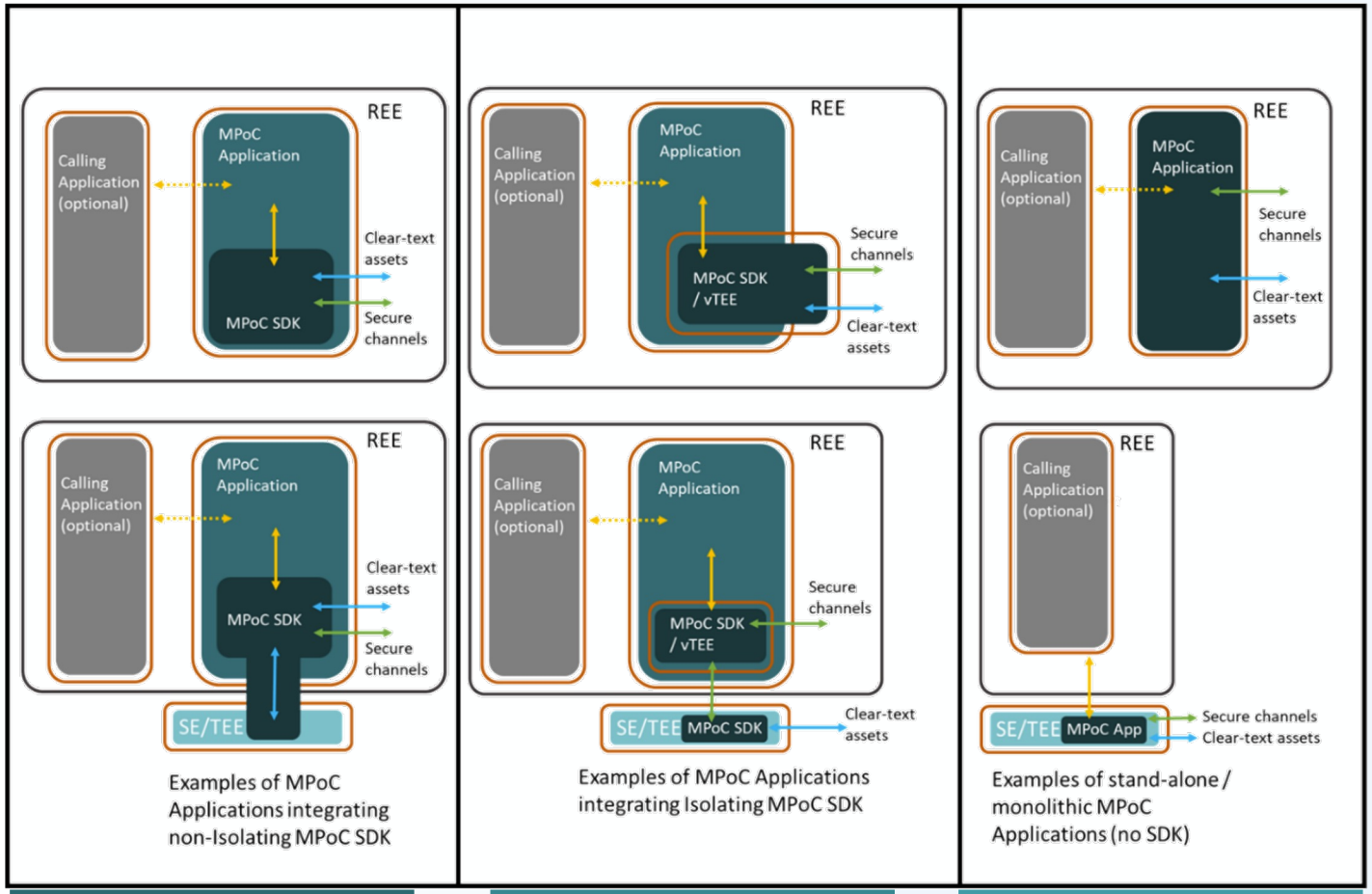
Technical aspects assessed against Domains 1 & 2

How are the operational aspects of the MPoC Application managed?

- Key management?
- Application distribution?
- Merchant relationship?
- A&M operation?

These are assessed when the MPoC Application is integrated into an overall MPoC Solution

Figure 3: Examples of MPoC Application Implementations



Complete testing required under Sections 2A & 2B

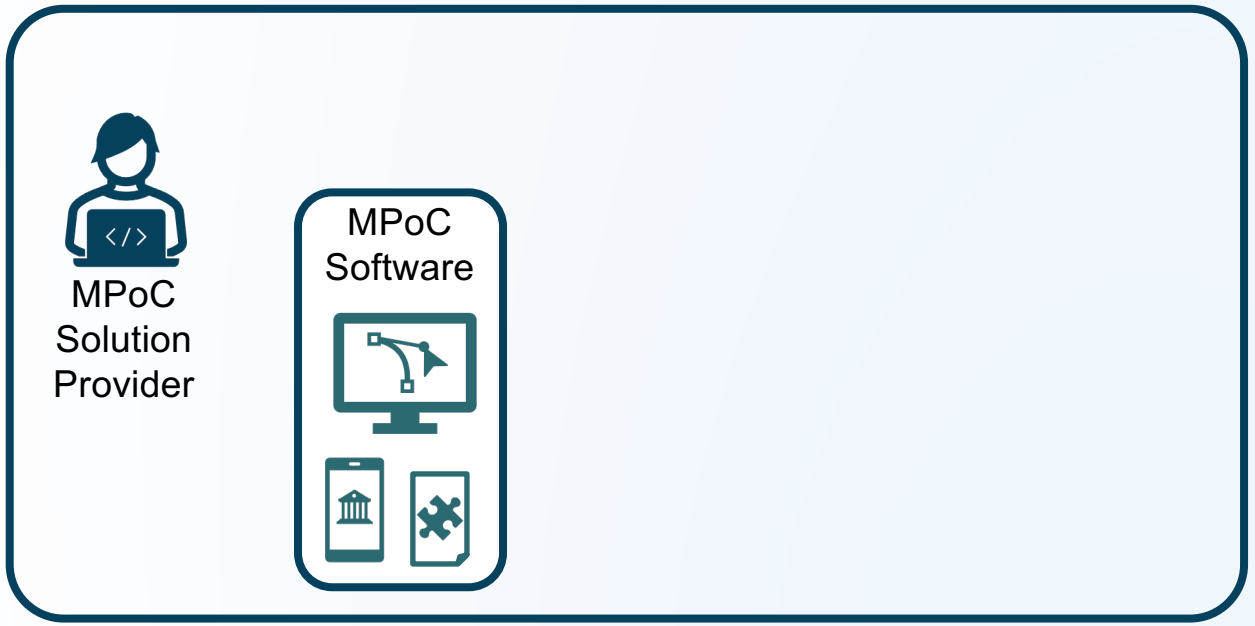
Lighter testing required under Section 2A

No testing required for calling application

Example MPoC Deployment Scenario

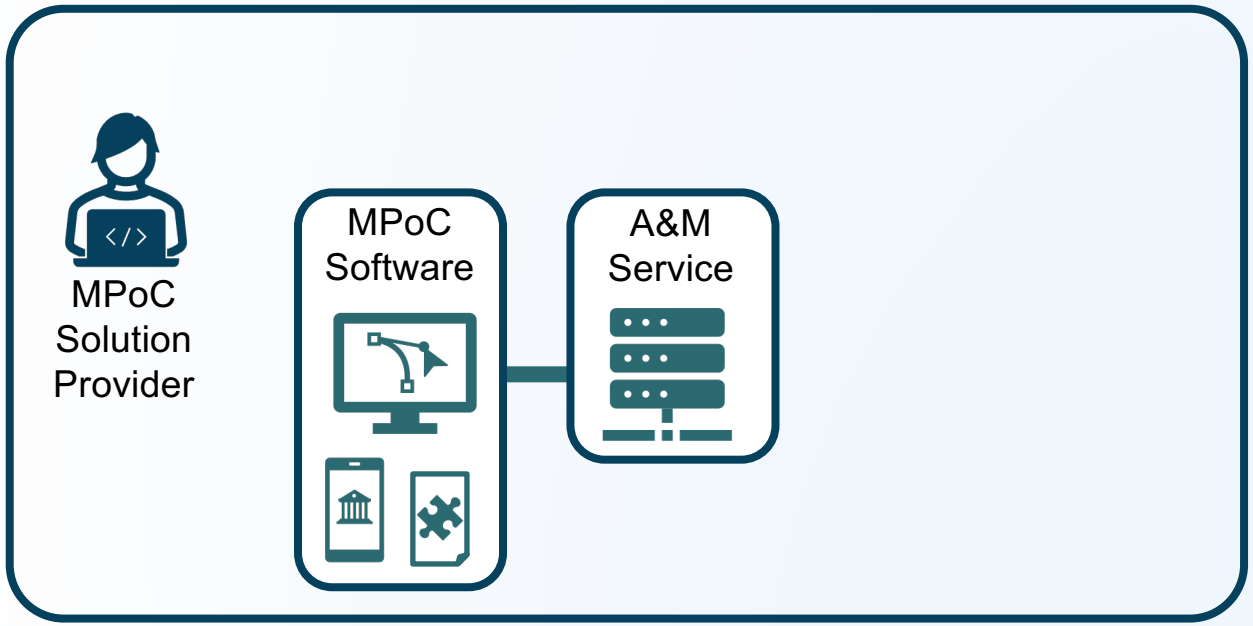
MPoC Solution Provider

Example MPoC Deployment Scenario



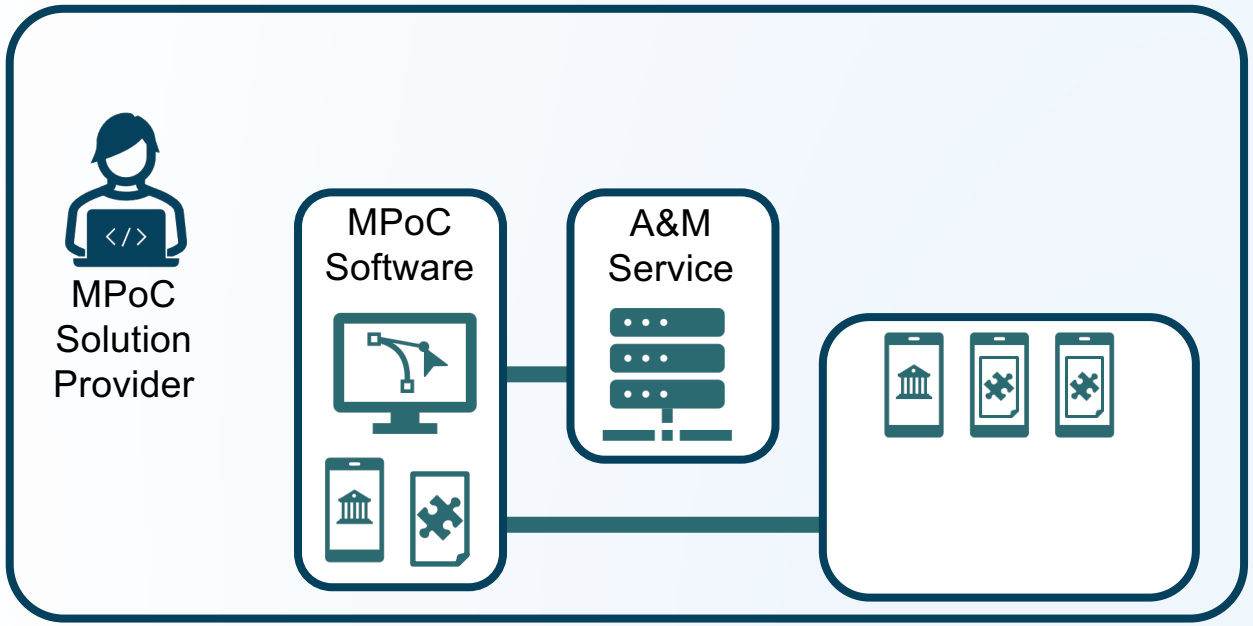
PCI Security Standards Council

Example MPoC Deployment Scenario



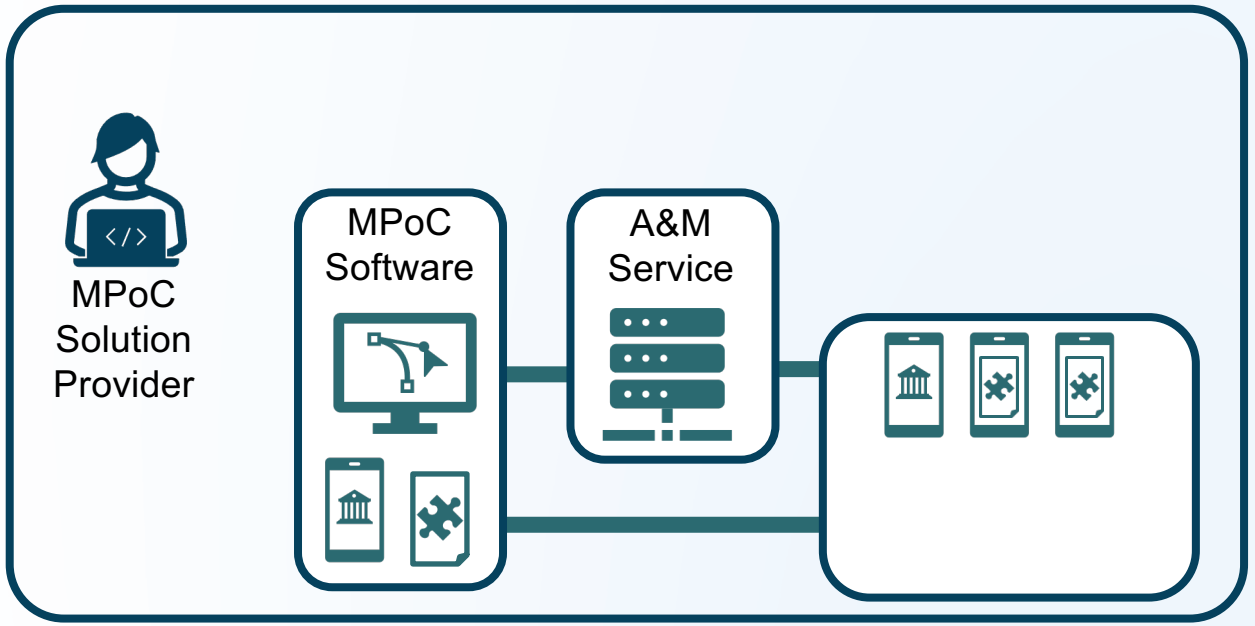
PCI Security Standards Council

Example MPoC Deployment Scenario



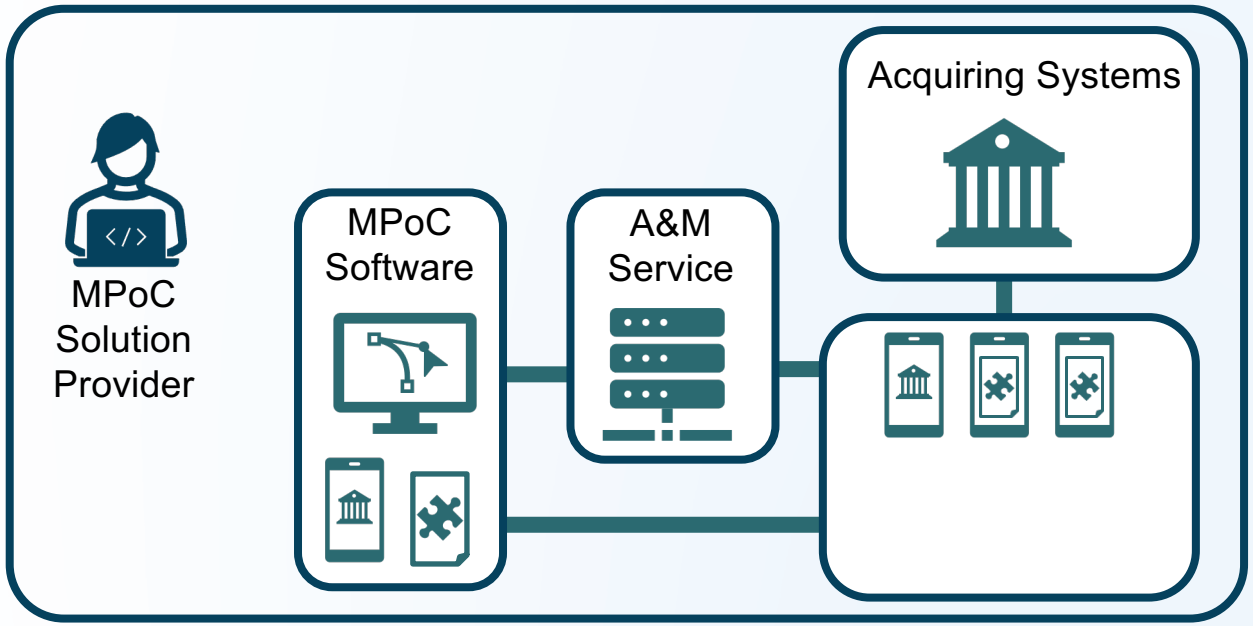
PCI Security Standards Council

Example MPoC Deployment Scenario



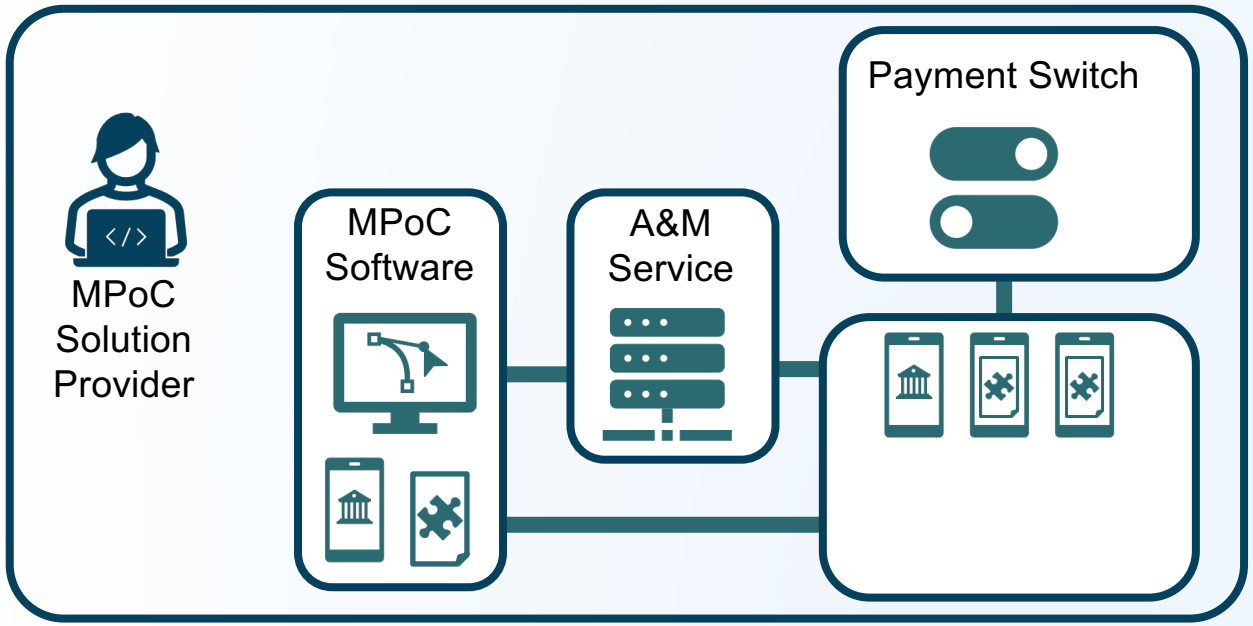
PCI Security Standards Council

Example MPoC Deployment Scenario



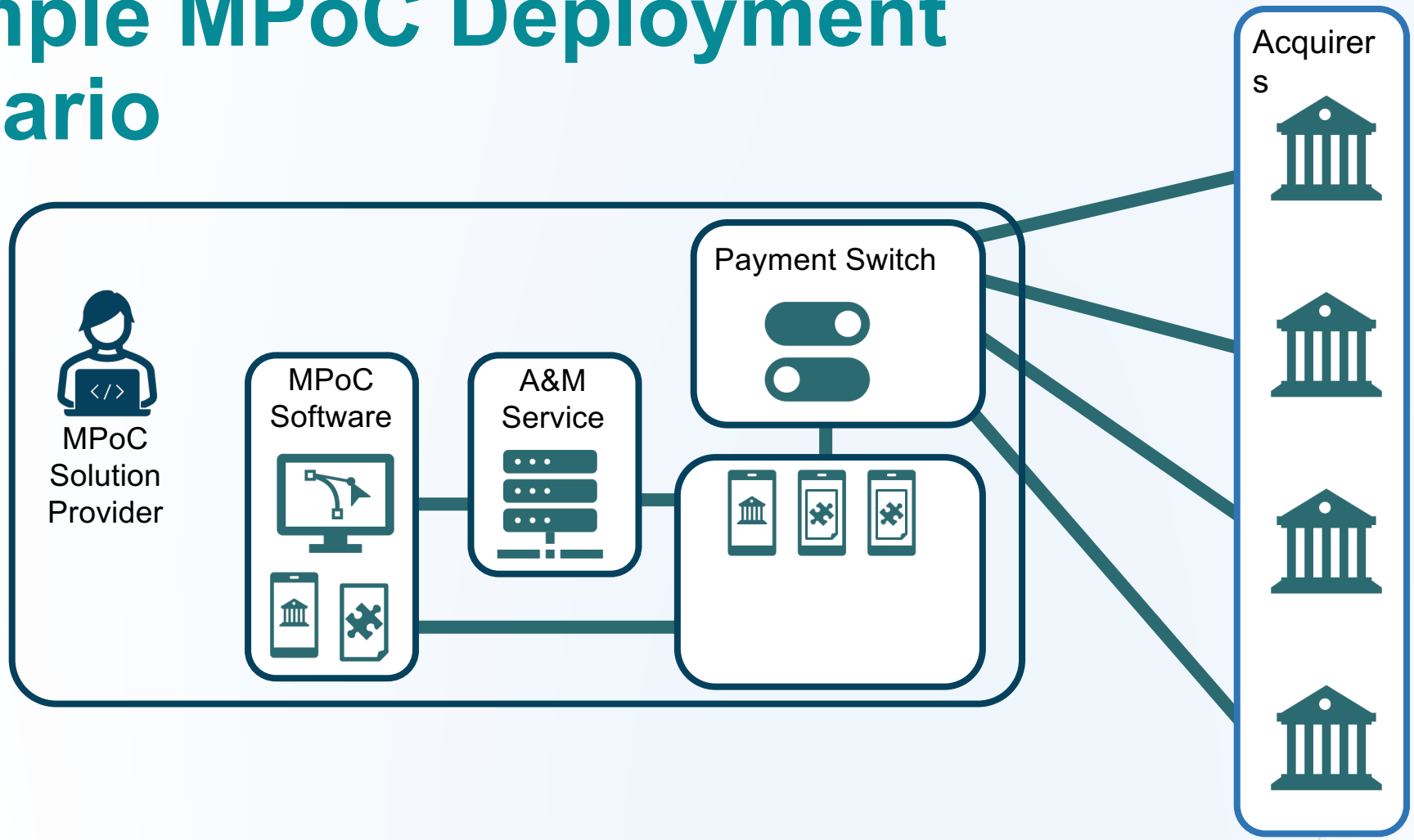
PCI Security Standards Council

Example MPoC Deployment Scenario



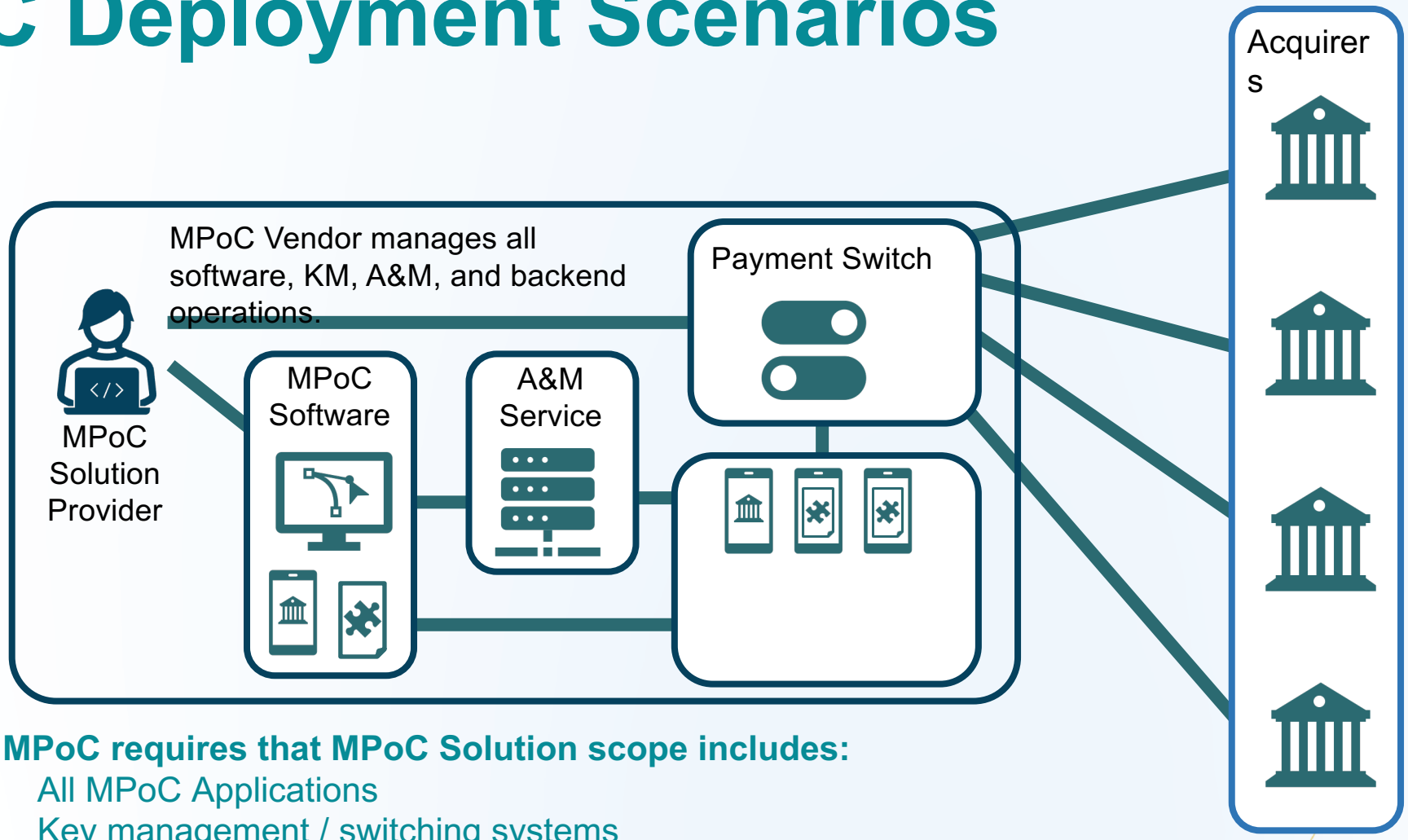
PCI Security Standards Council

Example MPoC Deployment Scenario



PCI Security Standards Council

MPoC Deployment Scenarios

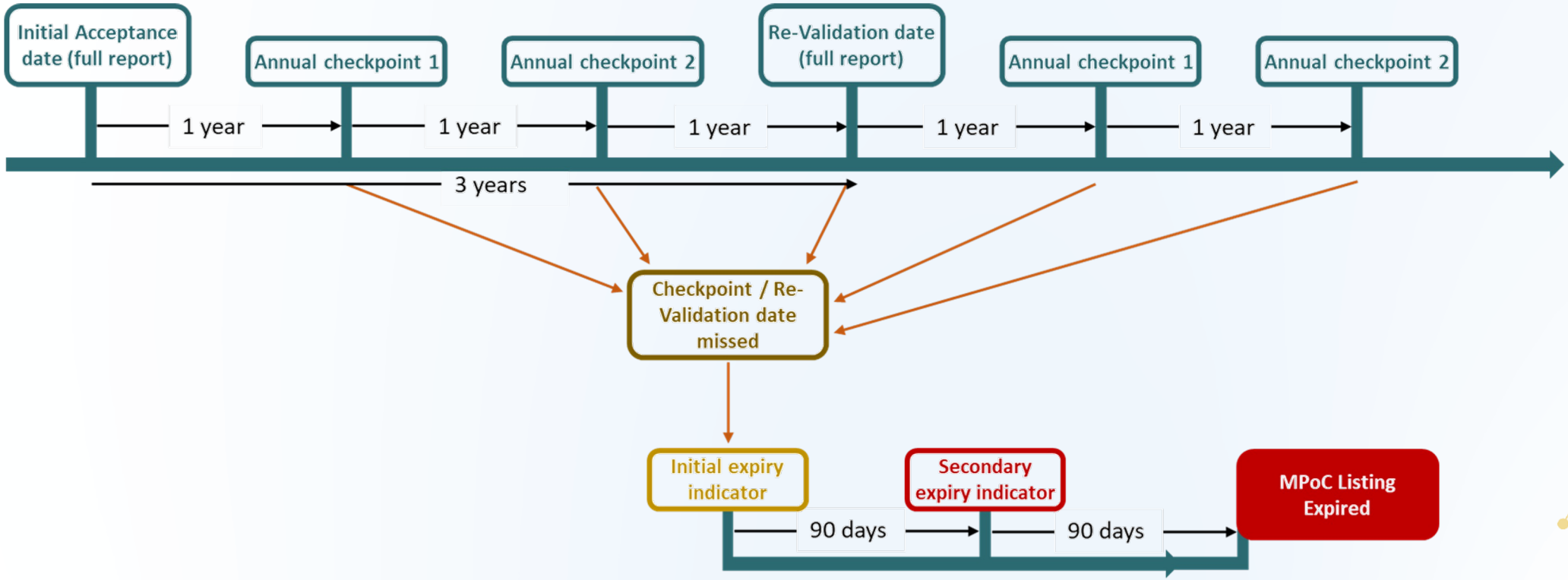


MPoC requires that MPoC Solution scope includes:

- All MPoC Applications
- Key management / switching systems

PCI Security Standards Council

MPoC Listing Cycle

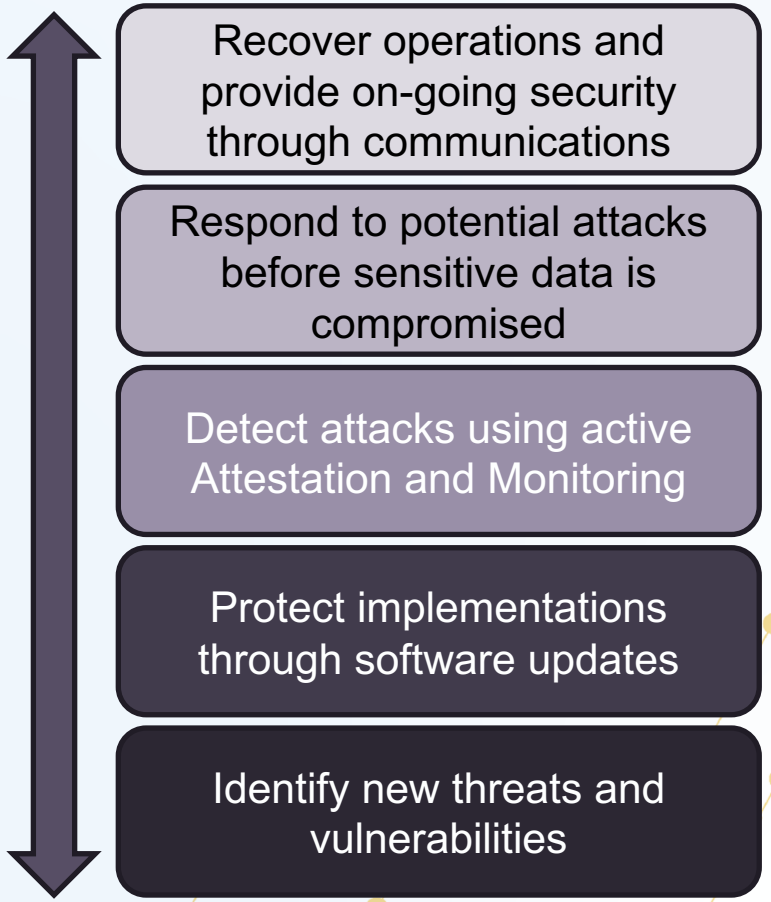


Submission of checkpoint /
Re-validation during this period returns
MPoC Product to good standing

PCI Security Standards Council

MPoC Foundations

- The MPoC Software/Solution vendor does not control the COTS platforms on to which they deploy
- COTS platform security changes over time
- EMV-based transactions provide additional security when compared to magnetic stripe and manual PAN transactions
- New threats and security vulnerabilities are discovered almost every day
- MPoC Software is updated as required to protect against new attacks and vulnerabilities
- A&M systems are also continually updated to detect and respond to new attacks and vulnerabilities
- Merchant communications is essential to ensure they are kept secure and able to transact securely



PCI Security Standards Council

MPoC Annual Checkpoint

During Year 1 of 3
MPoC Vendors should prepare for Annual Checkpoint #1:

To avoid early administrative Expiry (Section *4.1.1*) - Starting on Day 1 (the date of initial Acceptance) – up to 12 Months after initial Acceptance:

The MPoC Vendor adopts the *MPoC Standard* requirements applicable to their MPoC Product as BAU to ensure their MPoC Product remains in compliance with the *MPoC Standard*.

Compliance of the MPoC Vendor and their MPoC Product with the *MPoC Standard* is BAU and directly aligned with security requirement timeframes as defined in *Table 2. Security Requirement Timeframes* of the *MPoC Standard*.

- No impact Changes are BAU and have supporting evidence as per the *MPoC Standard*. No impact Changes are not reported to the MPoC Lab until the following year (Annual Checkpoint #1).
- Administrative or implementation Changes are reported to the MPoC Lab as follows:
  - Any administrative Changes are submitted to PCI SSC by the same MPoC Lab that Validated the MPoC Product.
  - Any implementation Changes are submitted to PCI SSC by the same MPoC Lab that Validated the MPoC Product.
- Any implementation Changes that result in previously not-applicable requirements of the *MPoC Standard* becoming applicable after the Change, are adopted as per the *MPoC Standard*.

Compliance with the VRA is BAU.

Annual Checkpoint #1
MPoC Vendors should begin this checkpoint on or before the start of Year 2:

To avoid early administrative Expiry (Section *4.1.1*) - Annual Checkpoint #1 is due on or up to 90 days before the 12 Month anniversary of initial Acceptance.

The previous year's (Year 1) BAU compliance of the MPoC Vendor and their MPoC Product with the *MPoC Standard* must be Evaluated by the same MPoC Lab that Validated the MPoC Product for initial Acceptance (or else a full Evaluation is required).

The MPoC Vendor must attest and provide to the MPoC Lab for review:

- Confirmation of all No impact Changes that occurred 0-12 Months after initial Acceptance. All No impact Changes are reported to the MPoC Lab.
- Confirmation any administration Changes from 0-12 Months after Initial Acceptance were already submitted to PCI SSC by the same MPoC Lab that Validated the MPoC Product. Any previously un-reported administration Changes that occurred from 0 to 12 months after initial Acceptance are reported to the MPoC Lab.
- Confirmation any implementation Changes from 0-12 Months after initial Acceptance were already submitted to PCI SSC by the same MPoC Lab that Validated the MPoC Product. Any previously un-reported implementation Changes that occurred from 0 to 12 months after initial Acceptance are reported to the MPoC Lab.

The MPoC Vendor will permit the MPoC Lab to perform Live Testing of the MPoC Product to ensure that the MPoC Product complies with the *MPoC Standard*.

PCI Security Standards Council

MPoC – Status and Release

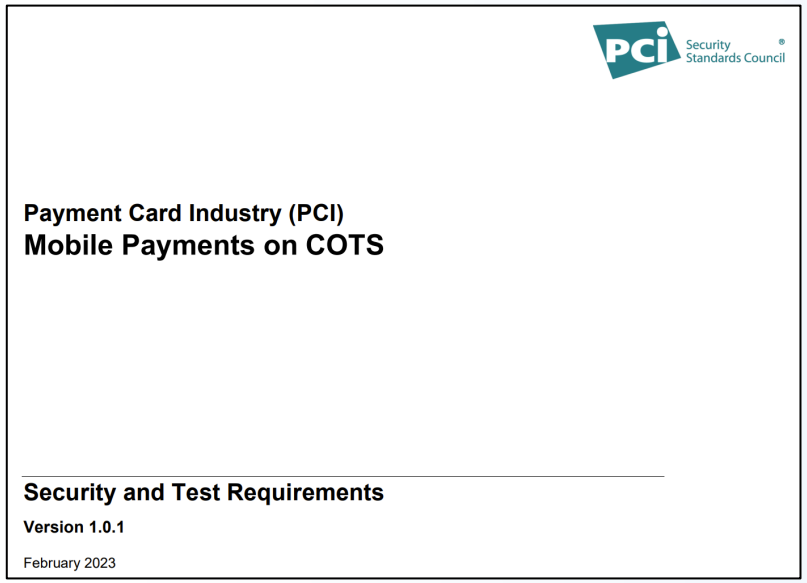
2022 Community Meetings

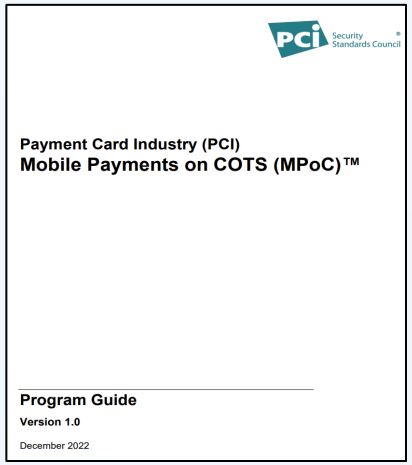
Portal and SPoC/CPoC Migration
Details to Come Q1/Q2 2023

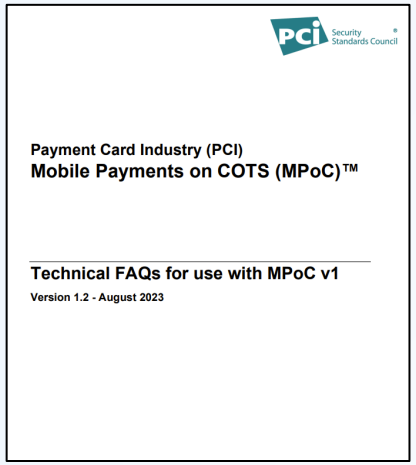
PCI Security Standards Council

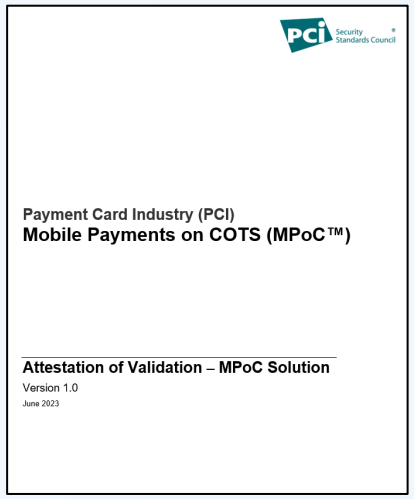
PCI MPoC – Status

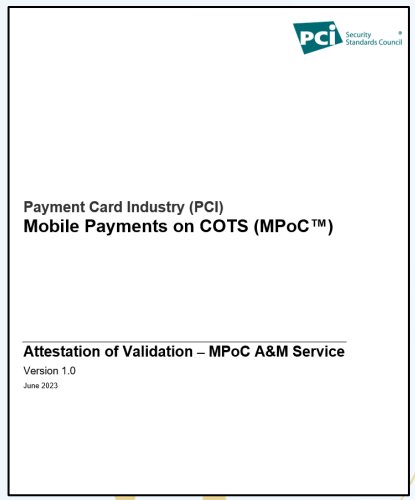
Current Status - 2023

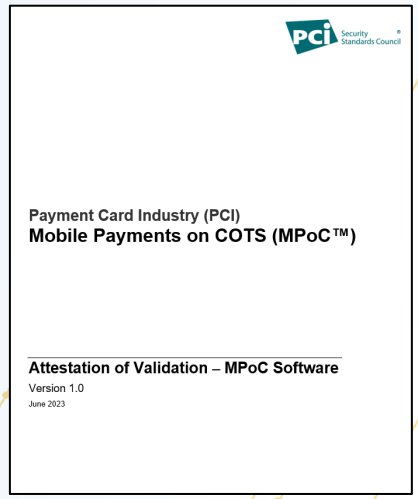












Summary

EMVCo & PCI SSC Working Together

- Security for mobile acceptance requires operational correctness as well as secure implementation:
  - EMV TapToMobile focuses on the operational aspects
  - PCI MPoC focuses on the security aspects
- EMVCo and PCI SSC are working together to help secure the next generation of acceptance products
- Mobile devices and terminals provide different benefits, and will continue to co-exist in acceptance environments

Talking Mobile Payments in 2015

PCI Security Standards Council

PCI Security Standards Council

Thank you!