Mobile Security and Standards Update

Andrew Jamieson, *PCI Security Standards Council*
Arman Aygen, *EMVCo*

Who is EMVCo?

EMVCo enables card-based payments to work seamlessly and securely worldwide.

Mission:

To facilitate the worldwide interoperability of secure payment transactions by developing and publishing the EMV® Specifications and their related testing processes

Specifications

Create, evolve and promote EMV Specifications

Approval and Evaluation

Facilitate approval and evaluation of products for compliance with EMV Specifications

EMVCo Marks

Manage marks that denote implementation of the EMV Specifications

Industry Engagement and Collaboration

Engage and collaborate with the payments industry

Industry Engagement

EMVCo engages with industry, regional and national bodies to help shape specifications that support the advancement of the global payment ecosystem.

EMVCo

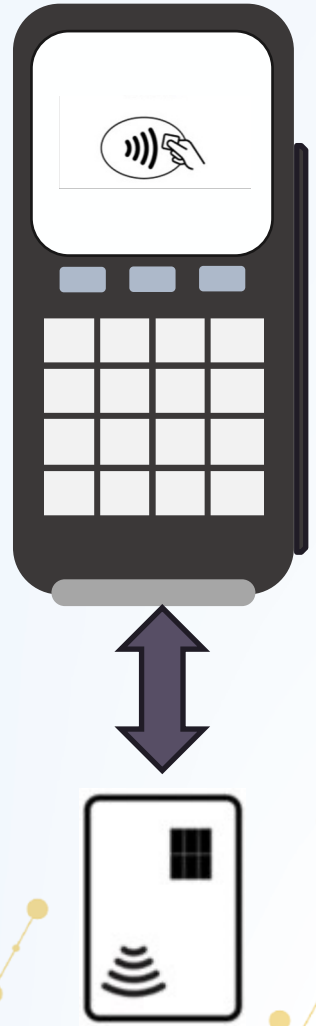
EMVCo & PCI SSC: Securing Payments Together

PCI Security Standards Council EMVCo

EMVCo & PCI SSC: Promoting Standards for 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

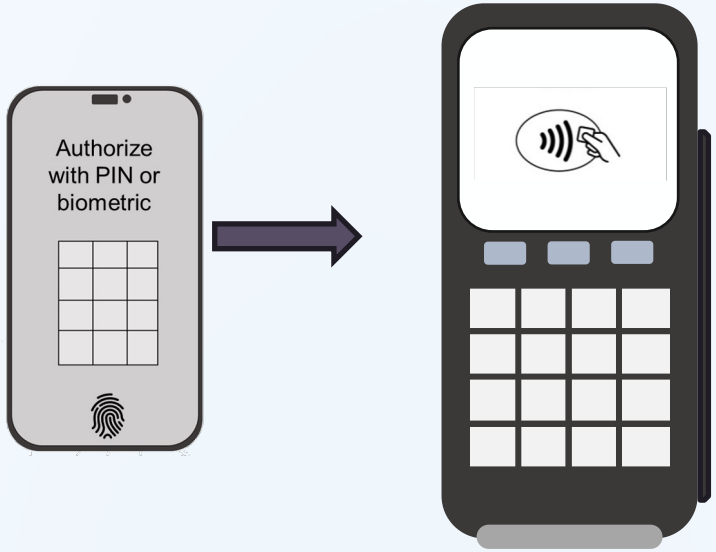
Offline PIN

PIN sent to card for validation

Online PIN

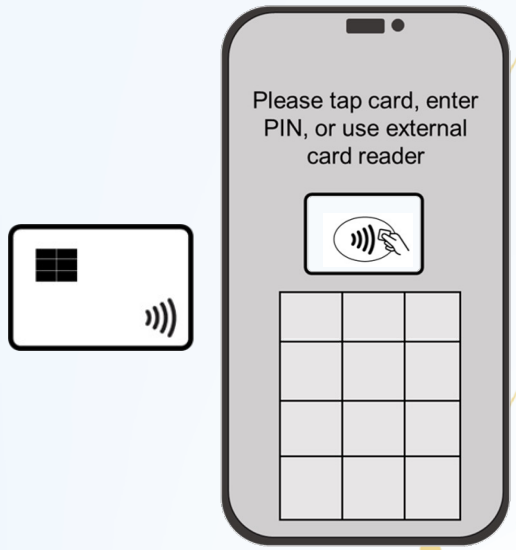
PIN sent to Issuer for validation

CDCVM



Cardholder authenticates on their own mobile device

SPoC

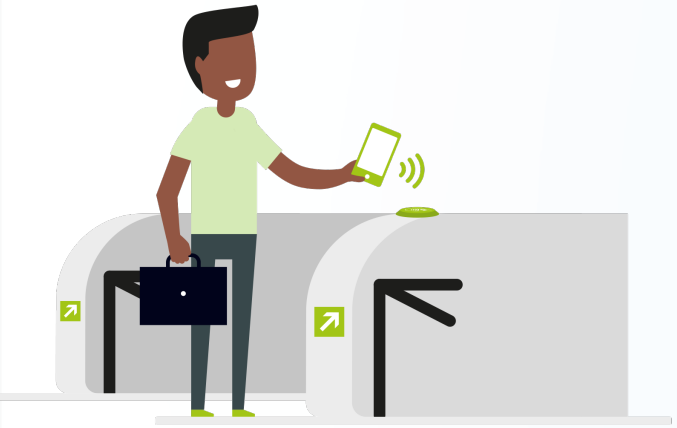


Cardholder authenticates on the merchant mobile device

PCI Security Standards Council

EMVCo

Contactless & Mobile Demand Drivers



Mobile devices have been used for payment for decades.

Initially based on SMS, it evolved into contactless.

Contactless and NFC offered the possibility for EMV® Chip transactions **beyond cards** with **mobiles** and **wearables**.

Now, this convenience is expanding from *making* payments with such devices, to *taking* payments on mobile.

- **1997** — Coca-Cola vending machines with SMS payment. Exxon Mobile uses RFID for payments.
- **1999** — Movie tickets purchasing through some mobile phones.
- **2001** — Domino's Pizza takes orders through cell phones.
- **2004** — Donations to nonprofit organizations through SMS.
- **2009** — Mobile payment market crosses $69 billion in sales.
- **2011** — Google introduces its wallet service.
- **2014** — Apple introduces Apple Pay
- **2015** — Samsung Pay and Android Pay become available.
- **2018** — Android 9 introduced with TapToMobile
- **2022** — Apple introduces Tap to Pay on its phones

Source: PeerBits, 2023

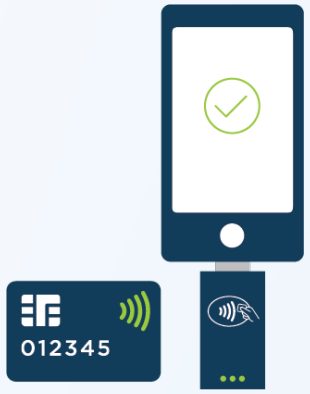
EMVCo

Evolution of consumer card acceptance devices

Dedicated devices were used for all acceptance environments to ensure:

- Interoperability
- Security
- A great user experience

Even in the most demanding acceptance environments, such as transit and retail.



Small businesses started using consumer mobile phones for payment, enabled through dedicated accessories embedding:

- Magstripe
- Contact
- And contactless readers

These accessories allow full compliance with EMV® Specifications (and PCI requirements).

Even more recently, NFC enabled devices are used for contactless card acceptance.

These devices can be:

- Off-the-shelf mobile phones
- Devices designed for professionals with payment in mind (but not as primary/sole use case)

EMVCo

The rise of mobile acceptance

Merchants have requested EMVCo explore mobile acceptance to promote familiarity and consistency for consumers.

Why?

- Contactless payments continue to grow post-pandemic.
- Merchants can easily accept payments anywhere in store.
- The growth of acceptance on mobile is hindered by the lack of consistent experience.
- Mobile-to-mobile payments open up the world of commerce:
  - **Independent vendors**, like electricians or window cleaners can accept payments on the move.
  - **Convenience retailers**, such as fast-food outlets and coffee shops, can accept payments anywhere.
  - **Transit operators** can easily accept card payments during journeys.

The Merchant Advisory Group (MAG) has joined discussions with EMVCo:

"We pushed for a more open usage of the new tap-on-glass technology, which could lead to a use case in which merchants can implement this technology for scan-in-store situations."

Expanding the Merchants' Voice, John Drechny, CEO, Merchant Advisory Group

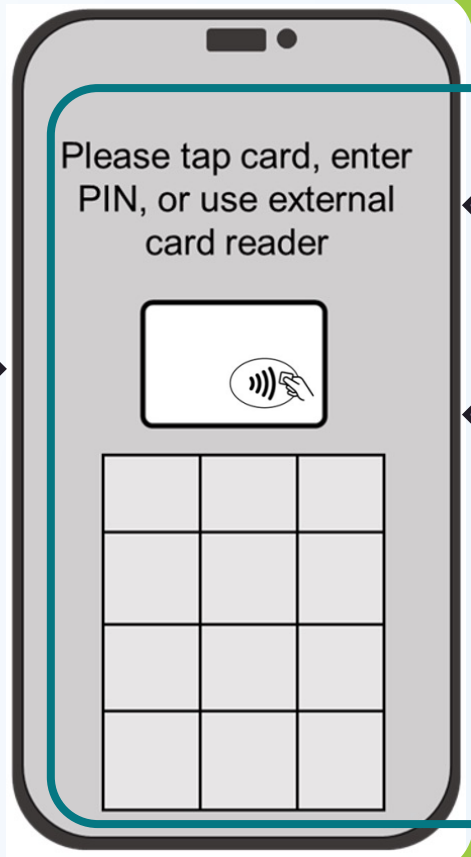
"Technology is now available to accept physical transactions without needing a dedicated physical terminal. Instead, the merchant's own smartphone can become a fully secure, PIN-enabled POS terminal. This technology, commonly known as SoftPOS, will change the world of commerce and payment acceptance."

Aite-Novarica (now Datos Insights)
Global Implementation of SoftPOS: The Next Generation of POS, April 2023

Improving Mobile Payment Acceptance Security And Interpretability

Communication between mobile device and payment instrument performed to EMV specifications

EMVCo is defining minimum acceptance criteria and evaluation process for ‘mobile’ devices



PIN & Payment processing

A&M Service

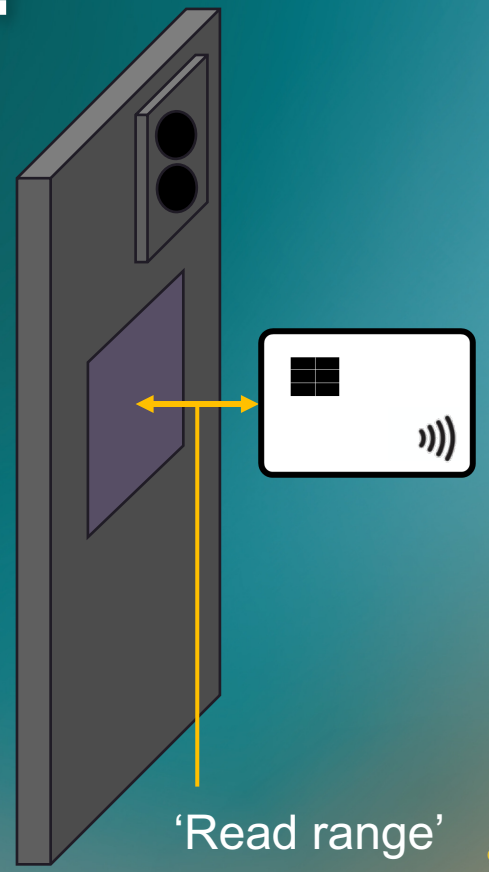
PCI MPoC validates the security of the MPoC Software, MPoC A&M Service, and MPoC Solution

PCI Security Standards Council

EMVCo

What Is TapToMobile?

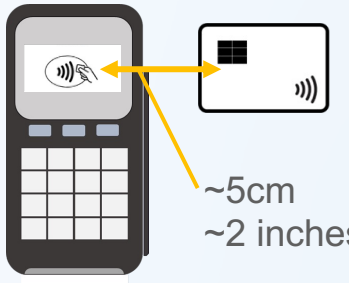
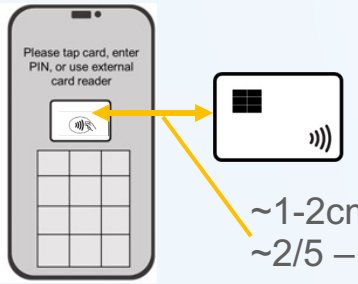
- EMVCo released the TapToMobile User Experience Guidelines in August 2021, focusing on the user experience aspects of Mobile Devices:
    - Where do I tap?
    - Point to tap may be on the reverse side of the screen
    - No fallback to chip or magstripe
- EMVCo launched its COTS (Commercial Off The Shelf) **Early Adopter Programme** in October 2020 until April 2022.
- A number of NFC-enabled devices were evaluated with respect to their ‘compatibility’ with EMV® compliant cards and mobiles.
- One of the major findings is that user experience on these devices depends mainly on their NFC strength or ‘read range’.



What's Next For EMVCo TapToMobile?

Introduce minimum acceptance criteria and an evaluation process for 'mobile' devices, in addition to those for POS devices, in function of the following levels of user experience:

- **Payment is seamless**, and keeping the traditional terminal LoA as is.
- **Payment is possible** and introducing a new Reduced Range X (namely 1 or 2cm) LoA.

Payment User Experience	Seamless	Possible
Applicable device	POS device  Open to any device	'Mobile Device'  Limited to handheld 'mobile' devices

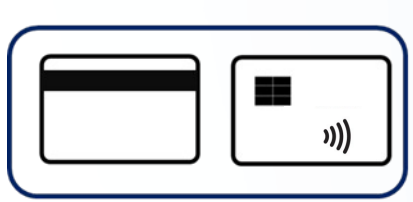
- EMVCo expects that Reduced Range acceptance criteria will evolve over time to support devices moving toward the seamless experience.

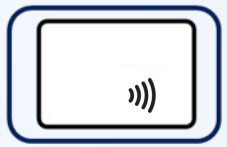
EMVCo

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

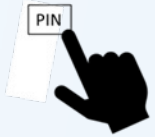
So; no PIN entry only, no MSR only*, no use of external SCRP with no account data input on the COTS device*



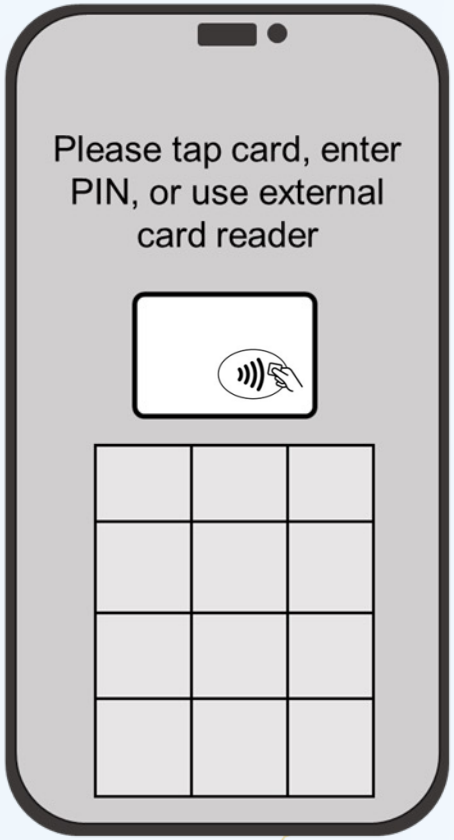


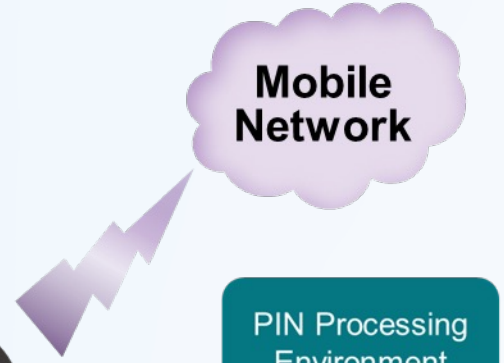
Mobile device can be used for reading contactless card

PINs can be entered directly into mobile device



External card readers can also be used for contact, MSR, and contactless cards





PIN Processing Environment

Payment Processing Environment

Attestation and Monitoring Environment

PCI Security Standards Council

* '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:

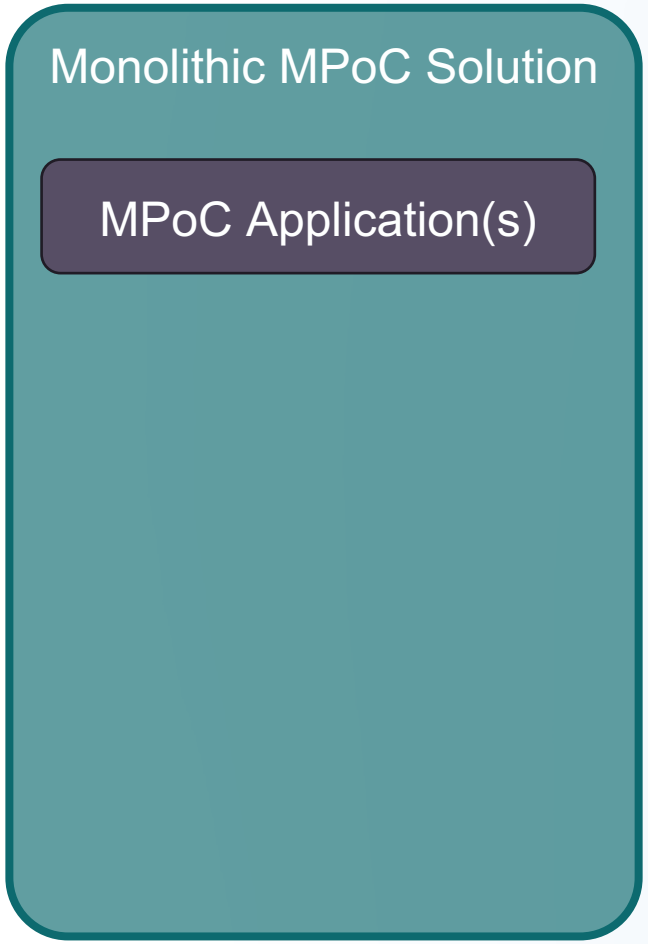
- A mobile/tablet device running Android/iOS
- A mobile/tablet device not running Android/iOS
- A non-consumer / commercial device, if it meets all other criteria (such as not designed solely for payments)
- A device which does not implement 'Google Play' store/services

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)

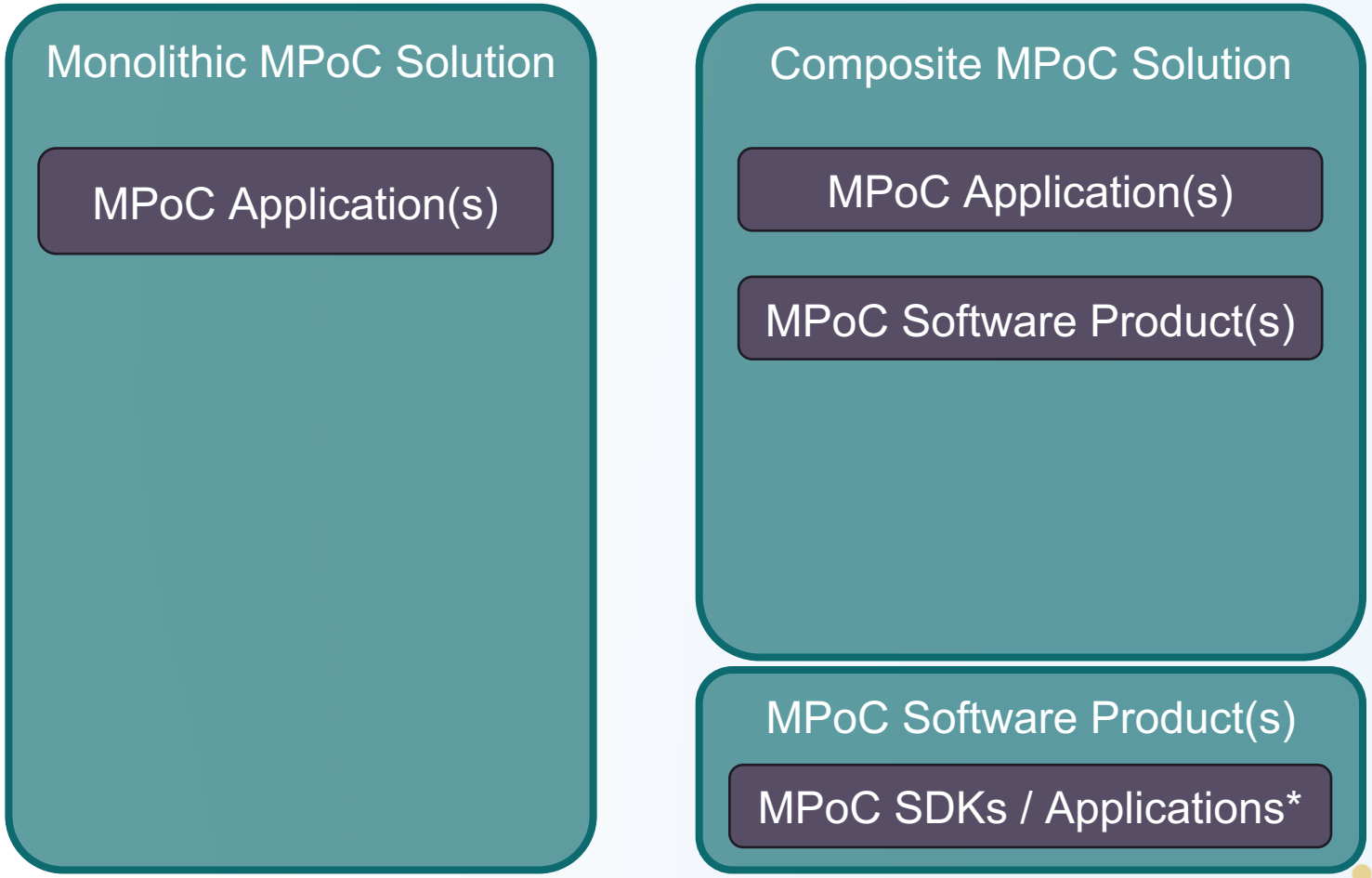
PCI Security Standards Council

MPoC Products Interaction



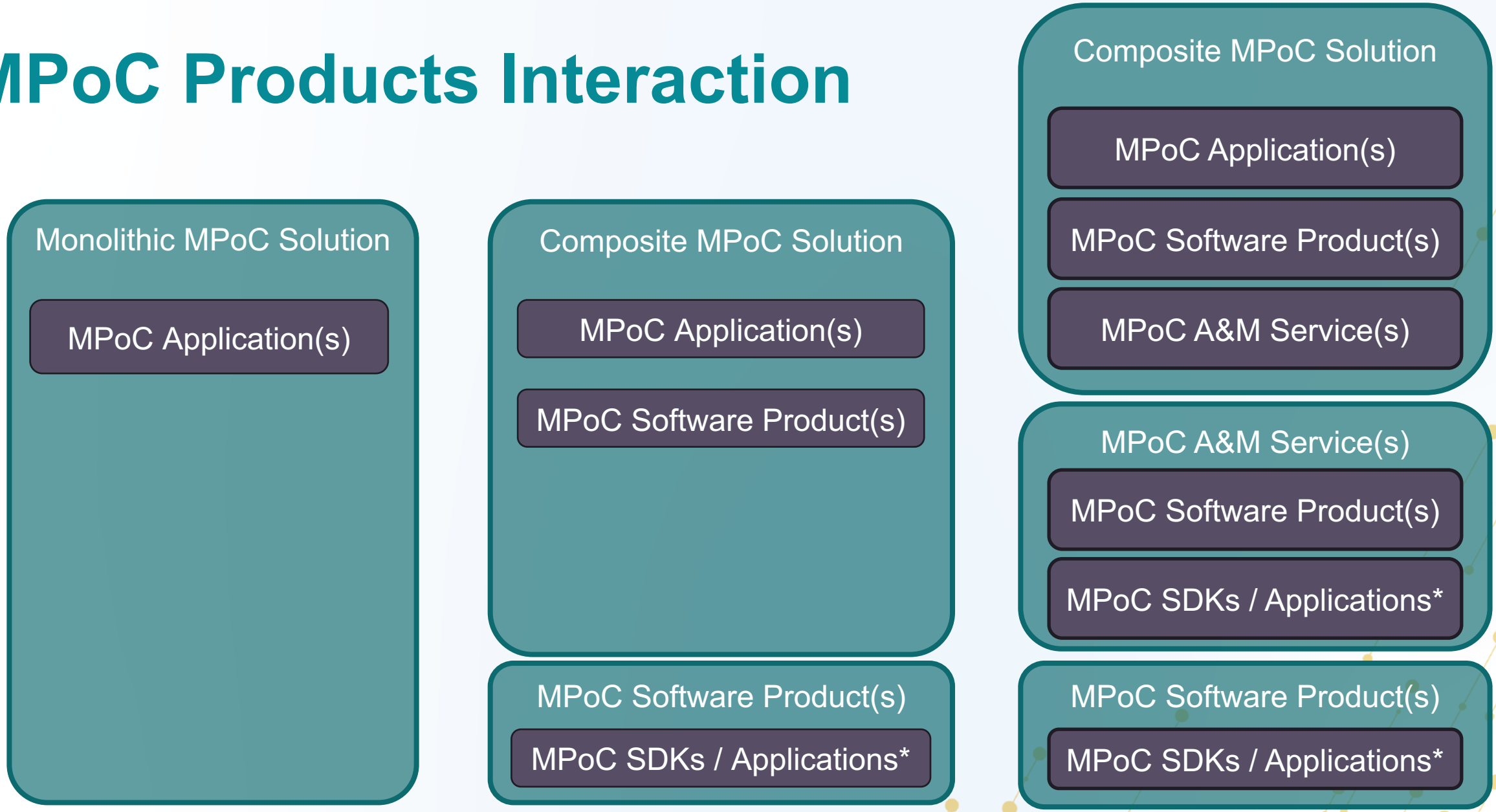
PCI Security Standards Council

MPoC Products Interaction



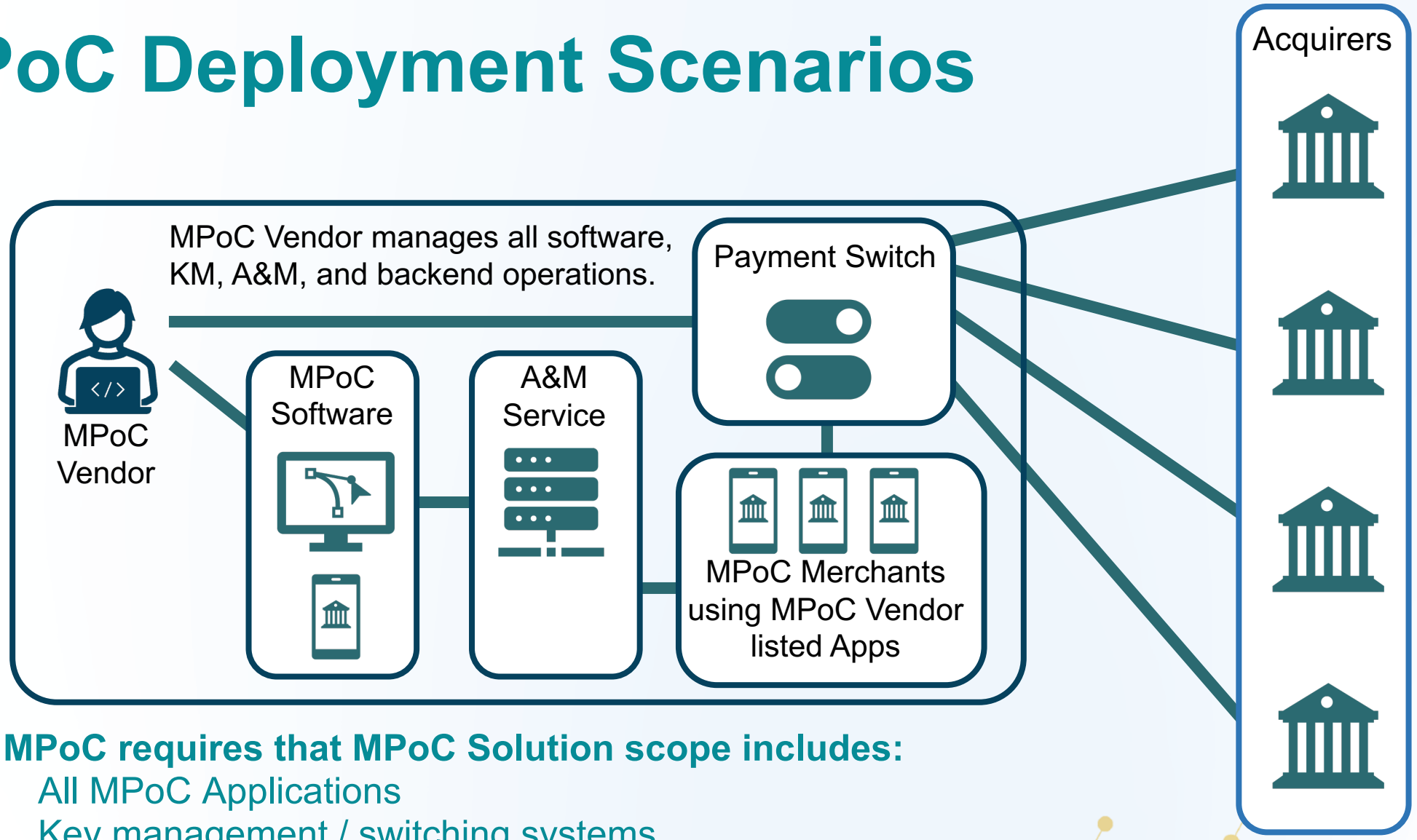
PCI Security Standards Council

MPoC Products Interaction



PCI Security Standards Council

MPoC Deployment Scenarios

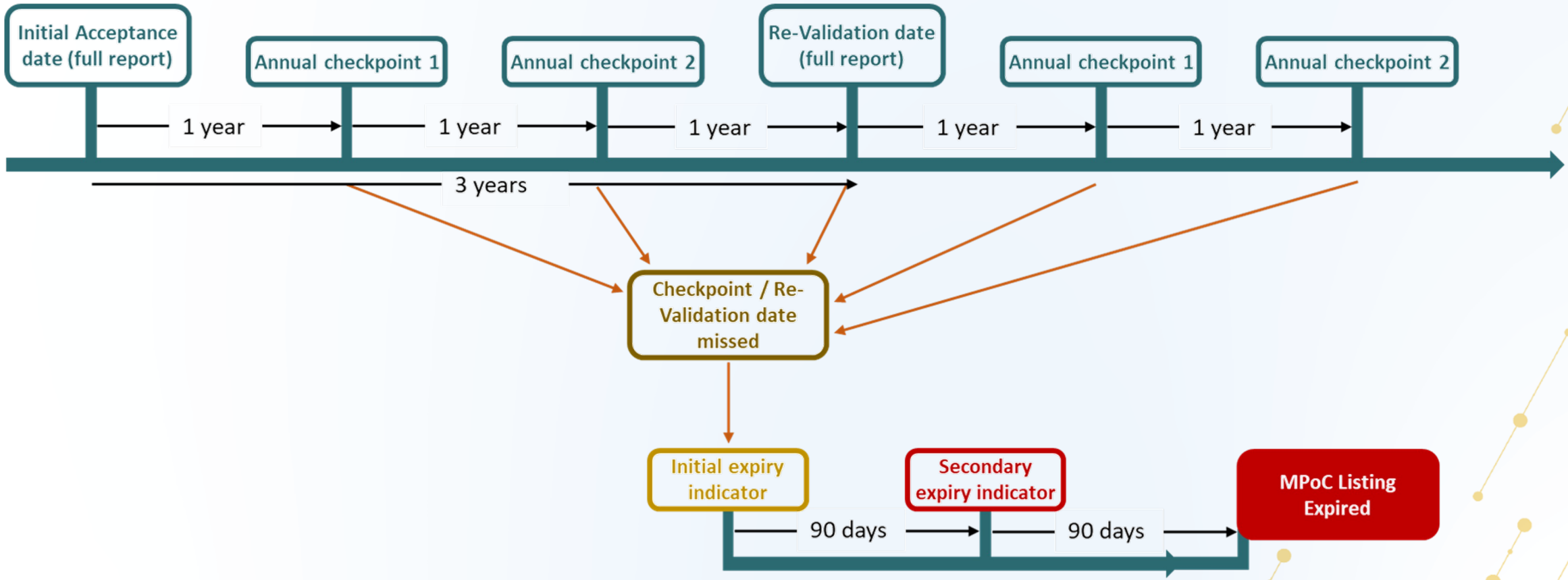


MPoC requires that MPoC Solution scope includes:

- All MPoC Applications
- Key management / switching systems

PCI Security Standards Council

MPoC Listing Cycle

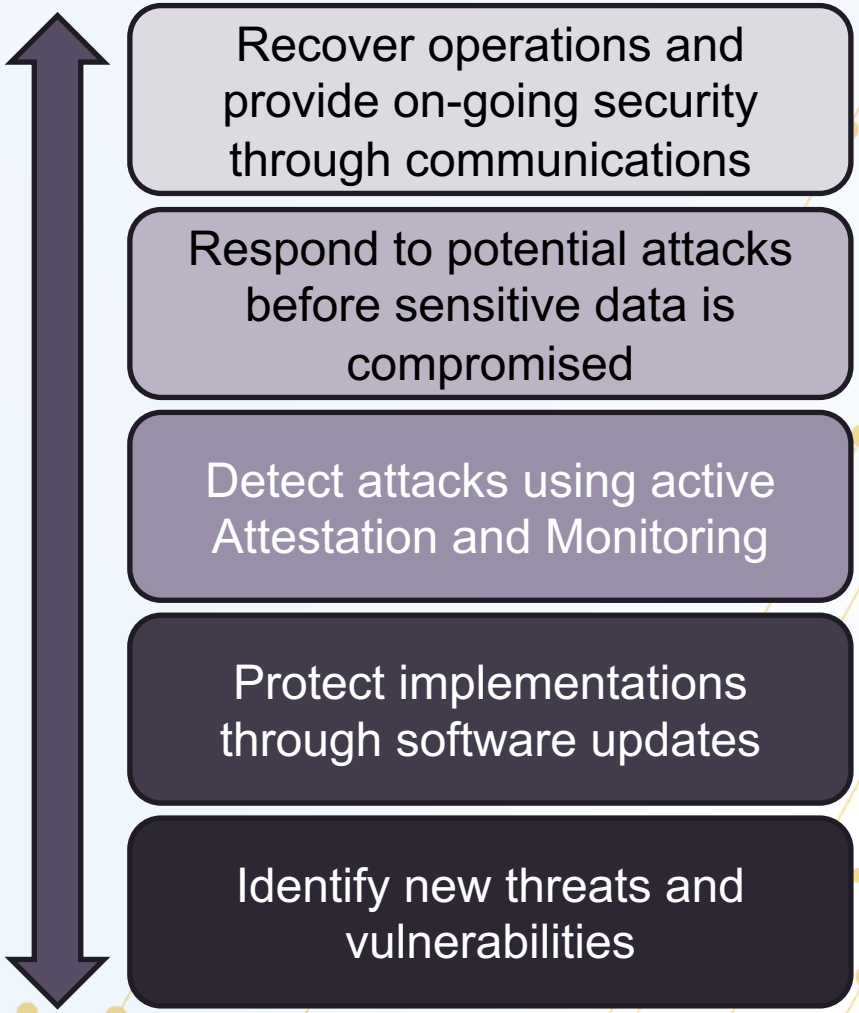


Submission of checkpoint / Re-validation during this period returns MPoC Product to good standing

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 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:

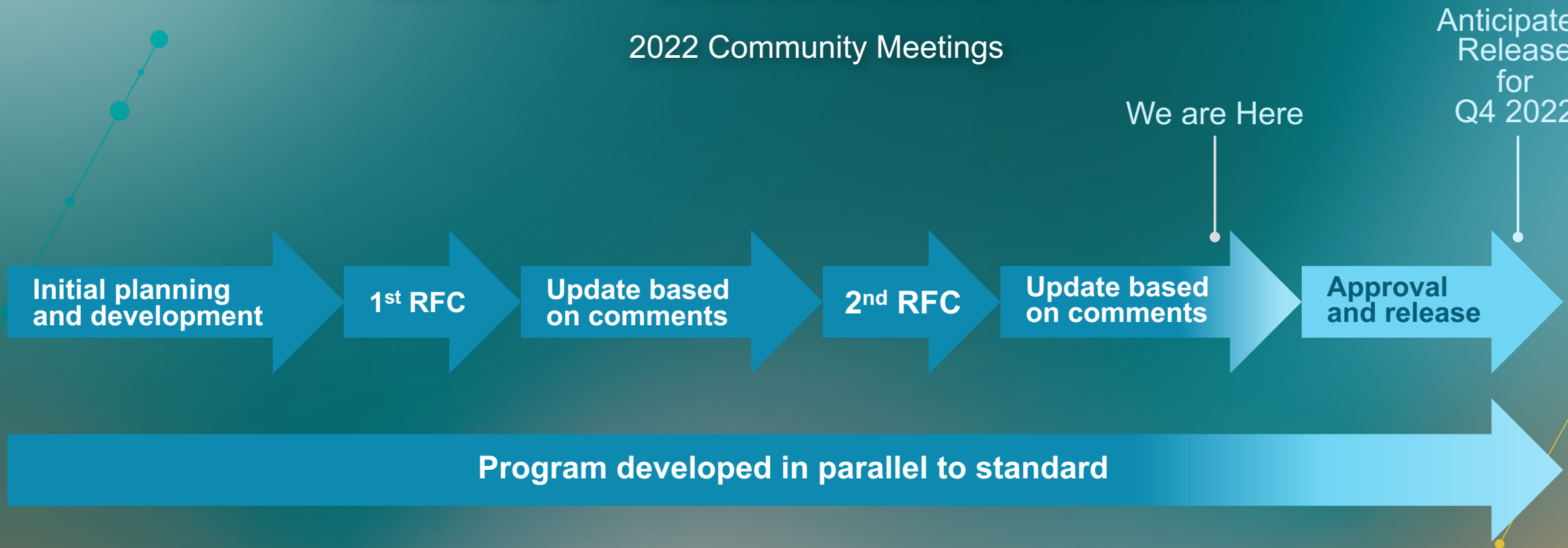
- Confirmation of all No impact Changes that occurred 0-12 Months after initial Acceptance. All No impact Changes are reported to the MPoC Lab.
- Confirmation any administration Changes from 0-12 Months after Initial Acceptance were already submitted to PCI SSC by the same MPoC Lab that Validated the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

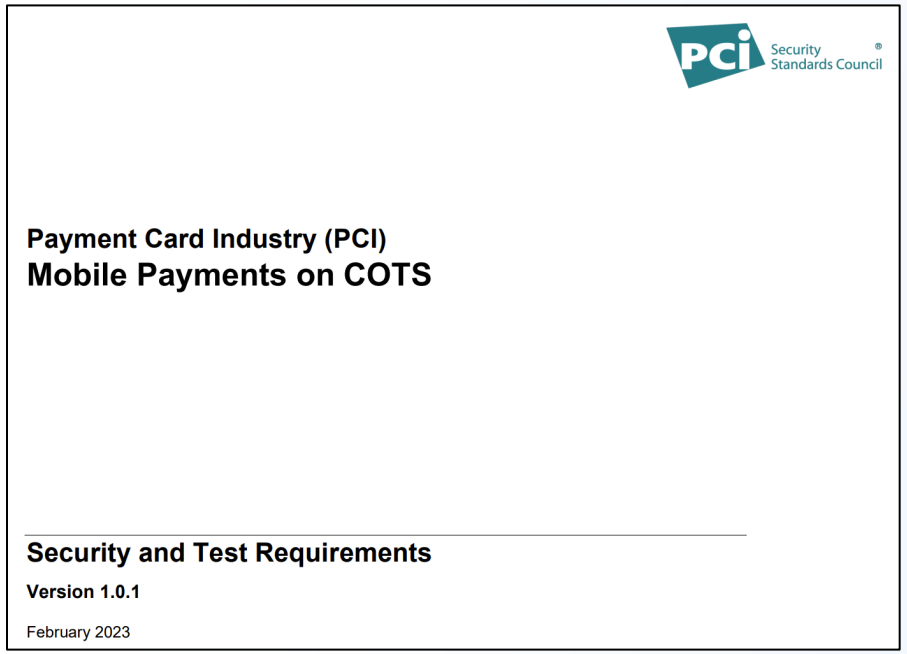


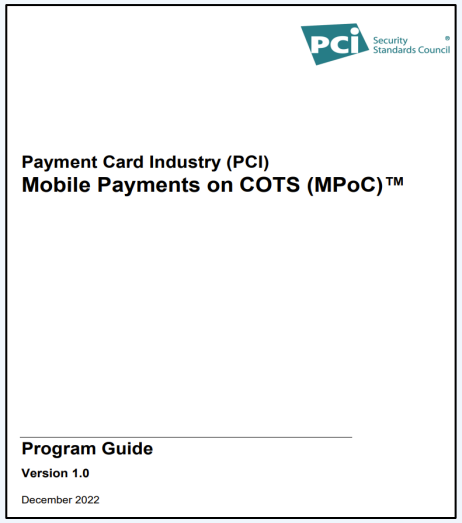
Portal and SPoC/CPoC Migration Details to Come Q1/Q2 2023

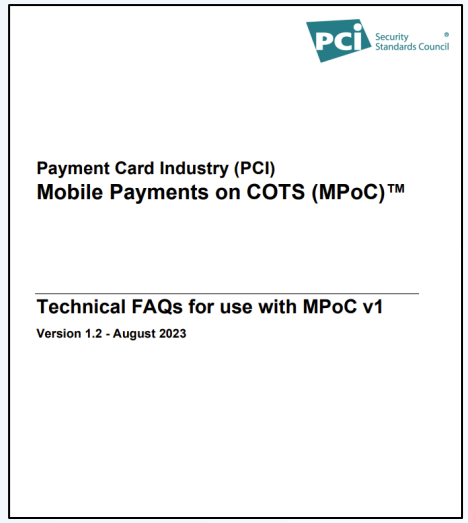
PCI Security Standards Council

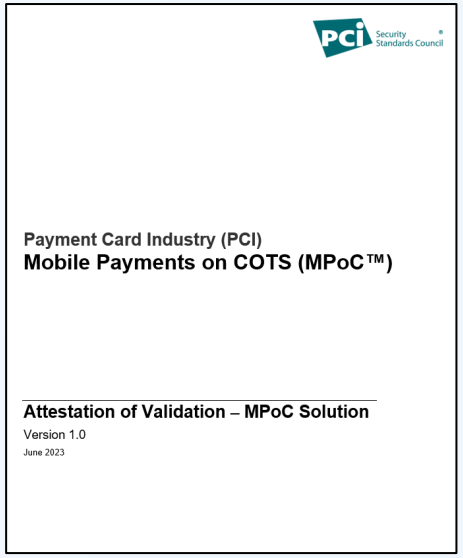
PCI MPoC – Status

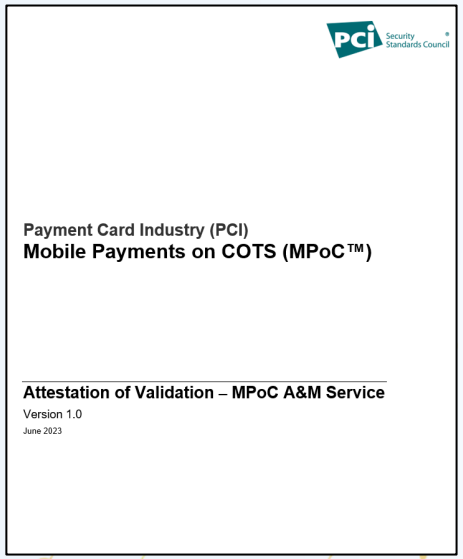
Current Status - 2023

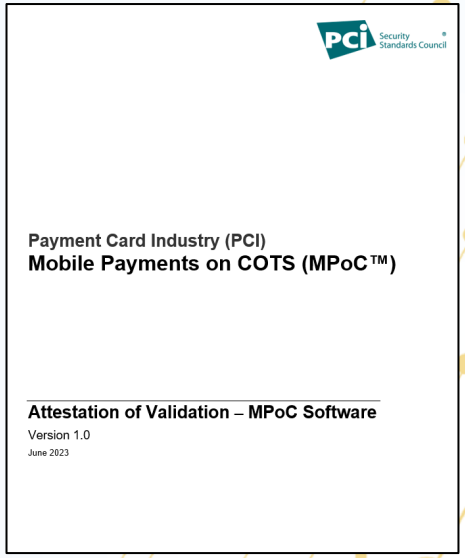












Summary

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

EMVCo

PCI Security Standards Council

Thank you!

PCI Security Standards Council

EMVCo

Europe Community Meeting 2023

PCI Security Standards Council