PCI MPoC Ecosystem, stakeholders & updates
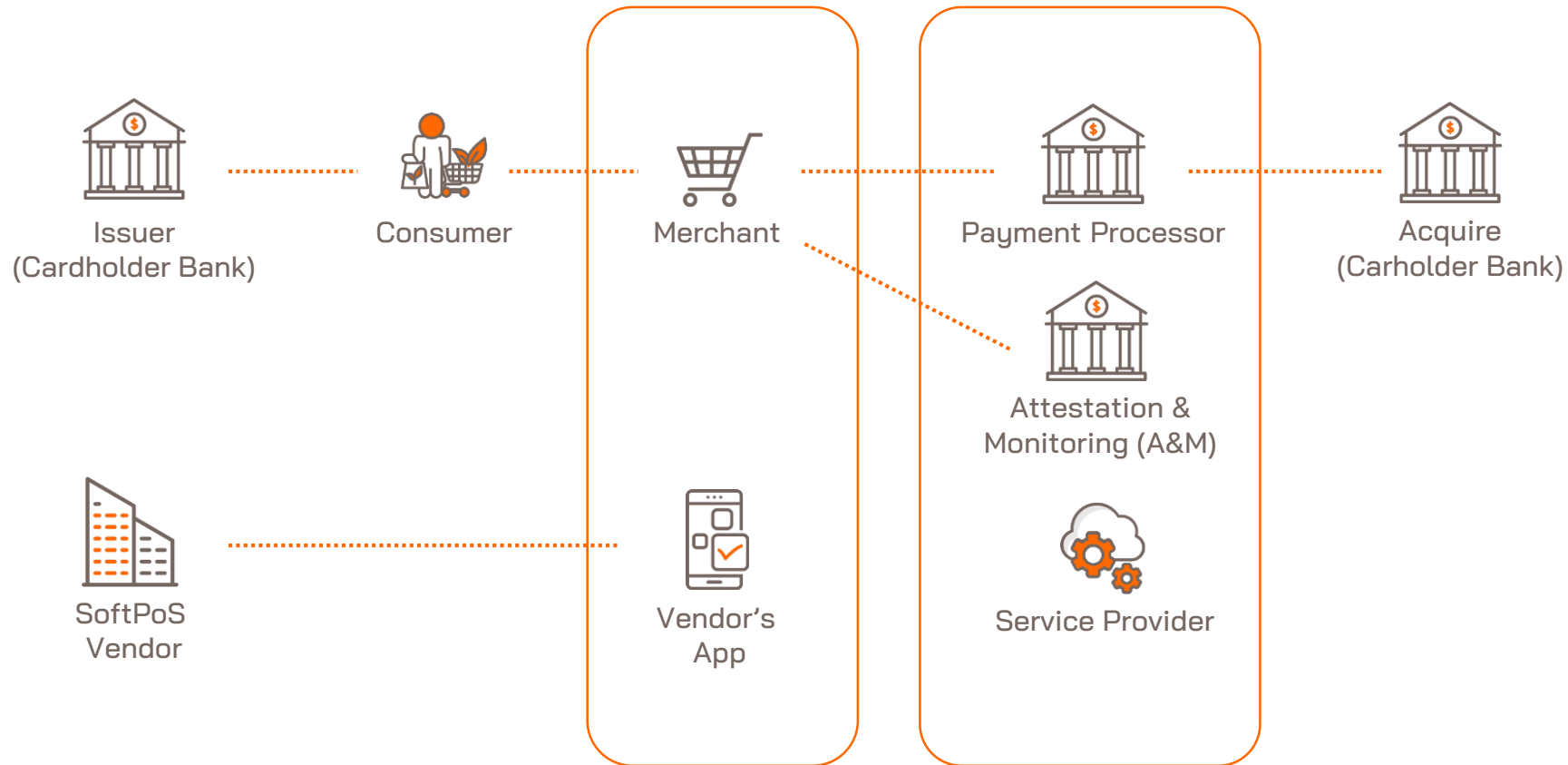
Cybersecurity Laboratories

Webinar

- January 2025
- Albert Martorell
- Public

PCI MPoC Stakeholders' Ecosystem

Were are you and your clients?

Issuer
(Cardholder Bank)

Consumer

Merchant

Payment Processor

Acquire
(Carholder Bank)

Attestation &
Monitoring (A&M)

SoftPoS
Vendor

Vendor's
App

Service Provider

PCI MPoC Certification Ecosystem

Who you need to talk with and why?

Issuer
(Cardholder Bank)

Consumer

Vendor's
App

Service Provider

Acquire
(Cardholder Bank)

VISA

EMVCo

mastercard

DISCOVER

AMERICAN EXPRESS

UnionPay 银联

JCB

PCI MPoC Certification Ecosystem

Who you need to talk with and why?

Issuer
(Cardholder Bank)

Consumer

Vendor's
App

Service Provider

Acquire
(Cardholder Bank)

PCI
Security
Standards Council ®

Common.SECC
Common Security Evaluation &
Certification Consortium

PCI SCC Programs

## What are the PCI certifications required?

Source: PCI SSC
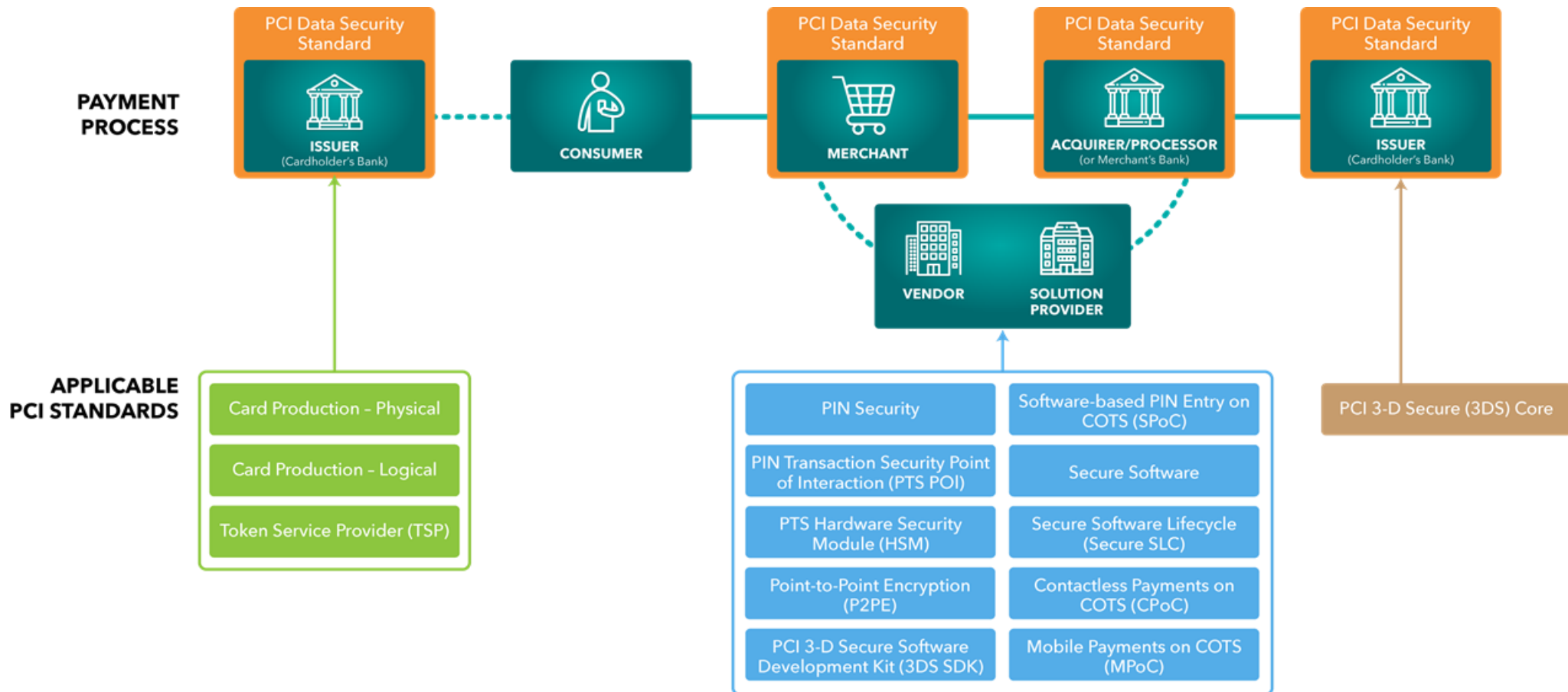
PCI MPoC relation with other PCI SSC programs

PCI PTS HSM
HSMs in the back-end environment used for PIN and account-data decryption, and related cryptographic-key operations require validation to PCI PTS HSM or **FIPS 140-2**, or 140-3, Level 3 (or 4).

PCI PTS POI
The use of PCI PTS POI devices or Non-PTS approved is allowed (see **Appendix E**). However, SRED functionality is mandatory.

PCI SSF
Compliance is not mandatory, but entities developing their own software are encouraged to refer to PCI SSC's security software standards and follow the outlined requirements as best practices in their development environments (see **Appendix D**).

PCI PIN:
This standard requires compliance to the PCI PIN requirements for any back-end systems involved in PIN processing. Key blocks are still required.

PCI DSS
PCI DSS operates independently from this standard. A back-end attestation and monitoring environment could be part of a cardholder data environment (CDE) or be completely separate from any CDE. MPoC is not within its scope, though there is a mapping between PCI MPoC **Appendix A** and PCI DSS requirements.

PCI-P2PE
Listed PCI P2PE solution is one method of validating that devices will provide encryption of account data at all times, as those devices and the applications are execute as part of a listed PCI P2PE solution.

PCI MPoC Implementations

What components/options did you implement?

- Do you supporting PIN entry?

- Do you using an external card reader? (PCI PTS POI - not only SCRPs)

- Do you implementing an SE or a TEE?

- Do you support other relevant components?

Source: PCI MPoC Security and Test Requirements
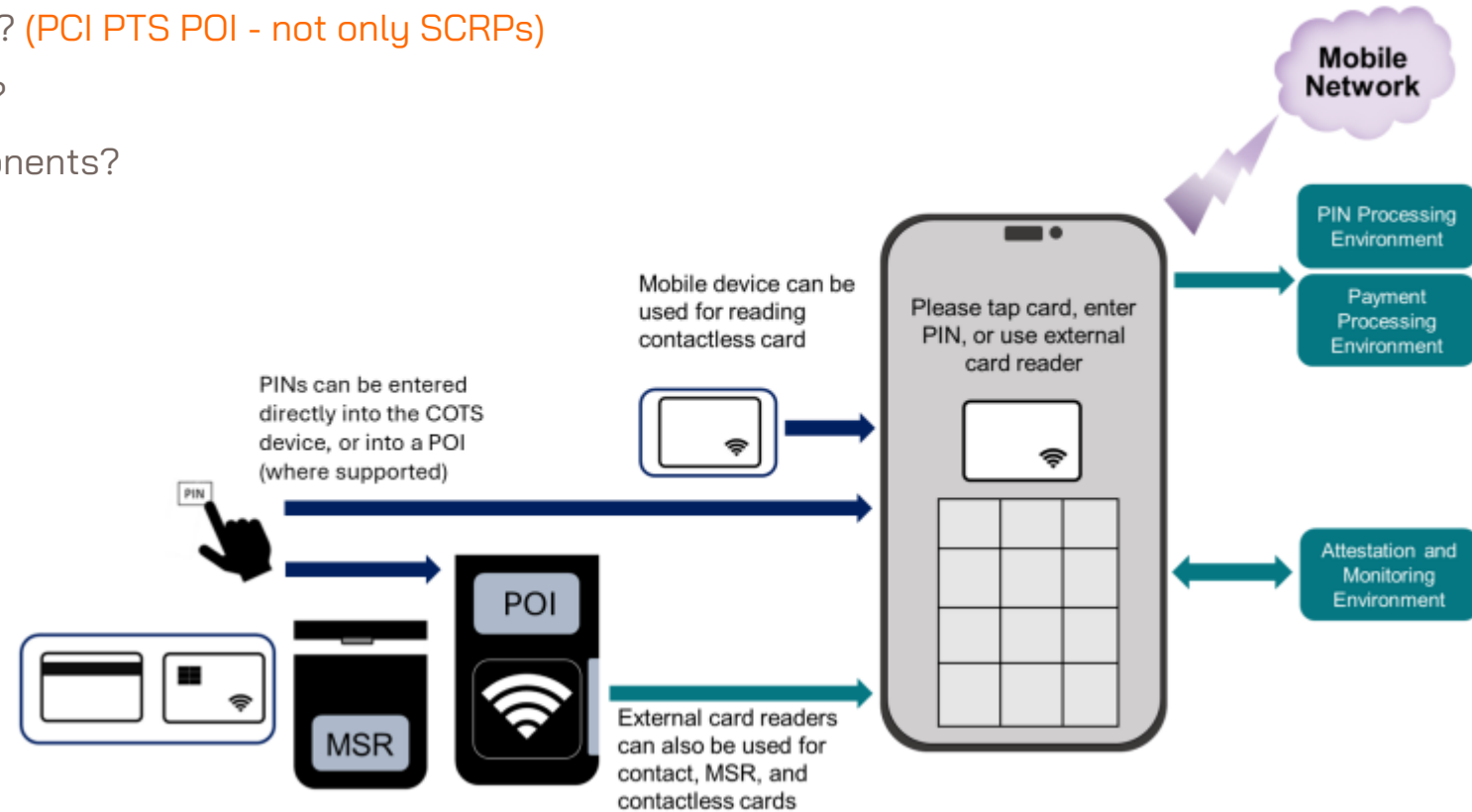
PCI MPoC Implementations

How did you implement them?

- Are you developing a monolithic solution?

- Are you a solution provider?

- Are you a software vendor?

- Are you a service provider?
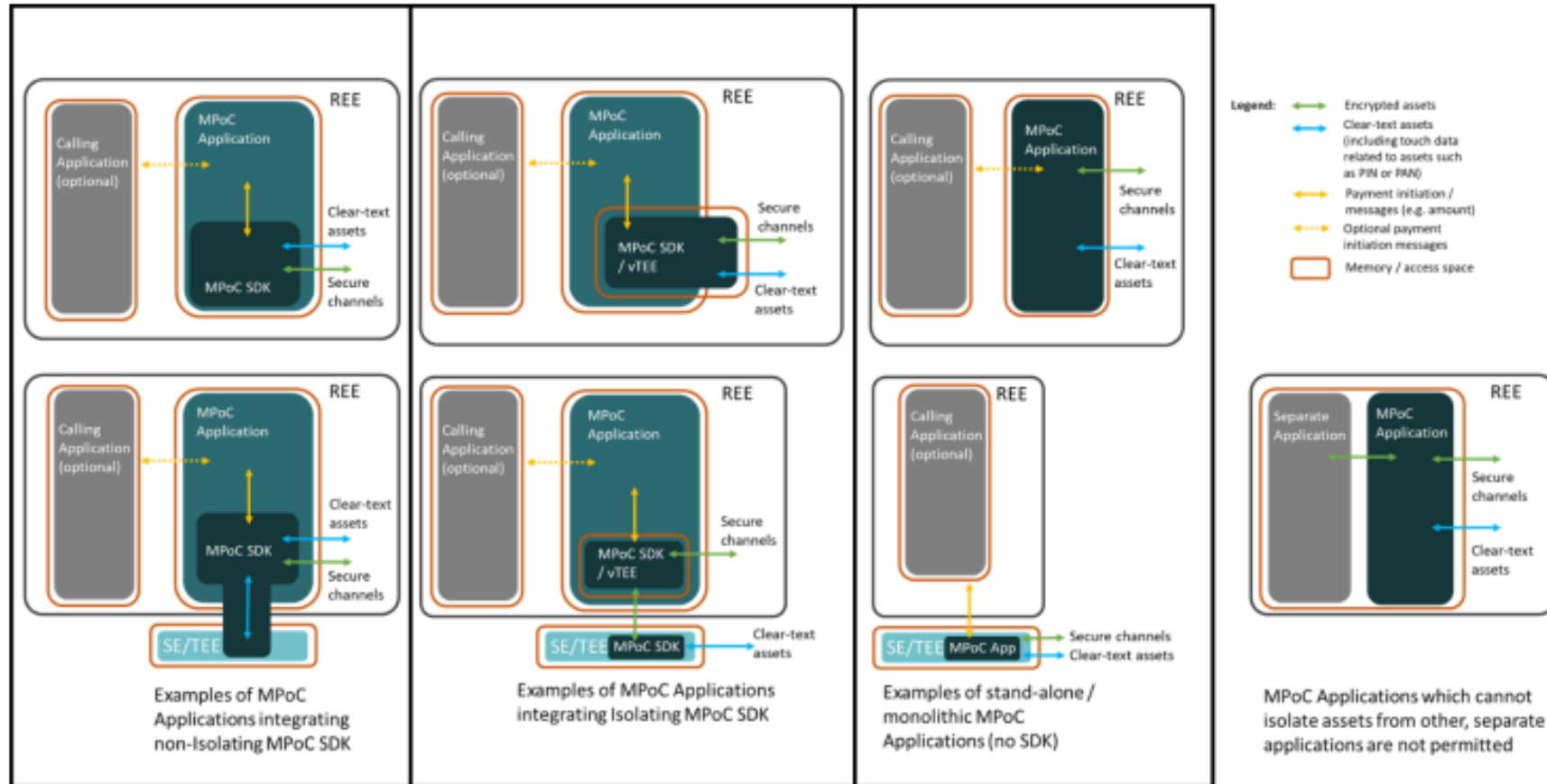
- Did you integrate an SDK?

Note: The MPoC SDK does not pass sensitive assets to another MPoC SDK or MPoC Application. Additionally MPoC SDK provides a mechanism to validate its version number
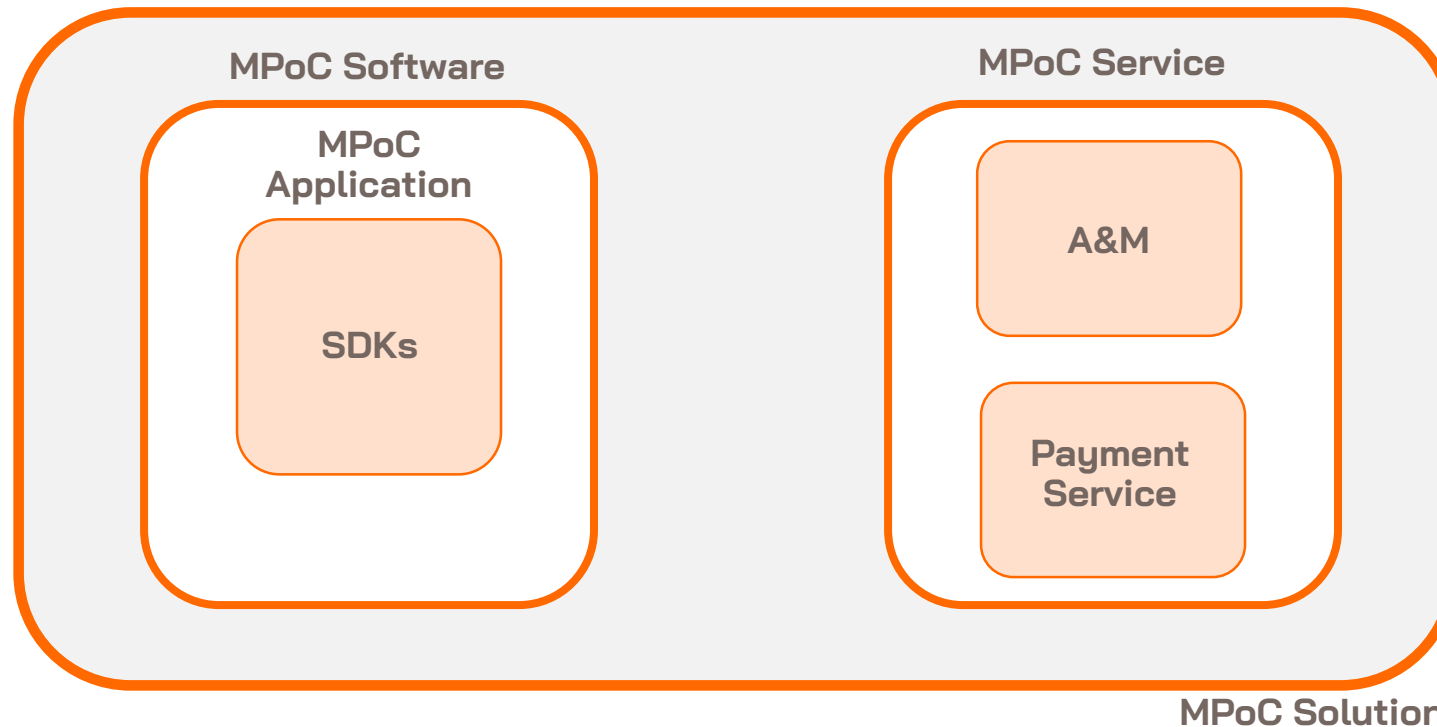

Example (1)

Example (2)

Example (3)

Example (4)

Source: PCI MPoC Security and Test Requirements
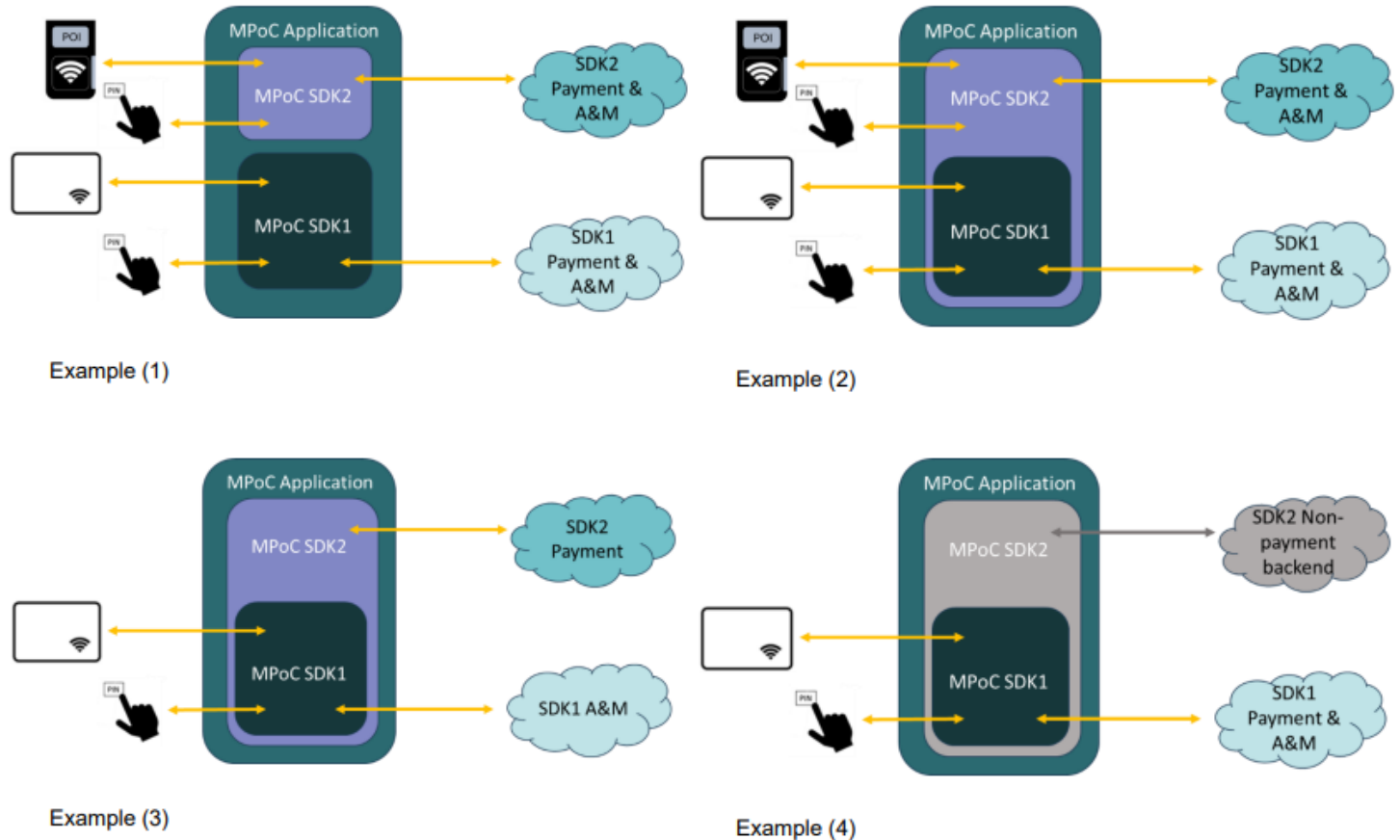
PCI MPoC Implementations

Were did you implement the Application and SDK?

Arplus⁺
laboratories

PCI MPoC Certification Options

MPoC Monolithic Solution, MPoC Software, MPoC Service

MPoC Software

MPoC Service

MPoC
Application

SDKs

A&M

Payment
Service

MPoC Solution

Note:

MPoC Standard require attended environment.

At a minimum, the solution includes the MPoC Application, attestation system, and the back-end systems and environments that perform attestation, monitoring, and payment processing

Use of MPoC implementations for non-payment acceptance, such as for transit validation where payment is processed by another system, is possible.

PCI MPoC Certification Options

MPoC Service in detail

MPoC Service

A&M

Payment Service

MPoC SW 1

MPoC SW 2

MPoC SW n
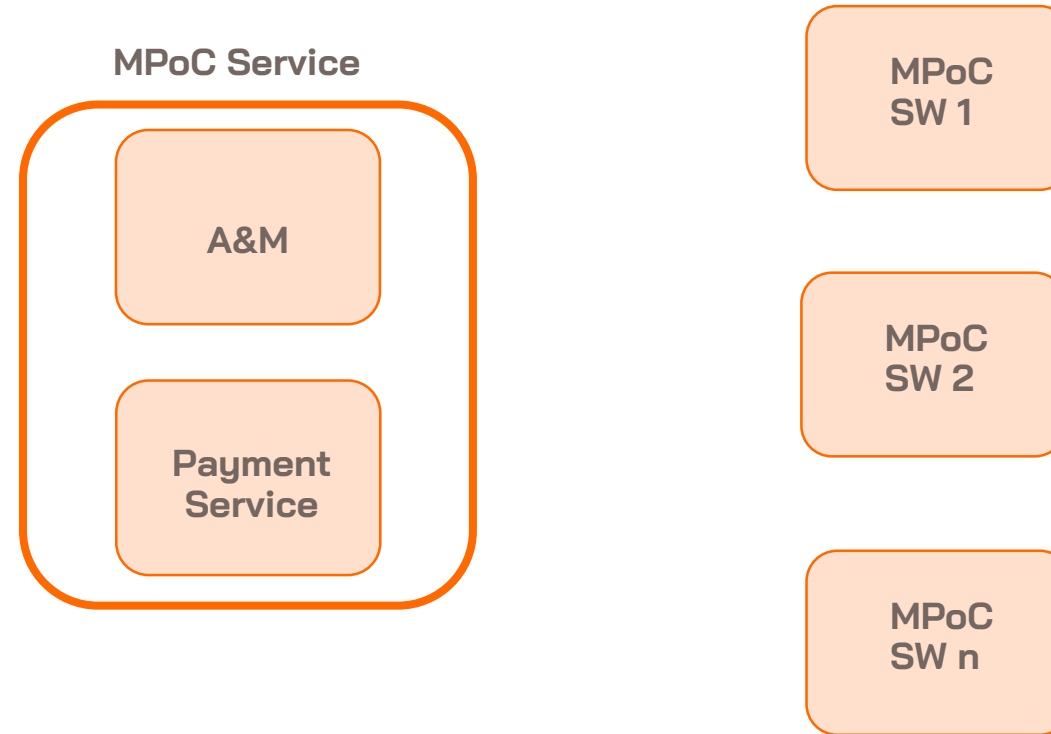
Note:

An MPoC Service may be listed with multiple services provided—so a single MPoC Service listing may provide both A&M Services and Payment Services (Payment processing and key management services).

An MPoC Service may include listing of both MPoC SDKs and MPoC Applications.

Summary of applicable requirements

MPoC Core Requirements	MPoC Software	MPoC Service (note 8)		MPoC Solution Integrating MPoC Software	MPoC Solution Integrating A&M Service	MPoC Solution Integrating A&M and Payment Service (NEW)	Monolithic MPoC Solution
		A&M	A&M & Payment Processing (NEW)				
Domain 1: MPoC Software Core Requirements	✓ (1D-1 [1,2], 1G-1[3])						✓ (1D-1 [1,2], 1G-1 N/A) (1C-5 N/A and 1G-1 Applicable)
Domain 2: MPoC Application Integration	✓ (2A[3-10]-2B(3)) (domain 2 no applicable)		✓ (2A[3-10]-2B(4))	✓ (2A(3)-2B(4)) (2A applicable)	✓ (2A(3)-2B(4)) (2A applicable)	✓ (2A(3)-2B(4))	(domain 2 applicable)
Domain 3: Attestation and Monitoring		✓	✓	✓			✓ (3A-1 N/A)
Domain 4: MPoC Software Management	✓ (4A-1(5), 4A-2(6), 4A-4(9)) (4A-4 was 5A-3, 4A-3 N/A)	✓ (No 4A-1) (4A-4 was 5A-3)	✓ (4A-1(5))	✓ (4A-4 was 5A-3)	✓ (4A-3(7)) (4A-4 was 5A-3, 4A-3 applicable)	✓ (4A-2(6), 4A-3(7))	✓ (4A-4 was 5A-3)
Domain 5: MPoC Solution			✓ (No 5A-2)	✓	✓	✓	✓

Summary of applicable requirements

MPoC Core Requirements	MPoC Software	MPoC Service (note 8)		MPoC Solution Integrating MPoC Software	MPoC Solution Integrating A&M Service	MPoC Solution Integrating A&M and Payment Service (NEW)	Monolithic MPoC Solution
		A&M	A&M & Payment Processing (NEW)				
Domain 1: MPoC Software Core Requirements	✓ (1D-1 [1,2], 1G-1[3])						✓ (1D-1 [1,2], 1G-1 N/A) (1C-5 N/A and 1G-1 Applicable)
Domain 2: MPoC Application Integration	✓ (2A[3-10]-2B(3)) (domain 2 no applicable)		✓ (2A[3-10]-2B(4))	✓ (2A(3)-2B(4)) (2A applicable)	✓ (2A(3)-2B(4)) (2A applicable)	✓ (2A(3)-2B(4))	(domain 2 applicable)
Domain 3: Attestation and Monitoring		✓	✓	✓			✓ (3A-1 N/A)
Domain 4: MPoC Software Management	✓ (4A-1(5), 4A-2(6), 4A-4(9)) (4A-4 was 5A-3, 4A-3 N/A)	✓ (No 4A-1) (4A-4 was 5A-3)	✓ (4A-1(5))	✓ (4A-4 was 5A-3)	✓ (4A-3(7)) (4A-4 was 5A-3, 4A-3 applicable)	✓ (4A-2(6), 4A-3(7))	✓ (4A-4 was 5A-3)
Domain 5: MPoC Solution			✓ (No 5A-2)	✓	✓	✓	✓

Summary of applicable requirements

MPoC Core Requirements	MPoC Software	MPoC Service (note 8)		MPoC Solution Integrating MPoC Software	MPoC Solution Integrating A&M Service	MPoC Solution Integrating A&M and Payment Service (NEW)	Monolithic MPoC Solution
		A&M	A&M & Payment Processing (NEW)				
Domain 1: MPoC Software Core Requirements	✓ (1D-1 [1,2], 1G-1[3])						✓ (1D-1 [1,2], 1G-1 N/A) (1C-5 N/A and 1G-1 Applicable)
Domain 2: MPoC Application Integration	✓ (2A[3-10]-2B(3)) (domain 2 no applicable)		✓ (2A[3-10]-2B(4))	✓ (2A(3)-2B(4)) (2A applicable)	✓ (2A(3)-2B(4)) (2A applicable)	✓ (2A(3)-2B(4))	(domain 2 applicable)
Domain 3: Attestation and Monitoring		✓	✓	✓			✓ (3A-1 N/A)
Domain 4: MPoC Software Management	✓ (4A-1(5), 4A-2(6), 4A-4(9)) (4A-4 was 5A-3, 4A-3 N/A)	✓ (No 4A-1) (4A-4 was 5A-3)	✓ (4A-1(5))	✓ (4A-4 was 5A-3)	✓ (4A-3(7)) (4A-4 was 5A-3, 4A-3 applicable)	✓ (4A-2[6], 4A-3(7))	✓ (4A-4 was 5A-3)
Domain 5: MPoC Solution			✓ (No 5A-2)	✓	✓	✓	✓

Summary of applicable requirements

MPoC Core Requirements	MPoC Software	MPoC Service (note 8)		MPoC Solution Integrating MPoC Software	MPoC Solution Integrating A&M Service	MPoC Solution Integrating A&M and Payment Service (NEW)	Monolithic MPoC Solution
		A&M	A&M & Payment Processing (NEW)				
Domain 1: MPoC Software Core Requirements	✓ (1D-1 [1,2], 1G-1(3))						✓ (1D-1 [1,2], 1G-1 N/A) (1C-5 N/A and 1G-1 Applicable)
Domain 2: MPoC Application Integration	✓ (2A[3-10]-2B(3)) (domain 2 no applicable)		✓ (2A[3-10]-2B(4))	✓ (2A(3)-2B(4)) (2A applicable)	✓ (2A(3)-2B(4)) (2A applicable)	✓ (2A(3)-2B(4))	(domain 2 applicable)
Domain 3: Attestation and Monitoring		✓	✓	✓			✓ (3A-1 N/A)
Domain 4: MPoC Software Management	✓ (4A-1[5], 4A-2[6], 4A-4[9]) (4A-4 was 5A-3, 4A-3 N/A)	✓ (No 4A-1) (4A-4 was 5A-3)	✓ (4A-1[5])	✓ (4A-4 was 5A-3)	✓ (4A-3[7]) (4A-4 was 5A-3, 4A-3 applicable)	✓ (4A-2[6], 4A-3[7])	✓ (4A-4 was 5A-3)
Domain 5: MPoC Solution			✓ (No 5A-2)	✓	✓	✓	✓

Summary of applicable requirements

MPoC Core Requirements	MPoC Software	MPoC Service (note 8)		MPoC Solution Integrating MPoC Software	MPoC Solution Integrating A&M Service	MPoC Solution Integrating A&M and Payment Service (NEW)	Monolithic MPoC Solution
		A&M	A&M & Payment Processing (NEW)				
Domain 1: MPoC Software Core Requirements	✓ (1D-1 [1,2], 1G-1[3])						✓ (1D-1 [1,2], 1G-1 N/A) (1C-5 N/A and 1G-1 Applicable)
Domain 2: MPoC Application Integration	✓ (2A[3-10]-2B(3)) (domain 2 no applicable)		✓ (2A[3-10]-2B(4))	✓ (2A(3)-2B(4)) (2A applicable)	✓ (2A(3)-2B(4)) (2A applicable)	✓ (2A(3)-2B(4))	(domain 2 applicable)
Domain 3: Attestation and Monitoring		✓	✓	✓			✓ (3A-1 N/A)
Domain 4: MPoC Software Management	✓ (4A-1(5), 4A-2[6], 4A-4[9]) (4A-4 was 5A-3, 4A-3 N/A)	✓ (No 4A-1) (4A-4 was 5A-3)	✓ (4A-1(5))	✓ (4A-4 was 5A-3)	✓ (4A-3(7)) (4A-4 was 5A-3, 4A-3 applicable)	✓ (4A-2[6], 4A-3(7))	✓ (4A-4 was 5A-3)
Domain 5: MPoC Solution			✓ (No 5A-2)	✓	✓	✓	✓

Summary of applicable requirements

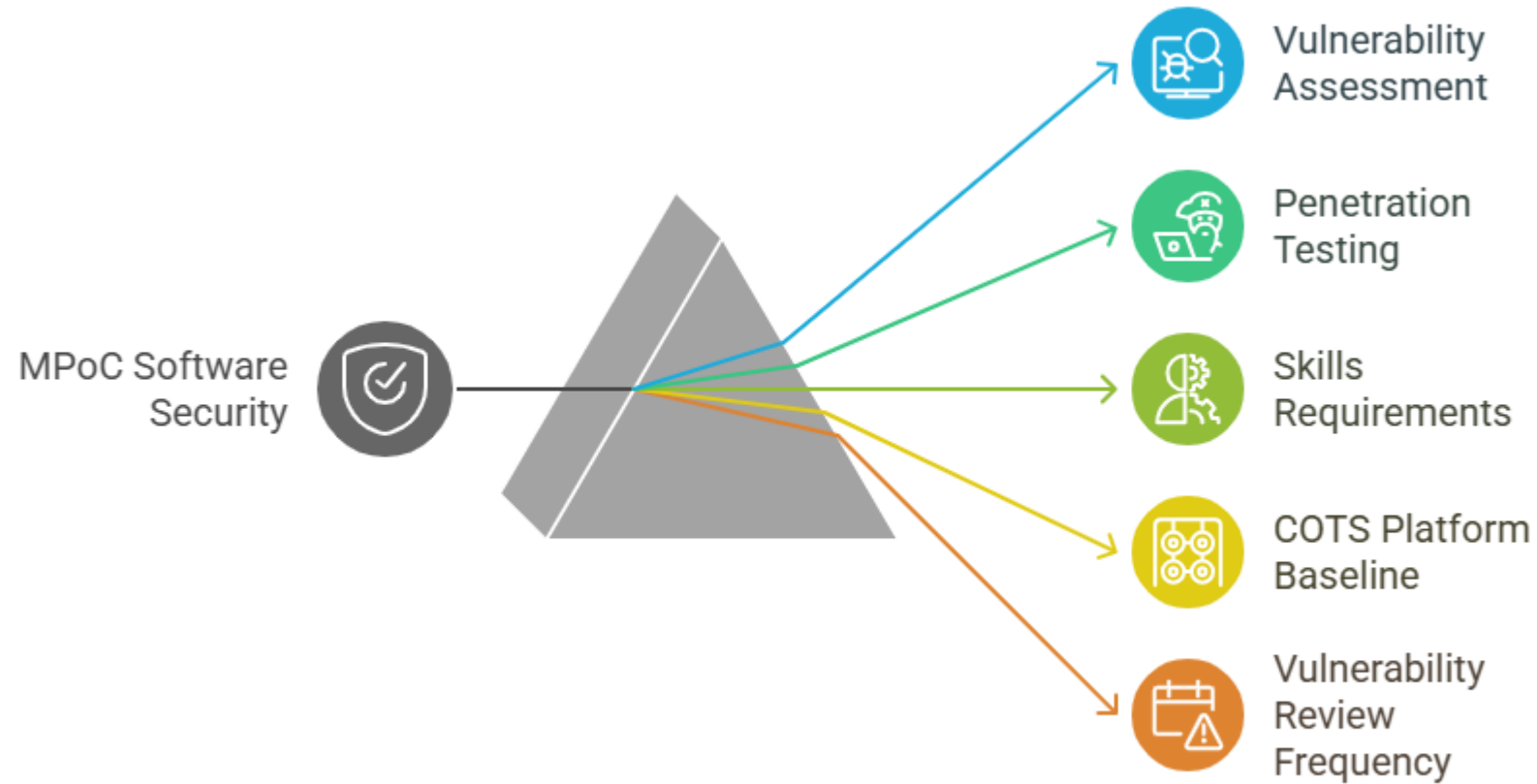| MPoC Core Requirements	MPoC Software	MPoC Service (note 8)		MPoC Solution Integrating MPoC Software	MPoC Solution Integrating A&M Service	MPoC Solution Integrating A&M and Payment Service (NEW)	Monolithic MPoC Solution
		A&M	A&M & Payment Processing (NEW)				
Domain 1: MPoC Software Core Requirements	✓ (1D-1 [1,2], 1G-1(3))						✓ (1D-1 [1,2], 1G-1 N/A) (1C-5 N/A and 1G-1 Applicable)
Domain 2: MPoC Application Integration	✓ (2A[3-10]-2B(3)) (domain 2 no applicable)		✓ (2A[3-10]-2B(4))	✓ (2A(3)-2B(4)) (2A applicable)	✓ (2A(3)-2B(4)) (2A applicable)	✓ (2A(3)-2B(4))	(domain 2 applicable)
Domain 3: Attestation and Monitoring		✓	✓	✓			✓ (3A-1 N/A)
Domain 4: MPoC Software Management	✓ (4A-1(5), 4A-2(6), 4A-4(9)) (4A-4 was 5A-3, 4A-3 N/A)	✓ (No 4A-1) (4A-4 was 5A-3)	✓ (4A-1(5))	✓ (4A-4 was 5A-3)	✓ (4A-3(7)) (4A-4 was 5A-3, 4A-3 applicable)	✓ (4A-2(6), 4A-3(7))	✓ (4A-4 was 5A-3)
Domain 5: MPoC Solution			✓ (No 5A-2)	✓	✓	✓	✓

Summary of applicable requirements

MPoC Core Requirements	MPoC Software	MPoC Service (note 8)		MPoC Solution Integrating MPoC Software	MPoC Solution Integrating A&M Service	MPoC Solution Integrating A&M and Payment Service (NEW)	Monolithic MPoC Solution
		A&M	A&M & Payment Processing (NEW)				
Domain 1: MPoC Software Core Requirements	✓ (1D-1 [1,2], 1G-1(3))						✓ (1D-1 [1,2], 1G-1 N/A) (1C-5 N/A and 1G-1 Applicable)
Domain 2: MPoC Application Integration	✓ (2A[3-10]-2B(3)) (domain 2 no applicable)		✓ (2A[3-10]-2B(4))	✓ (2A(3)-2B(4)) (2A applicable)	✓ (2A(3)-2B(4)) (2A applicable)	✓ (2A(3)-2B(4))	(domain 2 applicable)
Domain 3: Attestation and Monitoring		✓	✓	✓			✓ (3A-1 N/A)
Domain 4: MPoC Software Management	✓ (4A-1(5), 4A-2(6), 4A-4(9)) (4A-4 was 5A-3, 4A-3 N/A)	✓ (No 4A-1) (4A-4 was 5A-3)	✓ (4A-1(5))	✓ (4A-4 was 5A-3)	✓ (4A-3(7)) (4A-4 was 5A-3, 4A-3 applicable)	✓ (4A-2[6], 4A-3(7))	✓ (4A-4 was 5A-3)
Domain 5: MPoC Solution			✓ (No 5A-2)	✓	✓	✓	✓

Summary of applicable requirements

Self solution certification

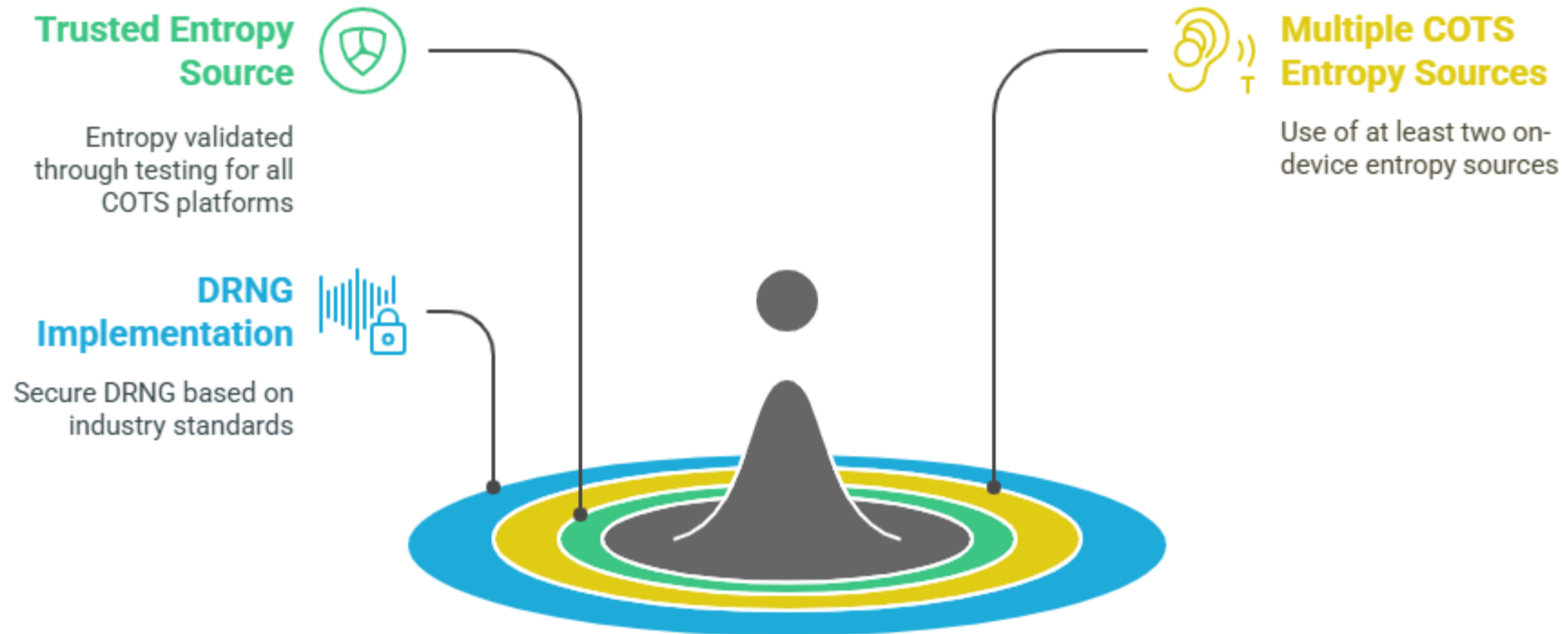| MPoC Core Requirements	MPoC Software	MPoC Service (note 8)		MPoC Solution Integrating MPoC Software	MPoC Solution Integrating A&M Service	MPoC Solution Integrating A&M and Payment Service (NEW)	Monolithic MPoC Solution
		A&M	A&M & Payment Processing (NEW)				
Domain 1: MPoC Software Core Requirements	✓ (1D-1 [1,2], 1G-1[3])		✓ (1D-1 [1,2], 1G-1[3])				✓ (1D-1 [1,2], 1G-1 N/A) (1C-5 N/A and 1G-1 Applicable)
Domain 2: MPoC Application Integration	✓ (2A[3-10]-2B(3)) (domain 2 no applicable)		✓ (2A[3-10]-2B(4))	✓ (2A(3)-2B(4)) (2A applicable)	✓ (2A(3)-2B(4)) (2A applicable)	✓ (2A(3)-2B(4))	(domain 2 applicable)
Domain 3: Attestation and Monitoring		✓	✓	✓			✓ (3A-1 N/A)
Domain 4: MPoC Software Management	✓ (4A-1[5], 4A-2[6], 4A-4[9]) (4A-4 was 5A-3, 4A-3 N/A)	✓ (No 4A-1) (4A-4 was 5A-3)	✓ (4A-1[5])	✓ (4A-4 was 5A-3)	✓ (4A-3[7]) (4A-4 was 5A-3, 4A-3 applicable)	✓ (4A-2[6], 4A-3[7])	✓ (4A-4 was 5A-3)
Domain 5: MPoC Solution			✓ (No 5A-2)	✓	✓	✓	✓

PCI MPoC vulnerability assessments

New and summary

PCI MPoC RNG

Entropy source

Trusted Entropy Source

Entropy validated through testing for all COTS platforms

DRNG Implementation

Secure DRNG based on industry standards

Multiple COTS Entropy Sources

Use of at least two on-device entropy sources

PCI MPoC Keys

How to manage cryptographic key

RSA 2048 for AES 128-256 Key Loading

Follow Appendix C Key Sizes and Strengths
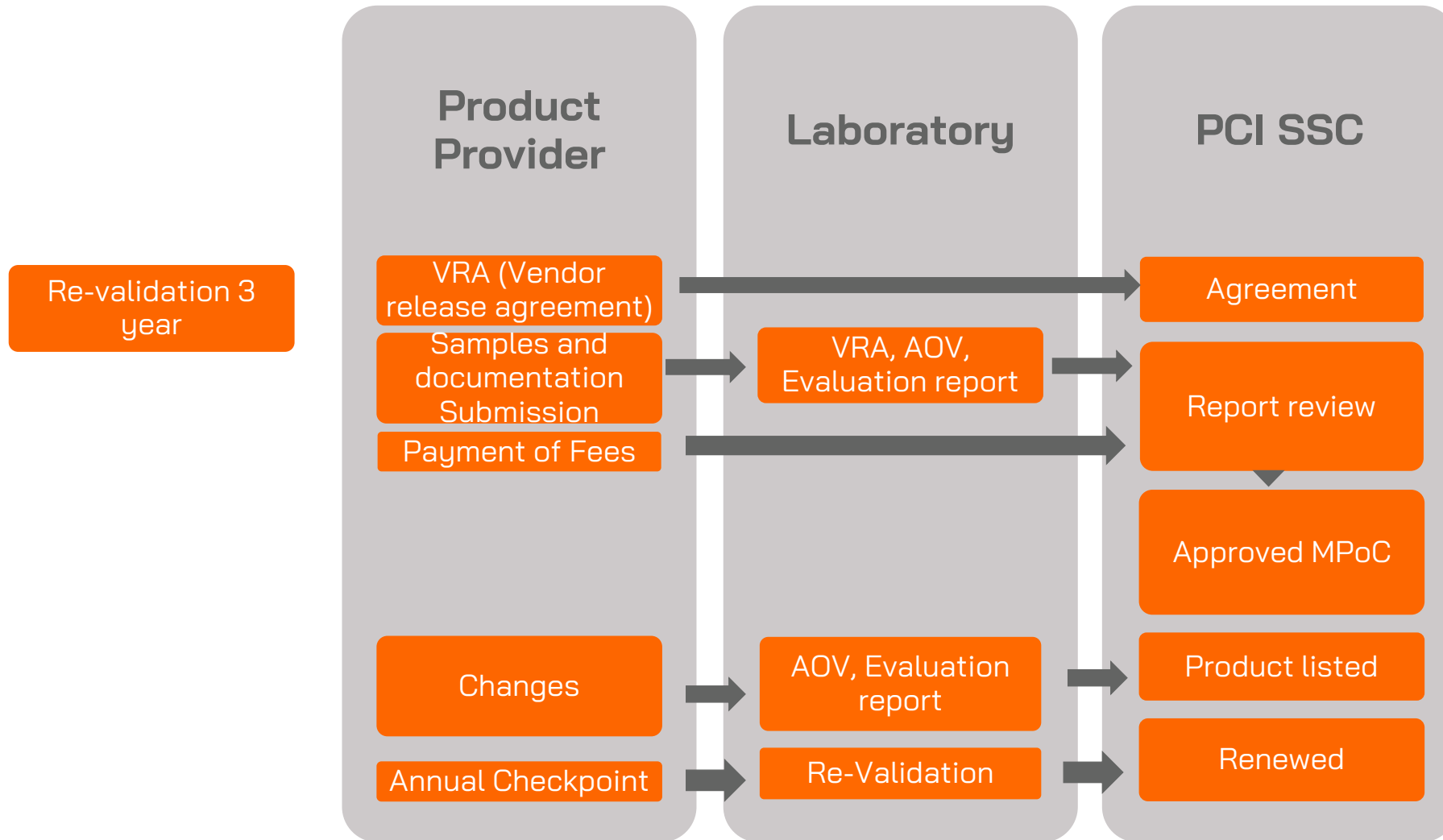
KEK can be weaker than key protecting, minimum 128-bit.

General Documentation

The general documents could be found in https://www.pcisecuritystandards.org/document_library/

Security Requirements

New · **MPoC Security and Test requirements** — Provides de security requirements and test requirements to comply.

Potential update · **MPoC Technical FAQS** — FAQS help as clarification of the scope and technical security requirements

Program

New · **MPoC Program Guide** — The MPoC Program Guide describes MPoC Program Requirements for candidate and existing MPoC Product Evaluation and Validation against the MPoC Standard by a PCI Recognized Laboratory, subsequent Acceptance by PCI SCC

Forms

To be updated · **MPoC Software, A&M Service and Solution AOVs** — The Attestation of Validations of components: MPoC Software, Attestation and Monitoring Service and Solution (merchant-attended). Attestation of Validation forms are official documents used to certify that a particular mobile payment solution or component has been evaluated and meets the required security standards

The PCI MPoC Process

Re-validation 3 year

Product Provider

Laboratory

PCI SSC

Product Provider	Laboratory	PCI SSC
VRA (Vendor release agreement)		Agreement
Samples and documentation Submission	VRA, AOV, Evaluation report	Report review
Payment of Fees		
		Approved MPoC
Changes	AOV, Evaluation report	Product listed
Annual Checkpoint	Re-Validation	Renewed

Thanks!

Applus⊕ laboratories

Join us on

TESTING AND CERTIFICATION CENTER

www.appluslaboratories.com