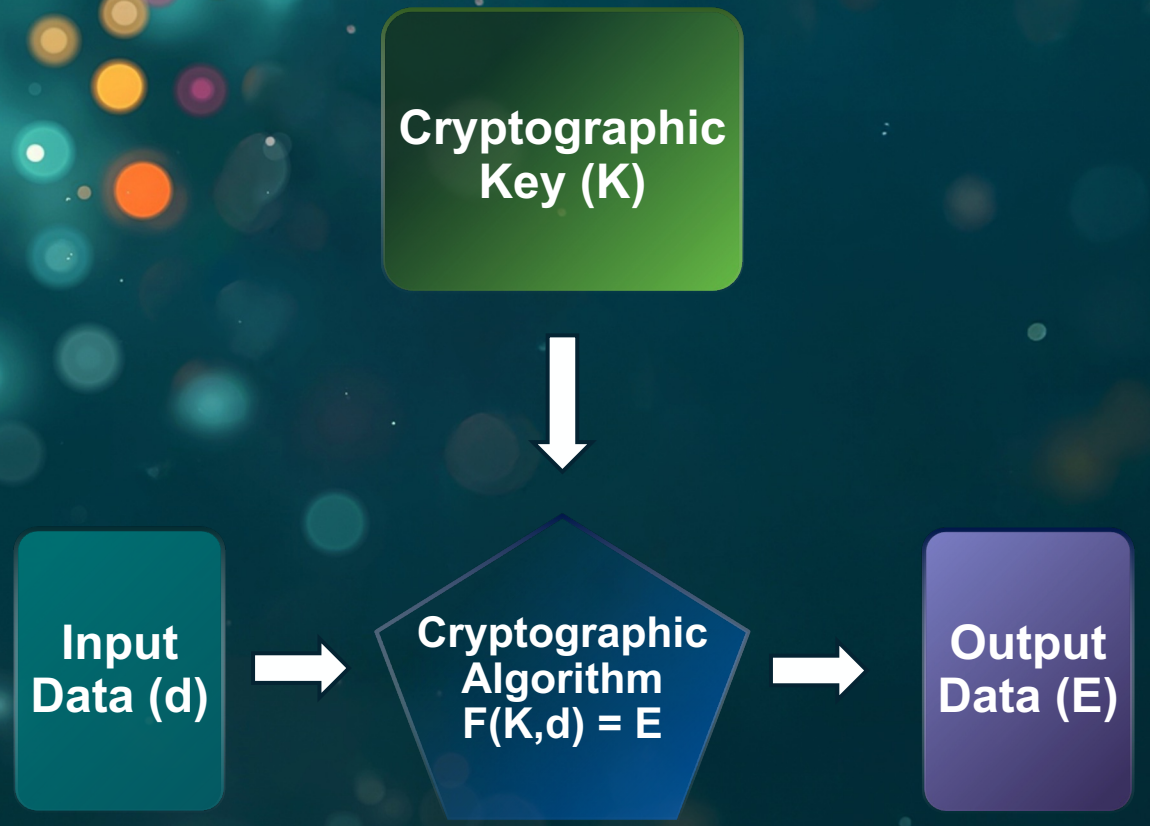


Securing the Keys:

Developing the New Key Management and Operations Standard

Why Key Management?

Cryptography is used to answer the question of "How do I protect this set of data?", reducing it to the question of "How do I protect this key?"



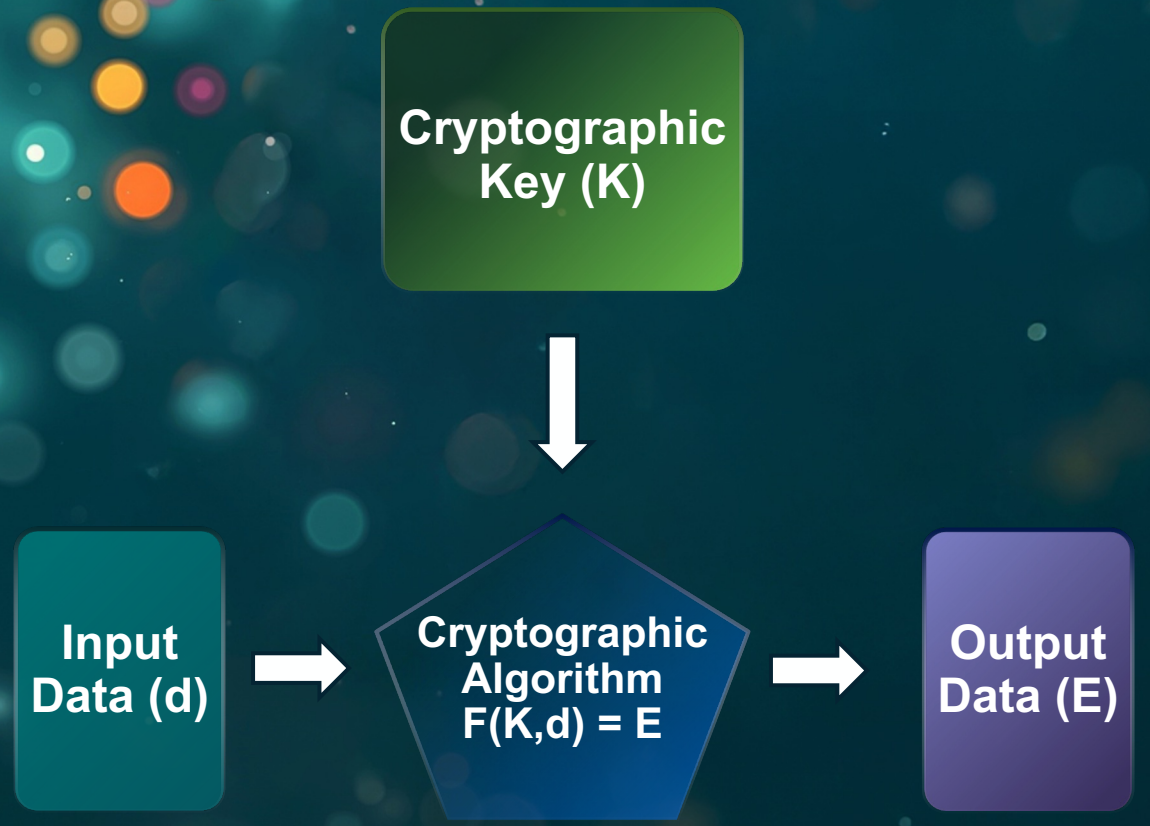
20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Why Key Management?

Cryptography is used to answer the question of "How do I protect this set of data?", reducing it to the question of "How do I protect this key?"

The only secret in this process is the key

If the key is known, guessable, brute-force-able, or otherwise insecure in some way, the encryption process has no security value



20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

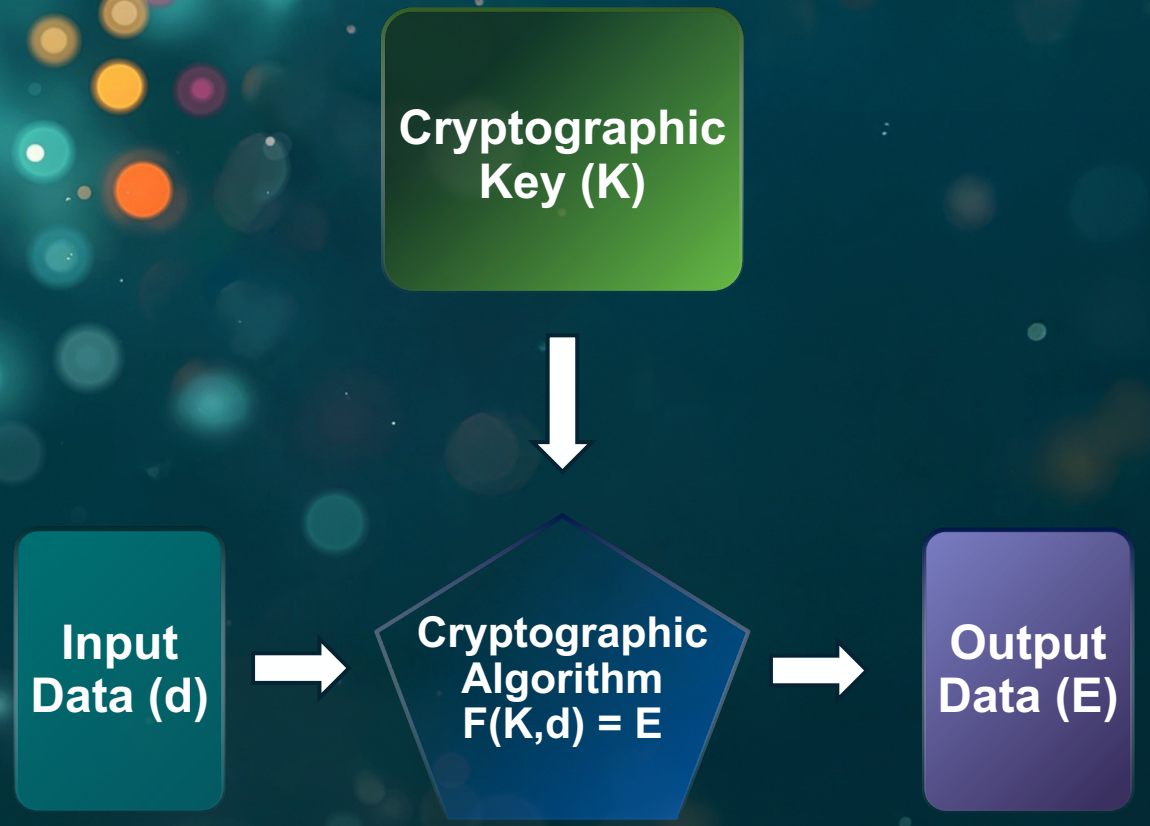
Why Key Management?

Cryptography is used to answer the question of "How do I protect this set of data?", reducing it to the question of "How do I protect this key?"

The only secret in this process is the key

If the key is known, guessable, brute-force-able, or otherwise insecure in some way, the encryption process has no security value

So "How do I protect this key?"
– The answer is key management!

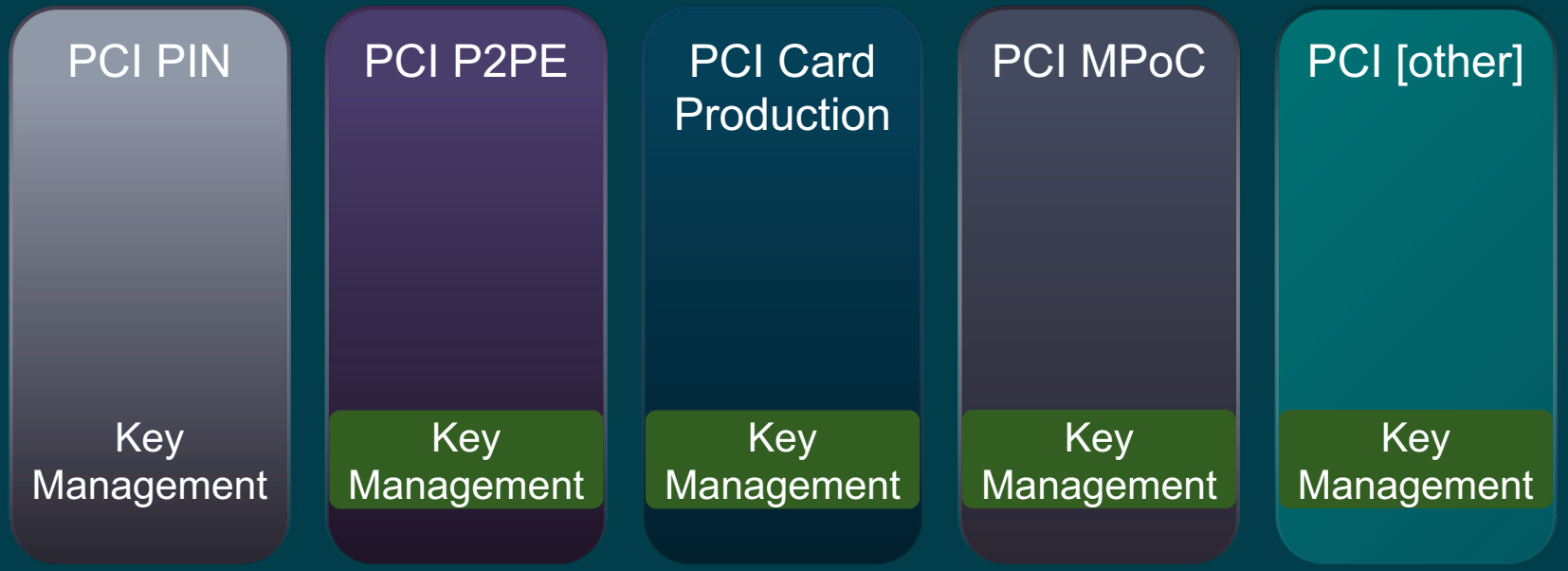


20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Key Management is a Vital Part of Security

Cryptography is used across all security standards and programs

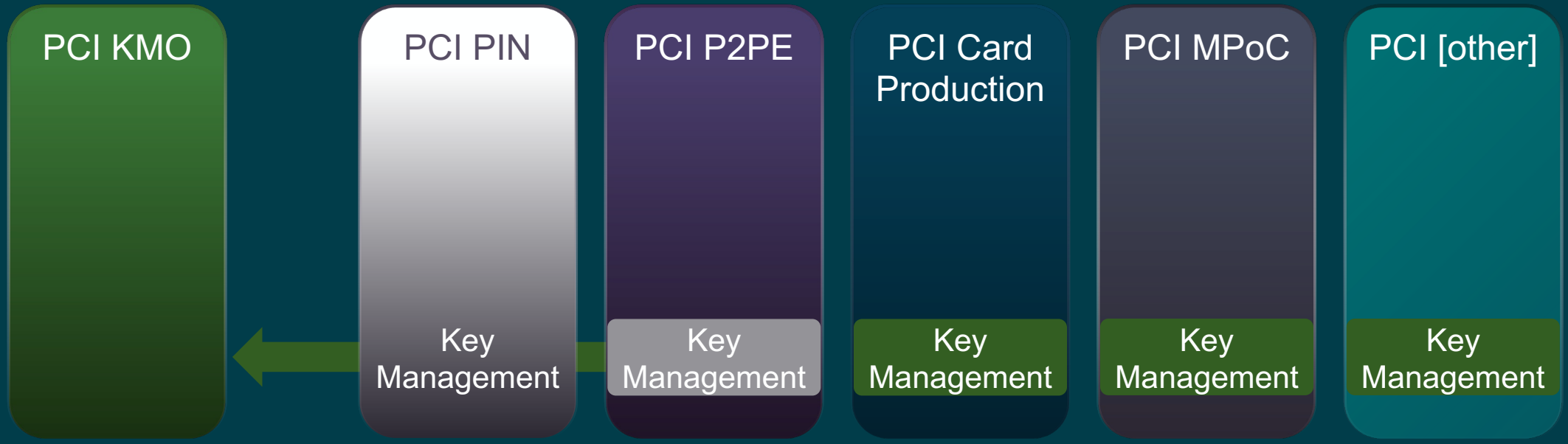
- Before PCI KMO, requirements for key management were separately replicated across each PCI standard



Key Management is a Vital Part of Security

Cryptography is used across all security standards and programs

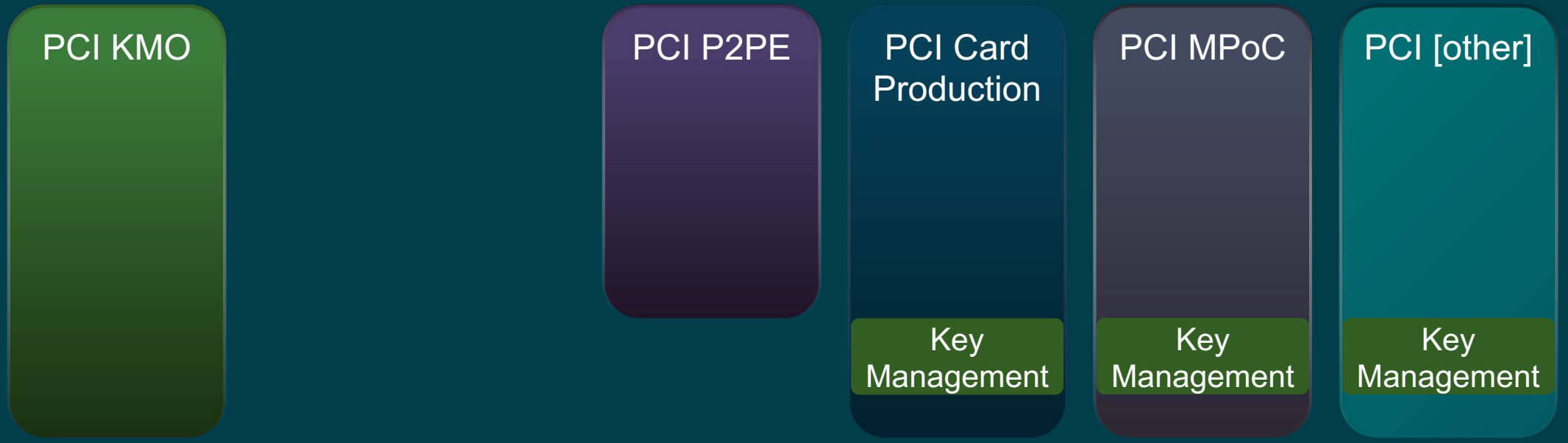
- Before PCI KMO, requirements for key management were separately replicated across each PCI standard
- PCI KMO is the start of consolidating those aspects, starting with PCI PIN and the key management aspects of PCI P2PE



Key Management is a Vital Part of Security

Cryptography is used across all security standards and programs

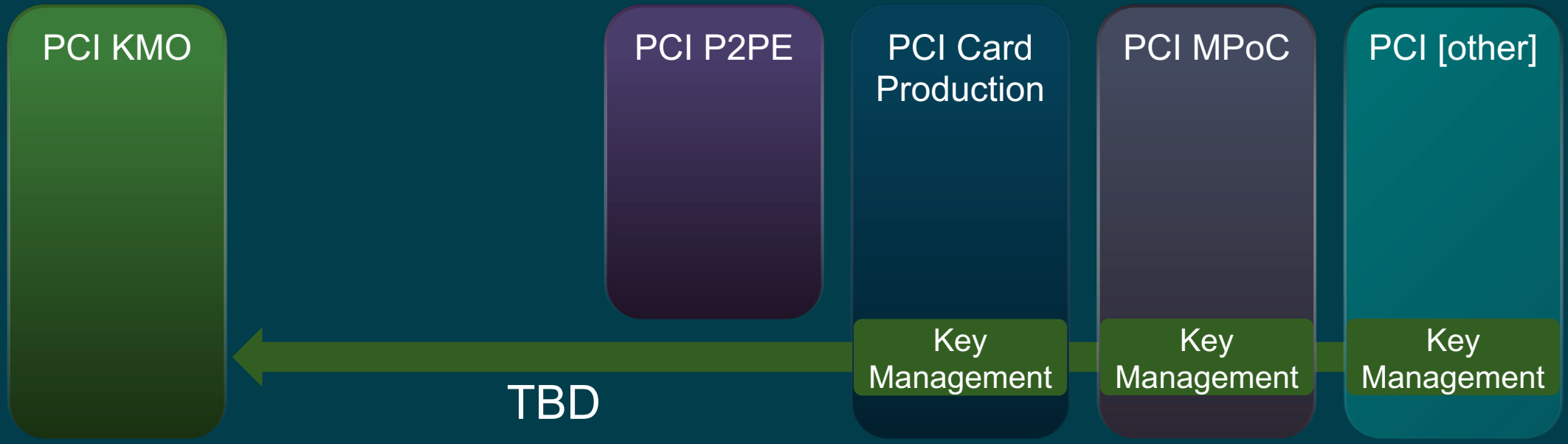
- Before PCI KMO, requirements for key management were separately replicated across each PCI standard
- PCI KMO is the start of consolidating those aspects, starting with PCI PIN and the key management aspects of PCI P2PE
- This allows us to reduce the number of standards and/or requirements we have (sunset date for PCI PIN TBD)



Key Management is a Vital Part of Security

Cryptography is used across all security standards and programs

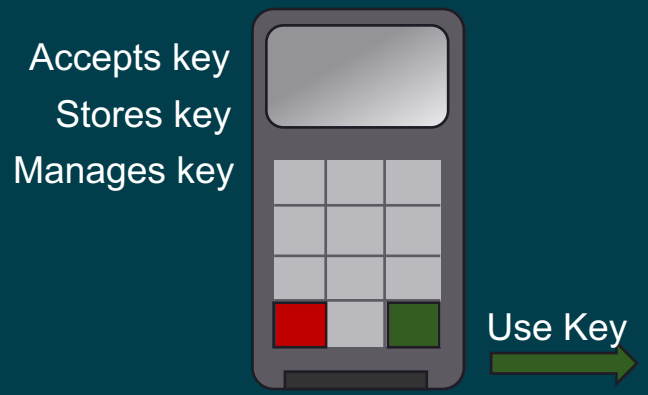
- Before PCI KMO, requirements for key management were separately replicated across each PCI standard
- PCI KMO is the start of consolidating those aspects, starting with PCI PIN and the key management aspects of PCI P2PE
- This allows us to reduce the number of standards and/or requirements we have (sunset date for PCI PIN TBD)
- Key management in other standards may be addressed at a later time (also to be determined)



Implementation vs Operations

Many systems support specific types of cryptographic implementation(s)

- Types of algorithms (AES, RSA, ECC, etc), and key sizes (128bit AES, 2048bit RSA, etc)
- Key sizes and ways of managing keys (e.g., DUKPT, simple master/session, etc)
- Remote key injection, local key loading, etc



Implementation vs Operations

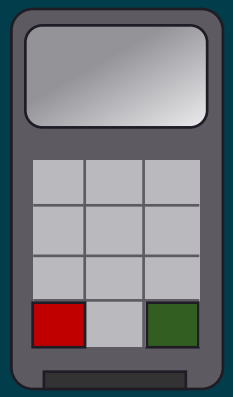
Many systems support specific types of cryptographic implementation(s)

- Types of algorithms (AES, RSA, ECC, etc), and key sizes (128bit AES, 2048bit RSA, etc)
- Key sizes and ways of managing keys (e.g., DUKPT, simple master/session, etc)
- Remote key injection, local key loading, etc

However, this only part of the story – the rest is covered by PCI KMO

- If multiple implementations are supported, one still needs to be chosen for use
- Keys still need to be generated, loading / operation / management methods selected and used
- Some cryptography is specific to payment data types
  - For example, PIN blocks are a specific mode of operation that applies only to PIN data
  - There are specific rules for how is mode of operation is to work in backend systems

Accepts key
Stores key
Manages key



Use Key

Generate Key

Load Key

Generate keys
Load keys
Manage keys
Translate data
Manage SCDs
… etc

PCI KMO

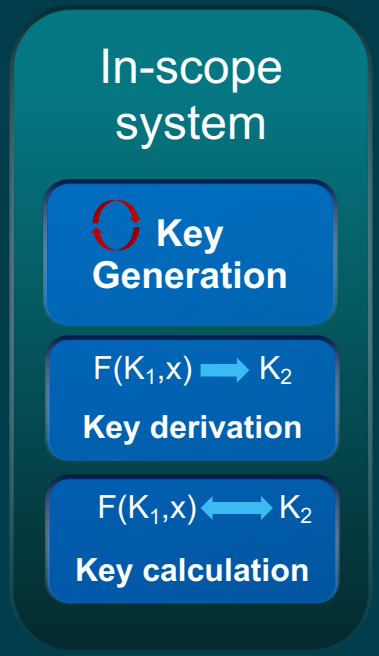
From ↓ \ To →	ISO 9564 formats 0, 3, 4	ISO 9564 format 1	ISO 9564 format 2
ISO 9564 formats 0, 3, 4	Permitted without change of PAN, or Permitted replacing PAN token with real PAN[1]	Permitted only with enforced UKPT[2] key management	Permitted for submission to a (contact) IC card
ISO 9564 format 1	Permitted	Permitted	Permitted for submission to a (contact) IC card
ISO 9564 format 2	Not permitted	Not permitted	Permitted for submission to a (contact) IC card

Notes:

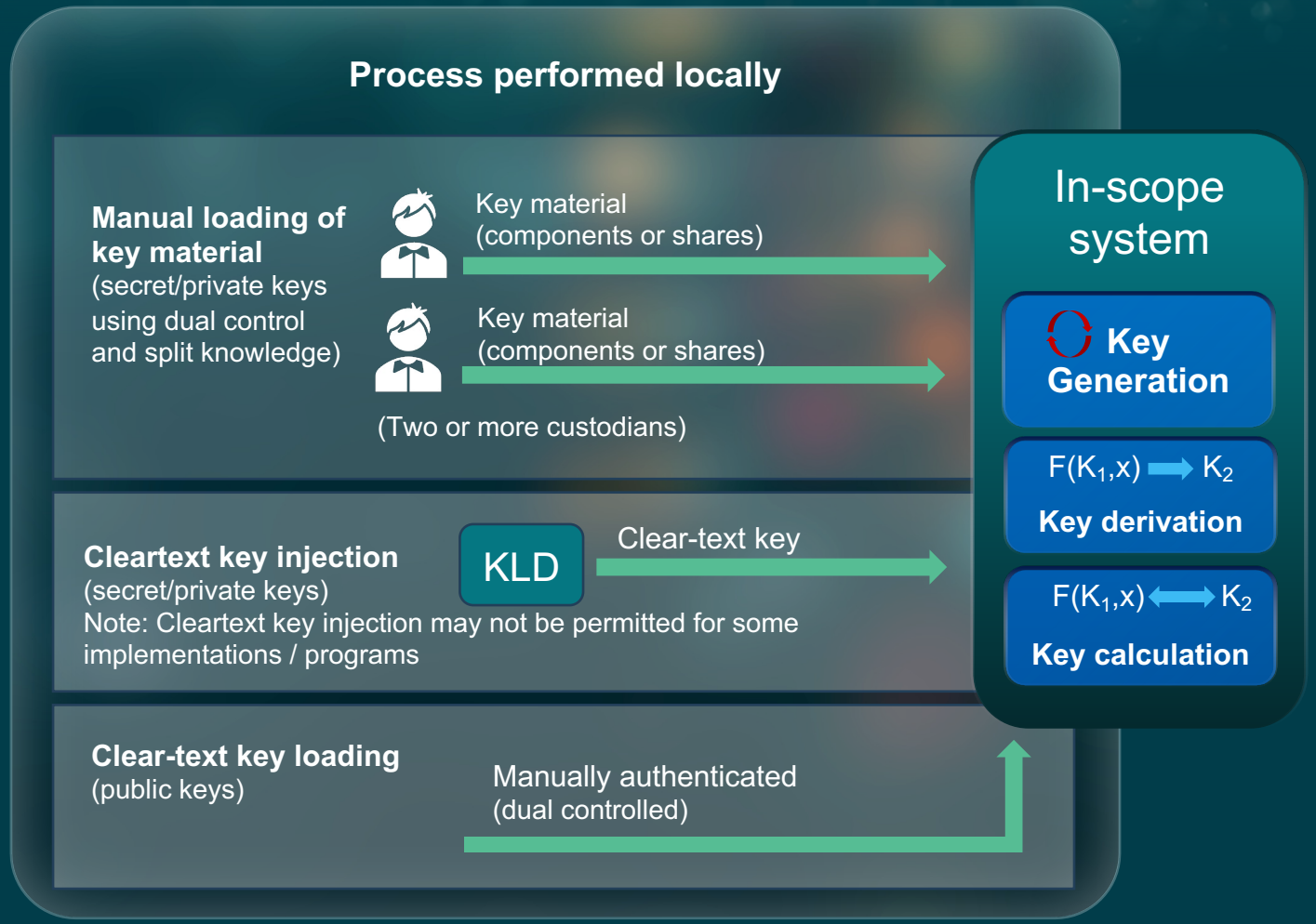
1) *Changing of a PAN is only permitted when there is cryptographic binding between the PAN token and the funding PAN, and the translation process validates this binding, OR when the HSM is operating in a sensitive state.*
2) *Enforced UKPT key management includes methods such as DUKPT as defined in ANSI X9.24.*

PCI KMO Key Loading / Key Establishment

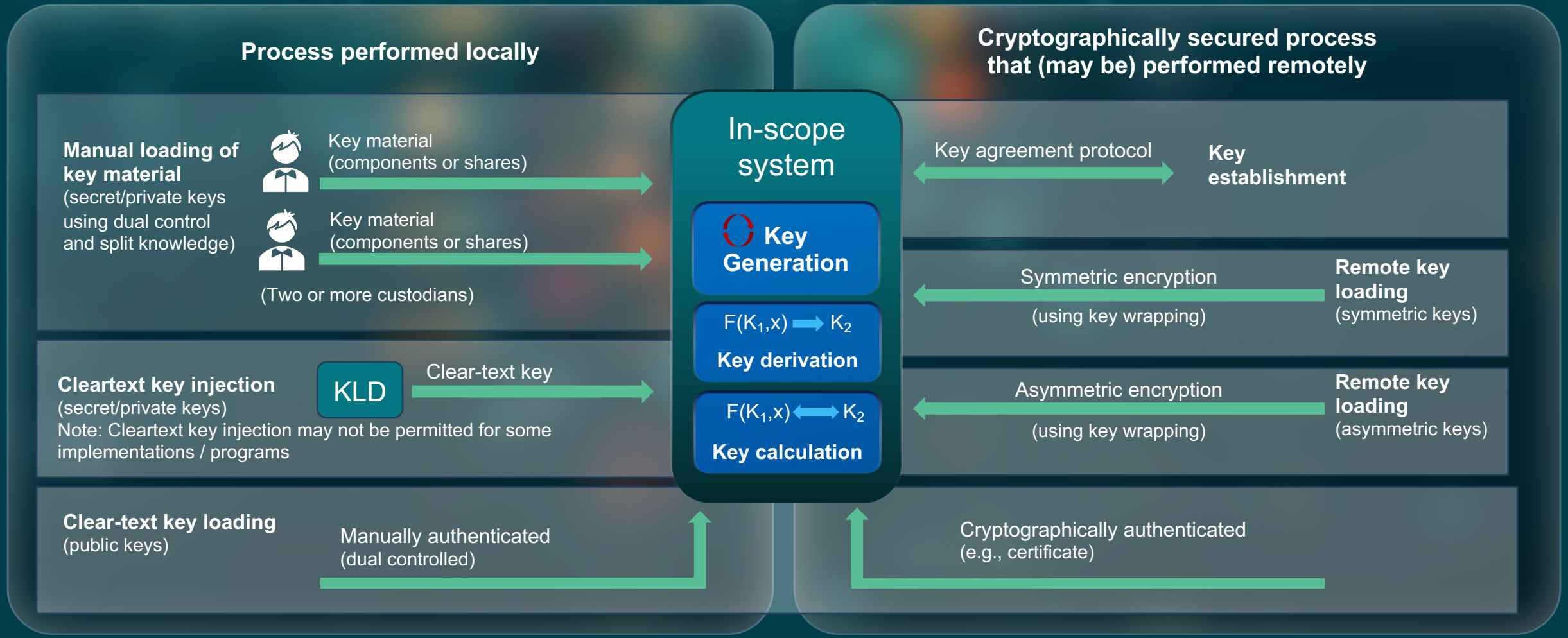
PCI KMO Key Loading / Key Establishment



PCI KMO Key Loading / Key Establishment



PCI KMO Key Loading / Key Establishment



Not all Key Management Is the Same

- Not all key management implementations are required to follow the same rules
- For example some PCI standards require the use of Secure Cryptographic Devices (SCDs), such as HSMs, POIs, and some do not
  - These devices are required by aspects of PCI PIN and PCI P2PE
  - But (as mentioned) PCI KMO is intended to ultimately support many different standards / programs
- PCI KMO handles this by splitting out requirements into different Domains
  - Requirements which apply to all implementations are in Domain 1
  - Requirements which may be optional, or may apply only to some implementations, are in other Domains (Domains 2 – 4)
- Domains also cover aspects such as physical security, data-specific requirements, and HSM-specific requirements (remote HSM, HSM-as-a-Service)
- KMO also uses terms that can be defined as required for different key types

Common Terms

KMO uses terms throughout which can be defined differently depending on the key data types being used (e.g., PIN keys or P2PE keys)

	PIN Keys	P2PE Keys
In-scope systems		
In-scope keys		
Approved key generation methods		
Key management types		
Approved key forms		
Acceptable cryptography		

Common Terms

KMO uses terms throughout which can be defined differently depending on the key data types being used (e.g., PIN keys or P2PE keys)

	PIN Keys	P2PE Keys
In-scope systems	PTS or FIPS140-2/3 SCDs MPoC Apps	PTS or FIPS140-2/3 SCDs
In-scope keys	PIN-security related keys	P2PE-security related keys
Approved key generation methods	Generation using an approved key gen function of an SCD	
Key management types	Fixed key & cleartext key loading not permitted	
Approved key forms	Wrapped in key-block, managed as key constituent material, in SCD	
Acceptable cryptography	112bit TDES or greater	112bit TDES UKPT or greater

PCI KMO Service Types

Service Type	Description
Decryption Management (DM)	An entity that manages the decryption environment for a componentized P2PE solution. **For P2PE keys only**
PIN-Processing Service (PPS)	An entity that performs PIN operations (such as verification and/or translation) that is not the card Issuer. **For PIN keys only**
Key-Injection Facility (KIF)	An entity that performs cryptographic key services for other entities or KMO Service types. Services may include, but are not limited to, key generation, conveyance, and/or (local) key loading. A KIF may include local and/or remote key-loading functions.
Signing Service Provider (SSP)	An entity that provides signing services for software or data packages (such as firmware, applications, configuration files, etc.) for other entities or KMO services.
Certification/Registration Authorities (CA/RA)	An entity that provides signing services for public keys (e.g., for X.509 or other non-X.509 certificates) for use in connection with the remote distribution of symmetric keys using asymmetric techniques. A Registration Authority (RA) performs registration services on behalf of a CA to vet requests for certificates that will be issued by the CA.
HSM-as-a-Service (HaaS)	An entity that manages an HSM cluster.

KMO Service → P2PE Components

KMO Service Type	Functions Provided	P2PE Component Type
Key Injection Facility (KIF)	Key Loading & Key Generation	P2PE KIF
Key Injection Facility (KIF)	Key Loading	P2PE KLCP
Key Injection Facility (KIF)	Key Generation	P2PE KMCP
Decryption Management (DM)		P2PE DMS
Certificate / Registration Authority (CA/RA)		P2PE CA/RA

For Listings which show support for P2PE key types

PIN Processing Service (PPS)
HSM-as-a-Service (HaaS)
Signing Service Provider (SSP)

Do not map onto a P2PE Component Type

P2PE EMS (EMCP/PDCP/PMCP)

Do not map onto KMO a Service

PCI KMO Outsourcing and Reusability

A primary goal of PCI KMO is to support an assess-once, use-many approach

- One assessment can cover multiple key data types
- Services can be used by other services to reduce scope
- Decryption Management (DM) is for P2PE keys only, PIN Processing Services (PPS) for PIN keys only

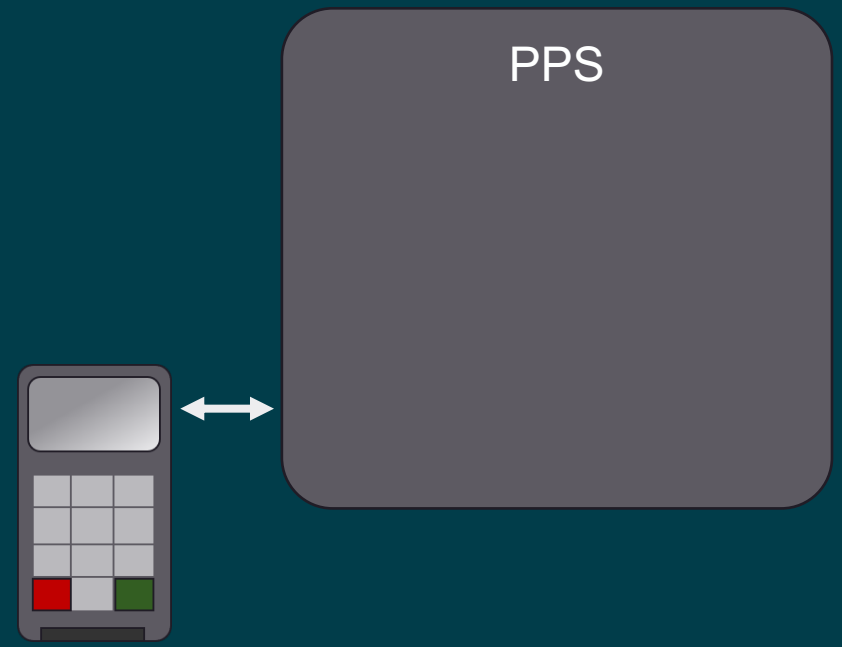
Outsourcing Matrix		Listed KMO Service Categories					
		DM	PPS	KIF	SSP	CA/RA	HaaS
Under Assessment	DM	✓	⊘	✓	✓	✓	✓
	PPS	⊘	✓	✓	✓	✓	✓
	KIF	⊘	⊘	✓	⊘	✓	✓
	SSP	⊘	⊘	⊘	✓	✓	✓
	CA/RA	⊘	⊘	⊘	⊘	✓	✓
	HaaS	⊘	⊘	⊘	⊘	⊘	✓

PCI KMO Outsourcing and Reusability

A primary goal of PCI KMO is to support an assess-once, use-many approach

- One assessment can cover multiple key data types
- Services can be used by other services to reduce scope
- Decryption Management (DM) is for P2PE keys only, PIN Processing Services (PPS) for PIN keys only

Outsourcing Matrix		Listed KMO Service Categories					
		DM	PPS	KIF	SSP	CA/RA	HaaS
Under Assessment	DM	✓	⊘	✓	✓	✓	✓
	PPS	⊘	✓	✓	✓	✓	✓
	KIF	⊘	⊘	✓	⊘	✓	✓
	SSP	⊘	⊘	⊘	✓	✓	✓
	CA/RA	⊘	⊘	⊘	⊘	✓	✓
	HaaS	⊘	⊘	⊘	⊘	⊘	✓

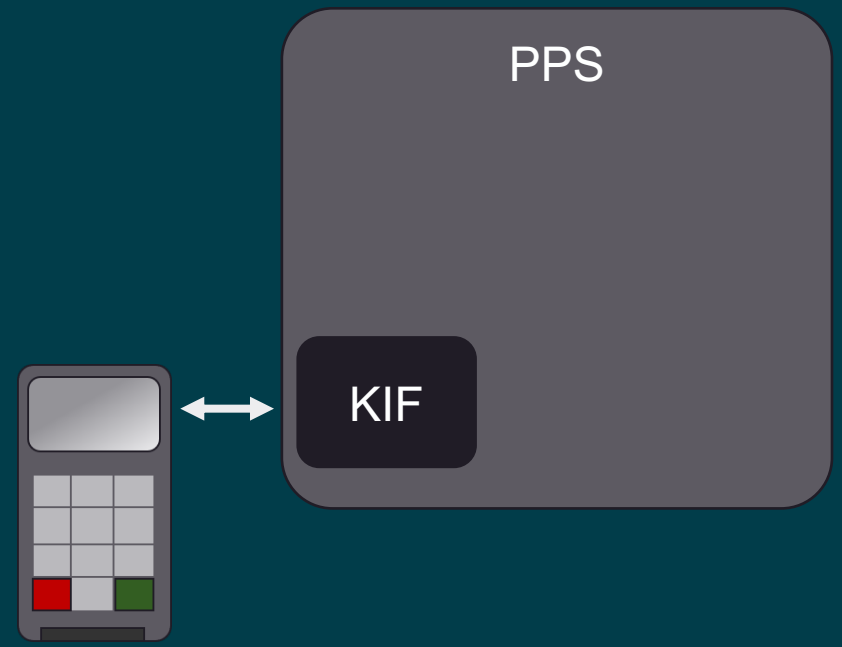


PCI KMO Outsourcing and Reusability

A primary goal of PCI KMO is to support an assess-once, use-many approach

- One assessment can cover multiple key data types
- Services can be used by other services to reduce scope
- Decryption Management (DM) is for P2PE keys only, PIN Processing Services (PPS) for PIN keys only

Outsourcing Matrix		Listed KMO Service Categories					
		DM	PPS	KIF	SSP	CA/RA	HaaS
Under Assessment	DM	✓	⊘	✓	✓	✓	✓
	PPS	⊘	✓	✓	✓	✓	✓
	KIF	⊘	⊘	✓	⊘	✓	✓
	SSP	⊘	⊘	⊘	✓	✓	✓
	CA/RA	⊘	⊘	⊘	⊘	✓	✓
	HaaS	⊘	⊘	⊘	⊘	⊘	✓

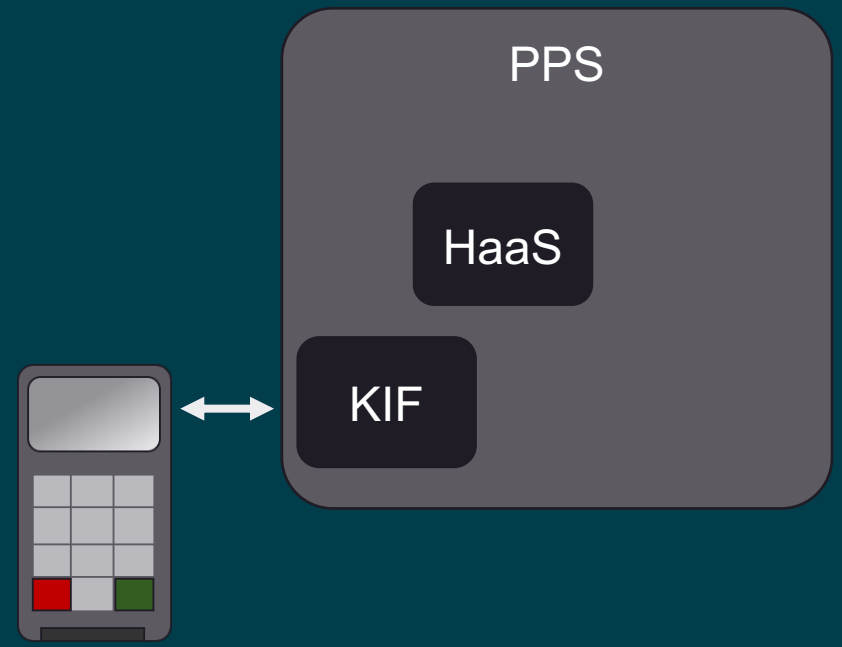


PCI KMO Outsourcing and Reusability

A primary goal of PCI KMO is to support an assess-once, use-many approach

- One assessment can cover multiple key data types
- Services can be used by other services to reduce scope
- Decryption Management (DM) is for P2PE keys only, PIN Processing Services (PPS) for PIN keys only

Outsourcing Matrix		Listed KMO Service Categories					
		DM	PPS	KIF	SSP	CA/RA	HaaS
Under Assessment	DM	✓	⊘	✓	✓	✓	✓
	PPS	⊘	✓	✓	✓	✓	✓
	KIF	⊘	⊘	✓	⊘	✓	✓
	SSP	⊘	⊘	⊘	✓	✓	✓
	CA/RA	⊘	⊘	⊘	⊘	✓	✓
	HaaS	⊘	⊘	⊘	⊘	⊘	✓

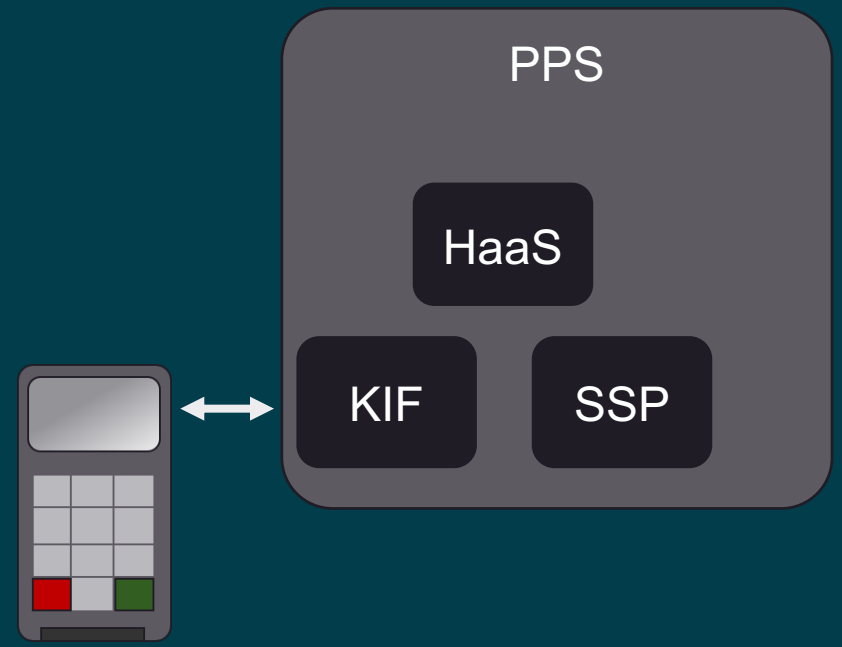


PCI KMO Outsourcing and Reusability

A primary goal of PCI KMO is to support an assess-once, use-many approach

- One assessment can cover multiple key data types
- Services can be used by other services to reduce scope
- Decryption Management (DM) is for P2PE keys only, PIN Processing Services (PPS) for PIN keys only

Outsourcing Matrix		Listed KMO Service Categories					
		DM	PPS	KIF	SSP	CA/RA	HaaS
Under Assessment	DM	✓	⊘	✓	✓	✓	✓
	PPS	⊘	✓	✓	✓	✓	✓
	KIF	⊘	⊘	✓	⊘	✓	✓
	SSP	⊘	⊘	⊘	✓	✓	✓
	CA/RA	⊘	⊘	⊘	⊘	✓	✓
	HaaS	⊘	⊘	⊘	⊘	⊘	✓

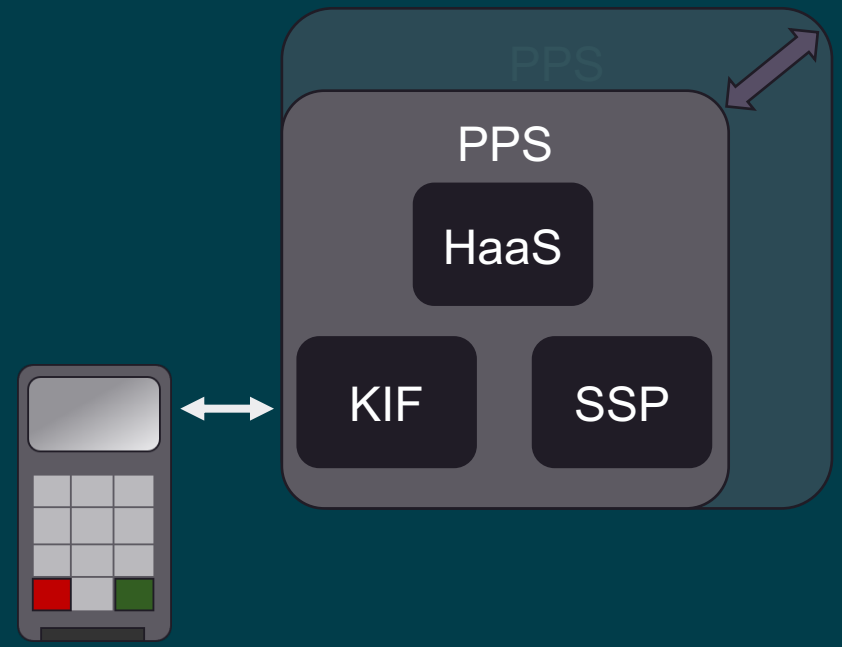


PCI KMO Outsourcing and Reusability

A primary goal of PCI KMO is to support an assess-once, use-many approach

- One assessment can cover multiple key data types
- Services can be used by other services to reduce scope
- Decryption Management (DM) is for P2PE keys only, PIN Processing Services (PPS) for PIN keys only

Outsourcing Matrix		Listed KMO Service Categories					
		DM	PPS	KIF	SSP	CA/RA	HaaS
Under Assessment	DM	✓	⊘	✓	✓	✓	✓
	PPS	⊘	✓	✓	✓	✓	✓
	KIF	⊘	⊘	✓	⊘	✓	✓
	SSP	⊘	⊘	⊘	✓	✓	✓
	CA/RA	⊘	⊘	⊘	⊘	✓	✓
	HaaS	⊘	⊘	⊘	⊘	⊘	✓



		Description	DM	PPS	KIF	SSP	CA / RA	HaaS
Domain 1: Core Requirements								
Control Objective 1A: Key Management Implementation								
	1A-1	Key-management scope	Applies to all KMO Service types					
	1A-2	Key-management design	Applies to all keys owned by entity					
	1A-3	Documented processes and audit trails	Applies to all KMO Service types					
	1A-4	Secure channels	Applies to all KMO Service types					
	1A-5	Key-custodian management	Applies if KCM is managed					
	1A-6	Management of in-scope and tamper-evident systems	Applies to all KMO Service types					
	1A-7	System authentication	Applies to all KMO Service types					
	1A-8	Cryptographic-key administration	Applies to all KMO Service types					
Control Objective 1B: Secure Key Generation								
	1B-1	Keys have sufficient entropy and strength	Applies to entities that generate keys					
Control Objective 1C: Secure Key Transmission, Conveyance, and Loading								
	1C-1	Secure key transmission, conveyance, and establishment	Applies to all KMO Service types					
Control Objective 1D: Secure Key Use and Operations								
	1D-1	Secret and private cryptographic keys are unique	Applies to all KMO Service types					
	1D-2	Management of potential key compromise	Applies to all KMO Service types					
	1D-3	Key archival and removal	Applies to all KMO Service types					
Domain 2: Remote HSM and HSM-as-a-Service Requirements								
Control Objective 2A: Remote HSMs								
	2A-1	Remote HSM access and operations	Where remote HSMs are used					X
Control Objective 2B: HSM-as-a-Service (HaaS)								
	2B-1	HSM-as-a-Service Key Management						X
	2B-2	HSM-as-a-Service Operations						X
	2B-3	HSM service logs						X

		Description	DM	PPS	KIF	SSP	CA / RA	HaaS
Domain 3: Data and Operation Specific Requirements								
Control Objective 3A: Data Specific Security Requirements								
	3A-1	PINs are processed in accordance with industry standards		X				1
	3A-2	Cryptographic keys and KCM are secured using SCDs	Applies to all PIN & P2PE Services					
	3A-3	P2PE backend systems are securely implemented	X					
Control Objective 3B: CA/RA and Signing Requirements								
	3B-1	Signing operations	4	4	4	X	X	2
	3B-2	CA/RA-specific requirements	4	4	4	4	X	2
	3B-3	Software/file-signing requirements	4	4	4	X	4	2
Control Objective 3C: HSM Specific Security Requirements								
	3C-1	FIPS validated HSMs	KMO Service using FIPS HSMs					
Control Objective 3D: Cryptographic Operations Outside of an SCD								
	3D-1	Backend encryption/decryption outside of an SCD	3					
Control Objective 3E: Best Practice Requirements								
	3E-1	POI devices implement secure channels	Optional: Not required / reviewed					
	3E-2	Key mgmt & crypto algorithms meet industry best practices	Optional: Not required / reviewed					
	3E-3	HSMs are validated & deployed for secure payments	Optional: Not required / reviewed					
Domain 4: Environmental Security Requirements								
Control Objective 4A: Physical Environment Requirements								
	4A-1	Minimally controlled environments	Applies as per Figure 2					
	4A-2	Controlled environments	Applies as per Figure 2					
	4A-3	Controlled-plus environments	Applies as per Figure 2					
	4A-4	Secure environments						
	4A-5	Secure storage and destruction	Applies to all PIN & P2PE Services					
Control Objective 4B: Logical Environment Requirements								
	4B-1	Secure networks	Applies to all PIN & P2PE Services					
	4B-2	Authentication controls	Applies to all PIN & P2PE Services					

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

		Description	DM	PPS	KIF	SSP	CA / RA	HaaS
Domain 1: Core Requirements								
Control Objective 1A: Key Management Implementation								
	1A-1	Key-management scope	Applies to all KMO Service types					
	1A-2	Key-management design	Applies to all keys owned by entity					
	1A-3	Documented processes and audit trails	Applies to all KMO Service types					
	1A-4	Secure channels	Applies to all KMO Service types					
	1A-5	Key-custodian management	Applies if KCM is managed					
	1A-6	Management of in-scope and tamper-evident systems	Applies to all KMO Service types					
	1A-7	System authentication	Applies to all KMO Service types					
	1A-8	Cryptographic-key administration	Applies to all KMO Service types					
Control Objective 1B: Secure Key Generation								
	1B-1	Keys have sufficient entropy and strength	Applies to entities that generate keys					
Control Objective 1C: Secure Key Transmission, Conveyance, and Loading								
	1C-1	Secure key transmission, conveyance, and establishment	Applies to all KMO Service types					
Control Objective 1D: Secure Key Use and Operations								
	1D-1	Secret and private cryptographic keys are unique	Applies to all KMO Service types					
	1D-2	Management of potential key compromise	Applies to all KMO Service types					
	1D-3	Key archival and removal	Applies to all KMO Service types					
Domain 2: Remote HSM and HSM-as-a-Service Requirements								
Control Objective 2A: Remote HSMs								
	2A-1	Remote HSM Access and operations	Where remote HSMs are used					X
Control Objective 2B: HSM-as-a-Service (HaaS)								
	2B-1	HSM-as-a-Service Key Management						X
	2B-2	HSM-as-a-Service Operations						X
	2B-3	HSM service logs						X

		Description	DM	PPS	KIF	SSP	CA / RA	HaaS
Domain 3: Secure Operations for Designated Data								
Control Objective 3A: Data Specific Security Requirements								
	3A-1	PANs are rendered unreadable anywhere they are stored						
	3A-2	Cryptographic keys and KCM are secured using SCDs	Applies to all PIN & P2PE Services					
	3A-3	PANs rendered unreadable anywhere they are transmitted						
Control Objective 3B: CA/RA and Signing Requirements								
	3B-1	Signing operations	X	X	X	X	X	X
	3B-2	CA/RA-specific requirements	4	4	4	4	X	2
	3B-3	CA/RA-specific signing requirements	X	X	X	X	X	X
Control Objective 3C: HSM Specific Security Requirements								
	3C-1	FIPS validated HSMs	KMO Service using HSM HSMs					
Control Objective 3D: Cryptographic Operations Outside of an SCD								
	3D-1	Keys are only used in the cryptographic SCDs for which they are intended						
Control Objective 3E: Best Practice Requirements								
	3E-1	POI devices implement secure reboot	Optional: Not required / reviewed					
	3E-2	Key mgmt & crypto algorithms meet industry best practices	Optional: Not required / reviewed					
	3E-3	HSMs are shipped & deployed in accordance with vendor guidance	Optional: Not required / reviewed					
Domain 4: Environmental Security Requirements								
Control Objective 4A: Physical Environment Requirements								
	4A-1	Minimally controlled environments	Applies as per Figure 2					
	4A-2	Controlled environments	Applies as per Figure 2					
	4A-3	Controlled-plus environments	Applies as per Figure 2					
	4A-4	Secure environments						
	4A-5	Secure storage and destruction	Applies to all PIN & P2PE Services					
Control Objective 4B: Logical Environment Requirements								
	4B-1	Secure networks	Applies to all PIN & P2PE Services					
	4B-2	Administrative controls	Applies to all PIN & P2PE Services					

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

		Description	DM	PPS	KIF	SSP	CA / RA	HaaS
Control Objective 1A: Key Management Implementation								
	1A-1	Key-management policy and procedures	Applies to all keys owned by entity					
	1A-2	Key-management design	Applies to all keys owned by entity					
	1A-3	Documented processes and audit trails	Applies to all KMO Service types					
	1A-4	Secure channels	Applies to all KMO Service types					
	1A-5	Key custodian management	Applies if KCMs is managed					
	1A-6	Management of in-scope and tamper-evident systems	Applies to all KMO Service types					
	1A-7	System authentication	Applies to all KMO Service types					
	1A-8	Cryptographic-key administration	Applies to all KMO Service types					
Control Objective 1B: Secure Key Generation								
	1B-1	Keys have sufficient entropy and strength	Applies to entities that generate keys					
Control Objective 1C: Secure Key Transmission, Conveyance, and Loading								
	1C-1	Secure key transmission, conveyance, and establishment	Applies to all KMO Service types					
Control Objective 1D: Secure Key Use and Operations								
	1D-1	Secret and private cryptographic keys are unique	Applies to all KMO Service types					
	1D-2	Management of potential key compromise	Applies to all KMO Service types					
	1D-3	Key archival and removal	Applies to all KMO Service types					
Domain 2: Remote HSM and HSM-as-a-Service Requirements								
Control Objective 2A: Remote HSMs								
	2A-1	Remote HSM access and operations	Where remote HSMs are used					X
Control Objective 2B: HSM-as-a-Service (HaaS)								
	2B-1	HSM-as-a-Service Key Management						X
	2B-2	HSM-as-a-Service Operations						X
	2B-3	HSM service logs						X

		Description	DM	PPS	KIF	SSP	CA / RA	HaaS
Control Objective 3A: Data Specific Security Requirements								
	3A-1	PANs are rendered unreadable anywhere they are stored	X	X	X	X	X	X
	3A-2	Cryptographic keys and KCM are secured using SCDs	Applies to all PIN & P2PE Services					
	3A-3	SCDs managed in accordance with documented POI	X	X	X	X	X	X
Control Objective 3B: CA/RA and Signing Requirements								
	3B-1	Signing operations	X	X	X	X	X	X
	3B-2	CA/RA-specific requirements	4	4	4	4	X	2
	3B-3	Cert profile/issuance requirements	X	X	X	X	X	X
Control Objective 3C: HSM Specific Security Requirements								
	3C-1	FIPS validated HSMs	Applies to all KMO Services using PCI-approved HSMs					
Control Objective 3D: Cryptographic Operations Outside of an SCD								
	3D-1	Sensitive operations are cryptographically bound to SCDs	X	X	X	X	X	X
Control Objective 3E: Best Practice Requirements								
	3E-1	POI devices implement secure reboot	Optional: Not required / reviewed					
	3E-2	Key mgmt & crypto algorithms meet industry best practices	Optional: Not required / reviewed					
	3E-3	HSMs are configured & deployed to secure components	Optional: Not required / reviewed					
Domain 4: Environmental Security Requirements								
Control Objective 4A: Physical Environment Requirements								
	4A-1	Minimally controlled environments	Applies as per Figure 2					
	4A-2	Controlled environments	Applies as per Figure 2					
	4A-3	Controlled-plus environments	Applies as per Figure 2					
	4A-4	Secure environments	X	X	X	X	X	X
	4A-5	Secure storage and destruction	Applies to all PIN & P2PE Services					
Control Objective 4B: Logical Environment Requirements								
	4B-1	Secure networks	Applies to all PIN & P2PE Services					
	4B-2	Administration controls	Applies to all PIN & P2PE Services					

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

		Description	DM	PPS	KIF	SSP	CA / RA	HaaS
Domain 1: Core Requirements								
Control Objective 1A: Key Management Implementation								
	1A-1	Key-management policy and procedures	Applies to all keys and key types					
	1A-2	Key-management design	Applies to all keys owned by entity					
	1A-3	Documented processes and audit trails	Applies to all KMO Service types					
	1A-4	Secure channels	Applies to all KMO Service types					
	1A-5	Key-custodian management	Applies if KCMs is managed					
	1A-6	Management of in-scope and tamper-evident systems	Applies to all KMO Service types					
	1A-7	System authentication	Applies to all KMO Service types					
	1A-8	Cryptographic-key administration	Applies to all KMO Service types					
Control Objective 1B: Secure Key Generation								
	1B-1	Keys have sufficient entropy and strength	Applies to entities that generate keys					
Control Objective 1C: Secure Key Transmission, Conveyance, and Loading								
	1C-1	Secure key transmission, conveyance, and establishment	Applies to all KMO Service types					
Control Objective 1D: Secure Key Use and Operations								
	1D-1	Secret and private cryptographic keys are unique	Applies to all KMO Service types					
	1D-2	Management of potential key compromise	Applies to all KMO Service types					
	1D-3	Key archival and removal	Applies to all KMO Service types					
Domain 2: Remote HSM and HSM-as-a-Service Requirements								
Control Objective 2A: Remote HSMs								
	2A-1	Remote HSM access and operations	Where remote HSMs are used					X
Control Objective 2B: HSM-as-a-Service (HaaS)								
	2B-1	HSM-as-a-Service Key Management						X
	2B-2	HSM-as-a-Service Operations						X
	2B-3	HSM service logs						X

		Description	DM	PPS	KIF	SSP	CA / RA	HaaS
Domain 3: Data and Operation Specific Requirements								
Control Objective 3A: Data Specific Security Requirements								
	3A-1	PINs are processed in accordance with industry standards		X				1
	3A-2	Cryptographic keys and KCM are secured using SCDs	Applies to all PIN & P2PE Services					
	3A-3	P2PE backend systems are securely implemented	X					
Control Objective 3B: CA/RA and Signing Requirements								
	3B-1	Signing operations	4	4	4	X	X	2
	3B-2	CA/RA-specific requirements	4	4	4	4	X	2
	3B-3	Software/file-signing requirements	4	4	4	X	4	2
Control Objective 3C: HSM Specific Security Requirements								
	3C-1	FIPS validated HSMs	KMO Service using FIPS HSMs					
Control Objective 3D: Cryptographic Operations Outside of an SCD								
	3D-1	Backend encryption/decryption outside of an SCD	3					
Control Objective 3E: Best Practice Requirements								
	3E-1	POI devices implement secure channels	Optional: Not required / reviewed					
	3E-2	Key mgmt & crypto algorithms meet industry best practices	Optional: Not required / reviewed					
	3E-3	HSMs are validated & deployed for secure payments	Optional: Not required / reviewed					
Domain 4: Environmental Security Requirements								
Control Objective 4A: Physical Environment Requirements								
	4A-1	Minimally controlled environments	Applies as per Figure 2					
	4A-2	Controlled environments	Applies as per Figure 2					
	4A-3	Controlled-plus environments	Applies as per Figure 2					
	4A-4	Secure environments						
	4A-5	Secure storage and destruction	Applies to all PIN & P2PE Services					
Control Objective 4B: Logical Environment Requirements								
	4B-1	Secure networks	Applies to all PIN & P2PE Services					
	4B-2	Authentication controls	Applies to all PIN & P2PE Services					

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

		Description	DM	PPS	KIF	SSP	CA / RA	HaaS
Domain 1: Core Requirements								
Control Objective 1A: Key Management Implementation								
	1A-1	Key-management policy and procedures	Applies to all KMO Service types					
	1A-2	Key-management design	Applies to all keys owned by entity					
	1A-3	Documented processes and audit trails	Applies to all KMO Service types					
	1A-4	Secure channels	Applies to all KMO Service types					
	1A-5	Key custodian management	Applies if KCMs is managed					
	1A-6	Management of in-scope and tamper-evident systems	Applies to all KMO Service types					
	1A-7	System authentication	Applies to all KMO Service types					
	1A-8	Cryptographic-key administration	Applies to all KMO Service types					
Control Objective 1B: Secure Key Generation								
	1B-1	Keys have sufficient entropy and strength	Applies to entities that generate keys					
Control Objective 1C: Secure Key Transmission, Conveyance, and Loading								
	1C-1	Secure key transmission, conveyance, and establishment	Applies to all KMO Service types					
Control Objective 1D: Secure Key Use and Operations								
	1D-1	Secret and private cryptographic keys are unique	Applies to all KMO Service types					
	1D-2	Management of potential key compromise	Applies to all KMO Service types					
	1D-3	Key archival and removal	Applies to all KMO Service types					
Domain 2: Remote HSM and HSM-as-a-Service Requirements								
Control Objective 2A: Remote HSMs								
	2A-1	Remote HSM access and operations	Where remote HSMs are used					X
Control Objective 2B: HSM-as-a-Service (HaaS)								
	2B-1	HSM-as-a-Service Key Management						X
	2B-2	HSM-as-a-Service Operations						X
	2B-3	HSM service logs						X

		Description	DM	PPS	KIF	SSP	CA / RA	HaaS
Domain 3: Device Operations and Management Requirements								
Control Objective 3A: Data Specific Security Requirements								
	3A-1	Sensitive data processed in the memory of a device is protected						
	3A-2	Cryptographic keys and KCM are secured using SCDs	Applies to all PIN & P2PE Services					
	3A-3	SCDs are validated to approved security requirements						
Control Objective 3B: CA/RA and Signing Requirements								
	3B-1	Signing operations	X	X	X	X	X	X
	3B-2	CA/RA-specific requirements	4	4	4	4	X	2
	3B-3	CA/RA-specific security requirements	X	X	X	X	X	X
Control Objective 3C: HSM Specific Security Requirements								
	3C-1	FIPS validated HSMs	Applies to devices using PCI-approved HSMs					
Control Objective 3D: Cryptographic Operations Outside of an SCD								
	3D-1	Keys used in unprotected memory are unpredictable and SCD-specific						
Control Objective 3E: Best Practice Requirements								
	3E-1	POI devices implement secure reversion	Optional: Not required / reviewed					
	3E-2	Key mgmt & crypto algorithms meet industry best practices	Optional: Not required / reviewed					
	3E-3	HSMs are implemented securely per vendor guidance	Optional: Not required / reviewed					
Domain 4: Environmental Security Requirements								
Control Objective 4A: Physical Environment Requirements								
	4A-1	Minimally controlled environments	Applies as per Figure 2					
	4A-2	Controlled environments	Applies as per Figure 2					
	4A-3	Controlled-plus environments	Applies as per Figure 2					
	4A-4	Secure environments						
	4A-5	Secure storage and destruction	Applies to all PIN & P2PE Services					
Control Objective 4B: Logical Environment Requirements								
	4B-1	Secure networks	Applies to all PIN & P2PE Services					
	4B-2	Authentication controls	Applies to all PIN & P2PE Services					

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Remote HSMs and HSM-as-a-Service (Domain 2)

PCI KMO is specifically designed to support the use of remote HSMs as well as HSM-as-a-Service implementations

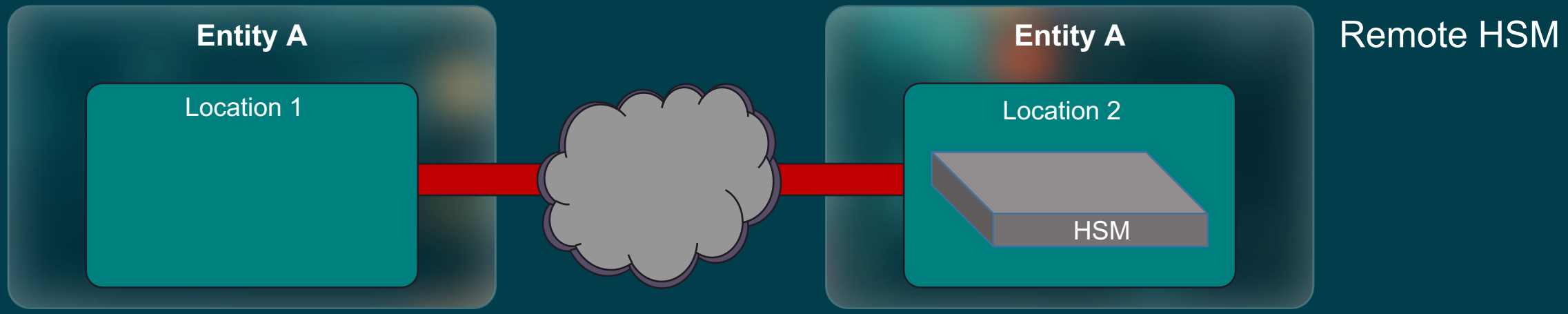
Control Objective 2A: Remote HSMs

- 2A-1 Remote HSM Access and Operations

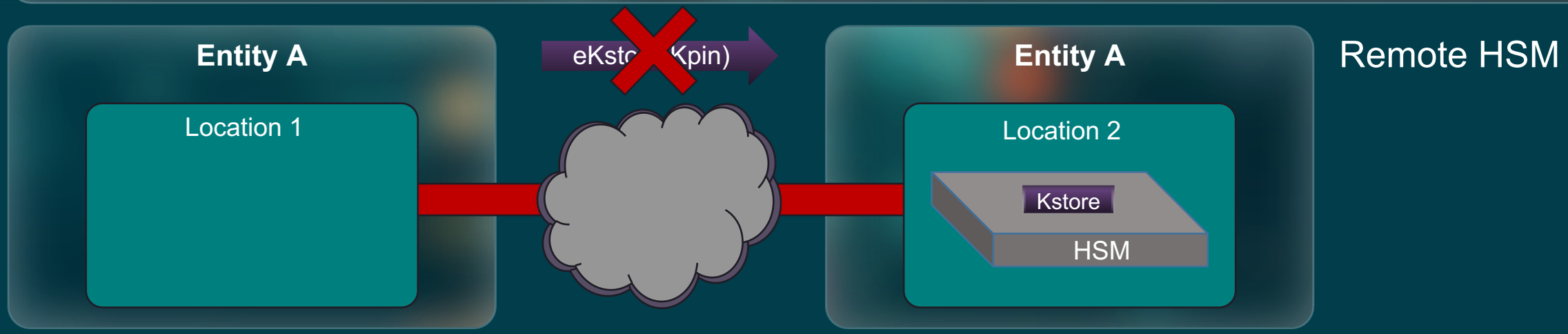
Control Objective 2B: HSM-as-a-Service (HaaS)

- 2B-1 HSM-as-a-Service Key Management
- 2B-2 HSM-as-a-Service Operations
- 2B-3 HSM service logs

Remote HSMs (Section 2A)

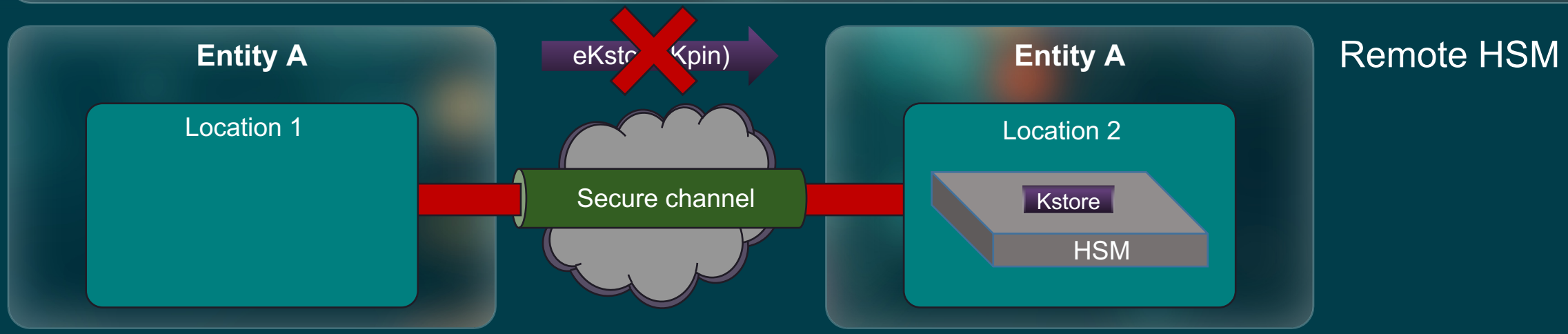


Remote HSMs (Section 2A)



2A-1.1 Local storage keys are used only for storage and are not used for key distribution.

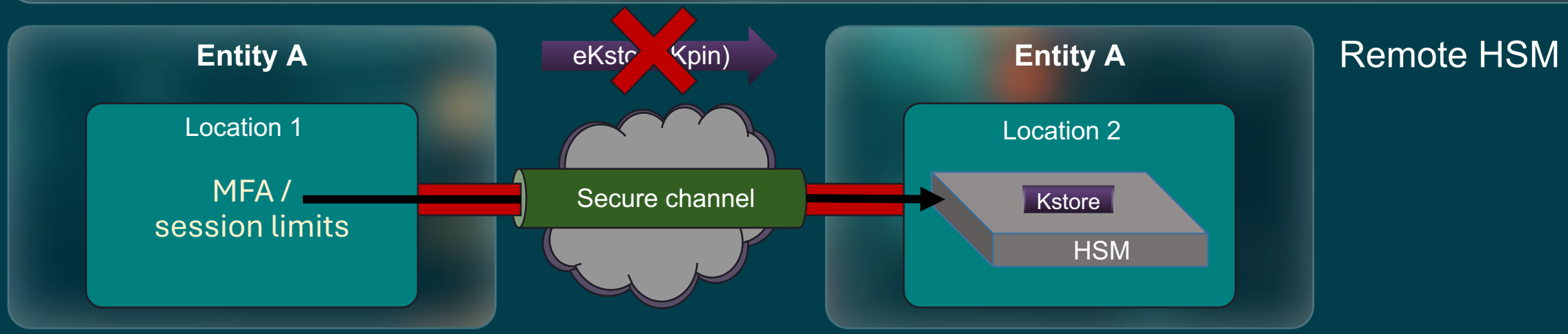
Remote HSMs (Section 2A)



2A-1.1 Local storage keys are used only for storage and are not used for key distribution.

2A-1.2 All connections to/from the HSM that traverse any out-of-scope networks implement Secure channel(s) meeting the requirements of Section 1A-4.

Remote HSMs (Section 2A)



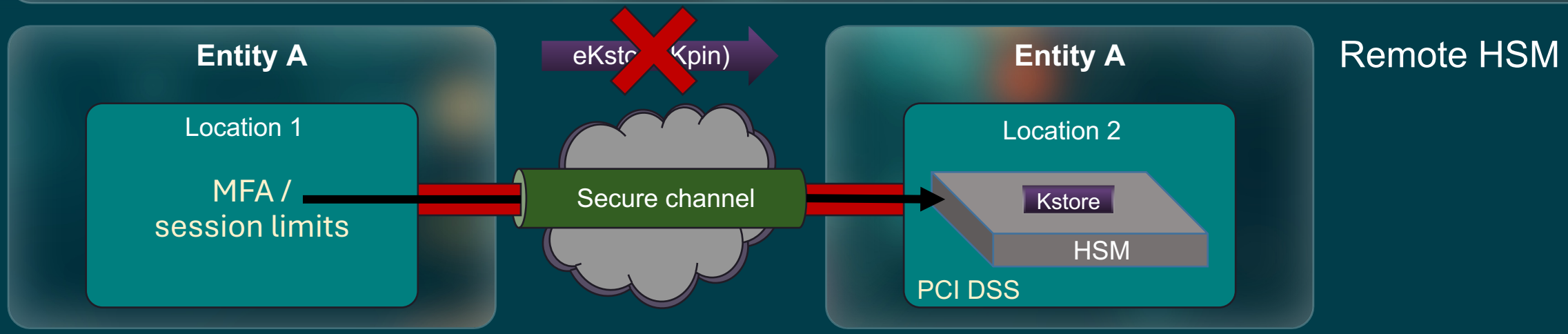
2A-1.1 Local storage keys are used only for storage and are not used for key distribution.

2A-1.2 All connections to/from the HSM that traverse any out-of-scope networks implement Secure channel(s) meeting the requirements of Section 1A-4.

2A-1.3 MFA is required for establishment of a non-console session with the HSM, using at least one SCD or HMD-bound factor.

2A-1.4 Authenticated administration sessions are terminated after no more than 15 minutes of idle time, and no more than 24 hours of continuous operation without any reauthentication.

Remote HSMs (Section 2A)



2A-1.1 Local storage keys are used only for storage and are not used for key distribution.

2A-1.2 All connections to/from the HSM that traverse any out-of-scope networks implement Secure channel(s) meeting the requirements of Section 1A-4.

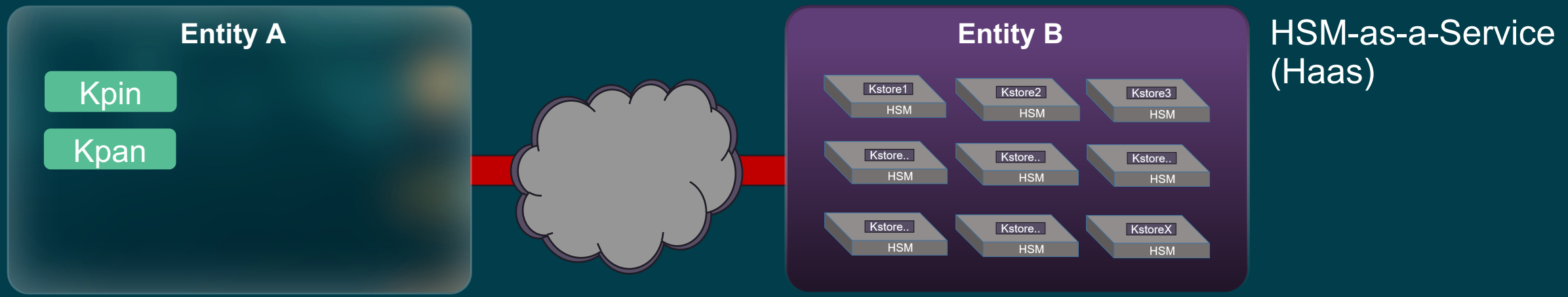
2A-1.3 MFA is required for establishment of a non-console session with the HSM, using at least one SCD or HMD-bound factor.

2A-1.4 Authenticated administration sessions are terminated after no more than 15 minutes of idle time, and no more than 24 hours of continuous operation without any reauthentication.

2A-1.5 Where cleartext account data may be present, the environment(s) containing the HSM(s) are validated against the requirements of PCI DSS.

2A-1.6 Remote provisioning of initial keys is performed securely, preventing monitoring, Attacker-In-The-Middle, pre-play, and replay attacks.

HSM-as-a-Service (Section 2B)



HSM-as-a-Service (Haas)

HSM-as-a-Service (Section 2B)

2B-1.2 Secret and private cryptographic keys that are not directly managed or owned by the HSM tenant are either unique per HSM tenant, or are generated by the HSM and never exported.

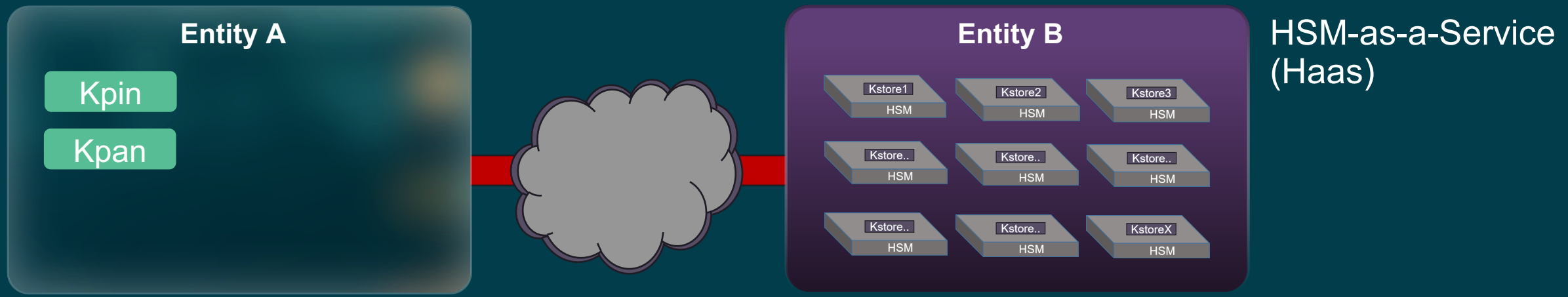
2B-1.3 The HSM-as-a-service offering is implemented so that the compromise of any cryptographic key within the hierarchy of any one HSM tenant cannot impact the presence or security of cryptographic keys for any other tenant.

2B-1.4 The loading and access of keys and key-constituent material are isolated per HSM tenant.

2B-1.5 The HSM service supports the ability to disable or suspend access and use of cryptographic keys owned by any HSM tenant, without impacting the service to any other HSM tenant.

2B-1.6 Operations performed with the cryptographic keys of, or on behalf of, an HSM tenant are cryptographically authenticated by that HSM tenant (or authorized agent).

2B-1.7 The HSM service securely establishes a unique provisioning key for each HSM tenant for any online-based provisioning.



Data Specific Security & CA/RA Signing Service Requirements (Sections 3A & 3B)

Section 3A outlines specific non-core requirements where the applicability may depend on the referencing standard/program, the type of data being encrypted, etc

- Includes areas specific to PIN processing, use of Secure Cryptographic Devices, and backend security

Section 3B provides the requirements for CA/RA implementations, as well as Signing Service Providers (SSPs) which sign code or data objects (e.g., for POI devices)

Where SCDs or CA/RA operations are in scope, the environments where they must be stored / operated are called out in these Sections, but the requirements for these areas are assessed under Domain 4

FIPS-validated HSM Requirements (Section 3C)

PCI KMO recognises two validation methods for HSMs - FIPS140-2/3 or PCI HSM

FIPS140-2/3 is not specifically designed for payment HSMs (as is PCI HSM)

- This means it can lack validation of important aspects required of a payment HSM (e.g, handling of key blocks, common key management methods, PIN translation, etc)

FIPS-validated HSM Requirements (Section 3C)

PCI KMO recognises two validation methods for HSMs - FIPS140-2/3 or PCI HSM

FIPS140-2/3 is not specifically designed for payment HSMs (as is PCI HSM)

- This means it can lack validation of important aspects required of a payment HSM (e.g, handling of key blocks, common key management methods, PIN translation, etc)

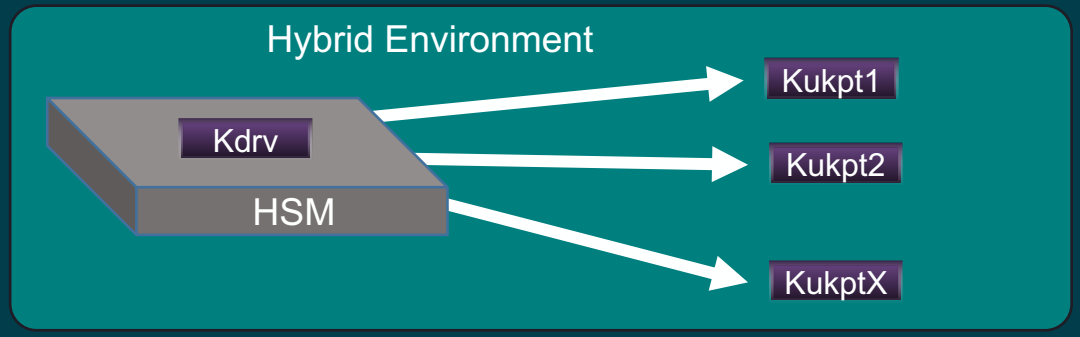
This is managed in KMO through a set of requirements dedicated to FIPS-validated HSMs

- Not equivalent to a lab assessment, but validates how the HSM is operated securely
  - HSM functions are operated within the tamper-responsive boundary
  - Keys stored external to the HSM are wrapped, including key purpose metadata
  - PIN operations are performed within the tamper-responsive boundary
  - Any virtualisation is performed externally to the HSM
- Only applies to HSMs which rely on FIPS140-2/3 validation
  - If validation to PCI HSM exists, that can be used to descope these requirements

Cryptographic operations outside of an SCD (Section 3D)

PCI KMO simplifies the 'hybrid' decryption requirements of PCI P2PE

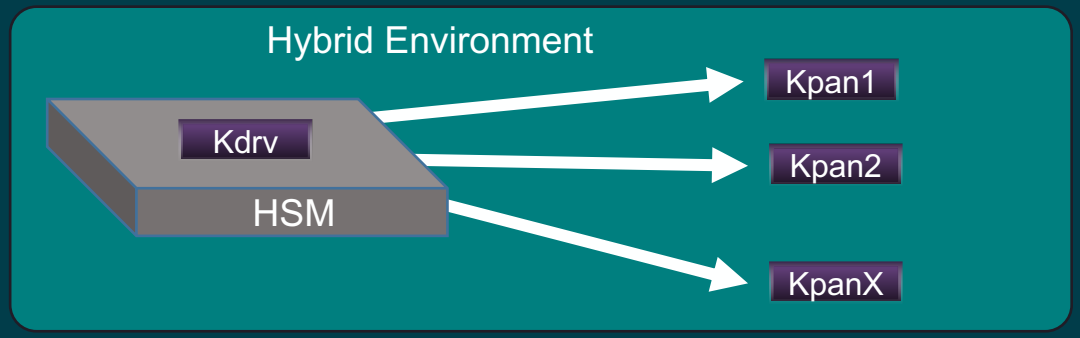
- Where transaction-unique, forward-secret keys are exposed outside of an SCD / HSM



Cryptographic operations outside of an SCD (Section 3D)

PCI KMO simplifies the 'hybrid' decryption requirements of PCI P2PE

- Where transaction-unique, forward-secret keys are exposed outside of an SCD / HSM
- PCI KMO has five test procedures for this type of implementation
  - Environment must meet applicable requirements (e.g., PCI DSS)
  - Data keys are unique-per-transaction and forward secret
  - Data keys are only used during the transaction
  - Data keys have a defined / limited purpose and are restricted to this use
  - The SCD prevents the exposure of the derivation key and associated secrets



Best Practice Requirements (Section 3E)

These two statements about key management and cryptography are both true:

- They are not not a static field – what is acceptable changes over time
- It can be difficult to quickly change these implementations

Best Practice Requirements (Section 3E)

These two statements about key management and cryptography are both true:

- They are not a static field – what is acceptable changes over time
- It can be difficult to quickly change these implementations

To address these, PCI KMO has some *optional* 'best practice' requirements

- These best practice requirements are not mandatory, and even if assessed and failed they will not impact a PCI KMO listing
- However, they indicate where things *may* be changing into the future

Best Practice Requirements (Section 3E)

Security Requirements	Test Procedures	Guidance
Security Objective: Cryptographic methods are implemented to secure data against attacks using cryptographically relevant quantum computers.		
3E-2.1 Secure channels support the use of post-quantum cryptography.	**3E-2.1.a** Confirm through examination that secure channels support the use of post-quantum cryptography.	**Purpose** Secure channels can be especially useful in transitions to securing implementations from cryptographically relevant quantum computers (CRQC), as the changing of cipher suites to use post-quantum cryptography (PQC) can often be an easier and quicker path than the changing of the data-level cryptography used in devices such as POIs.
3E-2.2 PIN processing environments support processing using ISO format 4 PIN blocks.	**3E-2.2.a** Confirm through examination and interview that PIN processing environments support processing using ISO format 4 PIN blocks.	**Purpose** Use of algorithms with an effective key strength of 128 bits (or above), as supported by ISO format 4 PIN blocks, represents a significant increase in security over the TDES algorithm used in many existing PIN processing implementations. 128-bit AES is potentially exposed to attack using Grovers algorithm. However, scaling of this type of attack is difficult enough that NIST considers 128-bit AES suitable as a PQC 'level 1' algorithm.
3E-2.3 Top-level HSM keys (storage and master keys) provide an effective security level at least equal to 256-bit AES.	**3E-2.3.a** Confirm through examination and interview that top-level HSM keys (storage and master keys) provide an effective security level at least equal to 256-bit AES.	**Purpose** Keys at higher levels of the key hierarchy require more protection and security, as their exposure can have a wider and more damaging impact. HSM master keys are at the top of all, and therefore should implement the best possible level of security.

Security Requirements	Test Procedures	Guidance
3E-2.4 Remote key-distribution methods allow for the use of quantum-safe asymmetric algorithms.	**3E-2.4.a** Confirm through examination and interview that remote key-distribution methods allow for the use of quantum-safe asymmetric algorithms.	**Purpose** Remote key distribution often requires the use of asymmetric algorithms. Classical cryptographic algorithms such as RSA and ECC are open to attack by cryptographically relevant quantum computers. To prevent such attacks, remote key distribution methods can require the exclusive use of post-quantum cryptography, or use 'hybrid' cryptographic methods which include both classical and PQC methods. **References** For further details on post-quantum cryptography as it relates to the PCI standards, see the PCI SSC Cryptography Guidance document.
3E-2.5 TDEA is used only with key management that ensures unique-keys-per-transaction.	**3E-2.5.a** Confirm through examination and interview that TDEA is used only with key management that ensures unique-keys-per-transaction.	**Purpose** Although the security provided by TDEA is less than that provided by AES, some of the concerns with this algorithm can be mitigated through regular rotation of the keys used. The best practice implementation of this is to ensure that keys are changed after each transaction, using a UKPT method such as ANSI X9.24 DUKPT.
3E-2.6 BDKs are never exported from under the protection of the HSM that was used to generate the BDK.	**3E-2.6.a** Confirm through examination and interview that BDKs are never exported from under the protection of the HSM that was used to generate the BDK.	**Purpose** Base Derivation Keys (BDKs) are used to derive keys for a population of transaction-originating devices, and by this nature are extremely sensitive. Exposure of a single BDK could compromise the cryptography used to protect sensitive data on many thousands of devices. To reduce the risk of exposure, a BDK should not be exposed outside of the protection of the HSM used to generate the BDK. This includes exposure as key-constituent material or loading of the BDK into other SCDs, such as key-loading devices.
3E-2.7 Key distribution and agreement cryptography and protocols implement forward-secrecy.	**3E-2.7.a** Confirm through examination and interview that key distribution and agreement cryptography and protocols implement forward secrecy.	**Purpose** Forward-secrecy prevents the recovery of past keys, even if server keys are compromised.

Examples of *optional / non-mandatory* best practice requirements

Physical Environments (Sections 4A-1 to 4A-4)

Uncontrolled environment
(PCI DSS Req 9.x applies if non-PIN account data is present)

- Transmission and storage of encrypted & authenticated wrapped keys
- Handling of key constituent material by custodians (including manual entry)
- Transmission of key constituent material in TEA bags or SCDs
- Storage of key constituent material & keys in SCDs (excluding operational HSMs)

Physical Environments (Sections 4A-1 to 4A-4)

Uncontrolled environment
(PCI DSS Req 9.x applies if non-PIN account data is present)

- Transmission and storage of encrypted & authenticated wrapped keys
- Handling of key constituent material by custodians (including manual entry)
- Transmission of key constituent material in TEA bags or SCDs
- Storage of key constituent material & keys in SCDs (excluding operational HSMs)

Minimally controlled environment (4A-1)

- Operational HSMs meeting FIPS140-2/3 Level 4 or unrestricted PCI HSM (including virtualization systems implemented within a PCI HSM)
- Storage of key constituent material in TEA bags in safe
- Safe(s) meeting EN1143-1 Grade V+ or UL687 TL-30x6 (or above)

Ingress / egress controls

- Electronic access controls or physical access controls

Boundary of environment

- Physical or tamper evident controls prevent ingress

Security of in-scope systems

- HSMs secured to prevent removal

Physical Environments (Sections 4A-1 to 4A-4)

Uncontrolled environment
(PCI DSS Req 9.x applies if non-PIN account data is present)

- Transmission and storage of encrypted & authenticated wrapped keys
- Handling of key constituent material by custodians (including manual entry)
- Transmission of key constituent material in TEA bags or SCDs
- Storage of key constituent material & keys in SCDs (excluding operational HSMs)

Minimally controlled environment (4A-1)

- Operational HSMs meeting FIPS140-2/3 Level 4 or unrestricted PCI HSM (including virtualization systems implemented within a PCI HSM)
- Storage of key constituent material in TEA bags in safe
- Safe(s) meeting EN1143-1 Grade V+ or UL687 TL-30x6 (or above)

Controlled environment (4A-2)

- Operational HSMs meeting:
  - FIPS140-2/3 Level 3 (or below)
  - PCI HSM (with listing requiring controlled environment)
- Display/writing/printing of cleartext key constituent material
- Transmission of encrypted but unauthenticated keys (including keys protected by a secure channel only)
- Safe(s) meeting EN1143-1 Grade III or UL687 TL-30 (or above)

Ingress / egress controls

- Electronic access controls or physical access controls
- Electronic access controls only
- Supervised entry/exit points
- Vistors supervised
- Alarms on access
- No single occupancy for > 30 seconds
- Video monitoring of activity

Boundary of environment

- Physical or tamper evident controls prevent ingress
- Physical controls are required to prevent ingress
- Limited openings in physical barrier

Security of in-scope systems

- HSMs secured to prevent removal
- Monitoring of in-scope systems

Physical Environments (Sections 4A-1 to 4A-4)

Uncontrolled environment
(PCI DSS Req 9.x applies if non-PIN account data is present)

- Transmission and storage of encrypted & authenticated wrapped keys
- Handling of key constituent material by custodians (including manual entry)
- Transmission of key constituent material in TEA bags or SCDs
- Storage of key constituent material & keys in SCDs (excluding operational HSMs)

Minimally controlled environment (4A-1)

- Operational HSMs meeting FIPS140-2/3 Level 4 or unrestricted PCI HSM (including virtualization systems implemented within a PCI HSM)
- Storage of key constituent material in TEA bags in safe
- Safe(s) meeting EN1143-1 Grade V+ or UL687 TL-30x6 (or above)

Controlled environment (4A-2)

- Operational HSMs meeting:
  - FIPS140-2/3 Level 3 (or below)
  - PCI HSM (with listing requiring controlled environment)
- Display/writing/printing of cleartext key constituent material
- Transmission of encrypted but unauthenticated keys (including keys protected by a secure channel only)
- Safe(s) meeting EN1143-1 Grade III or UL687 TL-30 (or above)

Controlled-Plus environment (4A-3)

- HSM virtualisation systems (external to HSM)
- Transmission of cleartext keys (for legacy systems)
- Transmission of cleartext key constituent material

Ingress / egress controls

- Electronic access controls or physical access controls
- Electronic access controls only
- Supervised entry/exit points
- Vistors supervised
- Alarms on access
- No single occupancy for > 30 seconds
- Video monitoring of activity
- Dual control and anti-passback
- Motion sensors (where applicable)
- 24hr power backup

Boundary of environment

- Physical or tamper evident controls prevent ingress
- Physical controls are required to prevent ingress
- Limited openings in physical barrier
- Physical controls include consideration of adjacent areas
- Resists attempted use of powered cutting tools

Security of in-scope systems

- HSMs secured to prevent removal
- Monitoring of in-scope systems
- Environment on contains key management systems

Physical Environments (Sections 4A-1 to 4A-4)

Uncontrolled environment
(PCI DSS Req 9.x applies if non-PIN account data is present)

- Transmission and storage of encrypted & authenticated wrapped keys
- Handling of key constituent material by custodians (including manual entry)
- Transmission of key constituent material in TEA bags or SCDs
- Storage of key constituent material & keys in SCDs (excluding operational HSMs)

Minimally controlled environment (4A-1)

- Operational HSMs meeting FIPS140-2/3 Level 4 or unrestricted PCI HSM (including virtualization systems implemented within a PCI HSM)
- Storage of key constituent material in TEA bags in safe
- Safe(s) meeting EN1143-1 Grade V+ or UL687 TL-30x6 (or above)

Controlled environment (4A-2)

- Operational HSMs meeting:
  - FIPS140-2/3 Level 3 (or below)
  - PCI HSM (with listing requiring controlled environment)
- Display/writing/printing of cleartext key constituent material
- Transmission of encrypted but unauthenticated keys (including keys protected by a secure channel only)
- Safe(s) meeting EN1143-1 Grade III or UL687 TL-30 (or above)

Controlled-Plus environment (4A-3)

- HSM virtualisation systems (external to HSM)
- Transmission of cleartext keys (for legacy systems)
- Transmission of cleartext key constituent material

Secure environment (4A-4)

- CA/RA operations

Ingress / egress controls

- Electronic access controls or physical access controls
- Electronic access controls only
- Supervised entry/exit points
- Vistors supervised
- Alarms on access
- No single occupancy for > 30 seconds
- Video monitoring of activity
- Dual control and anti-passback
- Motion sensors (where applicable)
- 24hr power backup
- Occupancy sensors 24/7 and no single occupancy
- Supervision of visitors by two authorised individuals

Boundary of environment

- Physical or tamper evident controls prevent ingress
- Physical controls are required to prevent ingress
- Limited openings in physical barrier
- Physical controls include consideration of adjacent areas
- Resists attempted use of powered cutting tools

Security of in-scope systems

- HSMs secured to prevent removal
- Monitoring of in-scope systems
- Environment on contains key management systems
- Removing in-scope systems requires authorisation

Logical Environments (Sections 4B-1 & 4B-2)

Requirements based broadly on a subset of PCI DSS:

4B-1 Secure networks

4B-2 Authentication controls

These sections include requirements for:

- On-going vulnerability management processes
- Network security controls
- User/operator ID and authentication

Summary

PCI KMO is intended as a single-source for requirements covering key management operations

- Supporting different key data types, and key management aspects
- Includes data-specific requirements where appropriate

It is designed to modular and support an assess-once-use-many approach

- A single assessment can cover different key data types
- Implementations can rely on existing KMO Services to meet requirements
- Requirements for remote and HSM-as-a-Service are explicitly considered

Format and requirements are updated to current best practice

- Including explicit ‘best practice requirements’
- Consideration for new algorithms and processes