Our “Key” Experience in PCI PIN / P2PE / FIPS 140-3

PCI Security Standards Council

atsec Information Security

Di Li, Principal Consultant

What issues do we encounter during the assessment?

PCI PIN Security, PCI P2PE, FIPS 140-3

Too many terms regarding key management

Key generation, convey, transmission, loading, establishment, transport, destruction, zeroization, distribution, injection …

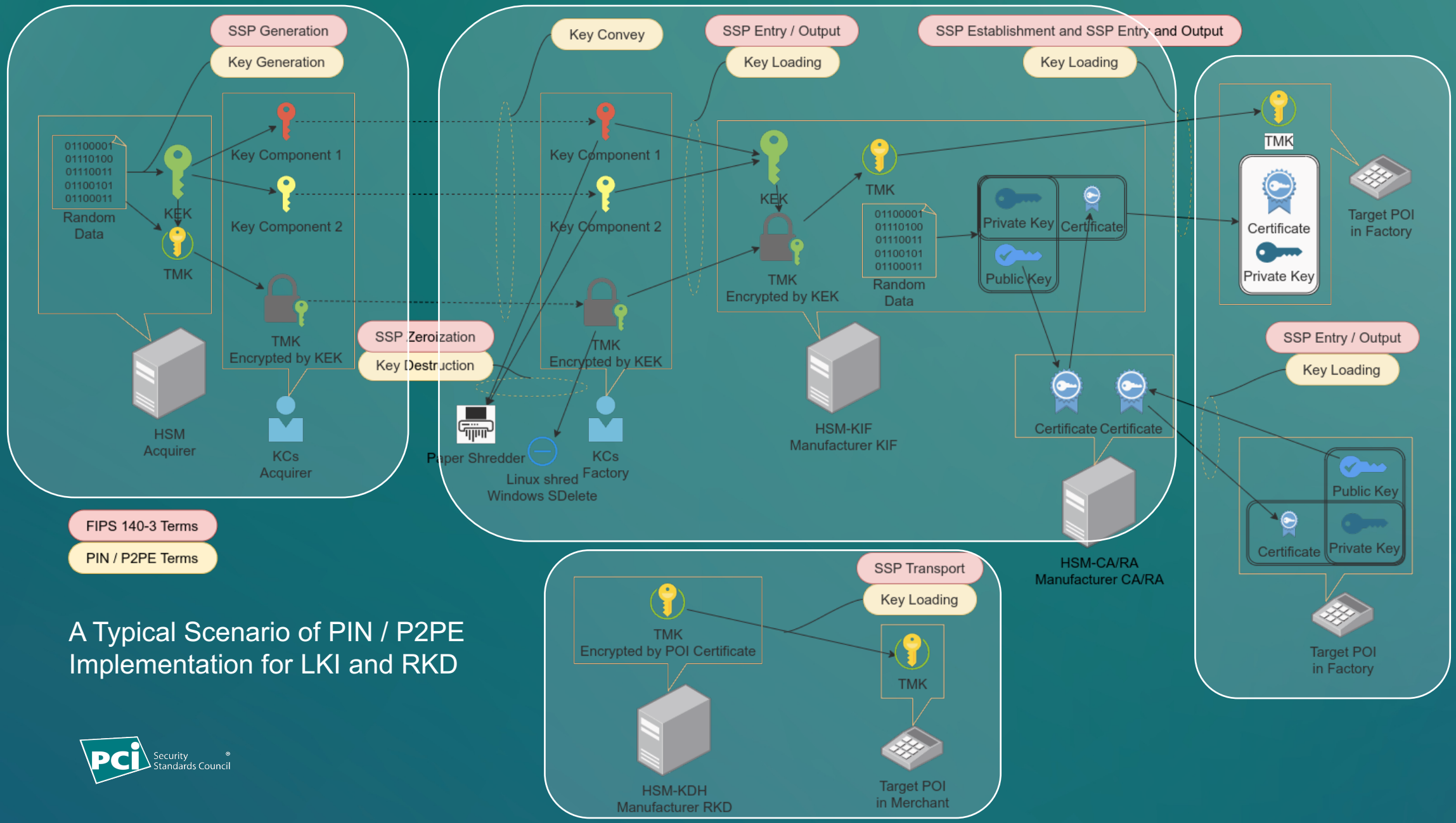
Lack of precise definitions

Existing definitions hardly map to real scenario

How we are trying to make it clear:

PARTY A acts on **WHAT DATA** within / to **PARTY B** in order to **ACHIEVE WHAT PURPOSE**

PCI Security Standards Council



A Typical Scenario of PIN / P2PE Implementation for LKI and RKD

PCI Security Standards Council

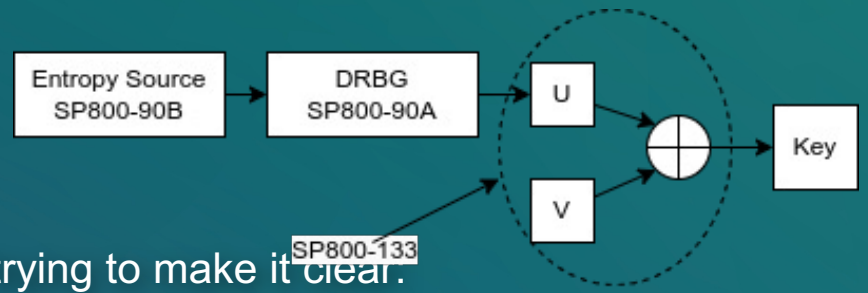
Key Management Activity - Key Generation

Used in: PCI PIN Security, PCI P2PE, FIPS 140-3

Existing definition:

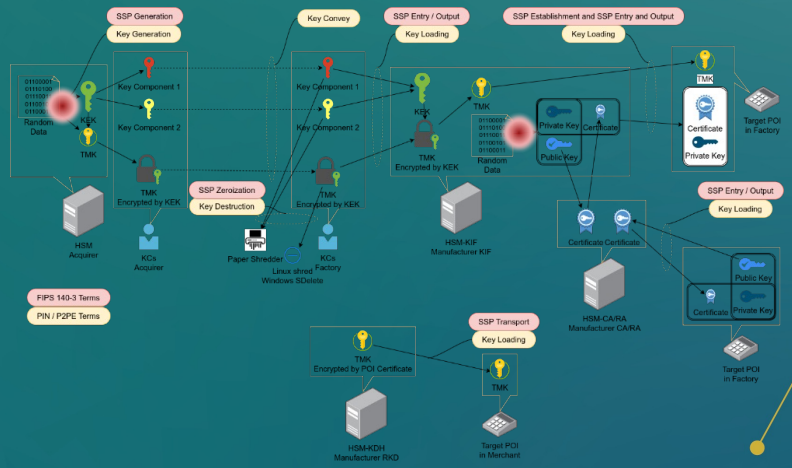
PIN / P2PE: Creation of a new key for subsequent use.

FIPS:



How we are trying to make it clear:

SCD generates **random data** within **SCD** in order to **be used as key or keypair**



Security Standards Council

Key Management Activity - Key Convey

Used in: PCI PIN Security, PCI P2PE

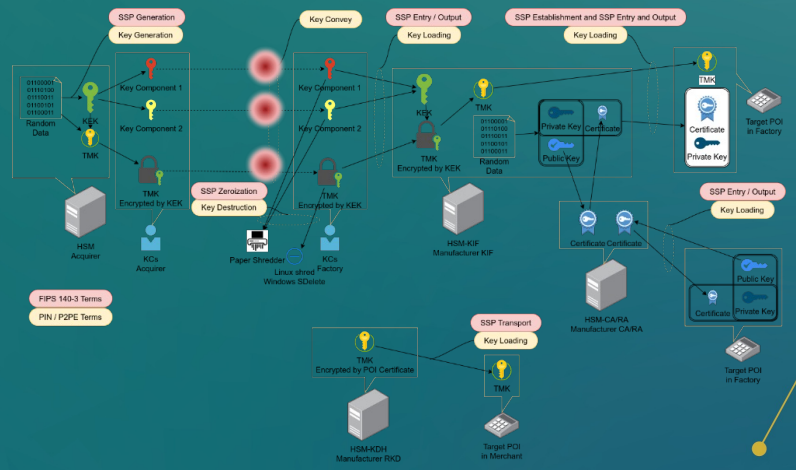
Existing definition:

PIN / P2PE: No*

FIPS: No

How we are trying to make it clear :

Sender (person) transmits the **key components, key shares, plaintext public key, encrypted private key, encrypted secret key** to **receiver (person)** in order to **share the same secret**



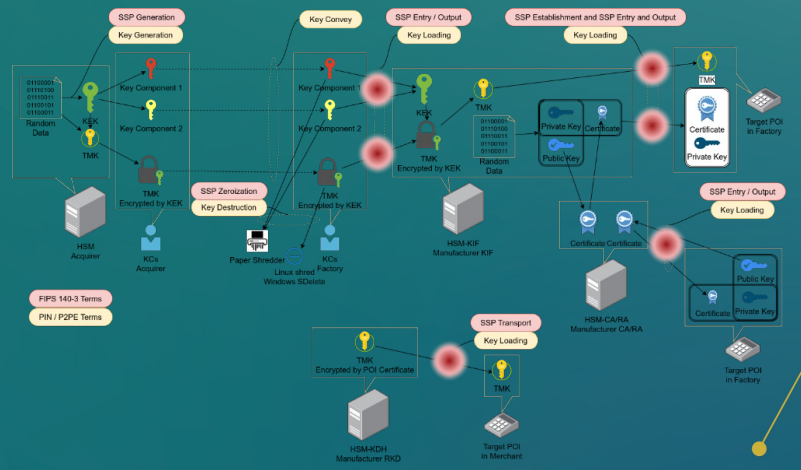
Key Management Activity - Key Loading

Used in: PCI PIN Security, PCI P2PE

Existing definition:

- PIN / P2PE Key Loading: Process by which a key is transferred manually or electronically into an SCD.
- PIN / P2PE Manual key loading: The entry of cryptographic keys into an SCD from a printed form, using devices such as buttons, thumb wheels, keyboard, or a touchscreen.

FIPS: No



PCI Security Standards Council

What does “Key Loading” look like in FIPS 140-3?

Used in: FIPS 140-3

IG 9.5 A SSP Establishment and SSP Entry and Output

Process of making available a shared SSP to one or more entities

P: Plaintext

E: Encrypted using an approved security function listed in SP 800-140C (sections 6.2.2 or 6.2.6)

SE: SSP Establishment that uses an approved or allowed method listed in IG D.F or IG D.G.

TC: Trusted Channel per ISO/IEC 19790:2012 Section 7.3.4 and IG 3.4.A

SK: Plaintext Split Knowledge using a TC

CSP Entry Format – Table 2

		Distribution (Establishment)											
		Manual				Automated				Manual Wireless			
Entry (Input / Output)	Direct	Keyboard, Number pad, Thumbwheel, Switch, Dial, etc.											
		1[0]	2[0]	3	4								
		P/E/ SE	P/E/ SE	TC/SK /E/SE	TC/SK /E/SE								
	Electronic	Smart Cards, Token, PC card, Diskettes, Key Loaders, OS, etc.				**SSP Establishment** SSP Transport or SSP Agreement				Bluetooth, Induction, Infrared (IR), Ultra Wideband (UWB), etc.			
		1[0]	2[0]	3	4	1	2	3	4	1	2	3	4
		P/E/ SE	P/E/ SE	TC/SK /E/SE	TC/SK /E/SE	SE	SE	SE	SE	E/SE	E/SE	E/SE	E/SE

PCI Security Standards Council

What does “Key Loading” look like in FIPS 140-3? (cont.)

Used in: FIPS 140-3

IG D.F Key agreement

is a method of SSP establishment where the resultant key is a function of information contributed by two or more participants, so that no party can predetermine the value of the key independently of the other party’s contribution using automated methods. Key agreement is performed using key agreement schemes.

Scenario 1 (SP800-56Br2)

Scenario 2 (SP800-56Ar3)

Scenario 3 (ECC scheme using curves in IG C.A)

CSP Entry Format – Table 2

Entry (Input / Output)		Distribution (Establishment)											
		Manual				Automated				Manual Wireless			
	Direct	Keyboard, Number pad, Thumbwheel, Switch, Dial, etc.											
		1[0]	2[0]	3	4								
		P/E/ SE	P/E/ SE	TC/SK /E/SE	TC/SK /E/SE								
	Electronic	Smart Cards, Token, PC card, Diskettes, Key Loaders, OS, etc.				SSP Establishment SSP Transport or SSP Agreement				Bluetooth, Induction, Infrared (IR), Ultra Wideband (UWB), etc.			
		1[0]	2[0]	3	4	1	2	3	4	1	2	3	4
		P/E/ SE	P/E/ SE	TC/SK /E/SE	TC/SK /E/SE	SE	SE	SE	SE	E/SE	E/SE	E/SE	E/SE

PCI Security Standards Council

What does “Key Loading” look like in FIPS 140-3? (cont.)

Used in: FIPS 140-3

IG D.G Key transport

is a method of SSP establishment whereby one party (the sender) selects a value for the secret keying material and then securely distributes that value to another party (the receiver). Key transport can be provided using either symmetric or asymmetric techniques.

Key encapsulation (SP800-56Br2)

Key wrapping (SP800-38F, encryption + authentication)

CSP Entry Format – Table 2

		Distribution (Establishment)											
		Manual				Automated				Manual Wireless			
Entry (Input / Output)	Direct	Keyboard, Number pad, Thumbwheel, Switch, Dial, etc.											
		1[6]	2[6]	3	4								
		P/E/ SE	P/E/ SE	TC/SK /E/SE	TC/SK /E/SE								
	Electronic	Smart Cards, Token, PC card, Diskettes, Key Loaders, OS, etc.				**SSP Establishment** SSP Transport or SSP Agreement				Bluetooth, Induction, Infrared (IR), Ultra Wideband (UWB), etc.			
		1[6]	2[6]	3	4	1	2	3	4	1	2	3	4
		P/E/ SE	P/E/ SE	TC/SK /E/SE	TC/SK /E/SE	SE	SE	SE	SE	E/SE	E/SE	E/SE	E/SE

Key Management Activity - Key Loading

Used in: PCI PIN Security, PCI P2PE

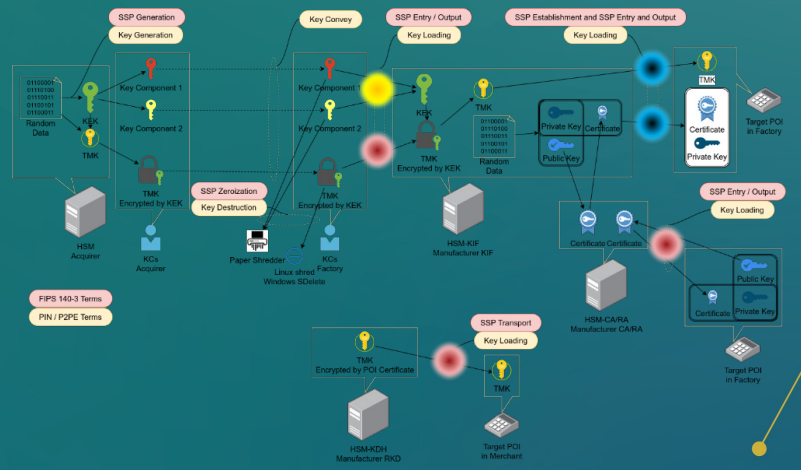
How we are trying to make it clear :

Manual Key Loading:

- **Receiver (person)** loads the **key components, key shares** into **SCD** in order to **restore original key from components / shares**

Automated Key Transport :

- **SCD** transports the **encrypted private key, encrypted secret key** into **SCD** in order to **decrypt and get plaintext private key, plaintext secret key**
- ~~**SCD** transports the **plaintext private key, secret key** into **SCD** in order to **perform remote key distribution or transaction**~~



Key Management Activity - Key Destruction

Used in: PCI PIN Security, PCI P2PE, FIPS 140-3

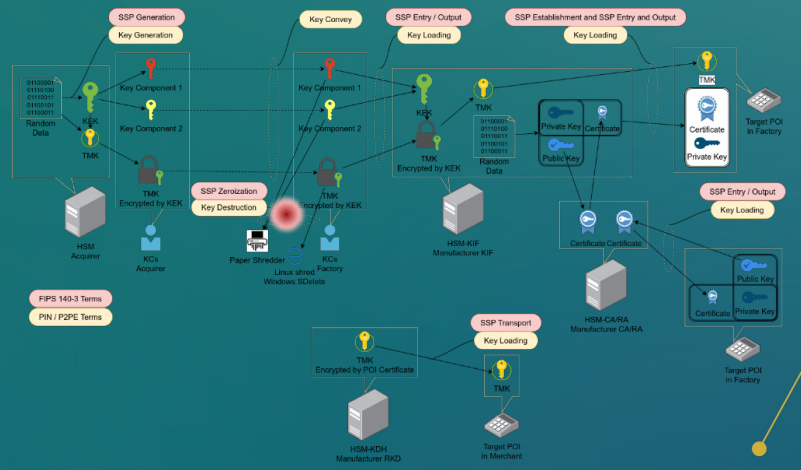
Existing definition:

PIN / P2PE: Occurs when an instance of a key in one of the permissible key forms no longer exists at a specific location.

FIPS: Method of destruction of stored data and unprotected SSPs to prevent retrieval and reuse

How we are trying to make it clear :

SCD securely delete / zeroize **all keys** within **SCD** in order to **prevent retrieval and reuse**



PCI Security Standards Council

Business Oriented - Key Injection

Used in: PCI PIN Security, PCI P2PE

Existing definition:

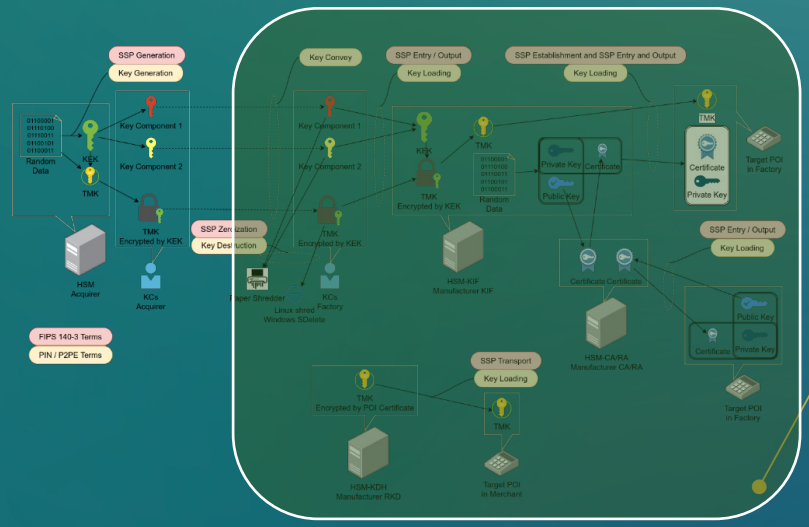
PIN / P2PE: No

FIPS: No

How we are trying to make it clear :

POI Manufacturer transmits the **secret key of Fixed Key scheme, MK of MK/SK scheme, IPEK of DUKPT scheme** to **target POI** in order to **perform transaction**

Note: key injection may cover key convey, key loading, remote key distribution



Business Oriented - Remote Key Distribution

Used in: PCI PIN Security, PCI P2PE

Existing definition:

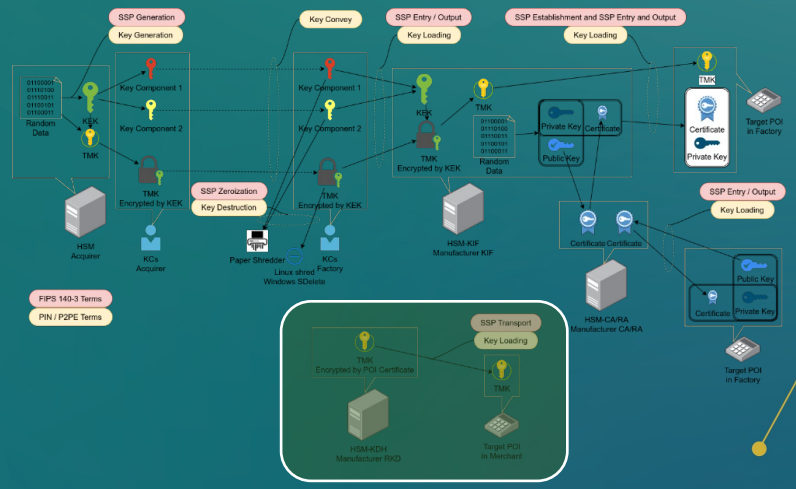
PIN / P2PE: No

FIPS: No

How we are trying to make it clear :

KDH remotely loads the **asymmetric encapsulated secret key of Fixed Key scheme, MK of MK/SK scheme, IPEK of DUKPT scheme** to **target POI** in order to **perform transaction**

Note: It’s part of the key injection



PCI Security Standards Council

Summary

Current issues when talking with vendors:

- Some key management activities are not defined clearly: key convey, key injection, key distribution
- Key injection and distribution: are they key management activities or business processes?

How we are trying to make it simpler and clearer:

- Key Convey is person-to-person process
- Key Injection and Remote Key Distribution are business-oriented process
- Split “Key Loading” into Manual Key Loading and Automated Key Transport