PCI PIN SECURITY COMPLIANCE

Why Security is not an option

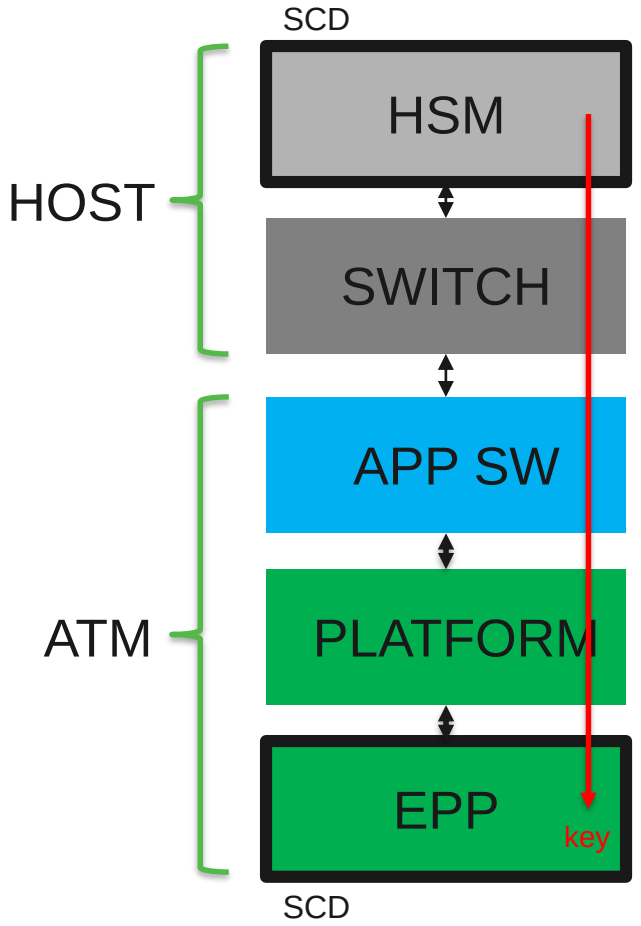
Charlie Harrow
Global Security
May 2016

Agenda

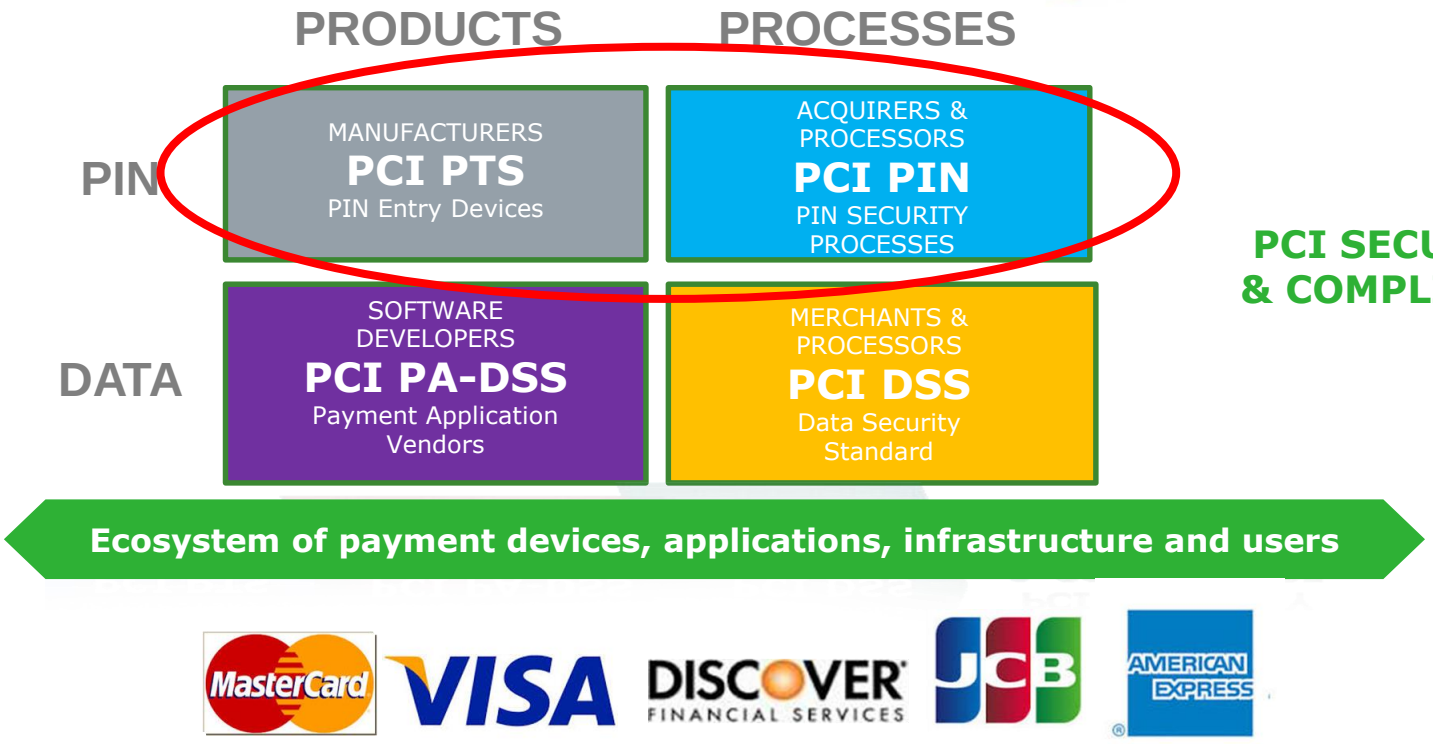
- NCR EPP3
- PCI Requirements Changes that impact ATM PIN Entry Devices
- NCR Strategy for Compliance
- NCR implementation
  - TR34, TR31
- References
- Take Aways

Executive Summary

- PCI requirements are coming into effect that will change the way that PIN encryption keys are managed.
- These requirements mean changes to Remote Key Distribution systems, changes to the way that symmetric keys are encrypted, changes to how keys are deleted from PIN pads, and a change to the timing of PIN encryption within a PIN Entry Device.
- NCR ATMs are already compliant with these requirements.
- To comply with the changes, NCR has implemented standards based, open, interoperable solutions.



PCI – SUITE OF STANDARDS



PCI SECURITY & COMPLIANCE

PCI PTS FAQs

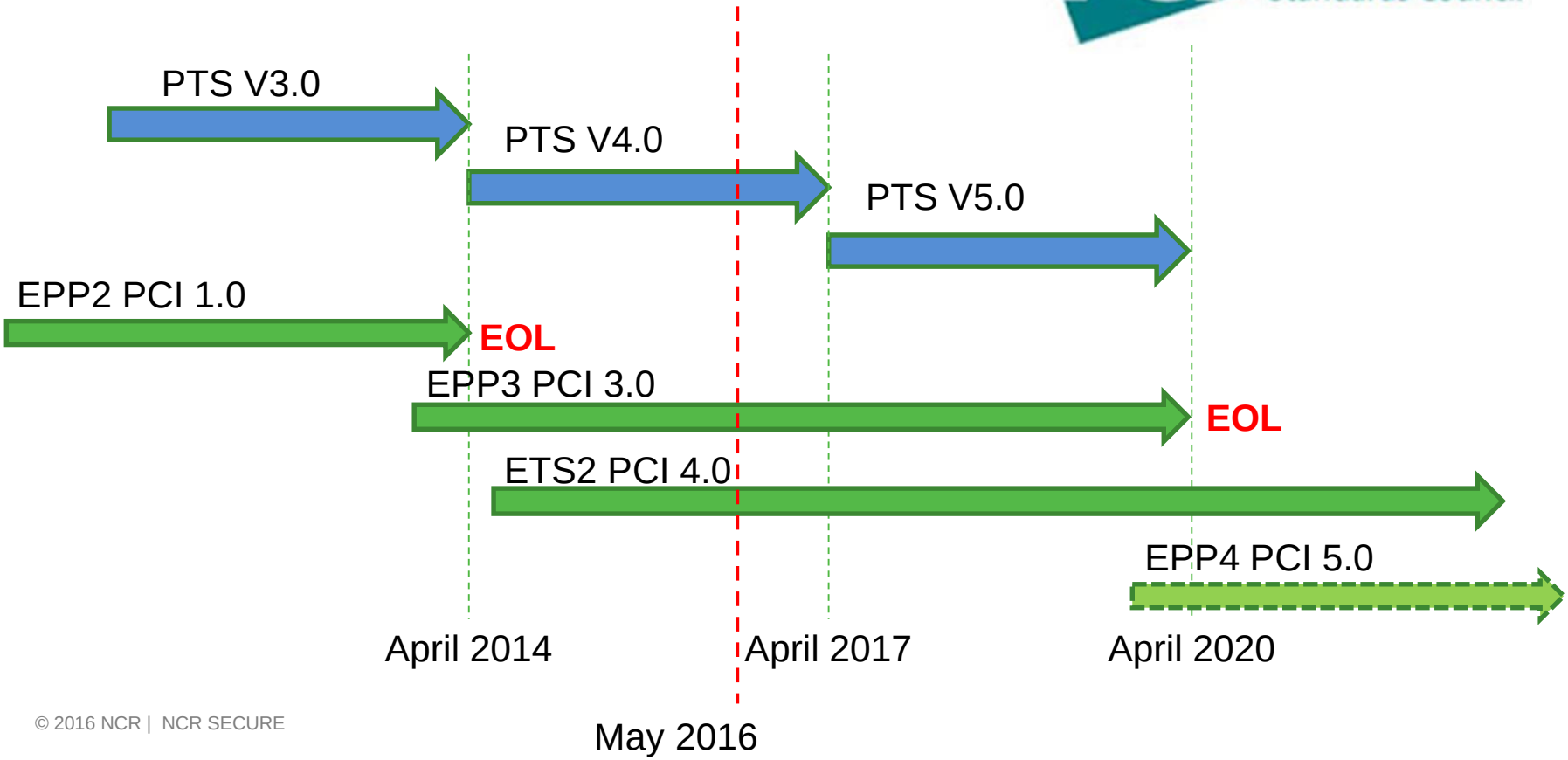
Q What mandates does PCI SSC have for PCI POI compliance?
A *PCI SSC only publishes the PCI POI Security Requirements and associated testing procedures. Compliance dates for PCI POI devices will be set by each of the individual payment brands.*

Q Do the PCI POI Security Requirements cover POS, EPP, and ATM devices?
A *At present, PCI POI Security Requirements address the following approval classes: EPP, Non-PED, PED, SCR, and UPT.*

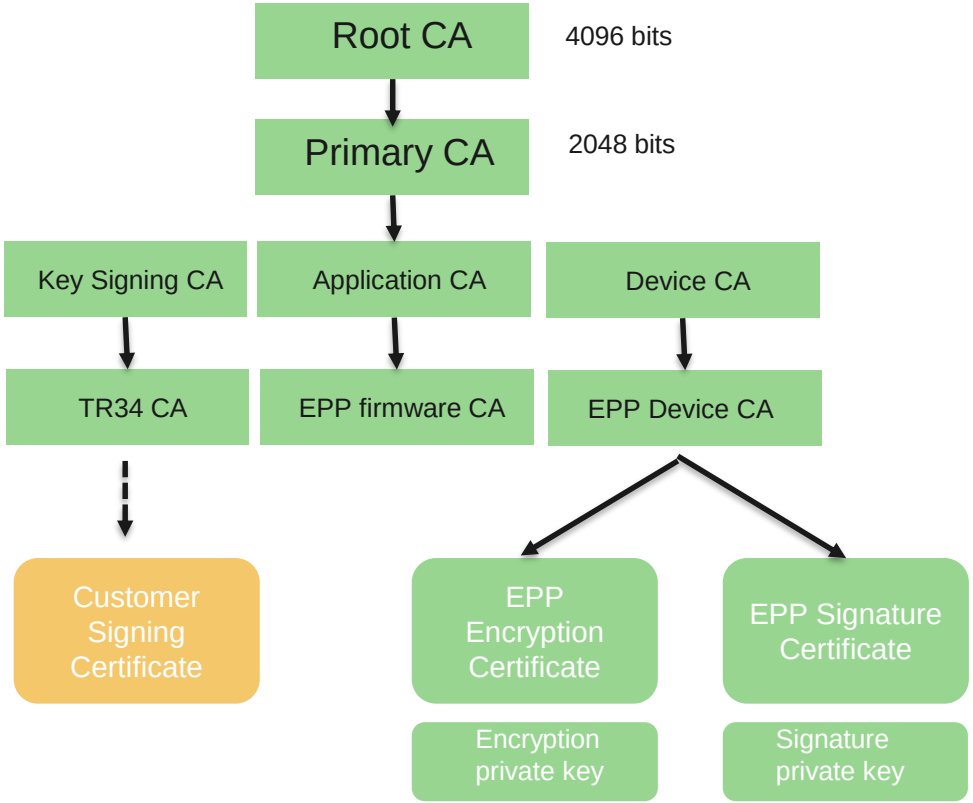
Q How do the PCI POI Security Requirements integrate with EMV terminal type approval?
A *The EMV functionality testing and approval process is totally separate and independent from the POI physical and logical security evaluation process.*

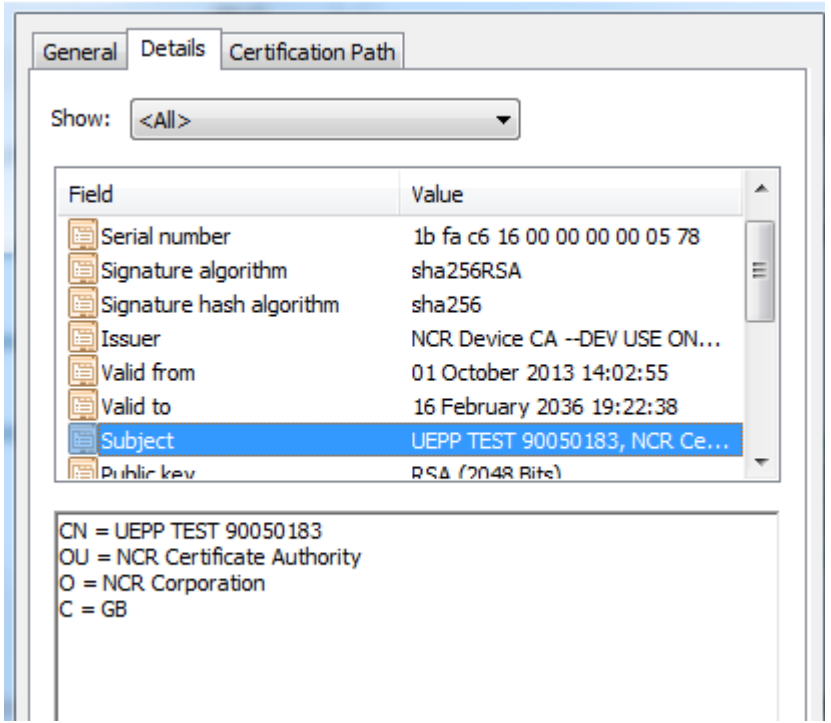
Source: PCI POI General FAQ May 2013

PCI PTS Roadmap



NCR EPP3


Root CA
4096 bits
Primary CA
2048 bits
Key Signing CA
Application CA
Device CA
TR34 CA
EPP firmware CA
EPP Device CA
Customer Signing Certificate
EPP Encryption Certificate
EPP Signature Certificate
Encryption private key
Signature private key


General
Details
Certification Path
Show:
<All>
Field
Value
Serial number
1b fa c6 16 00 00 00 00 05 78
Signature algorithm
sha256RSA
Signature hash algorithm
sha256
Issuer
NCR Device CA --DEV USE ON...
Valid from
01 October 2013 14:02:55
Valid to
16 February 2036 19:22:38
Subject
UEPP TEST 90050183, NCR Ce...
Public key
RSA (2048 Bits)
CN = UEPP TEST 90050183
OU = NCR Certificate Authority
O = NCR Corporation
C = GB

PCI PTS 3.0 AND BEYOND

WHAT ARE THE CHANGES THAT IMPACT ATM OPERATION?

- SHA-1 HASHING ALGORITHM MUST DISCONTINUED
- SUPPORT FOR KEY WRAPPING
- KEY DELETION COMMANDS REQUIRE AUTHENTICATION
- PIN ENCRYPTION MUST OCCUR IMMEDIATELY AFTER PIN ENTRY

These functions are already present in the EPP3

PCI PTS 4.0 & PCI PIN 2.0

INTRODUCES INDIVIDUAL MANDATE TIMEFRAMES

SHA-1 HASHING ALGORITHM MUST NOT BE USED – DEC 2016

SUPPORT FOR KEY WRAPPING – JAN 2018

KEY DELETION COMMANDS REQUIRE AUTHENTICATION – JAN 2017

PIN ENCRYPTION ONE MINUTE AFTER PIN ENTRY – APRIL 2016

PCI PIN

PCI PTS

PCI PTS 4.0 & PCI PIN 2.0

INTRODUCES INDIVIDUAL MANDATE TIMEFRAMES

SHA-1 HASHING ALGORITHM MUST NOT BE USED – DEC 2016

SUPPORT FOR KEY WRAPPING – JAN 2018

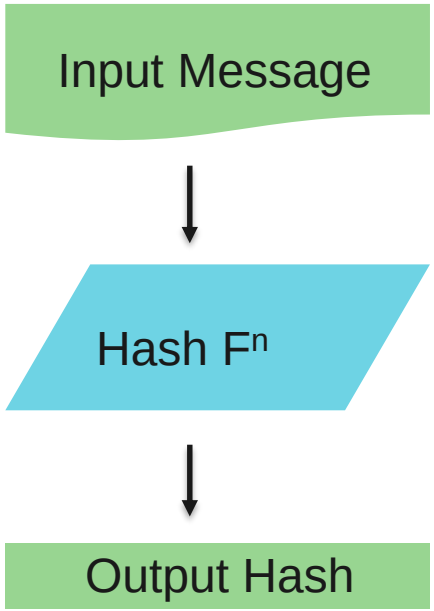
KEY DELETION COMMANDS REQUIRE AUTHENTICATION – JAN 2017

PIN ENCRYPTION ONE MINUTE AFTER PIN ENTRY – APRIL 2016

PCI PIN

PCI PTS

Hashing Algorithm



(Variable length)

(Fixed length)

Cryptographic One Way Function

- A **hash function** is any **function** that can be used to map data of arbitrary size to data of fixed size.
- Hash functions must be **one way**. i.e. it must not be possible to recover the input message from the hash
- A hash function is a fundamental building block in creating a **digital signature**.
- Digital signatures are created by encrypting a message hash with a private key.
- Digital signatures are a fundamental building block in ATM Remote Key systems.

PCI PIN 2.0 & SHA-1

Requirement 10: *All key-encryption keys used to transmit or convey other cryptographic keys must be (at least) as strong as any key transmitted or conveyed.*

10-1 All key-encryption keys used to encrypt for transmittal or conveyance of other cryptographic keys must be (at least) as strong as the key being sent, as delineated in Annex C, except as noted below for RSA keys used for key transport and for TDEA keys.

- DEA keys used for encrypting keys must be at least double-length keys (have bit strength of 80 bits) and use the TDEA in an encrypt, decrypt, encrypt mode of operation for key-encipherment.
- A double- or triple-length DEA key must not be encrypted with a DEA key of lesser strength.
- TDEA keys shall not be used to protect AES keys.
- TDEA keys shall not be used to encrypt keys greater in strength than 112 bits.
- RSA keys used to transmit or convey other keys must have bit strength of at least 80 bits.
- RSA keys encrypting keys greater in strength than 80 bits shall have bit strength at least 112 bits.

Note: *Entities that are in the process of migrating from older devices to PCI devices approved against version 3 or higher of the PCI POI Security Requirements—and thus have a mixed portfolio of devices—may use RSA key sizes less than 2048 and use SHA-1 to help facilitate the migration. However, in all cases, version 3 or higher devices must implement RSA using key sizes of 2048 or higher and SHA-2 within 24 months of the publication of these requirements when used for key distribution using asymmetric techniques in accordance with Annex A.*

PCI PTS 4.0 & PCI PIN 2.0

INTRODUCES INDIVIDUAL MANDATE TIMEFRAMES

SHA-1 HASHING ALGORITHM MUST NOT BE USED – DEC 2016

SUPPORT FOR KEY WRAPPING – JAN 2018

PCI PIN

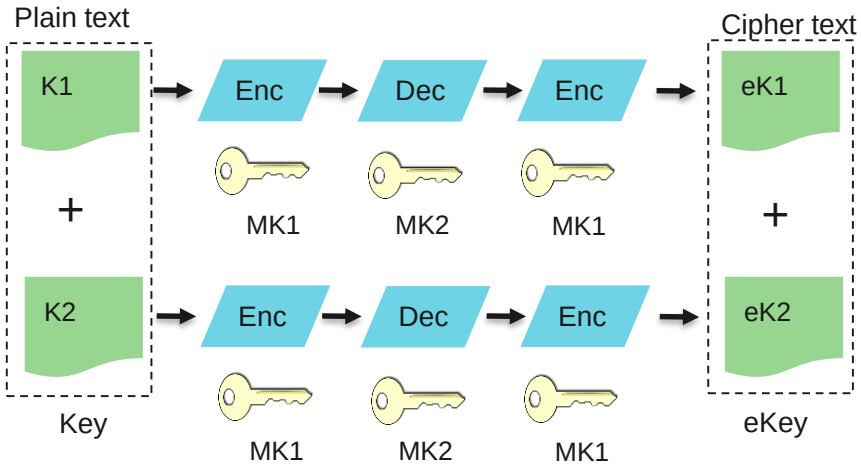
KEY DELETION COMMANDS REQUIRE AUTHENTICATION – JAN 2017

PIN ENCRYPTION ONE MINUTE AFTER PIN ENTRY – APRIL 2016

PCI PTS

Key Wrapping

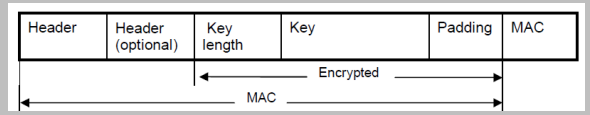
TDEA Key Encipherment :
Double length keys



No attribute information or binding

Key Blocks

- A key block is a structure for an enciphered key that contains;
  - Attribute Information
  - Confidential Data
  - A Binding Method
- NCR will use the ANSI TR31 key block format.



PCI PIN 2.0 & TR31

Requirement 18: *Procedures must exist to prevent or detect the unauthorized substitution (unauthorized key replacement and key misuse) of one key for another or the operation of any cryptographic device without legitimate keys.*

18-1 Synchronization errors must be monitored to help reduce the risk of an adversary's substituting a key known only to them. Procedures must exist and be followed for investigating repeated synchronization errors for online processes such as online key exchanges or transmission or processing of PIN-based transactions.

Note: *Multiple synchronization errors in PIN translation may be caused by the unauthorized replacement or substitution of one stored key for another, or the replacement or substitution of any portion of a TDEA key, whether encrypted or unencrypted.*

18-2 To prevent or detect usage of a compromised key, key-component packaging, or containers that show signs of tampering must result in the discarding and invalidation of the component and the associated key at all locations where they exist.

18-3 Effective 1 January 2018, encrypted symmetric keys must be managed in structures called key blocks. The key usage must be cryptographically bound to the key using accepted methods.

Acceptable methods of implementing the integrity requirements include, but are not limited to:

- A MAC computed over the concatenation of the clear-text attributes and the enciphered portion of the key block, which includes the key itself,
- A digital signature computed over that same data,
- An integrity check that is an implicit part of the key-encryption process such as that which is used in the AES key-wrap process specified in ANSI X9.102.

PCI PTS 4.0 & PCI PIN 2.0

INTRODUCES INDIVIDUAL MANDATE TIMEFRAMES

SHA-1 HASHING ALGORITHM MUST NOT BE USED – DEC 2016

SUPPORT FOR KEY WRAPPING – JAN 2018

PCI PIN

KEY DELETION COMMANDS REQUIRE AUTHENTICATION – JAN 2017

PIN ENCRYPTION ONE MINUTE AFTER PIN ENTRY – APRIL 2016

PCI PTS

Key Delete / PIN Encrypt Timing

Authenticated Key Deletion

- Key Deletion is now defined as a sensitive function.
- Sensitive functions require authentication, e.g. dual control password entry, digital signature on the command or a MAC.
- Signed Key Deletion is an inherent function in TR34
- An alternative MAC based delete function will be available for any customer not using RKM.
- This requirement has implications for ATM or EPP decommissioning, procedures must be modified to ensure authenticated key deletion occurs

PIN Encrypt Timing

- ATM PIN encryption is a 2 step process.
  - Get PIN
  - Encrypt PIN
- This is a vestigial attribute of ATMs, from when original ATM designs had separate keyboards and encryptor modules.
- PCI rules did not originally specify a time limit between the commands, but now a 5 minute limit is in force.
- This limit will be reduced to 1 minute.
- ATM software application design must take this into account

PCI PTS 4.0 & KEY DELETE

POI Requirement B7

Q 7 **June (update) 2015: Devices may have functions for zeroizing secret and private keys in the device. This functionality is regarded as a sensitive service that requires authentication. In some cases there is an upstream effect where software changes must occur on interfaces points, such as ATM platforms, applications, switches and hosts that interface with EPPs. Is there any dispensation from this requirement?**

A *All devices implementing this functionality must meet the requirement. However, the device may do so by implementing a new authenticated deletion command to the EPP command set, in addition to the existing commands. This must be coded as an either/or option such that both methods would not be available at the same time. Once the authenticated option is chosen, this would permanently lock out the non-authenticated commands.*

In all cases a time bound validity period must exist to force the upstream software changes to be implemented within a set timeframe. PCI will allow three years from the publication of this FAQ for those applications to be modified. This abeyance only applies to encrypting PIN Pads designed and used for ATMs.

Effective 1 January 2017, all newly approved EPPS must only support authenticated deletion capability. EPPs approved prior to January 2017 with non-authenticated deletion capability are not required to be upgraded to authenticated deletion capability to maintain PCI compliance.

PCI PTS 4.0 & PIN ENCRYPT TIMING

POI Requirement B6

Q 5 **April 2013: B6 requires that online PINs must be encrypted immediately after PIN entry is complete. It is further stipulated that plaintext PINs must not exist for more than one minute from the completion of the cardholder's PIN entry. In all cases, erasure of the plaintext PIN must occur before the tamper-detection mechanisms can be disabled using attack methods described in A1. Are there any circumstances where a plaintext PIN can exist for more than one minute?**

A *Some ATMs have implemented intelligent deposit technologies to enhance the customer experience. As a result, some deposit transactions take longer than one minute and result in the PIN being cleared from the buffer after one minute and the cardholder then needing to start the transaction over, and in some cases, unable to complete the transaction at all. In those cases, the ATM applications require modification to prompt for PIN re-entry if a transaction goes over the time out period, rather than requiring the entire transaction to be re-started.*

In order to allow a sufficient time for the modification of those applications, PCI will allow three years from the publication of this FAQ for those applications to be modified. During this three-year abeyance, the unenciphered PIN may remain in the buffer for up to five minutes. However, the PIN must remain protected from compromise using attack methods described in A1, and the test laboratory shall take into consideration the lack of timely encipherment when designing attacks.

This abeyance only applies to encrypting PIN Pads designed and used for ATMs.

NCR STRATEGY FOR MIGRATION

PCI changes afford the opportunity to migrate to industry standard key management techniques, discontinue use of proprietary methods, and increase security.

1. SHA-1: NCR signature based RKM will be replaced by ANSI TR34 RKM
2. Key wrapping will be supported using ANSI TR31 key block
3. Authenticated Key Deletion is implicit in TR34
4. PIN encrypt enforced within 1 minute of PIN entry.

Requirements 1-3 already OPTIONAL functions in EPP3

NCR STRATEGY FOR MIGRATION

Why has NCR taken this approach?

1. Current vendor RKM solutions are proprietary; this means that different host systems are required on Multivendor estates, they must be maintained separately, audited separately. Moving to an open standards based approach removes this overhead and inefficiency.
2. Using open standards based technology will improve security. X9 publications are produced by industry experts and peer reviewed, providing greater assurance than could be provided by a single vendor proprietary design.
3. Using open standards based technology simplifies the audit process. It takes expertise and experience to be able to verify a proprietary Remote Key scheme against the requirements of PCI PIN or ANSI TR39. TR34 is known to be compliant with the requirements of X9.24-2

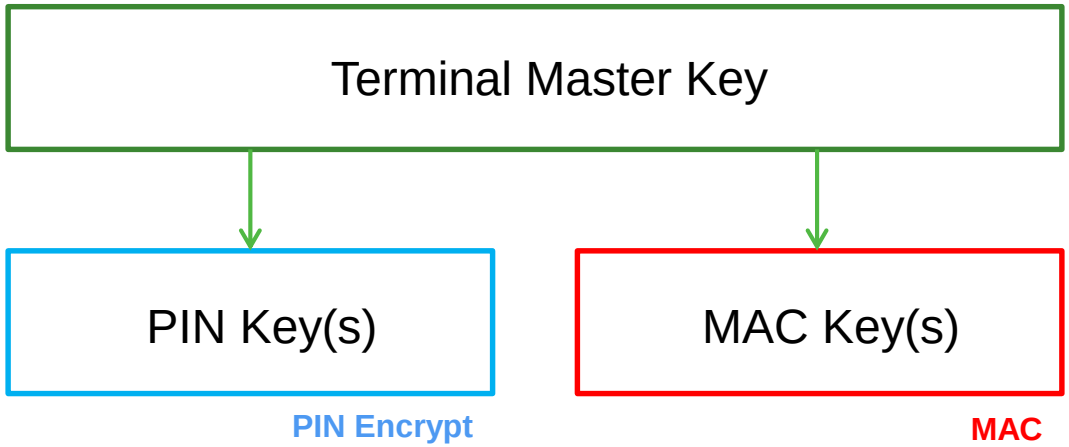
LEGACY KEY LOADING AND STORAGE

KEY LOADING

KEY USAGE

MANUAL
RKM
E-RKM

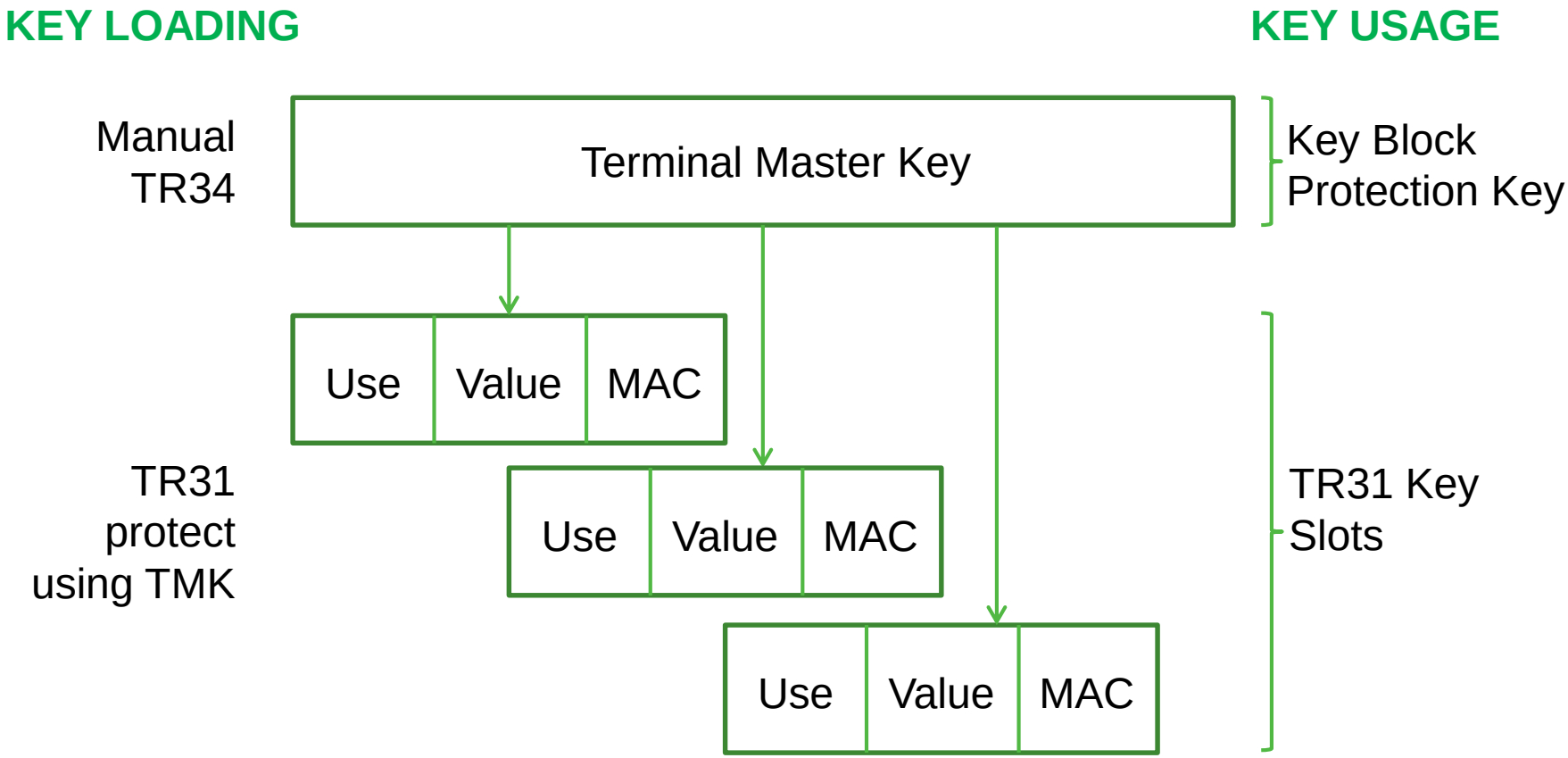
T-ECB
encrypt
with TMK



Parent Key
Space

Child Key
Spaces

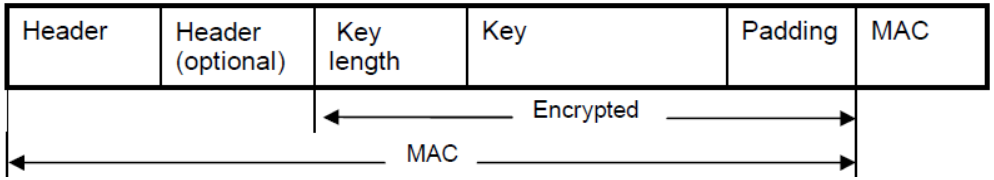
COMPLIANT KEY LOADING AND STORAGE



TR31

TR31

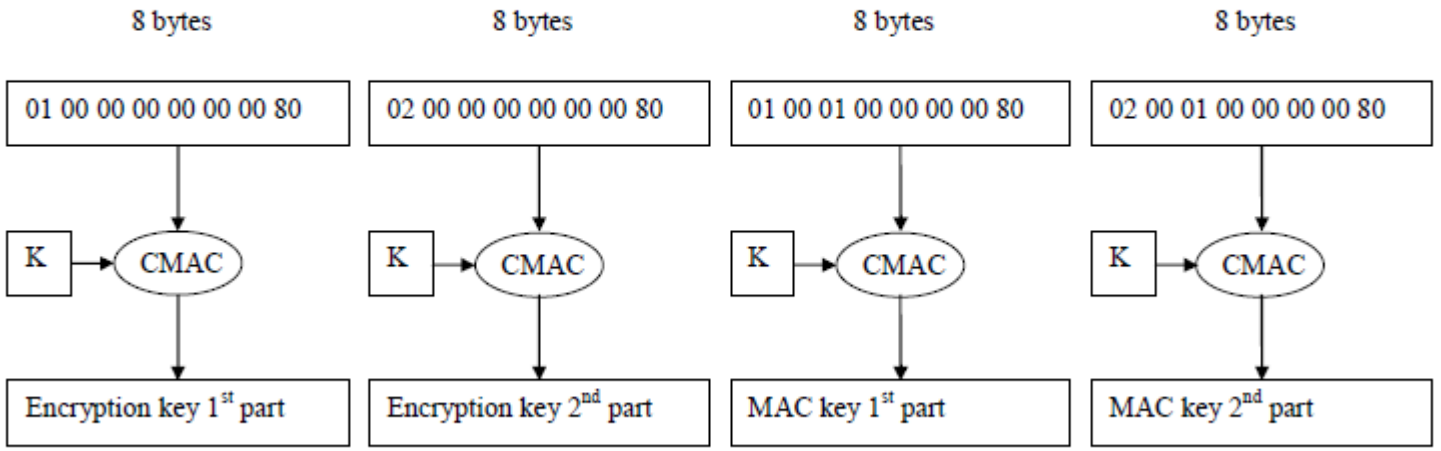
- **Used to transport the working keys (protected with the Key Block Protection Key)**
- **Compliant with the requirements of ANS X9.24-1**
- **Sometimes known as the ‘ANSI key block’**
- **Supports multiple encryption algorithms e.g. TDEA, AES etc**



TR31 – KEY DERIVATION

Encryption and MAC Keys are automatically derived from the KBPK by the EPP

Figure 1 — Deriving a 2-Key TDEA MAC and Encryption Key



K = KBPK

EPP3 TR31 SUPPORTED USAGE AND MODES

Key Usage

Value	Hex	Definition
‘D0’	0x44, 0x30	Data Encryption
‘I0’	0x49, 0x30	Initialization Vector(IV)
‘K0’	0x4B, 0x30	Key Encryption, or wrapping
‘M0’	0x4D, 0x30	0x30 ISO 16609 MAC algorithm 1 (using TDEA)
‘M1’	0x4D, 0x31	ISO 9797-1 MAC Algorithm 1
‘M3’	0x4D, 0x33	ISO 9797-1 MAC Algorithm 3
‘P0’	0x50, 0x30	PIN Encryption
All Numeric Values		Reserved for Proprietary use

Mode of Use

Value	Hex	Definition
‘B’	0x42	Both Encrypt and Decrypt
‘C’	0x43	MAC calculate (Generate or Verify)
‘D’	0x44	Decrypt Only
‘E’	0x45	Encrypt Only
‘G’	0x47	MAC Generate only
‘N’ (See note 1)	*0x4E*	*No special restrictions or note applicable*
‘S’	0x53	Signature Only
‘V’	0x56	MAC Verify Only

Note 1 – This mode is not supported.

TR34 REMOTE KEY MANAGEMENT

- Used to transport the initial Master Key (Key Block Protection Key)
- Based on NCR E-RKM, but uses X.509 certificates
- Certificates use SHA-256
- Uses the concept of ‘key binding’ to lock the initial customer certificate to the EPP
- Compliant with the requirements of ASC X9.24-2
- Compliant with the requirements of PCI PIN Annex A

NCR Remote Key Protocol Comparison

Basic RKM

- Uses NCR proprietary format certificates
- One-time certificate request required from NCR
- Certificates use SHA-1
- Does not comply with PCI PIN Annex A

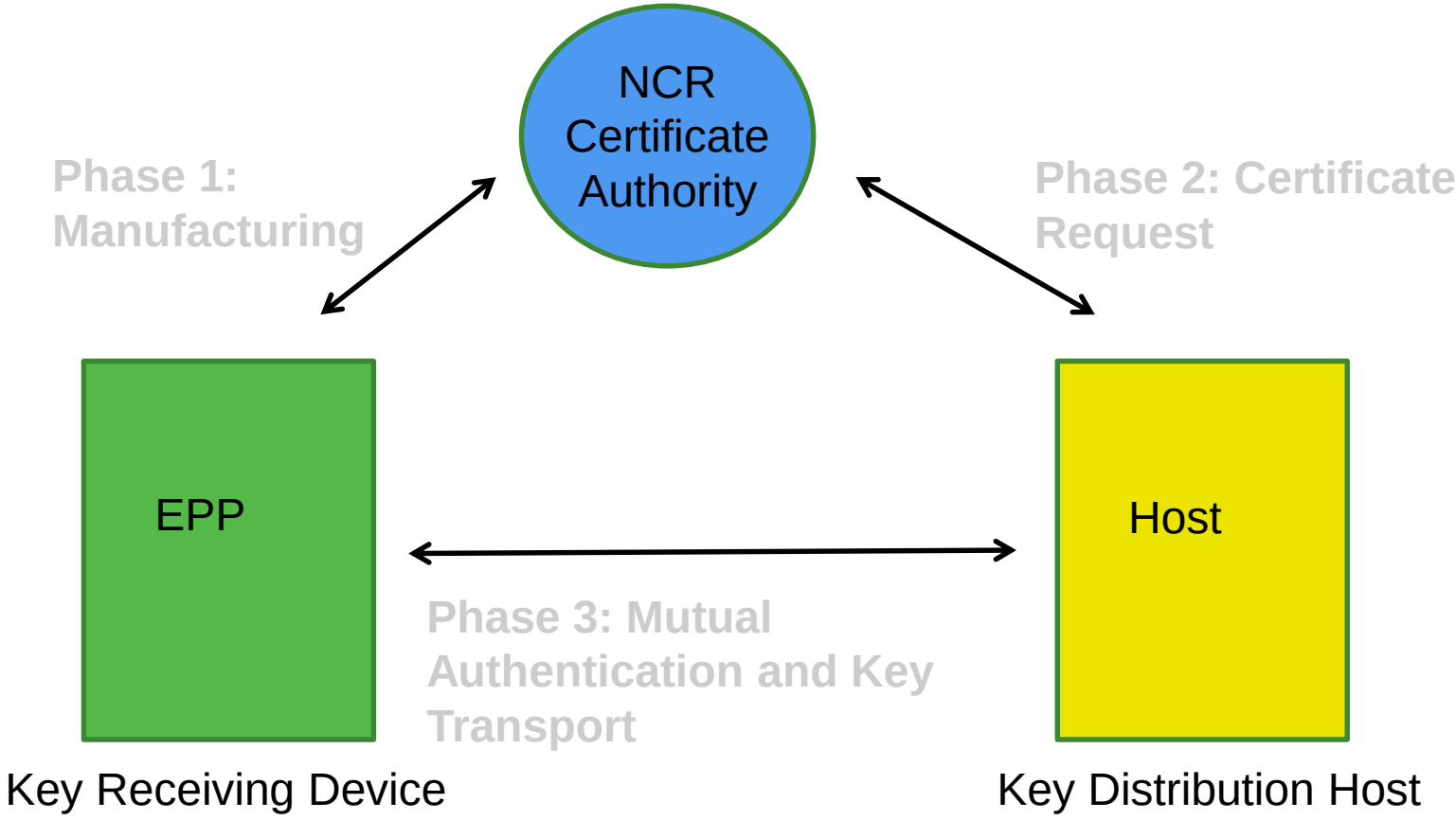
Enhanced RKM

- Uses NCR proprietary format certificates
- One-time certificate request required from NCR
- Certificates use SHA-1
- Public key is bound to EPP
- Anti-replay in protocol
- Will not comply with PCI PIN Annex A from Dec 2016

TR34 RKM

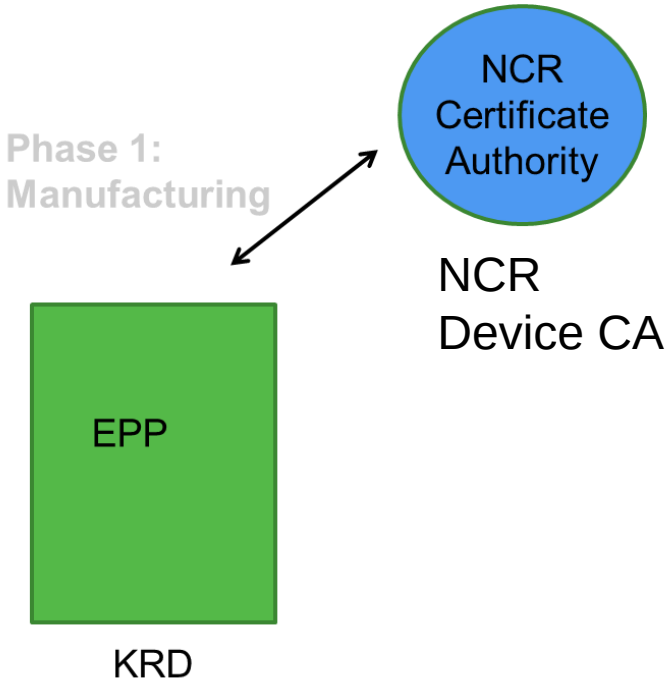
- X.509 certificate format
- One-time TR34 certificate request required from NCR
- Certificates use SHA-2
- Certificate is bound to EPP
- Anti-replay in protocol
- Full CA support
- Complies with PCI PIN Annex A

TR34 REMOTE KEY MANAGEMENT

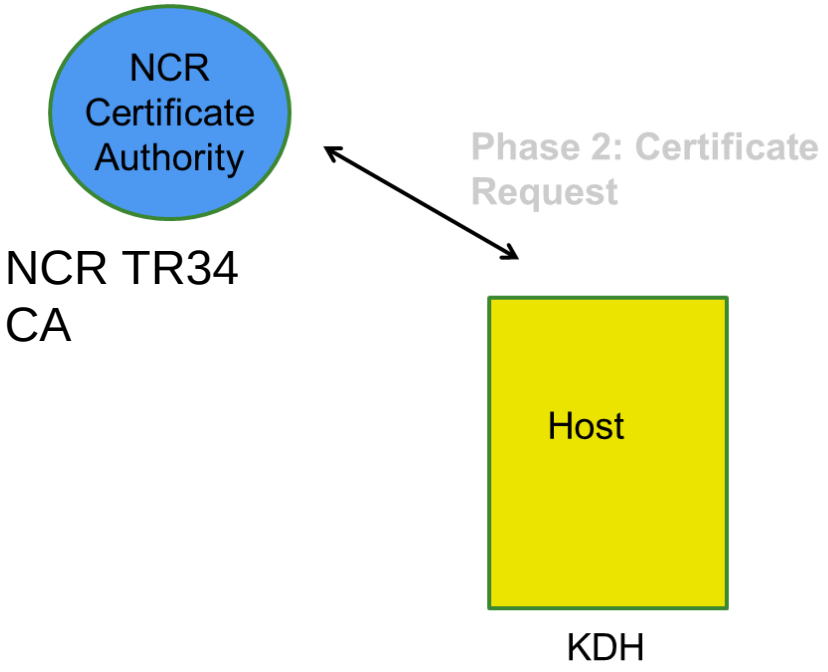


TR34: 1 - MANUFACTURING

- NCR Manufactures PIN Entry Devices at our secure facility in Budapest , Hungary (H.5 rated, ISO 13491-2)
- EPPs self generate 2 RSA key pairs, one for encryption, one for signature.
- EPP generates a Certificate Request.
- CR is sent through Secure link to NCR CA in Dundee, Scotland
- Certificates returned to EPP via same secure channel.
- NCR systems audited annually against PCI PIN and TR39



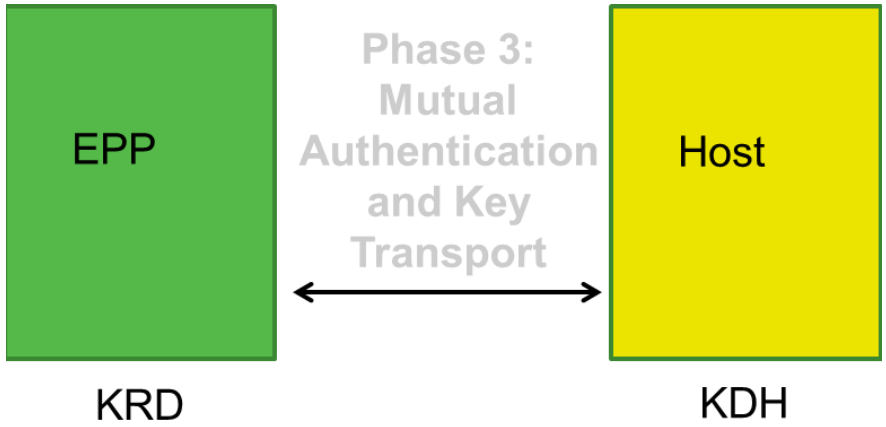
TR34: 2 – CERTIFICATE REQUEST



- New TR34 Certificate Requests are required for all Hosts.
- Legacy certificates are not compatible with TR34.
- There will likely be a charge for a TR34 certificate request.
- NCR will return 2 CA certs, and a fresh CRL
  - NCR DEVICE CA cert, NCR TR34 CA cert

TR34: 3 – BINDING & KEY LOADING

- KRD and KDH exchange credentials.
- KRD credential includes the KRD ID (serial number)
- KDH credential includes a CRL
- Upon successful load of KDH credential, KDH is now bound to the KRD.
- Key transport is preceded by KRD sending a RND to the KDH
- KBPK protected with the KRD public key
- Key transport token includes a CRL



KDH BIND PHASE

Table 3— KDH Bind Phase

#	A (KRD)		B (KDH)
1.	Prepare KRD Credential Token (A1)	CT_{KRD} →	Validate KRD Credential Token (B1)
2.			Store: $Cred_{KRD}$
3.	Validate KDH Credential Token (A2)	CT_{KDH} ←	Prepare KDH Credential Token (B2)
4.	Store: $Cred_{KDH}$		

KDH BIND PHASE

KRD will validate:

- CRL freshness
- CRL signature
- KDH cert signature
- KDH cert validity
- KDH is not in CRL
- KRD is not already bound

KBPK TRANSPORT

Table 4 — TDEA Symmetric Key Transport Phase

#	A (KRD)		B (KDH)
1.	Generate Random Number Token RT_{KRD} (A1)	RT_{KRD} →	Receive Random Number R_{KRD} (B1)
2.			Store: R_{KRD}
3.			Generate Transported TDEA Symmetric Key K_n (B2)
4.			Generate Ephemeral TDEA Symmetric Key K_E (B3)
5.			Encipher Key Block BE (B4)
6.			Encipher Ephemeral TDEA Symmetric Key (B5)
7.	Verify Key Token (A2)	KT_{KDH} ←	Construct Key Token KT_{KDH} (B6)
8.	Decipher Key Block Store: K_n		

KBPK TRANSPORT

KBPK Token Creation

- Receive RND from KRD
- Generate KBPK
- Generate K_E
- Encrypt Version, KBPK, KDH ID, Header with K_E to create Encrypted Block
- Encrypt K_E with E_{KRD} to create Encrypted Key
- Construct token RND, header, Encrypted Key, Encrypted Block
- Sign token with S_{KDH}
- Create message Token, Signature, CRL and send to KRD

KBPK Token Validation

KRD will validate:

- CRL freshness
- CRL signature
- KDH is not in CRL
- Token Signature
- Check RND match
- Decipher Key, Block
- Check ID of KDH matches KDH credential
- Validates encrypted header matches clear header

Then stores KBPK

KDH BIND OPTIONS

EPP will support:

1. **Bind: Initial load of KDH cert**
2. **UnBind: Authorised deletion of bound KDH cert.**
3. **ReBind: Allows transfer for ownership from KDH_A to KDH_B, without an Unbind command. Re-Bind is signed by KDH_A**

TR34 KRD Unbind From KDH

KRD will only unbind if presented with authorisation

- A command to unbind from a KDH must be signed by the private key of the KDH which is being unbound.
- The act of unbinding will delete all symmetric keys in the EPP – fulfilling the requirement for authenticated key delete
- A Rebind option is also available. This allows a KDH to be replaced without going through an unbind.

References

- PCI POI PTS Security Requirements V4.1c
- PCI PTS POI Technical FAQ V4 April 2016
- PCI PIN V2.0
- PCI PIN Technical FAQ V2 April 2016

www.pcissc.com

Standard	Subject / Comments
ISO 9564-1 / X9.8-1	PIN Management and Security
ISO 9564-2 / X9.8-2	Approved Algorithms
ISO 13491 / X9.97	Secure Cryptographic Devices
ISO 11568	Key management
X9.24-1	Symmetric Key management using Symmetric Techniques
X9.24-2	Symmetric Key management using Asymmetric Techniques
ISO 16609	Requirements for message authentication using symmetric techniques
X9 TR31	Interoperable method of key bundling that meets the requirements of X9.24-1
X9 TR34	Interoperable method of key distribution that meets the requirements of X9.24-2

SUMMARY & TAKE AWAYS

- **PCI PIN and PTS requirements will drive changes in the way that ATM PIN Entry Devices operate.**
  1. Remote Key
  2. Key Wrapping
  3. Key Deletion
  4. PIN Encrypt Timing
- **Check your host provider for compliance readiness**
- **Check your ATM application version for compliance readiness**
- **TR34 RKM will require a new certificate request to NCR**

PCI Security Standards Council™

BOARD MEMBER
Accredited Standards Committee X9, Inc.
X9™
Financial Industry Standards

Questions received during the webinar

Q1: At the ATM level, the EPP keyboard is set to INTL-20 or INTL-61. Does INTL-61 meet the new requirements?
A1: EPP3 ships with INTL_61 which has support for TR34,TR31. I would recommend an upgrade to INTL_64 prior to any TR34/31 development work because INTL_64 includes important bug fixes.

Q2: Hi, During a recent LINK Attestation Audit one problem we faced was trying to ascertain the relevant firmware version on our (PCI Compliant) EPPs. The PCI Standards website seems to list three certified firmware versions for the EPP. Is there a way to discover the version we are running without a visit to each location?
A2: Yes. EPP firmware versions, and hardware version, can be queried remotely. NCR Professional Services can assist with the implementation of this capability.

Q3: Some of our ATM machines are PTS 1.0 and cannot conform to the SHA2 standard. Will our organization need to discontinue these devices after December 2016?
A3: No. The requirement to implement SHA-2 only applies to PCI 3.0, and above, devices. However, the Key Wrapping requirement appears to apply to all devices.

Questions received during the webinar

Q4: Can you address the Personas EPP, I believe it would be EPP 1, and where it fits in PCI 4
A4: The Personas EPP is approved to meet the requirements of PCI PTS 1.0. This version is now expired, and consequently, no more Personas EPPs can be used for new deployments. NCR has no plans to develop a PCI PTS V4.0 EPP for use in Personas ATMs. Of the new PCI PIN requirements mentioned in the webinar, the SHA-2 requirement does not apply to PCI PTS 1.0 devices, but the Key Wrapping requirement does.

Q5: Could you tell me what means POI?
A5: PCI PTS POI = Payment Card Industry PIN Transaction Security Point OF Interaction

Q6: Do we have a new version of the PCI requirements
A6: All versions of PCI requirements are available on the PCI website. The specific versions referenced in this webinar are listed on the Reference slide. The next version of PCI PTS will come into effect in April 2017


NCR