



Visa Europe

Data Field Encryption:  
Device and Key  
Management Guidance

Version 1.0

March 2010





## DISCLAIMER

This guidance is given for information purposes only and does not constitute specific advice. In so far as is legally permissible, Visa Europe does not accept any responsibility or liability in respect of, and recipients should not rely on, its contents. Whilst every reasonable effort has been made to ensure the accuracy of information provided by Visa Europe in this document, Visa Europe makes no representation and gives no warranty as to the accuracy of its contents or their suitability for use in any particular situation.

## Table of Contents

Overview .....	4
Technical Reference .....	5
<b>SECTION 1: CONTROL OBJECTIVES .....</b>	<b>7</b>
Point of Sale Encryption Device .....	7
<b>Key Management.....</b>	<b>7</b>
Objective 1: Encryption Methodologies .....	7
Objective 2: Key Generation .....	7
Objective 3: Key Distribution.....	7
Objective 4: Key Loading.....	8
Objective 5: Key Usage.....	8
Objective 6: Key Administration.....	9
Objective 7: Device Management.....	10
<b>SECTION 2: ADDITIONAL GUIDANCE .....</b>	<b>11</b>
Point of Sale Encryption Device .....	11
<b>Key Management.....</b>	<b>15</b>
Objective 1: Encryption Methodologies .....	15
Objective 2: Key Generation .....	16
Objective 3: Key Distribution.....	17
Objective 4: Key Loading.....	20
Objective 5: Key Usage.....	23
Objective 6: Key Administration.....	25
Objective 7: Device Management.....	29
<b>ANNEX A .....</b>	<b>33</b>
Symmetric Key Distribution using Asymmetric Techniques.....	33
Point of Sale Encryption Device .....	33
<b>Key Management.....</b>	<b>33</b>
Objective 2: Key Generation .....	33
Objective 3: Key Distribution.....	34
Objective 4: Key Loading.....	35
Objective 5: Key Usage.....	36
Objective 6: Key Administration.....	37
Objective 7: Device Management.....	42
<b>ANNEX B .....</b>	<b>46</b>
Key Injection Facilities.....	46
Point of Sale Encryption Device .....	46
<b>Key Management.....</b>	<b>47</b>
Objective 2: Key Generation .....	47
Objective 3: Key Distribution.....	48
Objective 4: Key Loading.....	50
Objective 5: Key Usage.....	53

Objective 6: Key Administration.....	55
Objective 7: Device Management.....	56
<b>Glossary.....</b>	<b>58</b>

## Overview

Data field encryption, commonly referred to as “end-to-end” encryption, “point-to-point” encryption or “account data” encryption, defines a process to protect transaction data both in storage and in transit within an enterprise, limiting the clear-text availability of cardholder data and sensitive authentication data. If properly implemented, data field encryption can increase transaction security and render data useless to fraudsters in the event of a compromise.

To provide guidance on the secure implementation of data field encryption solutions, and following on from Visa Europe’s best practices for Data Field Encryption<sup>1</sup>, Visa Europe has developed this enhanced guidance document. As part of this guidance, it is important to note that Visa Europe is not mandating the use of data field encryption solutions. This guidance simply describes the minimum security requirements that would be required to demonstrate a robust key management implementation of any data field encryption solution. As data field encryption solutions evolve Visa Europe may at its discretion issue periodic updates to this document.

The document is structured as follows:

- Section 1 details the high-level control objectives that a data field encryption solution must satisfy in order to be considered secure.
- Section 2 expands upon these high-level objectives and describes more specific security requirements for the device performing the encryption operation within the merchant environment as well as for the entity providing the back-end key management and decryption functions.
- Annex A of this document provides supplementary requirements for entities involved in the implementation of symmetric key distribution using asymmetric keys (remote key distribution) including guidance for those entities involved in the operation of Certification Authorities.
- Annex B provides supplementary requirements for entities acting as key injection facilities.

Entities involved in remote key distribution and/or providing key injection facilities are subject both to the requirements stipulated in the main control objective and implementation guidance sections of this document as well as the relevant criteria stipulated in Annex A and/or Annex B.

For your convenience, a glossary of commonly used terms is included at the end of this document.

Please note that throughout this document, other implementation methods may be considered for each requirement, provided that the alternative method both meets the intent of the original requirement and yields *at least* an equivalent level of security.

Any questions and/or comments pertaining to the content of this document should be addressed to [datasecuritystandards@visa.com](mailto:datasecuritystandards@visa.com).

---

<sup>1</sup> [http://www.visaeurope.com/documents/ais/best\\_practices\\_for\\_data\\_field\\_encryption.pdf](http://www.visaeurope.com/documents/ais/best_practices_for_data_field_encryption.pdf)

## Technical Reference

From time to time, standards change to more completely reflect the state of both technology and the threat environment at a particular point in time. It is necessary to ensure that the correct technical reference is used when evaluating whether a process, technique, piece of equipment, or policy is compliant with a specific requirement. At the time of writing, the following standards are reflected in the composite security requirements present in this document:

- **ANSI X3.92:** Data Encryption Algorithm
- **ANSI X9.24 (Part 1):** Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques
- **ANSI X9.42:** Public Key Cryptography for the Financial Service Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography
- **ANSI X9.52:** Triple Data Encryption Algorithm: Modes of Operation
- **EMV:** Integrated Circuit Card Specification for Payment Systems, version 4.2 (June 2008)—Book 2: Security and Key Management
- **FIPS PUB 140–2:** Security Requirements for Cryptographic Modules.
- **ISO/IEC 10116:2006:** Information technology -- Security techniques -- Modes of operation for an n-bit block cipher
- **ISO 11568–1:** Banking - Key Management (Retail), Part 1: Principles
- **ISO 11568–2:** Banking - Key Management (Retail), Part 2: Symmetric ciphers, their key management and life cycle
- **ISO 11568–4:** Banking Key Management (Retail), Part 4: Key management techniques using public key cryptosystems
- **ISO 11770–2:** Information Technology—Security Techniques— Key Management, Part 2: Mechanisms Using Symmetric Key Management Techniques
- **ISO 11770–3:** Information Technology—Security Techniques—Key Management, Part 3: Mechanisms Using Asymmetric Techniques (RSA and Diffie-Hellman)
- **ISO 13491–1:** Banking—Secure Cryptographic Devices (Retail), Part 1: Concepts, Requirements, and Evaluation Methods
- **ISO 13491-2:** Banking—Secure Cryptographic Devices (Retail), Part 2: Compliance Checklists for Devices used in Financial Transactions.
- **ISO TR19038:** Guidelines on Triple DES Modes of Operation.
- **NIST Special Publication 800-22 Rev. 1:** A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications
- **NIST Special Publication 800-57 Part 1:** Recommendation for Key Management - Part 1: General.
- **NIST Special Publication 800-57 Part 2:** Best Practices for Key Management Organizations.
- **Payment Card Industry (PCI):** PIN Security Requirements.
- **Payment Card Industry (PCI):** Data Security Standard (PCI DSS).

- **Payment Card Industry (PCI):** Encrypting Data PAD (EPP) Security Requirements Manual.
- **Payment Card Industry (PCI):** Encrypting PIN PAD (EPP) Derived Test Requirements.
- **Payment Card Industry (PCI):** POS Data Entry Device Security Requirements Manual.
- **Payment Card Industry (PCI):** POS Data Entry Device Derived Test Requirements.

## Section 1: Control Objectives

### Point of Sale Encryption Device

1. Encryption of account data must be performed in equipment that is resilient to physical and logical compromise.
2. Limit cleartext availability of account data to the point of encryption and the point of decryption.

### Key Management

#### Objective 1: Encryption Methodologies

**Account Data must be processed using cryptographic methodologies that ensure account data is kept secure.**

1. Key management, cryptographic algorithms and cryptographic key lengths must be consistent with international and/or regional standards.

#### Objective 2: Key Generation

**Cryptographic keys used for data field encryption/decryption, and related key management keys, must be created using processes that ensure that it is not possible to predict any key or determine that certain keys are more probable than other keys.**

2. All keys and key components must be generated using an approved random or pseudo-random process.
3. Compromise of the key-generation process must not be possible without collusion between at least two trusted individuals.
4. Documented procedures must exist and must be demonstrably in use for all key generation processing.

#### Objective 3: Key Distribution

**Keys must be conveyed or transmitted in a secure manner.**

5. Cryptographic keys must be conveyed or transmitted securely
6. Any single unencrypted key component must at all times during its transmission, conveyance, or movement between any two organisational entities be: Under the continuous supervision of a person with authorised access to this component, OR locked in a security container (including tamper evident packaging) in such a way that it can be obtained only by a person with authorised access to it, OR in a physically secure TRSM.

7. All key encryption keys used to transmit or convey other cryptographic keys must be (at least) as strong as any key transmitted or conveyed.
8. Documented procedures must exist and must be demonstrably in use for all key transmission and conveyance processing.

#### **Objective 4: Key Loading**

**Key loading to cryptographic devices must be handled in a secure manner.**

9. Unencrypted secret keys must be entered into cryptographic devices using the principles of dual control and split knowledge.
10. The mechanisms used to load secret keys, such as terminals, external PIN pads, key guns, or similar devices and methods must be protected to prevent any type of monitoring that could result in the unauthorised disclosure of any component.
11. All hardware and passwords used for key loading must be managed under dual control.
12. The loading of keys or key components must incorporate a validation mechanism such that the authenticity of the keys is ensured and it can be ascertained that they have not been tampered with, substituted, or compromised.
13. Documented procedures must exist and be demonstrably in use (including audit trails) for all key-loading activities.

#### **Objective 5: Key Usage**

**Keys must be used in a manner that prevents or detects their unauthorised usage.**

14. Unique secret cryptographic keys must be in use for each identifiable link between encryption and decryption points.
15. Procedures must exist to prevent or detect the unauthorised substitution (unauthorised key replacement and key misuse) of one key for another or the operation of any cryptographic device without legitimate keys.
16. Cryptographic keys must only be used for their sole intended purpose and must never be shared between production and test systems.
17. All secret keys present and used for any function must be unique (except by chance) to that device.

## Objective 6: Key Administration

### Keys must be administered in a secure manner.

18. Secret keys used for encrypting data field encryption keys, or for data field encryption, must never exist outside of a cryptographic device, except when encrypted or securely stored and managed using the principles of dual control and split knowledge.
19. Procedures must exist and must be demonstrably in use to replace any known or suspected compromised key and its subsidiary keys (those keys encrypted with the compromised key) to a value not feasibly related to the original key.
20. Key variants must only be used in devices that possess the original key. Key variants must not be used at different levels of the key hierarchy e.g. a variant of a key encryption key used for key exchange cannot be used as a working key or as a master file key for local storage.
21. Secret keys and key components that are no longer used or have been replaced must be securely destroyed.
22. Access to secret keys and key material must be limited to properly designated key custodians, and their backups, on a need-to-know basis
23. Logs must be kept for any time that keys, key components, or related materials are removed from storage or loaded to a cryptographic device.
24. Backup copies of secret keys must exist only for the purpose of reinstating keys that are accidentally destroyed or are otherwise inaccessible. The backups must exist only in one of the allowed storage forms for that key.
25. Documented procedures must exist and must be demonstrably in use for all key administration operations.

## **Objective 7: Device Management**

**Equipment used to process account data and keys must be managed in a secure manner.**

26. Cryptographic devices must be placed into service only if there is assurance that the equipment has not been substituted or subjected to unauthorised modifications or tampering prior to the loading of cryptographic keys.
27. Procedures must exist that ensure the destruction of all cryptographic keys and all account data within any cryptographic device removed from service.
28. Any cryptographic device capable of encrypting a key and producing cryptograms of that key must be protected against unauthorised use to encrypt known keys or known key components. This protection must take the form of either or both of the following: a) dual access controls are required to enable the key encryption function, b) physical protection of the equipment (e.g. locked access to it) under dual control.
29. Documented procedures must exist and must be demonstrably in use to ensure the security and integrity of cryptographic devices placed into service, initialised, deployed, used, and decommissioned.

## Section 2: Additional Guidance

### Point of Sale Encryption Device

1 **Encryption of account data must be performed in equipment that protects cryptographic keys against physical and logical compromise**

#### Physical Characteristics

The transaction originating cryptographic device used must have a negligible probability of being successfully penetrated to disclose all, or part of, any secret key, or account data. This can be realised by performing encryption operations using devices that conform to the requirements for a Tamper-Resistant Security Module (TRSM) as defined in ISO 9564:1, ISO 13491 (all parts) / ANSI X9.97 (all parts) or equivalent. Other implementation methods may be considered; provided it can be proven that they provide at least the same level of security.

Penetration of the device, irrespective of the type of solution deployed, shall cause immediate erasure of all account data, secret keys as well as all useful residues of secret keys contained within it.

If the device permits access to internal areas (e.g., for service or maintenance), it is not possible utilising this access to insert a bug that would disclose any secret key or account data. Immediate access to any secret key, or account data is either prevented by the design of the internal areas (e.g., by enclosing components with access to secret keys or account data into tamper-resistant/responsive enclosures), and/or it has a mechanism so that access to internal areas causes the immediate erasure of all secret keys and account data.

It must not be possible to compromise the security of the device, or cause the device to output clear-text account data by altering environmental or operational conditions.

The device must only be used for its specified purpose. It must not be possible for the device to be operated in an unauthorised manner or beyond the scope of the operating procedures specified for the equipment.

## Logical Characteristics

The device shall perform a self-test, which includes integrity and authenticity tests on code within the device (that provides security protections needed to comply with device security requirements) upon start-up and at least once per day for signs of tampering, and whether the device is in a compromised state. In the event of a failure, the device and its functionality fail in a secure manner.

The software and firmware provided with the device, and any changes made to it thereafter, must be inspected and reviewed using a documented and auditable process, and certified as being free from hidden and unauthorised or undocumented functions. The software and/or firmware elements of the cryptographic device must be developed as part of a secure software development lifecycle and hardened in-line with international and/or regional standards (e.g. PA-DSS).

If the device allows software and/or configuration updates, the device shall cryptographically authenticate all updates and if the authenticity cannot be confirmed, the update shall be rejected and deleted.

The device's functionality shall not be influenced by logical anomalies such as (but not limited to) unexpected command sequences, unknown commands, commands in a wrong device mode and supplying wrong parameters or data which could result in the device outputting clear-text secret keys or account data.

The full track data or magnetic stripe equivalent in a chip card shall not be retained any longer, or used more often, than strictly necessary. The device must automatically clear its internal buffers when either:

- The transaction is completed, or
- The device has timed out waiting for the response from the cardholder or merchant.

If the device may be accessed remotely, all access attempts must be cryptographically authenticated. If the authenticity of the access request cannot be confirmed, the access request shall be denied.

If the device supports multiple applications, it must enforce the separation between applications. It must not be possible that one application interferes with or tampers with another application or the OS of the device, including modifying data objects belonging to another application.

The operating system of the device must contain only the software (components and services) necessary for the intended operation. The operating system must be configured securely and run with least privilege. The security policy enforced by the device must not allow unauthorised or unnecessary functions. API functionality and commands that are not required in to support specified functionality must be disabled (and where possible, removed) before the equipment is commissioned.

If the device operates over an IP network, the IP stack and ancillary IP services such as DNS, DHCP etc. must be securely implemented. A vulnerability assessment must be carried out to ensure that the IP stack and any ancillary services used do not contain exploitable vulnerabilities.

Any security protocols used by the device (such as SSL/TLS, IPSec, PPTP, proprietary protocols, etc.) must be securely implemented in-line with international best practices.

There is no mechanism in the device that would allow the outputting of clear-text account data.

The device supports data origin authentication for all encrypted messages following guidance specified in ISO/IEC 19772:2009 (or equivalent). The ordering of how authentication and encryption are applied to transaction messages shall not result in a weakening of the secure implementation.

Access to sensitive services requires authentication. Sensitive services provide access to functions that process sensitive data such as cryptographic keys, passwords and account data. Entering or exiting sensitive services shall not reveal or otherwise affect sensitive data.

To minimize the risks from unauthorised use of sensitive services, limits on the number of actions that can be performed and a time limit imposed, after which the device is forced to return to its normal mode.

## **2 | Limit cleartext availability of account data to the point of encryption and the point of decryption.**

All account data must be encrypted with the following exceptions:

- A maximum of the first six and last four digits of the PAN may be left in the clear for routing purposes. If encrypted data will only ever be transmitted to by a single, known end-point and not routed further, then all account data should be encrypted.
- A maximum of the first six and last four digits of the PAN may be displayed by the payment terminal and/or printed on the transaction receipt, in settlement reports, used for selection of account on file, etc. This does not supersede national, regional or international laws or regulations in place for displaying cardholder data.

Sensitive authentication data must not be stored after authorisation even if encrypted (as per PCI DSS).

Account data shall not appear in the clear outside of the device.

If the cryptographic device produces an output log, account data must be protected (as per PCI DSS requirement 3.4) prior to output. Sensitive authentication data must be securely deleted from the record before it is logged.

Security control(s) must be in place on the cryptographic device that limits/prevents access to cleartext sensitive data and account data prior to encryption.

The point of decryption must monitor for the presence of incoming clear-text data. The point of decryption must have response procedures in place to alert relevant staff should an encrypting device unexpectedly begin transmitting clear-text data. All affected parties must be aware of these procedures.

## Key Management

For the remainder of this document, the term cryptographic device shall be used to represent both Hardware Security Modules (HSM) and transaction originating Tamper Resistant Security Modules (TRSM), e.g. PED devices. Where the requirements apply only to a specific type of device this device will be referenced explicitly.

### Objective 1: Encryption Methodologies

**Account data must be processed using cryptographic methodologies that ensure account data is kept secure.**

#### 1 Key management, cryptographic algorithms and cryptographic key lengths must be consistent with international and/or regional standards

Cryptographic keys must be managed in accordance with internationally recognised key management standards (e.g. ISO 11568 (all parts)/ANSI X9.24 (all parts) or equivalent).

Account data must be encrypted using only ISO or ANSI X9.52 approved encryption algorithms (e.g. AES, TDES). The encryption algorithm should use a mode of operation and a padding mechanism described in ISO/IEC 10116:2006 (or equivalent). Any method used to produce encrypted text that relies on non-ISO or non-ANSI approved modes of operation shall be evaluated by at least one independent security evaluation organisation (e.g. a standards body), accompanied by a proof of security and subjected to a peer review; such methods shall also be implemented following all guidelines of said evaluation and peer review including any recommendations for associated key management.

The following table summarises minimum required key lengths for commonly used algorithms:

Algorithm	Bit Length
TDES	112
AES	128
RSA	2048
ECC	224
SHA	224

**Note:** Double length TDES (112-bits) keys should not be used for more than one million transactions. In cases where the number of transactions potentially processed through the system using a “single” 112 bits TDES key greatly exceeds one million, triple length TDES (168-bits) keys or AES should be used. Note that key management schemes that greatly limit the number of transaction processed by a single key, such as Derived Unique Key Per Transaction (DUKPT) can be used to ensure that any individual key is used only a limited number of times.

## Objective 2: Key Generation

**Cryptographic keys used for data field encryption/decryption, and related key management keys, must be created using processes that ensure that it is not possible to predict any key or determine that certain keys are more probable than other keys.**

### 2 | **All keys and key components must be generated using an approved random or pseudo-random process**

Random or pseudo-random number generation is critical to the security and integrity of all cryptographic systems. All cryptographic key-generation relies upon good quality, randomly generated values. An independent laboratory must certify self-developed implementations of a cryptographic pseudo-random number generator, which includes testing in accordance to the statistical tests defined in NIST SP 800-22 revision 1.

### 3 | **Compromise of the key-generation process must not be possible without collusion between at least two trusted individuals**

The output of the key generation process must be monitored by at least two authorised individuals who ensure there is no unauthorised mechanism that might disclose a cleartext key or key component as it is transferred between the key generation cryptographic device and the device or medium receiving the key or key component.

Multi-use/purpose computing systems shall not be used for key generation where any cleartext secret key or key component thereof appears in unprotected memory.

Printed key components must be printed within blind mailers or sealed immediately after printing so that only the party entrusted with it can observe each component and so that tampering can be detected.

Any residue from the printing, export, display or recording process that might disclose a component must be destroyed immediately.

#### **4 | Documented procedures must exist and must be demonstrably in use for all key generation processing**

Written key creation procedures must exist and be known by all affected parties (key custodians, supervisory staff, technical management, etc.). All key creation events must be documented.

### **Objective 3: Key Distribution**

#### **Keys must be conveyed or transmitted in a secure manner**

#### **5 | Cryptographic keys must be conveyed or transmitted securely**

Specific techniques (and supporting documentation) must exist detailing how keys are transferred in order to maintain their integrity and/or confidentiality. An encryption key, typically a Key Encryption Key (KEK), must be transferred by physically forwarding the separate components of the key using different communication channels or must be transmitted in ciphertext form. Key components must be transferred in either tamper-evident packaging, within a TRSM (e.g. FIPS approved smartcard) or in ciphertext form (if encrypted, component key encrypting keys must follow all relevant key management guidance specified in this document). No person shall have access to any cleartext key during the transport process.

A person with access to one component of a key, or to the media conveying this component, must not have access to any other component of this key or to any other medium conveying any other component of this key. Components of encryption keys must be transferred using different communication channels, such as different courier services. It is not sufficient to send key components for a specific key on different days using the same communication channel.

Public keys must be conveyed in a manner that protects their integrity and authenticity

Public keys must use a mechanism independent of the actual conveyance method that provides the ability to validate the correct key was received.

**6 Any single unencrypted key component must at all times during its transmission, conveyance, or movement between any two organisational entities be: Under the continuous supervision of a person with authorised access to this component, OR locked in a security container (including tamper evident packaging) in such a way that it can be obtained only by a person with authorised access to it, OR in a physically secure Tamper Resistant Security Module (TRSM).**

Key components must be protected by encryption, by inclusion in a TRSM (e.g. FIPS approved smartcard), or by storage within tamper-evident packaging and the separate parts must be managed under the strict principles of dual control and split knowledge. This means that each component requires dual control and split knowledge. No single person shall be able to access or use all components of a single cryptographic key. Any sign of package tampering must result in the destruction and replacement of the set of components, as well as any keys encrypted under this (combined) key.

No one but the authorised key custodian (and designated backup(s)) shall have physical access to a key component prior to transmittal or upon receipt of a component. Mechanisms must exist to ensure that only authorised custodians place key components into tamper-evident packaging for transmittal and that only authorised custodians open tamper-evident packaging containing key components upon receipt, this includes checking the serial number of the tamper evident packing upon receipt of a component package. Details of the serial number of the package must be transmitted separately to the package itself.

**7 All key encryption keys used to transmit or convey other cryptographic keys must be (at least) as strong as any key transmitted or conveyed**

Cryptographic algorithms used for key transport, exchange or establishment must use key lengths that are deemed acceptable for the algorithm being used. For the minimum key lengths please refer to requirement 1 in the key management section of this

document.

**8 Documented procedures must exist and must be demonstrably in use for all key transmission and conveyance processing**

Written procedures must exist and be known to all affected parties. Conveyance or receipt of keys managed as components or otherwise outside a cryptographic device must be documented.

## Objective 4: Key Loading

Key loading to Cryptographic devices must be handled in a secure manner.

9	<b>Unencrypted secret keys must be entered into cryptographic devices using the principles of dual control and split knowledge</b>
<p>Procedures must be established that will prohibit any one custodian from having access to all components of a single secret key.</p> <p>A Master File Key (MFK) and any KEK loaded in component form must be loaded using the principles of dual control and split knowledge.</p> <p>For manual key loading, dual control requires split knowledge of the key among the custodians (in instances where a secure key loading device is used, only dual control is required). Manual key loading may involve the use of media such as paper or specially designed key-loading hardware devices.</p> <p>Any other cryptographic device loaded with the same key components must combine all entered key components using an identical process.</p> <p>Key establishment protocols using public key cryptography may also be used to distribute secret keys. These must meet the requirements detailed in Annex A of this document.</p>	

10	<b>The mechanisms used to load secret keys, such as terminals, external PIN pads, key guns, or similar devices and methods must be protected to prevent any type of monitoring that could result in the unauthorised disclosure of any component</b>
<p>A cryptographic device must transfer a plaintext secret key only when at least two authorised individuals are identified by the device (e.g. by means of passwords or other unique means of identification).</p> <p>Plaintext keys and key components must be transferred into a cryptographic device only when it can be ensured that there is no unauthorised mechanism at the interface between the conveyance medium and the cryptographic device that might disclose the</p>	

transferred keys, and that the device has not been subject to any prior tampering which could lead to the disclosure of keys or account data.

The injection of key components from electronic medium to a cryptographic device (and verification of the correct receipt of the component is confirmed, if applicable) results in either of the following:

- The medium is placed into secure storage, if there is a possibility it will be required for future re-insertion of the component into the cryptographic device, or
- All traces of the component are erased or otherwise destroyed from the electronic medium.

For keys transferred from the cryptographic device that generated the key to an electronic key-loading device:

- The key-loading device is a physically secure TRSM(e.g. FIPS approved smartcard), designed and implemented in such a way that any unauthorised disclosure of the key is prevented; and
- The key-loading device is under the supervision of a person authorised by management, or stored in a secure container such that no unauthorised person can have access to it; and
- The key-loading device is controlled so that only authorised personnel under dual control can access, use or enable it to output a key into another cryptographic device. Such personnel must ensure that a key-recording device is not inserted between the TRSM and the receiving cryptographic device; and
- The key-loading device must not retain any information that might disclose the key or a key that it has successfully transferred.

The medium upon which a component resides must be physically safeguarded at all times.

Any tokens, EPROMs, or other key component holders used in loading encryption keys must be maintained using the same controls used in maintaining the security of hard copy key components. These devices must be in the physical possession of only the designated component holder and only for the minimum practical time.

If the component is not in human comprehensible form (e.g. in a PROM, in a smart card or on a magnetic stripe card), it is in the physical possession of only one person for the minimum practical time until the component is entered into a cryptographic device.

If the component is in human readable form (e.g. printed within a PIN-mailer type document), it is only visible at one point in time

to only one person (the designated component custodian) and only for the duration of time required for this person to privately enter the key component into a cryptographic device. Printed key component documents are not opened until immediately prior to entry.

A key custodian must never have (or never have had in the past) access to more than one key component of a single key.

**11 All hardware and passwords used for key loading must be managed under dual control.**

Any hardware used in the key-loading function must be controlled and maintained in a secure environment under dual control.

All cable attachments must be examined before each application to ensure they have not been tampered with or compromised.

Any physical (e.g. brass) key(s) used to enable key loading must not be in the control or possession of any one individual who could use those keys to load secret cryptographic keys under single control.

Use of the equipment must be monitored and a log of all key-loading activities maintained for audit purposes.

**12 The loading of keys or key components must incorporate a validation mechanism such that the authenticity of the keys is ensured and it can be ascertained that they have not been tampered with, substituted, or compromised**

A cryptographic-based validation mechanism helps to ensure the authenticity and integrity of keys and components (e.g. testing key check values, hashes or other similar unique values that are based upon the keys or key components being loaded), see ISO 11568.

The public key must have its authenticity and integrity ensured.

A plaintext public key must only exist within a certificate, PKCS #10 or a secure cryptographic device.

Public keys not stored in certificates, PKCS #10s or in a secure cryptographic device must be stored encrypted, or have a MAC (Message Authentication Code) created using the algorithm defined in **ISO 9807**, in order to ensure authenticity and integrity.

**13 Documented procedures must exist and be demonstrably in use (including audit trails) for all key-loading activities**

Written procedures must exist and be known to all parties involved in cryptographic key loading. All key loading events must be documented.

**Objective 5: Key Usage**

**Keys must be used in a manner that prevents or detects their unauthorised usage.**

**14 Unique secret cryptographic keys must be in use for each identifiable link between encryption and decryption points**

Where two organisations share a key to encrypt account data (including a key encryption key used to encrypt a data encryption key) communicated between them, that key must be unique to those two entities and must not be given to, or used by, any other entity. Where symmetric keys are used to encrypt account data, the keys must be unique per transaction originating TRSM.

**Note:** Keys may exist at more than one pair of locations for disaster recovery or load balancing (e.g. dual processing sites) but must be protected in-line with all other requirements specified in this document.

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

The unauthorised replacement, or substitution, of one stored key for another or the replacement or substitution of any portion of a key, whether encrypted or unencrypted, must be prevented. Documented procedures must exist and be demonstrably in use describing how the replacement and/or substitution of one key for another is prevented.

Key component documents and their packaging that show signs of tampering must result in the discarding and invalidation of all components and the associated key at all locations where they exist.

**16 Cryptographic keys must only be used for their sole intended purpose and must never be shared between production and test systems**

Encryption keys must only be used for the purpose they were intended (e.g. Key Encryption Keys must not be used as Data Encryption Keys). This is necessary to limit the magnitude of exposure should any key(s) be compromised. Using keys only as they are intended to be used also significantly strengthens the security of the underlying system.

Private keys shall only be used to create digital signatures and to perform decryption operations. Each individual private key shall only be used for a single purpose.

Keys must never be shared or substituted in a processor's production and test systems. Except by chance, production keys must never be present or used in a test system and test keys must never be present or used in a production system.

Encryption or decryption of arbitrary data using any account data encrypting key or key-encrypting key contained in the device is not allowed. The device must enforce that account data keys, key-encipherment keys, and PIN-encryption keys have different values and that PIN encryption keys must not be used for data encryption and vice versa.

**17 All secret keys present and used for any function must be unique (except by chance) to that device**

Any secret key used to encrypt account data in a transaction originating TRSM must be known only in that device and in HSMs at the minimum number of facilities consistent with effective system operations. Disclosure of the key in one such device must not provide any information that could be feasibly used to determine the key in any other such device.

In a master/session key approach, the master key(s) and all session keys must be unique to each device. If a device interfaces with more than one decryption end-point, the TRSM must have a unique key or set of keys for each end-point. These unique keys, or set of keys, must be totally independent and not variants of one another.

Keys that are generated by a derivation process and derived from the same Base Derivation Key must use unique data for the derivation process such that all transaction originating TRSMs receive unique secret keys. Key derivation must be performed prior to a key being loaded/sent to the recipient transaction originating TRSM. This requirement does not preclude multiple unique keys being loaded on a single device.

## Objective 6: Key Administration

Keys are administered in a secure manner.

18	<b>Secret keys used for encrypting data field encryption keys, or for data field encryption, must never exist outside of a cryptographic device, except when encrypted or securely stored and managed using the principles of dual control and split knowledge</b>
----	--

Effective implementation of these principles requires the existence of barriers beyond procedural controls to prevent access to any key component. For example, an effective implementation could have physically and separate locking containers that only the appropriate key custodian (and their designated backup(s)) could access.

Key components may be stored on tokens (e.g. integrated circuit cards). These tokens must be stored in a secure manner to prevent unauthorised access of the key components. For example, if key components are stored on tokens that are secured in safes, more than one authorised person might have access to these tokens. Therefore, additional protection is needed for each token (possibly by using tamper-evident packaging) to enable the token's owner to determine if a token was used by another person.

In particular, key components for each specific custodian must be stored in a separate secure repository that is only accessible by the custodian or designated backup(s). Furniture-based locks, or containers with a limited set of unique keys are not sufficient to meet this requirement.

If a key is stored on a token and a PIN or similar mechanism is used to access the token, only that token's owner (or designated backup(s)) must have possession of both the token and its corresponding PIN.

Printed or magnetically recorded key components must reside only within tamper-evident packaging such that the component

cannot be ascertained without opening the packaging.

Keys that are used to encrypt other keys or to encrypt account data, and which exist outside of a cryptographic device, must be encrypted using keys of equivalent or greater strength as defined in requirement 2 in the key management section of this document,

If secret keys are encrypted using public key cryptography for distribution to transaction originating TRSMs, as part of a key-establishment protocol, the requirements detailed in Annex A of this document must be met.

19	<b>Procedures must exist and must be demonstrably in use to replace any known or suspected compromised key and its subsidiary keys (those keys encrypted with the compromised key) to a value not feasibly related to the original key</b>
----	--

Key components must never be reloaded when there is any suspicion that either the originally loaded key or the cryptographic device has been compromised. If suspicious alteration is detected, new keys must not be installed until the cryptographic device has been inspected and assurance reached that the equipment has not been subject to any form of unauthorised modification.

A cryptographic key must be replaced with a new key whenever the compromise of the original key is known or suspected. In addition, all keys encrypted under or derived using, that key must be replaced with a new key within the minimum feasible time. The replacement key must not be a variant of the original key, or an irreversible transformation of the original key.

Procedures must include a documented escalation process and notification to organisations that currently share or have previously shared the key(s). The procedures should include a damage assessment and specific actions to be taken with system software and hardware, encryption keys, encrypted data, etc.

Specific events must be identified that would indicate a compromise may have occurred. Such events may include, but are not limited to:

- Missing cryptographic devices.
- Tamper-evident seals or package numbers or dates and times not agreeing with log entries.
- Tamper-evident seals or packages that have been opened without authorisation or show signs of attempts to open or

penetrate.

- Indications of physical or logical access attempts to the processing system by unauthorised individuals or entities.

If attempts to load a secret key or key component into a cryptographic device fail, the same key or component must not be loaded into a replacement device unless it can be ensured that all residue of the key or component has been erased from or otherwise destroyed in the original device.

**20 Key variants must only be used in devices that possess the original key. Key variants must not be used at different levels of the key hierarchy e.g. a variant of a key encryption key used for key exchange cannot be used as a working key or as a master file key for local storage**

A secret key used to encrypt account data must never be used for any other cryptographic purpose. A key used to encrypt the Data Encryption Key (DEK) must never be used for any other cryptographic purpose. However, variants of the same key may be used for different purposes. Any variant of the DEK or a key used to encrypt the DEK must be protected in the same manner i.e. under the principles of dual control and split knowledge.

Variants of an MFK must not be used external to the (logical) configuration that houses the MFK itself.

**21 Secret keys and key components that are no longer used or have been replaced must be securely destroyed**

Instances of keys that are no longer used or that have been replaced by a new key must be destroyed. Keys maintained on paper must be burned, pulped or shredded in a cross-cut shredder.

- If the key is stored in EEPROM, the key should be overwritten with binary 0s (zeros) a minimum of three times.
- If the key is stored on EPROM or PROM, the chip should be smashed into many small pieces and scattered.

Other permissible forms of a key instance (physically secured, encrypted or components) must be destroyed following the procedures outlined in **ISO-11568-2**. In all cases, a third party—who is not a custodian for any component of that key—must observe the destruction and sign an affidavit of destruction.

The procedures for destroying keys that are no longer used or that have been replaced by a new key must be documented. Key encryption key components used for the conveyance of working keys must be destroyed after successful loading and validation as being operational.

**22 Access to secret keys and key material must be limited to properly designated key custodians, and their backups, on a need-to-know basis**

Limiting the number of key custodians to a minimum helps reduce the opportunity for key compromise. In general, the designation of a primary and a backup key custodian for each component is sufficient, such that the fewest number of key custodians are necessary to enable effective key management. This designation must be documented by having each custodian and backup custodian sign a key custodian form. The forms must specifically authorise the custodian and identify the custodian's responsibilities for safeguarding key components or other keying material entrusted to them and specify an effective date and time for the custodians access. Key custodian forms should also be signed by management authorising the access.

**23 Logs must be kept for any time that keys, key components, or related materials are removed from storage or loaded to a cryptographic device**

At a minimum, logs must include the date and time in/out, component identifier, purpose of access, name and signature of custodian accessing the component, tamper evident package number pre and prior to removal (if applicable).

**24 Backup copies of secret keys must exist only for the purpose of reinstating keys that are accidentally destroyed or are otherwise inaccessible. The backups must exist only in one of the allowed storage forms for that key**

The backup copies must be securely stored with proper access controls, under at least dual control, and subject to at least the same level of security control as operational keys in line with all requirements specified in this document.

The creation of backup copies (including cloning) must require a minimum of two authorised individuals to enable the process. All requirements applicable for the original keys also apply to any backup copies of keys and their components.

**Note:** It is not a requirement to have backup copies of key components or keys.

**25 Documented procedures must exist and must be demonstrably in use for all key administration operations**

Written procedures must exist and all affected parties must be aware of those procedures. All activities related to key administration must be documented. This includes all aspects of key administration, including a defined cryptographic key change policy for each key layer defined in the key hierarchy (this applies to both symmetric and asymmetric key types), as well as:

- Security awareness training.
- Role definition - nominated individual with overall responsibility.
- Background checks for personnel.

Management of personnel changes, including revocation of access control and other privileges when personnel move must also be included within the procedures.

## **Objective 7: Device Management**

**Equipment used to process account data and keys must be managed in a secure manner.**

**26 Cryptographic devices must be placed into service only if there is assurance that the equipment has not been substituted or subjected to unauthorised modifications or tampering prior to the loading of cryptographic keys**

Cryptographic devices must only be placed into service if there is assurance that the equipment has not been subject to unauthorised modification, substitution, or tampering or is otherwise subject to misuse.

To achieve this, controls must exist to protect secure TRSMs from unauthorised access before, during, and after installation. Access to all cryptographic hardware must be documented, defined, logged and controlled. Cryptographic devices must not use default keys or data.

A documented security policy must exist that specifies personnel with authorised access to all secure cryptographic devices. Unauthorised individuals must not be able to access, modify, or substitute any secure cryptographic device. A documented “chain of custody” must exist to ensure that all cryptographic hardware is controlled from its receipt through its installation and use.

Controls must ensure that all installed hardware components are from a legitimate source.

Dual control mechanisms must exist to prevent substitution of secure cryptographic devices, both in service and spare or backup devices. Procedural controls may exist to support the prevention and detection of substituted cryptographic devices, but cannot supplant the implementation of dual control mechanisms, which may be a combination of physical barriers and logical controls. This requires physical protection of the device up to the point of key insertion or inspection, and possibly testing of the device immediately prior to key insertion. Techniques include the following:

- a. Cryptographic devices are transported from the manufacturer’s facility to the place of key-insertion using a trusted courier service. The devices are then securely stored at this location until key-insertion occurs.
- b. Cryptographic devices are shipped from the manufacturer’s facility to the place of key-insertion in serialised, counterfeit-resistant, tamper-evident packaging. The devices are then stored in such packaging, or in secure storage, until key-insertion occurs.
- c. The manufacturer’s facility loads into each cryptographic device a secret, device-unique “transport-protection token.” The cryptographic device used for key-insertion has the capability to verify the presence of the correct “transport-protection token” before overwriting this value with the initial key that will be used.
- d. Each cryptographic device is carefully inspected and perhaps tested immediately prior to key-insertion using due diligence. This is done to provide reasonable assurance that it is the legitimate device and that it has not been subject to any unauthorised modifications.
  - o Devices must incorporate self-tests to ensure their correct operation. Devices must not be re-installed unless there is assurance they have not been tampered with or compromised.
  - o Controls must exist and be in use to ensure that all physical and logical controls and anti-tamper mechanisms used are not modified or removed.
- e. The cryptographic device, when shipped from the key loading facility to the initial point of use, and stored en route, must be under auditable controls that can account for the location of every encryption module at any point in time.
- f. Procedures must be in place to transfer accountability for the cryptographic device from the key-loading facility.
- g. Procedures must be in place to retire cryptographic device that have reached the end of their deployment lifecycle. This

includes, but is not limited to, securely erasing all data from the device.

Documented inventory control and monitoring procedures must exist to track equipment by both physical and logical identifiers in such a way as to:

- Protect the equipment against unauthorised substitution or modification until a secret key has been loaded into it; *and*
- Detect lost or stolen equipment, *and*
- Ensure data origin authentication of encrypted messages coming from a legitimate transaction originating TRSM.

Procedures must include ensuring that a counterfeit device possessing all the correct operational characteristics plus fraudulent capabilities has not been substituted for a legitimate device.

Notwithstanding how the device is inspected and tested, it is mandatory to verify the device serial number against the purchase order, invoice, waybill or similar document to ensure that device substitution has not occurred. Documents used for this process must be received via a different communication channel (i.e., the control document used must not have arrived with the equipment).

**27 Procedures must exist that ensure the destruction of all cryptographic keys and any account data within any cryptographic device removed from service**

If a cryptographic device has been removed from service, all keys stored within the device that have been used (or potentially could be used) for any cryptographic purpose must be destroyed.

- All critical initialisation, deployment, usage, and decommissioning processes must impose the principles of dual control and split knowledge (e.g. key or component-loading, firmware or software-loading, and verification and activation of anti-tamper mechanisms).
- Key and data storage must be zeroised when a device is decommissioned.

If necessary to comply with the above, the device must be physically destroyed so that it cannot be placed into service again, or allow the disclosure of any secret data or keys.

28	<b>Any cryptographic device capable of encrypting a key and producing cryptograms of that key must be protected against unauthorised use to encrypt known keys or known key components. This protection must take the form of either or both of the following: a) dual access controls are required to enable the key encryption function, b) physical protection of the equipment (e.g. locked access to it) under dual control</b>
----	--

Cryptographic devices must be managed in a secure manner in order to minimise the opportunity for key compromise or key substitution. Physical keys, authorisation codes, passwords, or other enablers must be managed so that no one person can use both the enabler(s) and the device which can create cryptograms of known keys or key components under a key encryption key used in production.

Unauthorised use of secure cryptographic devices (including key loading devices) shall be prevented or detected by:

- The device is at all times either locked or sealed in a tamper-evident cabinet or else is under the continuous supervision of at least two authorised people who ensure that any unauthorised use of the device would be detected;
- The device has functional or physical characteristics (e.g. passwords or physical high-security keys) that prevent use of the device except under the dual control of at least two authorised people, and when in a state in which it is useable, the device is under the continuous supervision of at least two such people who ensure that any unauthorised use of the device would be detected.

29	<b>Documented procedures must exist and must be demonstrably in use to ensure the security and integrity of cryptographic devices placed into service, initialised, deployed, used, and decommissioned</b>
----	--

Written procedures must exist and all affected parties must be aware of those procedures. Records must be maintained of the tests and inspections performed on cryptographic devices before they are placed into service, as well as devices being decommissioned.

Procedures that govern access to HSMs must be in place and known to data center staff and any others involved with the physical security of such devices.

## Annex A

### Symmetric Key Distribution using Asymmetric Techniques

This annex contains detailed requirements that apply to remote key establishment and distribution applications and are in addition to key and equipment management criteria stated in the main body of this document. Remote key distribution schemes should be used for initial key loading only e.g. establishment of the TDES key hierarchy, such as a terminal master key. Standard symmetric key exchange mechanisms should be used for subsequent symmetric key exchanges, except where a device requires a new key initialisation due to unforeseen loss of the existing terminal master key.

Certification Authority requirements apply to all entities signing public keys, whether in X.509 certificate based schemes or other designs. For purposes of these requirements, a certificate is any digitally signed value containing a public key.

The control objectives and security requirements are delineated as found in the preceding Technical Reference section of this document, and are in addition to those requirements.

### Point of Sale Encryption Device

No additional requirements

### Key Management

#### Objective 2: Key Generation

**Cryptographic keys used for data field encryption/decryption, and related key management keys, must be created using processes that ensure that it is not possible to predict any key or determine that certain keys are more probable than other keys.**

<b>2</b>	<b>All keys and key components must be generated using an approved random or pseudo-random process</b>
----------	--

Key pairs must be generated using a random or pseudo random process in accordance with PCI requirements, which includes testing in accordance to the statistical tests defined in NIST SP 800-22 revision 1.
--

Key-generation methods must meet the current ANSI and ISO standards for the algorithm(s) in question.

Secret keys are unique and are equally likely to be generated. The probability that any two cryptographic keys are identical is negligible.

**3 | Compromise of the key-generation process must not be possible without collusion between at least two trusted individuals**

Key pairs must either be generated by the device which will use the key pair, or if generated externally, the key pair and all related critical security parameters (e.g. secret seeds) must be deleted (zeroised) immediately after the transfer to the device which will use the key pair occurs.

### Objective 3: Key Distribution

#### Keys must be conveyed or transmitted in a secure manner

**5 | Cryptographic keys must be conveyed or transmitted securely**

Cryptographic algorithms used for key transport, exchange or establishment must use key lengths that are deemed acceptable for the algorithm being used.

For Diffie-Hellman implementations:

Entities must securely generate and distribute the system-wide parameters: generator  $g$ , prime number  $p$  and parameter  $q$ , the large prime factor of  $(p - 1)$ . The parameter  $p$  must be at least 2048 bits long, and parameter  $q$  must be at least 256 bits long. Each entity generates a private key  $x$  and a public key  $y$  using the domain parameters  $(p, q, g)$ . Each private key shall be statistically unique, unpredictable, and created using an approved random number generator which meets the requirements in accordance to the statistical tests defined in NIST SP 800-22 revision 1.

Entities must authenticate the Diffie-Hellman public keys using either DSA, a certificate, or a symmetric MAC (based on TDES –

see ISO 16609 - Banking -- Requirements for message authentication using symmetric techniques – Method 3 should be used).

#### **Objective 4: Key Loading**

**Key loading to cryptographic devices must be handled in a secure manner.**

12	<b>The loading of keys or key components must incorporate a validation mechanism such that the authenticity of the keys is ensured and it can be ascertained that they have not been tampered with, substituted, or compromised</b>
	<p>Cryptographic devices and Key Distribution Hosts (KDHs)) involved in using public key schemes must check the validity of other such devices involved in the communication prior to any key transport, exchange or establishment. Validation of authentication credentials must occur immediately prior to any key establishment. Examples of this kind of validation include checking current certificate revocation lists or embedding valid authorised key distribution host certificates in devices and disallowing communication with unauthorised key distribution hosts.</p> <p>Mechanisms must exist to prevent a non-authorised KDH from performing key transport, key exchange or key establishment with transaction originating TRSMs. An example of this kind of mechanism is through limiting communication between the transaction originating TRSM and KDH to only those KDHs contained in a list of valid KDHs managed by the transaction originating TRSM.</p> <p>Within an implementation design, there shall be no means available for “man in middle” attacks. System implementations must be designed and implemented to prevent replay attacks.</p> <p>Key pairs generated external to the device that uses the key pair must be securely transferred and loaded into the device and must provide for key protection in accordance with this document. That is, the secrecy of the private key and the integrity of the public key must be ensured.</p>

## Objective 5: Key Usage

Keys must be used in a manner that prevents or detects their unauthorised usage.

15	<b>Procedures must exist to prevent or detect the unauthorised substitution (unauthorised key replacement and key misuse) of one key for another or the operation of any cryptographic device without legitimate keys</b>
----	---

Cryptographic devices shall only communicate with a Certification Authority (CA) for the purpose of certificate signing (or for key injection where the certificate issuing authority generates the key pair on behalf of the TRSM); and with KDHS for key management, normal transaction processing and certificate (entity) status checking.

KDHS shall only communicate with transaction originating TRSMs for the purpose of key management and normal transaction processing; and with CAs for the purpose of certificate signing and certificate (entity) status checking.

16	<b>Cryptographic keys must only be used for their sole intended purpose and must never be shared between production and test systems</b>
----	--

Only one certificate shall be issued per key pair. Certificates for a key pair shall not be renewed using the same keys.

Mechanisms must be utilised to preclude the use of a key for other than its designated and intended purpose (i.e. keys are used in accordance with their certificate policy – (See RFC 3647- Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework for an example of content):

- CA certificate/certificate (entity) status checking (e.g. using Certificate Revocation Lists) signature keys, or signature keys for updating valid/authorised host lists in cryptographic devices cannot be used for any other purpose, other than subordinate entity certificate requests, certificate status checking, and self-signed root certificates. The keys used for certificate signing and certificate (entity) status checking (and if applicable, self signed roots) may be for combined usage, or may exist as separate keys dedicated to either certificate signing or certificate (entity) status checking.
- CAs that issue certificates to other CAs cannot be used to issue certificates to cryptographic devices.

Public key based implementations must provide mechanisms for restricting and controlling the use of public and private keys. For example, this can be accomplished through the use of X.509 compliant certificate extensions.

CA and KDH private keys cannot be shared between devices except for load balancing and disaster recovery. Private keys maintained in a cryptographic device cannot be shared.

**17 All secret keys present and used for any function must be unique (except by chance) to that device**

Secret keys must be uniquely identifiable in all hosts and cryptographic devices. Keys must be identifiable via cryptographically verifiable means (e.g. through the use of digital signatures or key check values).

### Objective 6: Key Administration

**Keys are administered in a secure manner.**

**18 Secret keys used for encrypting data field encryption keys, or for data field encryption, must never exist outside of a cryptographic device, except when encrypted or securely stored and managed using the principles of dual control and split knowledge**

Private keys used to sign certificates, certificate status lists, messages or for secret key protection must only exist in one of the following forms:

- Within a secure cryptographic device
- Encrypted using an algorithm and key size of equivalent or greater strength.
- As securely maintained components.

19	<b>Procedures must exist and must be demonstrably in use to replace any known or suspected compromised key and its subsidiary keys (those keys encrypted with the compromised key) to a value not feasibly related to the original key</b>
----	--

To provide for continuity of service in the event of the loss of a root key (e.g. through compromise or expiration), a key distribution management system and the associated end entities (KDHs, cryptographic devices) should provide support for more than one root.

Root CAs must provide for segmentation of risk to address key compromise. An example of this would be the deployment of subordinate CAs.

Mechanisms must be in place to address compromise of a CA due to, for example, key compromise or mismanagement. This must include procedures to revoke subordinate certificates and notify affected entities.

The CA must cease issuance of certificates if a compromise is known or suspected and perform a damage assessment, including a documented analysis of how and why the event occurred. In the event of the issuance of phony certificates with the compromised key, the CA should determine whether to recall and reissue all signed certificates with a newly generated signing key. Mechanisms (e.g. time stamping) must exist to ensure that fake certificates cannot be successfully used.

The compromised CA must notify any superior or subordinate CAs of the compromise. Subordinate CAs and KDHs should have their certificates reissued and distributed to them or be notified to apply for new certificates.

22	<b>Access to secret keys and key material must be limited to properly designated key custodians, and their backups, on a need-to-know basis</b>
----	---

All user access shall be directly attributable to an individual user e.g. through the use of unique IDs, and be restricted to actions authorised for that role through the use of a combination of CA software, operating system and procedural controls.

The system enforces an explicit and well-defined certificate security policy and certification practice statement. This must include that:

- CA systems that issue certificates to other CAs or to KDHS must be operated offline using a dedicated closed network (not a network segment). The network is only used for certificate issuance, revocation, or both certificate issuance and revocation. Outside network access shall exist only for the purposes of “pushing” certificate status information to relying parties (e.g. KDHS, cryptographic devices)
- No CA or Registration Authority (RA) software updates are done over the network (local console access must be used for CA or RA software updates).
- Non-console access requires two-factor authentication. This also applies to the use of remote console access.
- Remote user access to the CA or RA system environments shall be protected by authenticated encrypted sessions. No other remote access is permitted to the host platform(s) for system or application administration. Access for monitoring only (no create, update, delete capability) of online systems may occur without restriction.
- CA certificate (for TRSM/KDH authentication and validity status checking) signing keys must be enabled under multilevel controls.
- Certificate requests may be vetted (approved) using single user logical access to the RA application.

The CA shall require a separation of duties for critical CA functions to prevent one person from maliciously using a CA system without detection; the practice referred to as split knowledge and dual control. At a minimum, there shall be multi-person control for operational procedures such that no one person can gain control over the CA signing key(s).

For systems accessible via non-local console access, the operating system(s) utilised must be hardened. Services that are not necessary or that allow non-secure access (e.g. rlogin, rshell, etc. commands in Unix) must be removed or disabled. Unnecessary ports must also be disabled. Documentation must exist to support the enablement of all active services and ports.

Vendor default IDs which are required only as owners of objects or processes, or for installation of patches and upgrades, must be disabled from login except as necessary for a documented and specific business reason. Vendor default IDs such as “Guest” must be removed or disabled. Default passwords must be changed during initial installation.

Audit trails must include, but not be limited to all key management operations, such as key generation, backup, recovery, compromise, and destruction and certificate generation or revocation, together with the identity of the person authorising the operation and persons handling any key material (such as key components or keys stored in portable devices or media). The logs must be protected from alteration and destruction, and archived in accordance with all regulatory and legal requirements. Records pertaining to certificate issuance and revocation must at a minimum be retained for the life of the associated certificate.

Logical events are divided into operating system and CA application events. For both events the following will be recorded in the form of an audit record:

- date and time of the event,
- identity of the entity and/or user that caused the event,
- type of event, and
- success or failure of the event.

CA application logs must deploy a mechanism to prevent and detect attempted tampering of application logs.

Components of the system operated online, for example the RA, must include for operational support the use of pass phrase management techniques encompassing at a minimum the following:

- Minimum length of six characters using a mix of alphabetic, numeric, and special characters.
- System enforced expiration life not to exceed thirty days.
- System enforced minimum life of at least one day.
- Maximum invalid attempts not to exceed five before suspending the user ID.
- System enforced pass phrase history preventing the reuse of any pass phrase used in the last twelve months.
- Initial assigned pass phrases are pre-expired (user **must** replace at first logon).
- Vendor default pass phrases are changed at installation and where applicable, for updates.
- Pass phrases are not stored on any of the systems except in encrypted form or as part of a proprietary one way transformation process, such as those used in UNIX systems.
- The embedding of pass phrases in shell scripts, command files, communication scripts, etc., is strictly prohibited.

Log-on security tokens (e.g. smart cards) and cryptographic devices are not subject to the pass phrase management requirements for maximum and minimum timelines as stated above. Security tokens must have associated PINs/pass phrases to enable their usage. The PINs/pass phrases must be at least six characters using a mix of alphabetic, numeric, and special characters.

The on-line Certificate Processing system components must be protected by a firewall(s) and intrusion detection systems from

all unauthorised access including casual browsing and deliberate attacks. Firewalls must minimally be configured to:

- Deny all services not explicitly permitted.
- Disable or remove all unnecessary services, protocols, and ports.
- Fail to a configuration that denies all services, and requires a firewall administrator to re-enable services after a failure.
- Disable source routing on the firewall and external router.
- Not accept traffic on its external interfaces that appears to be coming from internal network addresses.
- Notify the firewall administrator in near real time of any item that may need immediate attention such as a break-in, little disk space available, or other related messages so that an immediate action could be taken.
- Run on a dedicated computer: All non-firewall related software, such as compilers, editors, communications software, etc. must be deleted or disabled.

Online systems must employ individually or in combination network and host based Intrusion Detection Systems (IDS) to detect inappropriate access. At a minimum, database servers and the application servers for RA and web, as well as the intervening segments must be covered.

**25 | Documented procedures must exist and must be demonstrably in use for all key administration operations**

CA operations must be dedicated to certificate issuance and management. All physical and logical CA system components must be separated from key distribution systems.

The certificate issuing and management authority may consist of one or more devices that are used for the issuance, revocation, and overall management of certificates and certificate status information.

Each CA operator must develop a certification practice statement (CPS) - (See RFC 3647- Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework for an example of content). This may take the form of a declaration by the CA operator of the details of its trustworthy system and the practices it employs in its operations and in support of the issuance of certificates. A CPS may take the form of either a specific single document or a collection of specific documents. The CPS must be consistent with the requirements described within this document. The CA shall operate in accordance with its CPS.

**Documented procedures exist and are demonstrably in use by CAs to validate the identity of the certificate requestor and**

recipient before issuing a digital certificate for the recipient's associated public key.

For CA and KDH certificate signing requests, including certificate or key validity status changes (e.g. revocation, suspension, replacement), verification must include validation that:

- The entity submitting the request is who it claims to be
- The entity submitting the request is authorised to submit the request on behalf of the certificate request's originating entity
- The entity submitting the request has a valid business relationship with the issuing authority (e.g. the vendor) consistent with the certificate being requested.
- The certificate signing request has been transferred from the certificate request's originating entity to the RA in a secure manner.
- RAs must retain documentation and audit trails relating to the identification of entities for all certificates issued and certificates whose status had changed for the life of the associated certificates.

## Objective 7: Device Management

**Equipment used to process account data and keys must be managed in a secure manner.**

28	<b>Any cryptographic device capable of encrypting a key and producing cryptograms of that key must be protected against unauthorised use to encrypt known keys or known key components. This protection must take the form of either or both of the following: a) dual access controls are required to enable the key encryption function, b) physical protection of the equipment (e.g. locked access to it) under dual control</b>
----	--

CA and RA database and application servers, and HSM devices must reside in a physically secure and monitored environment.

The physically secure environment must restrict access to only authorised personnel. The physically secure environment must have an intrusion detection system and restricted access via, for example, locks or tokens. Documented procedures exist for the granting and revocation of access privileges, which include reviewing manual or electronic logs of accesses. Certificate Processing, where the certificate is issued by a 3rd party, must:

- Operate in a physically secure dedicated room not used for any other business activities but certificate operations (stand-

alone).

- Provide for the documentation of all access granting, revocation, and review procedures and of specific access authorisations, whether logical or physical.
- Require dual control access. The room must never be occupied by a single individual for more than thirty (30) seconds. The enforcement mechanism must be automated. The system must enforce anti-pass-back.
- Use electronically (e.g. badge and/or biometric) managed dual occupancy.
- Allow access only to pre-designated staff with defined business needs and duties. Visitors must be authorised and escorted at all times.
- Use CCTV monitoring (motion activated systems that are separate from the intrusion detection system may be used) of the CA operating platform which must record to time lapse VCRs or similar mechanisms. Surveillance cameras must not be configured to allow the monitoring of computer screens, keyboards, PIN pads, etc.
- Require that personnel with access to the physically secure environment must not have access to the media (e.g. VCR tapes, digital recording systems, etc.) with the recorded surveillance data. Images recorded from the CCTV system must be securely archived for a period of no less than forty-five days. Systems using digital recording mechanism must have sufficient redundancy to prevent the loss of information necessary to reconstruct events for the most recent forty-five day period.
- Provide for continuous (motion activated systems may be used) lighting for cameras.
- Have a 24/7 intrusion detection system for the physically secure environment. Protect the secure area by motion detectors when unoccupied. This must be connected to the alarm system and automatically activated every time all authorised personnel have exited the secure area. Any windows in the secure area must be locked, protected by alarmed sensors, or otherwise similarly secured.
- Use access logs to record personnel entering the secure room, including documented reasons for the access. The logs may consist of either electronic, manual, or both. Visitors must sign an access log detailing name, organisation, date and time in and out and purpose of visit. The person escorting the visitor must also initial the log.
- Tie all access control and monitoring systems to an Uninterruptible Power Source (UPS).
- Document all alarm events. Under no circumstances shall an individual sign-off on an alarm event in which they were involved.
- Establish that the use of any emergency entry or exit mechanism must cause an alarm event.
- Require that all alarms for physical intrusion necessitate an active response by personnel assigned security duties within thirty minutes.
- Implement a process for synchronising the time and date stamps of the access, intrusion detection and monitoring

Root CAs and their equivalent operations must exist only in a high security environment. CAs and their associated RA servers that issue certificates to Key Distribution Hosts or subordinate CAs must additionally meet the following requirements:

- The physically secure environment must have true floor to ceiling (slab to slab) walls. Alternatively, solid materials, steel mesh or bars may be utilised below floors and above ceilings to protect against intrusions e.g. in a caged environment.
- This physically secure environment must have a 24/7 intrusion detection system:
  - The intrusion detection system must have 24-hour monitoring (including UPS).
  - The intrusion detection system must include the use of motion sensors.
- The system must be capable of and perform recording and archiving of alarm activity.
- Alarm activity must include unauthorised entry attempts or any deliberate or inadvertent actions that disable the intrusion detection system.
- All logged alarm activity information must be reviewed and resolved.
- One or more cameras must provide continuous (motion activated systems that are separate from the intrusion detection system may be used) monitoring of entry and exit to the physically secure environment. Lighting must exist for the camera images. Recording must be at a minimum of five frames equally every three seconds.
- Use three layers of physical security in the CA facility with increasing levels of access control for each of the following levels:

**Level One Barrier:**

This level consists of the entrance to the facility. The building or secure facility entrance will only allow the entrance of authorised personnel to the facility. A guarded entrance or foyer with a receptionist requires the use of a logbook to register authorised visitors (guests) to the facility.

**Level Two Barrier:**

This level secures the entrance beyond the foyer / reception area to the CA facility. This entrance must be monitored by a video recording system and require secure entry of authorised personnel only. All entry through this barrier must be logged. Single entry into this barrier is allowed. Authorised visitors must be escorted at all times when within this barrier.

**Level Three Barrier:**

This level provides access to the dedicated room housing the CA and signing engines. This entrance requires dual access. Personnel with access must be divided into an “A” group and a “B” group, such that access requires at least one member from each group. The A and B groups should correlate to separate organisational units.

Doors must have locks and all authorised personnel having access through this barrier must have successfully completed a background security check and are assigned resources (staff, dedicated personnel) of the CA operator. Other personnel that require entry to this level must be accompanied by two (2) authorised and assigned resources at all times.

CA Personnel (authorised individuals with a formal PKI role) entering the physically secure CA environment must sign an access logbook. This log must be maintained within the CA room. This logbook must include:

- Name and signature of the individual,
- Participant’s Organisation,
- Date and time in and out,
- Reason for visit.

Visitors (contractors, maintenance personnel, etc.) must also sign an access logbook. In addition to the aforementioned, the logbook for visitor access must include name and signature of the individuals escorting the visitor.

Access to the room creates an audit event, which must be logged. Motion sensors must be in place to activate cameras (if cameras are not recording all activity continually). Invalid access attempts also create audit records, which must be followed up by security personnel.

Automated login and logout enforcement of personnel is required at level three. This level must never be occupied by less than two persons except during the time of login and logout. This period for entrance and egress will not exceed thirty seconds. For time of single occupancy exceeding thirty seconds the system must automatically generate an audit event that must be followed up on by security personnel.

## Annex B

### Key Injection Facilities

This annex contains the specific requirements that apply to key injection facilities. It also provides implementation criteria on how these requirements can be realised. Other implementation methods may be considered, assuming that they provide at least the same level of security.

Unless otherwise stated the requirements detailed in this Annex are in addition to the guidance listed in the main body of this document. For key injection facilities participating in remote key establishment and distribution, requirements in Annex A also apply

### Point of Sale Encryption Device

1	<b>Encryption of account data must be performed in equipment that protects cryptographic keys against physical and logical compromise</b>
<p>Key injection facilities must only inject secret keys into equipment that conforms to the requirements for TRSMs. Key injection platforms and systems that include hardware devices for managing (e.g. generating and storing) the keys must ensure those hardware devices conform to the requirements for TRSMs. This can be realised by performing encryption operations using devices that conform to the requirements for a Tamper-Resistant Security Module (TRSM) as defined in ISO 9564:1, ISO 13491 (all parts) / ANSI X9.97 (all parts) or equivalent. Other implementation methods may be considered; provided it can be proven that they provide at least the same level of security.</p> <p>In the cases where sensitive data or account data is required to travel outside the tamper-resistant enclosure of a cryptographic device, the cryptographic device must encrypt the data directly at the point of entry within the secure cryptographic boundary of the cryptographic device to meet the requirements for compromise prevention. Cryptographic devices in which the cleartext (unencrypted) sensitive data or account data travels over cable or similar media from the point of entry to the cryptographic hardware encryption device do not meet this requirement.</p>	

## Key Management

### Objective 2: Key Generation

**Cryptographic keys used for data field encryption/decryption, and related key management keys, must be created using processes that ensure that it is not possible to predict any key or determine that certain keys are more probable than other keys.**

2	<b>All keys and key components must be generated using an approved random or pseudo-random process</b>
<p>Where the key injection platform includes features that generate keys, those keys must be generated in compliance with the relevant requirements specified in this document.</p> <p>Some key injection platforms may only “import” key components (instead of generating them), and those imported key components must be generated in accordance with the requirements detailed in the main body of these requirements.</p> <p>For key injection facilities participating in remote key establishment and distribution applications the requirements in Annex A also apply.</p>	

3	<b>Compromise of the key-generation process must not be possible without collusion between at least two trusted individuals</b>

Key injection facilities must implement procedures to protect the key generation process such that compromise of a key during its creation is not possible without collusion between at least two trusted individuals. Procedures must be in place to ensure that no one person can singly inject keys into devices. In addition to procedures, physical and logical barriers must exist to prevent and detect compromise of the key generation process.

Some key injection platforms use Personal Computer (PC) based software applications that do not support the use of cryptographic devices for the loading of keys. Such systems have inherent weaknesses that, if exploited, may cause the unauthorised disclosure of components and/or keys. The exploitation of some of the weaknesses could be possible without collusion. Therefore, key injection facilities that use PC-based key loading software platforms that do not support cryptographic devices must at a minimum implement the controls outlined in requirement 10 in this annex.

For Key Injection Facilities participating in remote key establishment and distribution applications, requirements in Annex A also apply.

### **Objective 3: Key Distribution**

#### **Keys must be conveyed or transmitted in a secure manner**

##### **5 | Cryptographic keys must be conveyed or transmitted securely**

Keys conveyed to a key injection facility must be conveyed in compliance with these requirements. Such keys can include, but are not limited to:

- Base Derivation Keys (BDKs) used in the Derived Unique Key Per Transaction (DUKPT) key management method;
- Key Encryption Keys used to encrypt the BDKs when the BDKs are conveyed between entities (e.g. from the BDK owner to a device manufacturer that is performing key injection on their behalf or from a merchant to a third party that is performing key injection on their behalf)
- Master Derivation Keys (MDKs) used to derive unique terminal master keys for devices;
- Terminal Master Keys used in the Master Key/Session Key key management method;
- Data encryption keys used in the fixed transaction key method;
- Public and private key pairs loaded into cryptographic devices for supporting remote key establishment and distribution applications,

- Digitally signed public key(s) that are signed by a device manufacturer's private key and subsequently loaded into a cryptographic device for supporting certain key establishment and distribution applications protocols (if applicable);
- Device manufacturer's authentication key loaded into a cryptographic device for supporting certain key establishment and distribution applications protocols (if applicable)

Keys conveyed from a key injection facility (including facilities that are a device manufacturer) must be conveyed in compliance with these requirements. Such keys can include, but are not limited to:

- Digitally signed HSM authentication public key(s) that are signed by a device manufacturer's private key and subsequently loaded into the HSM for supporting certain key establishment and distribution applications protocols (if applicable),
- Device manufacturer's authentication key loaded into the HSM for supporting certain key establishment and distribution applications protocols (if applicable).

6	<b>Any single unencrypted key component must at all times during its transmission, conveyance, or movement between any two organisational entities be: Under the continuous supervision of a person with authorised access to this component, OR locked in a security container (including tamper evident packaging) in such a way that it can be obtained only by a person with authorised access to it, OR in a physically secure Tamper Resistant Security Module (TRSM)</b>
No additional requirements see requirement 5 in this annex for a list of example keys.	

7	<b>All key encryption keys used to transmit or convey other cryptographic keys must be (at least) as strong as any key transmitted or conveyed</b>
No additional requirements see requirement 5 in this annex for a list of example keys.	
For Key Injection Facilities participating in remote key establishment and distribution applications requirements in Annex A apply.	



**Objective 4: Key Loading**

**Key loading to cryptographic devices must be handled in a secure manner.**

9	<b>Unencrypted secret keys must be entered into cryptographic devices using the principles of dual control and split knowledge</b>
<p>Key injection facilities must load keys (unencrypted secret keys must be loaded as key components) using dual control and split knowledge, see requirement 5 in this annex for a list of example keys.</p> <p>Key injection facilities must implement dual control and split knowledge controls for the loading of keys into equipment. Such controls can include (but are not limited to):</p> <ul style="list-style-type: none"><li>• Physical dual access controls that electronically provide for restricted entry and egress from a room dedicated to key injection such that the badge access system enforces the presence of at least two authorised individuals at all times in the room so that no one person can singly access the key loading equipment. Access is restricted to only appropriate personnel involved in the key loading process.</li><li>• Logical dual control via multiple logins with unique user ids to the key injection platform application such that no one person can operate the application to singly inject cryptographic keys into devices.</li><li>• Key injection platform applications that force the entry of multiple key components and the implementation of procedures that involve multiple key custodians that store and access key components under dual control and split knowledge mechanisms.</li><li>• Demonstrable procedures that prohibit key custodians from handing their components to any other individual for key entry.</li></ul> <p>For Key Injection Facilities participating in remote key establishment and distribution applications requirements in Annex A also apply.</p>	

10	<b>The mechanisms used to load secret keys, such as terminals, external PIN pads, key guns, or similar devices and methods must be protected to prevent any type of monitoring that could result in the unauthorised disclosure of any component</b>
----	--

Key injection facilities must ensure key loading mechanisms are not subject to disclosure of key components or keys.

Some key injection platforms use Personal Computer (PC) based software applications that do not support the use of cryptographic devices for the loading of keys. Such systems have inherent weaknesses that, if exploited, may cause the unauthorised disclosure of components and/or keys. These weaknesses include:

- XOR'ing of key components is performed in software.
- Cleartext keys and components can reside in software during the key loading process.
- Some systems require only a single password.
- Some systems store the keys (e.g. BDKs, TMKs) on removable diskettes or smart cards. These keys are in the clear with some systems.
- PCs, by default, are not managed under dual control. Extra steps (e.g. logical user IDs, physical access controls, etc.) must be implemented to prevent single control of a PC.
- Data can be recorded in the PC's non-volatile storage.
- Software Trojan Horses or keyboard sniffers can be installed on PCs.

Key Injection Facilities that use PC-based key loading software platforms that do not support cryptographic devices must minimally implement the following compensating controls:

PCs must be:

- Stand-alone (i.e., without modems, not connected to a LAN or WAN, not capable of wireless connections, etc.),
- Dedicated to only the key loading function (e.g. there must not be any other application software installed), and
- Located in a physically secure room that is dedicated to key loading activities.

All hardware used in key loading (including the PC) must be managed under dual control. Key injection must not occur unless there are minimally two individuals in the key injection room at all times during the process. If a situation arises that would cause only one person to be in the room, all individuals must exit until at least two can be inside.

PC access and use must be monitored and logs of all key loading must be maintained. These logs must be retained for a minimum of three years or as long as the devices are in use, whichever is longer. (The logs should be able to prove secure key loading for as long as the devices are in service). The logs must be regularly reviewed by an authorised person who does not have access to the room or to the PC. The reviews must be documented. The logs must include but not be limited to:

- Logs of access to the room from a badge access system,
- Logs of access to the room from a manual sign-in sheet,
- User sign-on logs on the PC at the operating system level,
- User sign-on logs on the PC at the application level,
- Logs of the device IDs and serial numbers that are loaded along with the date and time and the individuals performing the key injection,
- Video surveillance logs.

Cable attachments and the PC must be examined before each use to ensure the equipment is free from tampering. The PC must be started from a powered-off position every time key loading activities occur. The software application must load keys without recording any cleartext values on fixed or portable media or other unsecured devices. Cleartext keys must not be stored except within a cryptographic device.

The personnel responsible for the systems administration of the PC (e.g. a Windows Administrator who configures the PC's user IDs and file settings, etc.) must not have authorised access into the room – they must be escorted by authorised key injection personnel, and they must not have user IDs or passwords to operate the key injection application.

The key injection personnel must not have system's administration capability at either the O/S or the application level on the PC. The PC must not be able to boot from external media (e.g. floppies or CDs). It must boot from the hard drive only.

Key injection facilities must cover all openings on the PC that are not used for key injection with security seals that are tamper-evident and serialised. Examples include, but are not limited to, PCMCIA, network, infrared and modem connections on the PC, and access to the hard drive and memory. The seals must be recorded in a log and the log must be maintained along with the other key loading logs in a dual control safe. Verification of the seals must be performed prior to key loading activities.

If the PC application stores keys (e.g. BDKeys or TMKeys) on diskette or IC cards (smart cards or memory cards), the diskette and

smart cards must be secured under dual control when not in use (e.g. in a dual control safe). If possible, instead of storing the key on those media, the key should be manually entered at the start of each key injection session from components that are maintained under dual control and split knowledge (note: for DUKPT implementations, the BDK must be loaded from components each time and this requires manual tracking of the device ID counter and serial numbers from the previous key loading session).

Key injection facilities with PC applications that require passwords to be used to initiate decryption of keys on diskettes or smart cards must ensure the passwords are maintained under dual control and split knowledge. Manufacturer's default passwords for PC-based applications must be changed.

12	<b>The loading of keys or key components must incorporate a validation mechanism such that the authenticity of the keys is ensured and it can be ascertained that they have not been tampered with, substituted, or compromised</b>
----	---

For Key Injection Facilities participating in remote key establishment and distribution applications requirements in Annex A also apply.

## Objective 5: Key Usage

**Keys must be used in a manner that prevents or detects their unauthorised usage.**

15	<b>Procedures must exist to prevent or detect the unauthorised substitution (unauthorised key replacement and key misuse) of one key for another or the operation of any cryptographic device without legitimate keys</b>
----	---

Key injection facilities must implement controls to protect against unauthorised substitution of keys and to prevent the operation of devices without legitimate keys. Examples include but are not limited to:

- All key loading must be performed using dual control and split knowledge. Controls must be in place to prevent and detect

the loading of keys by any one single person. Controls include physical access to the room, logical access to the key loading application, video surveillance of activities in the key injection room, physical access to secret or private cryptographic key components or shares, etc.

- All devices loaded with keys must be tracked at each key loading session by serial number.
- Unloaded devices must be managed in accordance with requirement 26 in the main body of this document.
- Key injection facilities must use something unique about the transaction originating TRSM device (e.g. serial number) when deriving the key (e.g. DUKPT, TMK) injected into it.

For Key injection facilities participating in remote key establishment and distribution applications, requirements in Annex A also apply.

**16 Cryptographic keys must only be used for their sole intended purpose and must never be shared between production and test systems**

Key injection facilities must have a separate test system for the injection of test keys.

- Test keys must not be injected using the production platform and test keys must not be injected into production equipment.
- Production keys must not be injected using a test platform and production keys must not be injected into equipment that is to be used for testing purposes.
- Keys used for signing of test certificates must be test keys.
- Keys used for signing of production certificates must be production keys.

For key injection facilities participating in remote key establishment and distribution applications, requirements in Annex A also apply.

**17 All secret keys present and used for any function must be unique (except by chance) to that device**

Key Injection Facilities must ensure that unique keys are loaded into each device except by chance. The same key(s) must not

be loaded into multiple devices.

Key Injection Facilities that load DUKPT keys must use separate BDKeys for different entities.

Key Injection Facilities that load DUKPT keys for various terminal types for the same entity must use separate BDKeys per terminal type if the terminal IDs can be duplicated among the multiple types of terminals. In other words, the key injection facility must ensure that any one given key cannot be derived for multiple devices except by chance.

For key injection facilities participating in remote key establishment and distribution applications, requirements in Annex A also apply.

## Objective 6: Key Administration

**Keys are administered in a secure manner.**

18	<b>Secret keys used for encrypting data field encryption keys, or for data field encryption, must never exist outside of cryptographic devices, except when encrypted or securely stored and managed using the principles of dual control and split knowledge</b>
----	---

Key injection facilities must ensure that KEKs and secret data encryption keys do not exist outside of cryptographic devices except when encrypted or stored under dual control and split knowledge.

Some key injection platforms use Personal Computer (PC) based software applications that do not support the use of cryptographic devices for the loading of keys. Such systems have inherent weaknesses that, if exploited, may cause the unauthorised disclosure of components and/or keys. The exploitation of some of the weaknesses could be possible without collusion. Therefore, key injection facilities that use PC-based key loading software platforms that do not support cryptographic devices must at a minimum implement the controls outlined in requirement 10 in this annex.

For key injection facilities participating in remote key establishment and distribution applications, requirements in Annex A also apply.

19	<b>Procedures must exist and must be demonstrably in use to replace any known or suspected compromised key and its subsidiary keys (those keys encrypted with the compromised key) to a value not feasibly related to the original key</b>
For key injection facilities participating in remote key establishment and distribution applications, requirements in Annex A also apply.	

22	<b>Access to secret keys and key material must be limited to properly designated key custodians, and their backups, on a need-to-know basis</b>
For key injection facilities participating in remote key establishment and distribution applications, requirements in Annex A also apply.	

25	<b>Documented procedures must exist and must be demonstrably in use for all key administration operations</b>
For key injection facilities participating in remote key establishment and distribution applications, requirements in Annex A also apply.	

### **Objective 7: Device Management**

**Equipment used to process account data and keys must be managed in a secure manner.**

26	<b>Cryptographic devices must be placed into service only if there is assurance that the equipment has not been substituted or subjected to unauthorised modifications or tampering prior to the loading of cryptographic keys</b>
For key injection facilities participating in remote key establishment and distribution applications, requirements in Annex A also apply.	

27	<b>Procedures must exist that ensure the destruction of all cryptographic keys and any account data within any cryptographic devices removed from service</b>
----	---

Key injection facilities must have procedures to ensure keys are destroyed in cryptographic devices removed from service. This applies to any cryptographic device used in the key injection platform, as well as to any devices that have been loaded with keys and securely stored or warehoused on site that are subsequently deemed to be unnecessary and never to be placed into service.

If a key injection facility receives a used device to reload with keys, procedures must ensure that old keys that may be in the device are destroyed prior to loading of new keys. (The used device should have had its keys destroyed when it was removed from service, but this secondary check must be carried out to confirm that the keys were destroyed.)

28	<b>Any cryptographic device capable of encrypting a key and producing cryptograms of that key must be protected against unauthorised use to encrypt known keys or known key components. This protection must take the form of either or both of the following: a) dual access controls are required to enable the key encryption function, b) physical protection of the equipment (e.g. locked access to it) under dual control</b>
----	--

For key injection facilities participating in remote key establishment and distribution applications, requirements in Annex A also apply.

## Glossary

<b>Access Controls</b>	Ensuring that specific objects, functions, or resources can only be accessed by authorised users in authorised ways.
<b>Account Data</b>	At a minimum, account data contains the full PAN and (if present) any elements of sensitive authentication data. The following are also considered to be account data if sent in conjunction with the PAN: cardholder name, expiration date, or service code. Note: truncated, masked and hashed PAN data (with salt) is not considered account data. Encrypted data that satisfies the requirements stated in this guidance document is not considered to be account data.
<b>Algorithm</b>	A clearly specified mathematical process for computation; a set of rules, which, if followed, will give a prescribed result.
<b>ANSI</b>	American National Standards Institute. A U.S. standards accreditation organisation.
<b>Asymmetric cryptography (techniques)</b>	See Public Key Cryptography.
<b>ATM</b>	An unattended terminal that has electronic capability, accepts PINs, and disburses currency or checks.
<b>Authentication</b>	The process for establishing unambiguously the identity of an entity, organisation or person at a specific point in time.
<b>Authorisation</b>	The right granted to a user to access an object, resource or function.
<b>Authorise</b>	To permit or give authority to a user to communicate with or make use of an object, resource or function.
<b>Base (master) derivation key (BDK)</b>	See Derivation key.
<b>Cardholder</b>	An individual to whom a card is issued or who is authorised to use the card.
<b>Cardholder data</b>	At a minimum, cardholder data contains the full PAN. Cardholder data may also appear in the form of the full PAN plus any of the following: <ul style="list-style-type: none"> <li>• Cardholder name</li> <li>• Expiration date</li> <li>• Service Code</li> </ul>

	See <i>Sensitive Authentication Data</i> for additional data elements that may be transmitted or processed as part of a payment transaction.
<b>Certificate</b>	The public key and identity of an entity together with some other information, rendered unforgeable by signing the certificate with the private key of the certifying authority that issued that certificate.
<b>Certificate revocation</b>	The process of revoking an otherwise valid certificate by the entity that issued that certificate. Revoked certificates are placed on a certificate revocation list (CRL) or the information is conveyed using Online Certificate Status Protocol (OCSP) as specified in the product/service specification.
<b>Certificate Revocation List (CRL)</b>	A list of revoked certificates. For example, entities that generate, maintain and distribute CRLs can include the Root or subordinate CAs.
<b>Check value</b>	A computed value which is the result of passing a data value through a non-reversible algorithm. Check values are generally calculated using a cryptographic transformation which takes as input a secret key and an arbitrary string, and which gives a cryptographic check value as output. The computation of a correct check value without knowledge of the secret key shall not be feasible.
<b>Ciphertext</b>	Data in its encrypted form.
<b>Cleartext</b>	See Plaintext.
<b>Compromise</b>	In cryptography, the breaching of secrecy and/or security. A violation of the security of a system such that an unauthorised disclosure of sensitive information may have occurred. This includes the unauthorised disclosure, modification, substitution, or use of sensitive data (including plaintext cryptographic keys and other keying material).
<b>Computationally infeasible</b>	The property that a computation is theoretically achievable but is not feasible in terms of the time or resources required to perform it.
<b>Credentials</b>	Identification data for an entity, incorporating at a minimum the entity's distinguished name and public key
<b>Critical Security Parameters (CSP)</b>	Security-related information (e.g. cryptographic keys, authentication data such as passwords and PINs) appearing in plaintext or otherwise unprotected form and whose disclosure or modification can compromise the security of a TRSM or the security of the information protected by the device.

<b>Cryptographic boundary</b>	An explicitly defined continuous perimeter that establishes the physical bounds of a cryptographic module and contains all the hardware, software, and/or firmware components of a cryptographic module.
<b>Cryptographic key</b>	A parameter used in conjunction with a cryptographic algorithm that determines: <ul style="list-style-type: none"> <li>• The transformation of plaintext data into ciphertext data,</li> <li>• The transformation of ciphertext data into plaintext data,</li> <li>• A digital signature computed from data,</li> <li>• The verification of a digital signature computed from data,</li> <li>• An authentication code computed from data, or</li> <li>• An exchange agreement of a shared secret.</li> </ul>
<b>Cryptographic key component</b>	A parameter used in conjunction with other key components in an approved security function to form a plaintext cryptographic key or perform a cryptographic function.
<b>Data Encryption Algorithm (DEA)</b>	A published encryption algorithm used to protect critical information by encrypting data based upon a variable secret key. The Data Encryption Algorithm is defined in <b>ANSI X3.92: Data Encryption Algorithm</b> for encrypting and decrypting data. The algorithm is a 64-bit block cipher that uses a 64-bit key, of which 56 bits are used to control the cryptographic process and 8 bits are used for parity checking to ensure that the key is transmitted properly.
<b>Data Encryption(encipherment or exchange) Key (DEK)</b>	A cryptographic key that is used for the encryption or decryption of account data.
<b>Decipher</b>	See Decrypt.
<b>Decrypt</b>	A process of transforming ciphertext (unreadable) into plain text (readable).
<b>Derivation key</b>	A cryptographic key, which is used to cryptographically compute another key. A derivation key is normally associated with the DUKPT key management method. Derivation keys are normally used in a transaction-receiving (e.g. acquirer) TRSM in a one-to-many relationship to derive or decrypt the Transaction (the derived keys) Keys used by a large number of originating (e.g. terminals) TRSMs.
<b>DES</b>	Data Encryption Standard (see Data Encryption Algorithm). The National Institute of Standards and Technology Data Encryption Standard, adopted by the U.S. government as Federal Information

	Processing Standard (FIPS) Publication 46, which allows only hardware implementations of the data encryption algorithm.
<b>Digital signature</b>	The result of an asymmetric cryptographic transformation of data that allows a recipient of the data to validate the origin and integrity of the data and protects the sender against forgery by third parties or the recipient.
<b>Double-length key</b>	A cryptographic key having a length of 112 active bits plus 16 parity bits, used in conjunction with the TDES cryptographic algorithm.
<b>Dual control</b>	A process of using two or more separate entities (usually persons), who are operating in concert, to protect sensitive functions or information. Both entities are equally responsible for the physical protection of materials involved in vulnerable transactions. No single person must be able to access or to use the materials (e.g. cryptographic key). For manual key generation, conveyance, loading, storage, and retrieval, dual control requires split knowledge of the key among the entities. Also see “split knowledge.”
<b>DUKPT</b>	Derived Unique Key Per Transaction: a key management method that uses a unique key for each transaction, and prevents the disclosure of any past key used by the transaction originating TRSM. The unique Transaction Keys are derived from a base derivation key using only non-secret data transmitted as part of each transaction.
<b>EEPROM</b>	Electronically-Erasable Programmable Read-Only Memory.
<b>Electronic key entry</b>	The entry of cryptographic keys into a TRSM in electronic form using a key-loading device. The user entering the key may have no knowledge of the value of the key being entered.
<b>Encipher</b>	See Encrypt.
<b>Encrypt</b>	The (reversible) transformation of data by a cryptographic algorithm to produce ciphertext, i.e., to hide the information content of the data.
<b>Encrypting PIN Pad (EPP)</b>	A device for secure PIN entry and encryption in an unattended PIN acceptance device. An EPP may have a built in display or card reader, or rely upon external displays or card readers installed in the unattended device. An EPP is typically used in an ATM or other unattended device (e.g. an unattended kiosk or automated fuel dispenser) for PIN entry and is controlled by a device controller. An EPP has a clearly defined physical and logical boundary, and a tamper resistant or tamper evident

	shell.
<b>EPROM</b>	Erasable Programmable Read-Only Memory.
<b>Exclusive-OR</b>	Binary addition without carry, also known as modulo 2 addition, symbolised as “XOR” and defined as: <ul style="list-style-type: none"> <li>• <math>0 + 0 = 0</math></li> <li>• <math>0 + 1 = 1</math></li> <li>• <math>1 + 0 = 1</math></li> <li>• <math>1 + 1 = 0</math></li> </ul>
<b>FIPS</b>	Federal Information Processing Standard.
<b>Firmware</b>	The programs and data (i.e., software) permanently stored in hardware (e.g. in ROM, PROM, or EPROM) such that the programs and data cannot be dynamically written or modified during execution. Programs and data stored in EEPROM are considered as software.
<b>Hardware (Host) Security Module (HSM)</b>	A physically and logically protected hardware device that provides a secure set of cryptographic services.
<b>Hash function</b>	A (mathematical) function which takes any arbitrary length message as input and produces a fixed length output. It must have the property that it is computationally infeasible to discover two different messages, which produce the same hash result. It may be used to reduce a potentially long message into a “hash value” or “message digest” which is sufficiently compact to be input into a digital signature algorithm.
<b>Initialisation Vector</b>	A binary vector used as the input to initialise the algorithm for the encryption of a plaintext block sequence to increase security by introducing additional cryptographic variance and to synchronise cryptographic equipment. The initialisation vector need not be secret.
<b>Integrity</b>	Ensuring consistency of data; in particular, preventing unauthorised and undetected creation, alteration, or destruction of data.
<b>Interface</b>	A logical section of a TRSM that defines a set of entry or exit points that provide access to the device, including information flow or physical access.
<b>Irreversible transformation</b>	A non-secret process that transforms an input value to produce an output value such that knowledge of the process and the output value does not feasibly allow the input value to be determined.
<b>ISO</b>	International Organisation for Standardisation. An international standards accreditation organisation.

<b>Issuer</b>	The institution holding the account identified by the primary account number (PAN).
<b>Key</b>	See Cryptographic key.
<b>Key agreement</b>	A key establishment protocol for establishing a shared secret key between entities in such a way that neither of them can predetermine the value of that key. That is, the secret key is a function of information contributed by two or more participants.
<b>Key backup</b>	Storage of a protected copy of a key during its operational use.
<b>Key component</b>	See Cryptographic Key Component.
<b>Key derivation process</b>	A process, which derives one or more session keys from a shared secret and (possibly) other public information.
<b>Key destruction</b>	Occurs when an instance of a key in one of the permissible key forms no longer exists at a specific location.
<b>Key Distribution Host (KDH)</b>	A KDH is a processing platform used in conjunction with HSM(s) that generates keys and securely distributes those keys to TRSMs and the financial processing platform communicating with those TRSMs. A KDH shall not be used for certificate issuance, and must not be used for the storage of CA private keys.
<b>Key encrypting (encipherment or exchange) key (KEK)</b>	A cryptographic key that is used for the encryption or decryption of other keys.
<b>Key establishment</b>	The process of making available a shared secret key to one or more entities. Key establishment includes key agreement and key transport.
<b>Key generation</b>	Creation of a new key for subsequent use.
<b>Key instance</b>	The occurrence of a key in one of its permissible forms, i.e., plaintext key, key components, encrypted key.
<b>Key loading</b>	Process by which a key is manually or electronically transferred into a TRSM.
<b>Key loading device</b>	A self-contained unit that is capable of storing at least one plaintext or encrypted cryptographic key or key component that can be transferred, upon request, into a cryptographic module.
<b>Key management</b>	The activities involving the handling of cryptographic keys and other related security parameters (e.g. initialisation vectors, counters) during the entire life cycle of the keys, including their generation, storage, distribution, loading and use, deletion, destruction and archiving.
<b>Key pair</b>	A key pair comprises the two complementary keys for use with an asymmetric encryption algorithm.

	One key, termed the public key is expected to be widely distributed; and the other, termed the private key, is expected to be restricted so that it is only known to the appropriate entities.
<b>Key replacement</b>	Substituting one key for another when the original key is known or suspected to be compromised or the end of its operational life is reached.
<b>Key (secret) share</b>	Related to a cryptographic key generated such that a specified fraction of the total shares of such parameters can be combined to form the cryptographic key but such that less than a specified fraction does not provide any information about the key.
<b>Key storage</b>	Holding of the key in one of the permissible forms.
<b>Key transport</b>	A key establishment protocol under which the secret key is determined by the initiating party and transferred suitably protected.
<b>Key usage</b>	Employment of a key for the cryptographic purpose for which it was intended.
<b>Key variant</b>	A new key formed by a process (which need not be secret) with the original key, such that one or more of the non-parity bits of the new key differ from the corresponding bits of the original key.
<b>Keying material</b>	The data (e.g. keys and initialisation vectors) necessary to establish and maintain cryptographic keying relationships.
<b>Manual key loading</b>	The entry of cryptographic keys into a TRSM from a printed form, using devices such as buttons, thumb wheels or a keyboard.
<b>Master derivation key (MDK)</b>	See Derivation key.
<b>Master key</b>	In a hierarchy of Key Encrypting Keys and Transaction Keys, the highest level of Key Encrypting Key is known as a Master Key.
<b>Message</b>	A communication containing one or more transactions or related information.
<b>Node</b>	Any point in a network that does some form of processing of data, such as a terminal, acquirer, or switch.
<b>Non-reversible transformation</b>	See Irreversible Transformation.
<b>OCSP</b>	See Online Certificate Status Protocol.
<b>Online Certificate Status Protocol</b>	The Online Certificate Status Protocol (OCSP) enables applications to determine the (revocation) state of an identified certificate. OCSP may be used to satisfy some of the operational requirements of providing more timely revocation information than is possible with CRLs and may also be used to obtain additional status information.

	An OCSP client issues a status request to an OCSP responder and suspends acceptance of the certificate in question until the responder provides a response.
<b>Out-of-band notification</b>	Notification using a communication means independent of the primary communications means.
<b>Password</b>	A string of characters used to authenticate an identity or to verify access authorisation.
<b>Physical protection</b>	The safeguarding of a cryptographic module, cryptographic keys, or other keying materials using physical means.
<b>Physically secure environment</b>	An environment that is equipped with access controls or other mechanisms designed to prevent any unauthorised access that would result in the disclosure of all or part of any key or other secret data stored within the environment. Examples include a safe or purpose built room with continuous access control, physical security protection, and monitoring.
<b>PIN Entry Device (PED)</b>	A PED is a device for secure PIN entry and processing. The PED typically consists of a keypad for PIN entry, laid out in a prescribed format, a display for user interaction, a processor and storage for PIN processing sufficiently secure for the key management scheme used and firmware. A PED has a clearly defined physical and logical boundary and a tamper resistant or tamper evident shell.
<b>Plaintext</b>	Intelligible data that has meaning and can be read or acted upon without the application of decryption. Also known as cleartext.
<b>Plaintext key</b>	An unencrypted cryptographic key, which is used in its current form.
<b>Point-of-Interaction</b>	See Point of Transaction.
<b>Point-of-Transaction</b>	The physical location where a Merchant or Acquirer (in a Face-to-Face Environment) or an Unattended Acceptance Terminal (in an Unattended Environment) completes a Transaction Receipt.
<b>Private key</b>	A cryptographic key, used with a public key cryptographic algorithm that is uniquely associated with an entity and is not made public.  In the case of an asymmetric signature system, the private key defines the signature transformation. In the case of an asymmetric encryption system, the private key defines the decryption transformation.
<b>PROM</b>	Programmable Read-Only Memory.
<b>Pseudo-random</b>	A value that is statistically random and essentially

	random and unpredictable although generated by an algorithm.
<b>Public key</b>	<p>A cryptographic key, used with a public key cryptographic algorithm, uniquely associated with an entity, and that may be made public</p> <p>In the case of an asymmetric signature system, the public key defines the verification transformation. In the case of an asymmetric encryption system, the public key defines the encryption transformation. A key that is 'publicly known' is not necessarily globally available. The key may only be available to all members of a pre-specified group.</p>
<b>Public key (asymmetric) cryptography</b>	<p>A cryptographic technique that uses two related transformations, a public transformation (defined by the public key) and a private transformation (defined by the private key). The two transformations have the property that, given the public transformation, it is not computationally feasible to derive the private transformation.</p> <p>A system based on asymmetric cryptographic techniques can either be an encryption system, a signature system, a combined encryption and signature system, or a key agreement system.</p> <p>With asymmetric cryptographic techniques, there are four elementary transformations: sign and verify for signature systems, and encrypt and decrypt for encryption systems. The signature and the decryption transformation are kept private by the owning entity, whereas the corresponding verification and encryption transformations are published. There exists asymmetric cryptosystems (e.g. RSA) where the four elementary functions may be achieved by only two transformations: one private transformation suffices for both signing and decrypting messages, and one public transformation suffices for both verifying and encrypting messages. However, this does not conform to the principle of key separation and where used the four elementary transformations and the corresponding keys should be kept separate.</p>
<b>Random</b>	The process of generating values with a high level of entropy and which satisfy various qualifications, using cryptographic and hardware based 'noise' mechanisms. This results in a value in a set that has equal probability of being selected from the total population of possibilities, hence unpredictable.
<b>ROM</b>	Read-Only Memory.
<b>Root Certification Authority (RCA)</b>	The RCA is the top level Certification Authority in a

	Public Key Infrastructure. A RCA is a CA which signs its own public key with the associated private key. RCAs only issue certificates to subordinate CAs. Root CAs do not issue certificates directly to KDHs, EPPs or PEDs. RCAs may also issue certificate status lists for certificates within its hierarchy.
<b>Secret key</b>	A cryptographic key, used with a secret key cryptographic algorithm that is uniquely associated with one or more entities and should not be made public.
<b>Secure Cryptographic Device</b>	See TRSM
<b>Sensitive authentication data</b>	Security-related information (card validation codes/values, full track data from the magnetic stripe, magnetic-stripe image on the chip or elsewhere, PINs, and PIN blocks) used to authenticate cardholders, appearing in plain-text or otherwise unprotected form.
<b>Sensitive data</b>	Data which must be protected against unauthorised disclosure, alteration or destruction, especially cardholder data, sensitive authentication data and cryptographic keys, and includes design characteristics, status information, and so forth.
<b>Session key</b>	A key established by a key management protocol, which provides security services to data transferred between the parties. A single protocol execution may establish multiple session keys, e.g. an encryption key and a MAC key.
<b>Shared Secret</b>	The secret information shared between parties after protocol execution. This may consist of one or more session key(s), or it may be a single secret that is input to a key derivation function to derive session keys.
<b>Single-length key</b>	A cryptographic key having a length of 56 active bits plus 8 parity bits used in conjunction with the DES cryptographic algorithm.
<b>Software</b>	The programs and associated data that can be dynamically written and modified.
<b>Split knowledge</b>	A condition under which two or more entities separately have key components, which individually convey no knowledge of the resultant cryptographic key.
<b>Subordinate CA and Superior CA</b>	If one CA issues a certificate for another CA, then the issuing CA is termed the superior CA, and the certified CA is termed the subordinate CA. Subordinate CAs are typically used to segment risk. Subordinate CAs may issue certificates to KDHs, TRSMs. Subordinate CAs may also issue certificates to lower level CAs and issue certificate

	status lists regarding certificates the subordinate CA has issued.
<b>Symmetric key</b>	A cryptographic key that is used in symmetric cryptographic algorithms. The same symmetric key that is used for encryption is also used for decryption.
<b>System software</b>	The special software (e.g. operating system, compilers or utility programs) designed for a specific computer system or family of computer systems to facilitate the operation and maintenance of the computer system, programs, and data.
<b>Tamper-evident</b>	A characteristic that provides evidence that an attack has been attempted.
<b>Tamper-resistant</b>	A characteristic that provides passive physical protection against an attack.
<b>Tamper-responsive</b>	A characteristic that provides an active response to the detection of an attack, thereby preventing a success.
<b>Tampering</b>	The penetration or modification of internal operations and/or insertion of active or passive tapping mechanisms to determine or record secret data.
<b>TDEA</b>	See Triple Data Encryption Algorithm
<b>Terminal</b>	A device/system that initiates a transaction.
<b>Transaction</b>	A series of messages to perform a predefined function.
<b>Triple Data Encryption Algorithm (TDEA)</b>	The algorithm specified in ANSI X9.52, Triple Data Encryption Algorithm Modes of Operation.
<b>Triple Data Encryption Standard (TDES)</b>	See Triple Data Encryption Algorithm.
<b>Triple-length key</b>	A cryptographic key having a length of 168 active bits plus 24 parity bits, used in conjunction with the TDES cryptographic algorithm.
<b>TRSM</b>	Tamper-Resistant Security Module: the set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes (including cryptographic algorithms and key generation) and is contained within the cryptographic boundary. Also known as a secure cryptographic device.
<b>Trustworthy system</b>	Computer hardware and software which: <ul style="list-style-type: none"> <li>• are reasonably secure from intrusion and misuse;</li> <li>• provide a reasonable level of availability, reliability, and correct operation; and</li> <li>• are reasonably suited to performing their intended functions.</li> </ul>

<b>Unattended Acceptance Terminal (UAT)</b>	See Unattended Payment Terminal
<b>Unattended Payment Terminal (UPT)</b>	A cardholder-operated device that reads, captures, and transmits card information in an Unattended Environment, including, but not limited to, the following: <ul style="list-style-type: none"> <li>• ATM</li> <li>• Automated Fuel Dispenser</li> <li>• Ticketing Machine</li> <li>• Vending Machine</li> </ul>
<b>Unprotected memory</b>	Components, devices and recording media that retain data for some interval of time that reside outside the cryptographic boundary of a TRSM.
<b>Variant of a key</b>	A new key formed by a process (which need not be secret) with the original key, such that one or more of the non-parity bits of the new key differ from the corresponding bits of the original key.
<b>Verification</b>	The process of associating and/or checking a unique characteristic.
<b>Working key</b>	A key used to cryptographically process the transaction. A Working Key is sometimes referred to as a Data Key, communications key, session key, or transaction key.
<b>XOR</b>	See Exclusive-Or.
<b>Zeroise</b>	The degaussing, erasing, or overwriting of electronically stored data so as to prevent recovery of the data.