EPC020-08 12.12.2013

(Vol Ref. 7.4.1.00)

SEPA CARDS STANDARDISATION (SCS) "VOLUME"

BOOK 4

SECURITY REQUIREMENTS

PART OF THE APPROVED VERSION OF SCS VOLUME V7.0

Payments and Cash withdrawals with Cards in SEPA

Applicable Standards and Conformance Process

Volume v7.0 and its constituent Books supersede the SEPA Cards Standardisation Volume v6.0.

Abstract	This document contains the work on SEPA cards standardisation to date
Document Reference	EPC020-08
Issue	Book 7.4.1.00
Date of Version	12 December 2013
Reason for Issue	Publication
Reviewed	Approved for publication by the EPC Plenary of 12 December 2013 and endorsed by the CSG GM of 7 November 2013
Produced by	CSG Secretariat
Owned and Authorised by	EPC
Circulation	Public

Table of Contents

1 GENERAL

1.1 Book 4 - Executive summary

1.1.1 Scope

Following the restructuring of the 'SEPA Cards Standardisation Volume' Book of Requirements into separate work books, the section which deals with security aspects has been moved into what has now become Book 4. Please note that this book is focused on the security requirements for components of card payments systems. For other aspects such as functionality, interoperability and especially certification, readers must consult the relevant book within the Volume.

In creating Book 4, all the content has been fully reviewed, revised and expanded compared to the previous Volume chapter 5. This marks both the move towards alignment with Global Standards and the expansion of the security requirements definition beyond that of the POI to include security requirements for other components involved in the card payment chain such as:

- Contact Cards and Contactless Cards irrespective of form factor
- PIN security
- Data protection
- Transaction protection
- HSM (Hardware Security Module)

In expanding Book 4 on security requirements the aim has been to avoid generating new requirements unnecessarily and to include and reference existing standards and sets of requirements where these adequately address a particular area.

This book contains the high level requirements and not the methodology to be used to evaluate conformance with these requirements. This book contains only requirements for face to face transactions.

Vendors wishing to design, develop and submit a POI product for assessment against the requirements of this book will do so as described in Section 2.6.2, choosing the applicable sections of the book and appropriate criteria to apply to the product in question. This approach avoids the repetition for example of a 'Core' section which may apply to a number of different elements.

1.1.2 Out of Scope

Remote transactions are considered out of scope for this release of Book 4.

1.2 Description of changes since the last version of Book 4

This is the first version of Book 4.

2 SECURITY REQUIREMENTS

2.1 Introduction

The definition of Security Requirements is critical for all stakeholders, as they directly contribute to the level of trust and certainty that is expected from payments and with cards.

This chapter defines security requirements for:

- Cardholder data and PIN
- Terminal to Acquirer protocol
- Cards (including contactless)
- POI and HSM

which, where applicable, must be adhered to for a stakeholder to proclaim a product or service to be conformant with the Volume.

2.2 Cardholder Data Security Requirements

The Payment Card Industry Data Security Standard (PCI DSS) is the established baseline for protecting cardholder account data for all acceptance environments.

However, the degree to which the standard applies to a particular environment is to be determined by the different card schemes which will be supported in that payment context. Schemes may accept equivalent security services to meet the intent of the standard.

The position will be reviewed on an on-going basis upon not only the widespread global adoption and use of EMV approved Chip cards, but also the development of a robust authentication process for Card-Not Present (CNP) transactions that will keep cardholder account data secure.

2.3 Security Requirements Applicable to Terminal to Acquirer Protocols

Authenticity and integrity of data in all card payment messages are required to protect the financial system. The mechanism for this is to use cryptographic techniques[1]. These techniques can be applied to specific data elements in a message or to the message in its entirety. These security requirements apply in respect of both payment and terminal management. The protocol specification providers and terminal management suppliers will define the appropriate security requirements for their messages within their protocols to

[1] EPC342-08 Guidelines on algorithms usage and key management v2.0

provide authenticity and integrity in accordance with this Book. Card schemes may choose to accept the security provided by a terminal to acquirer protocol that meets their specific risk requirements.

2.4 PIN Security Requirements

When the PIN is entered and processed, it needs to be protected using the appropriate security standards as defined in PCI PIN Security Requirements and the other standards referenced therein.

ISO 9564 is the established baseline for protecting PINs during online transmission. The PIN should be protected by an ISO PIN block format.

For online transactions, PINs must be formatted according to ISO 9564–1 PIN block formats 0, 1 or 3 prior to encryption and must be encrypted. For format 0, a unique key per transaction is required. Format 1 should be avoided when the PAN is available.

Format 2 must only be used for PINs that are submitted from the ICC reader or the PED, to the ICC chip. If the PIN-block is sent encrypted to the ICC it shall be formatted in an encryption block according to ISO 9564, prior to encryption.

PINs enciphered using ISO format 0 or ISO format 3 must not be translated into any other PIN-block format other than ISO format 0 or ISO format 3. PINs enciphered using ISO format 1 may be translated into ISO format 0 or ISO format 3, but must not be translated back into ISO format 1.

If random values are not used unique key methods must be applied Such methods may involve the use of uni-directional, dynamic session keys (i.e. must not involve the use of fixed transaction keys). This applies to POI–to-Host and is recommended for Host-to-Host communication.

PIN encryption from the POI to the Issuer is a mandatory requirement for all online-to-issuer PIN transactions, in particular:

- The PIN must be encrypted inside a TRSM (PIN pad or PED) where the PIN is entered by the customer;
- The PIN must be translated from one cryptographic zone to another, inside an approved hardware security module (HSM) at a non-issuer host system, e.g. merchant and acquiring host.

2.5 Security Requirements For Cards

This section describes the generic security requirements for Smart Cards. The current section details the following:

- Scope of Evaluation, outline what parts & functions of the Smart Card are to be evaluated;
- Security Objectives & Assurance Level, outline of main security requirements.

To understand how this section can be used and what is required for a security evaluation of a Smart Card, refer to Book 5, which describes the requirements for Evaluation and the Certification Methodology.

2.5.1 Scope of the Evaluation

The Target of Evaluation includes all hardware and software components (including Payment Application) of the EMV card, needed to perform the payment functionality and to enforce its security. All other applications (payment or non-payment) and parts of the operating system are out of the scope of this evaluation.

Payment Application functionality, can consist of transactions and possibly card management functions, as specified by each payment scheme, or be designed as a multi Scheme payment application. In either case, it is assumed that the Smart Card will support the following basic EMV capabilities:

- Application Selection (at card level);
- Initiate Application Processing;
- Off-line communication with the terminal;
- Off-line Data Authentication (static or dynamic if the card supports dynamic RSA computation);
- On-line Authentication and communication with the issuer;
- Cardholder Verification (typically by PIN comparison);
- Card Action Analysis (card internal risk management);
- Transaction Certification;
- Script Processing (to update Payment Application parameters and software);
- Internal State Management, ensuring that the above functions are performed in a coherent way.

The following security requirements can be used to evaluate any Smart Card that supports the basic capabilities listed above. The Security Requirements can also be used for a Payment Application that supports only a subset of those basic capabilities. However it will be necessary for the card issuer and/or application developer to provide a clear description of options to be evaluated in these cases.

Considering that the EMV standard has been chosen for the migration to Chip and PIN in SEPA, EMV specifications are taken as a generic model for Payment Application functionality. Smart Card functionality is therefore modelled on the typical EMV transaction flow. The figure below shows the architecture and components on a typical multi-application Smart Card.

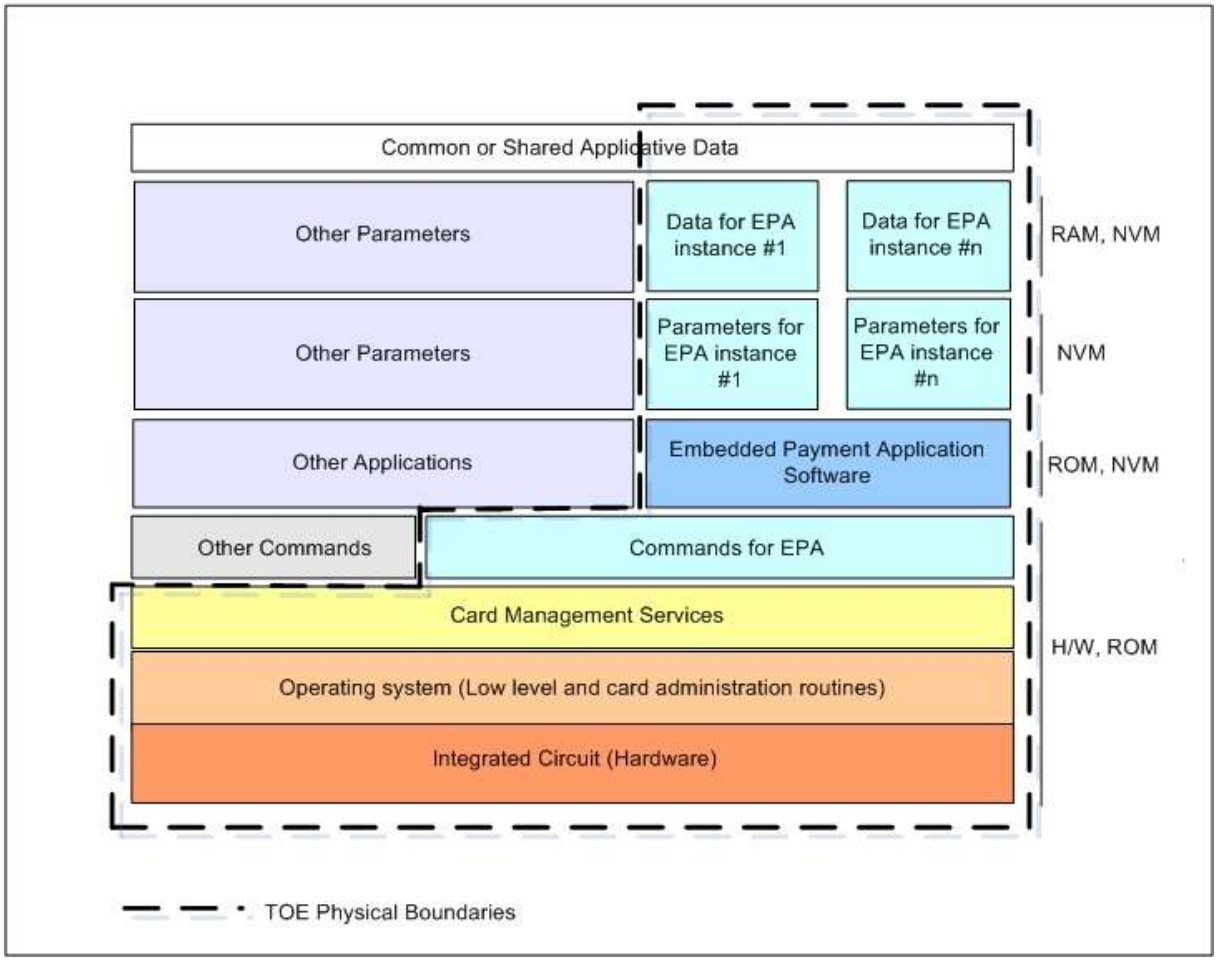

FIGURE 1: FINANCIAL PRESENTMENT

In this figure, the Embedded Payment Application software and data parameters (the Payment Application) are set on a platform comprising a Payment Application command library, relying on low-level software and then IC hardware. Instances of Payment Application applications are defined by a set of personalization data. Some Payment Application data may be shared with other applications (e.g. a global PIN).

The Smart Card encompasses all layers and embedded resources contributing to Payment Application functionality. Most banking smart cards may operate more than one application. In this case, all other applications fall outside the chip card perimeter, but stay within the chip card environment, so the evaluator can assess their impact on Payment Application security.

There is no restriction on card technology (mono- or multi- applicative, native or interpreted software, burnt or downloaded software), provided that all security requirements expressed in the following sections, and mainly focusing on Payment Application functionality, are met.

2.5.2 Chip Card Security Requirements

Security Objectives are high-level, free-text expression of main security requirements.

Assurance Level indicates the expected resistance of security features implemented by the card in order to meet its security objectives.

2.5.2.1 Security objectives

The following Security Objectives have to be met:

TP	**TRANSACTION PROTECTION** **The Smart Card enforces generation of unique certificates binding its users, following the transaction flow as defined by Payment Application specifications (e.g. [EMV])**	
TP1	O.GENUINE_ TRANSACTION_ONCE	The probability that two transaction certificates generated by a genuine Smart Card, including authentication certificates, transaction certificates, authorisation certificates…are equal must be very low. This is related to having genuine "unique" transactions.
TP2	O.TRANSACTION_BINDING	Transactions using offline PIN Verification must bind the cardholder. Transactions cannot be modified at the advantage of an attacker; certified terms of the transactions must not be modified, and transactions must not be modified such they can be denied.
TP3	O.INTENDED_TRANSACTION_FLOW	The normal Transaction flow as defined by the [Payment Application] specifications must be followed and any attempt at bypassing expected transaction steps shall be detected.
TP4	O.EXHAUSTIVE_PARAMETERS	The Smart Card must be secure for all the possible values of parameters.
SUA	**SMART CARD AUTHENTICATION AND CARDHOLDER VERIFICATION** **The Smart Card provides means for its authentication and can enforce cardholder verification, to prevent forgery and identity usurpation.**	
SUA1	O.AUTH	The Smart Card services must be protected from transaction forgery by ensuring Smart Card authentication during the processing of each payment transaction.

SUA2	O.CH_VER	When required by the transaction flow, the Smartcard shall verify the Cardholder. For PIN verification by the Card, the following apply: – Systematic counting to identify verification failure – Secure authentication invalidation when PIN is blocked – Secure authentication validation when PIN comparison succeeds
SUA3	O.ISSUER_AUTH	The Smart Card shall ensure the authentication of the Payment Application Issuer while processing any on-line transaction: – Non-repeatability of the authentication – Systematic script and transaction reject when Issuer cryptogram is invalid Secure transaction validation when Issuer cryptogram is valid, for both script processing and online authorisation processing.
SUA4	O.CARD_MANAGER	Card Management processing is authorised to the authenticated Payment Application Card Manager.
EP	**EXECUTION PROTECTION** **The Smart Card enforces protection of its services against service denial or corruption.**	
EP1	O.OPERATE	The Smart Card must ensure the continued operation of its services: Payment Application services and embedded payment application resources shall be available under normal conditions of use of the Smart Card.
EP2	O.ISOLATION	The Smart Card shall ensure isolation between the Payment Application and all other application(s) on the card, such that no other application can read or modify any Payment Application data.
DP	**DATA PROTECTION** **The Smart Card protects sensitive data from corruption and disclosure when required.**	
DP1	O.SECRECY	The Smart Card shall ensure that the storage and the manipulation of its sensitive

		information are protected against unauthorised disclosure (to users and embedded applications out of the TOE): – Payment Application Reference PIN – Payment Application Transaction PIN – Payment Application Keys
DP2	O.INTEGRITY	The Smart Card shall ensure that sensitive information managed or manipulated by the Smart Card is securely protected against any corruption or unauthorised modification: – Payment Application Cardholder Account Number – Payment Application Reference PIN – Payment Application Keys – Payment Application Card Secure Counters – Payment Application Selection Parameters – Payment Application Card Transaction Parameters – Payment Application Card Transaction Data – Payment Application Issuer Transaction Parameters – Payment Application Code – Payment Terminal Transaction Data when operated by the Smart Card
DP3	O.CRYPTO	The Payment Application keys and Payment Application reference PIN must be protected from potential exploitation of implementation security weaknesses that would lead to their values being determined and obtained.

SP	**SERVICES PROTECTION** **The Smart Card enforces its own security policy to prevent provided services from being attacked.**	
SP1	O.RISK_MNGT	The Smart Card shall ensure Card Risk Management: – Systematic counting of transactions (ATC) to prevent from replay – Secure verification of the ATC during the following transaction phases: ○ "Data Authentication" ○ "Card Action Analysis"
SP2	O.EPA_ISSUER	The Smart Card shall ensure that the issuer of the Payment Application is the only external user able to access the services for Smart Card parameter modification: – Payment Application Reference PIN, – Payment Application Keys, – Payment Application Selection Parameters, – Payment Application Card Transaction Parameters
SP3	O.DETECTION	The Smart Card shall administrate the detection of security violations: corruption of sensitive card content, access to restricted area, or improper conditions of use of the Smart Card. *Application note: the Smart Card will, for example, provide feedback to the Payment Application Issuer or the Card Manager, log the error, terminate the card, or block the embedded payment application.*

TABLE 2: SECURITY OBJECTIVES

2.5.2.2 *Assurance level*

Assurance gives grounds for confidence that a product meets its security objectives. The evaluation methodology will provide assurance through an evaluation of the product in order to determine its security properties. Higher assurance results from a need to undertake a greater evaluation effort, through a broader scope, a greater attention to fine details or a more robust evaluation process.

The assurance level to be associated with the Security Objectives listed above for Smart Cards shall be equivalent to the assurance package defined as EAL4 in the Common Criteria methodology[2]. Nevertheless an EAL4 set of assurance requirements shall be augmented respecting the following criteria:

Type of assurance augmentation	**Description**
Life Cycle Support _ Sufficiency of security measures.[3]	The developer is required to take sufficient measures to ensure integrity and/or authenticity of the product at development time and throughout secure deliveries during product life-cycle (e.g. to chip embedder, card initialiser, card personaliser…)
Vulnerability Analysis Advanced Methodical Vulnerability Analysis.[4]	It is the highest possible level for vulnerability analysis and penetration testing. It requires the card to resist all CC-referenced attacks on Smart Cards, either through software, hardware or combination of both. It is traditionally labelled as "*highly resistant*"

TABLE 3: EAL4 ASSURANCE CRITERIA

The assurance requirements should be split in two packages, one for the Smart Card itself and one for its development environment, allowing for separate package assessment. However, both assessments must be combined in order to demonstrate conformance to the whole set of requirements.

[2] Common Criteria Part 3 contains a catalogue of Security Assurance Requirements (SAR) and defines a set of Evaluation Assurance levels (EAL) numbered from 1 to 7, each level containing more or higher Security Assurance Requirements than the one before.

[3] ALC_DVS.2 (Life Cycle Support up to level 2)

[4] AVA_VAN.5 (vulnerability analysis up to level 5)

2.5.3 Contactless Card Security Requirements

For Contactless Cards the Security Objectives from paragraph 2.5.2.1 apply. In addition, the following Security Objectives are defined for Contactless Cards.

CC	Contactless Cards	
CC1	O.DI_CONTACTLESS_COUNTERS	When required by applicative specifications, DI (Dual Interface) cards must manage internal counters such as counters limiting their use in contactless mode without PIN verification (e.g. unitary and cumulated amounts). DI cards must protect them to the same level as they do for sensitive counters such as transaction count (ATC) or PIN tries count (PTC). The integrity and their capability must not allow them to be bypassed.
CC2	O.DI_PRIVACY	Some personal data present on the Contact part of the card (e.g. Cardholder Name, Log File) must not be exchanged through contactless transactions.
CC3	O.DI_DOS	DI cards must not be blocked, e.g. when receiving a series of wrong APDU-Commands, and must still continue to answer with an Error code in the APDU response.

TABLE 4: CONTACTLESS CARDS SECURITY REQUIREMENTS

Evaluation Policy:

For a card implementing a contactless interface, the evaluation methodology and assurance level shall comply with: “EAL4 +”. The + stands for AVA_VAN.5 and ALC_DVS.2

Evaluation schemes should include the Radio-Frequency (RF) channel as possible fault injection and leakage vectors.

2.5.4 Contactless Security Requirements for Mobile

A Mobile Contactless Payment (MCP) is initiated by an application residing within the Secure Element (SE), performing the payment functions related to an MCP, as dictated by the MCP issuer.

For Mobile Contactless Payments the Security Objectives from paragraph 2.5.2 and 2.5.3 apply.

In addition, the following Security Objectives are defined for Mobile as a form factor:

MP	MCP APPLICATION PROTECTION The MCP application is adequately protected from corruption.	
MP1	MCP.APP.CERTIFICATION	Combined certification of the platform (SE) + the MCP application residing on it shall be executed.
MP2	MCP.APP.INTERFERENCE	Verification of all other basic applications that are residing on the platform (SE) shall be executed.

TABLE 5: CONTACTLESS SECURITY REQUIREMENTS FOR MOBILE

As using Mobile as form factor is a new and evolving domain, additional requirements may apply. For guidance and recommendations, please refer to the "EMVCO handset requirements for contactless mobile payments" or others such as the "OMTP security threats on embedded consumer devices". The assurance level to be associated with the above Security Objectives for SEs shall be equivalent to the assurance package defined as EAL4+ in the Common Criteria methodology.

Nevertheless an EAL4+ set of assurance requirements shall be augmented regarding the following criteria:

It is the responsibility of the SE and MCP application suppliers, together with their own suppliers higher up in the supply chain, to decide how the security requirements are best met.

They may choose to organise the evaluation as a composition, using a previously evaluated IC or software platform. They may choose to use protection profiles for ICs or software platforms. Here, the efficiency of composition is significant. It is also appreciated that IC evaluation gives advanced notice on the capacity of IC state-of-the-art technology to defeat attackers. Therefore SE suppliers are encouraged to resort to it.

2.6 POI Security Requirements

2.6.1 Introduction

This section defines the applicable security requirements for all POI. These requirements are derived from PCI PTS v4.x requirements and from the CAS/OSeC requirements referred to in the table as "EPC Plus". They apply to all terminal types including stand-alone terminals, unattended POS terminals, encrypting PIN pad (EPP), contact or contactless acceptance, non PIN accepting devices, Mobile POS devices etc. These requirements are described in terms of evaluation modules that will allow significantly different configurations and POS architectures to be specified and evaluated with differing functionality to meet specific market needs. A benefit of this modular approach is that it will help vendors and developers conducting modular approvals or maintaining existing approvals to optimize evaluation costs and time particularly when laboratories are reviewing non-conventional architectures.

What follows is a complete list of harmonized security requirements for SEPA, categorised under the following modules:

- CORE - physical and logical requirements for PIN protection
- INTEGRATION - requirements for POI architectures with integrated components
- OPEN PROTOCOLS - requirements for POI's connected to open networks
- DATA - requirements for protection of cardholder data, transaction data and POI management data.
- DEVICE MANAGEMENT - requirements addressing the life cycle of the POI

Evaluation Module 1: Core Requirements ***Note:*** *in the following requirements, the device under evaluation is referred as the "device."*		
Section A – Core Physical Security Requirements		
Origin	**Number**	**Description of the requirement**
PCI	**A1**	The device uses tamper-detection and response mechanisms that cause it to become immediately inoperable and result in the automatic and immediate erasure of any sensitive data that may be stored in the device, such that it becomes infeasible to recover the sensitive data. These mechanisms protect against physical penetration of the device by means of (but not limited to) drills, lasers, chemical solvents, opening covers, splitting the casing (seams), and using ventilation openings; and there is not any demonstrable way to disable or defeat the mechanism and insert a PIN-disclosing bug or gain access to secret information without requiring an attack potential of at least 26 per device for identification and initial exploitation, with a minimum of 13 for exploitation, exclusive of the IC card reader[5]; and A2 ***Note:*** *The replacement of both the front and rear casings shall be considered as part of any attack scenario. All attacks shall include a minimum of ten hours' attack time for exploitation.*
PCI	**A2**	Failure of a single security mechanism does not compromise device security. Protection against a threat is based on a combination of at least two independent security mechanisms.

[5] As defined in Appendix B of the PCI PTS POI DTRs.

PCI	**A3**	The security of the device is not compromised by altering: • Environmental conditions • Operational conditions (An example includes subjecting the device to temperatures or operating voltages outside the stated operating ranges.)
PCI	**A4**	Sensitive functions or data are only used in the protected area(s) of the device. Sensitive data and functions dealing with sensitive data are protected from modification without requiring an attack potential of at least 26 for identification and initial exploitation, with a minimum of 13 for exploitation, exclusive of the IC card reader, for identification and initial exploitation5.
PCI	**A5**	There is no feasible way to determine any entered and internally transmitted PIN digit by monitoring sound, electro-magnetic emissions, power consumption or any other external characteristic available for monitoring-even with the cooperation of the device operator or sales clerk-without requiring an attack potential of at least 26 for identification and initial exploitation with a minimum of 13 for exploitation[6].

[6] As defined in Appendix B of the PCI PTS POI DTRs.

PCI	**A6**	Determination of any PIN-security-related cryptographic key resident in the device, by penetration of the device and/or by monitoring emanations from the device (including power fluctuations), requires an attack potential of at least 35 for identification and initial exploitation with a minimum of 15 for exploitation6. ***Note**: If the POI device has a keypad that can be used to enter non-PIN data, the device must meet at least one of the following: A7, B16, or E3.4.* • *A7 applies to any components or paths containing plaintext display signals between the cryptographic processor and display unit.* • *B16 applies to devices that allow for updates of prompts or use cryptography to communicate with a display, whether performed by the vendor or the acquirer.* • *E3.4 is appropriate for unattended devices that do not meet any of the aforementioned.*
PCI	**A7**	The unauthorized alteration of prompts for non-PIN data entry into the PIN entry key pad such that PINs are compromised, i.e., by prompting for the PIN entry when the output is not encrypted, cannot occur without requiring an attack potential of at least 18 per device for identification and initial exploitation with a minimum of 9 for exploitation6.
PCI	**A8**	The device provides a means to deter the visual observation of PIN values as they are being entered by the cardholder.
EPC PLUS	**A8.a**	It is optional to have a privacy shield on a PED. However if a privacy shield is in place then it shall be according to [EPC Guidelines on Privacy Shields.].
PCI	**A9**	It is not feasible to penetrate the device to make any additions, substitutions, or modifications to the magnetic-stripe reader and associated hardware or software, in order to determine or modify magnetic-stripe track data, without requiring an attack potential of at least 16 per device, for identification and initial exploitation, with a minimum of 8 for exploitation6.

PCI	**A10**	Secure components intended for unattended devices contain an anti-removal mechanism to protect against unauthorized removal and/or unauthorized re-installation. Defeating or circumventing this mechanism must require an attack potential of at least 18 per device for identification and initial exploitation, with a minimum of 9 for exploitation6.
PCI	**A11**	If PIN entry is accompanied by audible tones, the tone for each entered PIN digit is indistinguishable from the tone for any other entered PIN digit.
Section B - Core Logical Security Requirements		
Origin	**Number**	**Description of the requirement**
PCI	**B1**	The device performs a self-test, which includes integrity and authenticity tests upon start-up and at least once per day to check 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 device must reinitialize memory at least every 24 hours.
PCI	**B2**	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 the clear-text PIN or other sensitive data.
PCI	**B3**	The firmware, and any changes thereafter, have been inspected and reviewed using a documented and auditable process, and certified as being free from hidden and unauthorized or undocumented functions.
EPC PLUS	**B3.a**	The vendor's processes in Requirement B3 must be evaluated by the testing laboratory.
PCI	**B4**	If the device allows updates of firmware, the device cryptographically authenticates the firmware and if the authenticity is not confirmed, the firmware update is rejected and deleted.

PCI	**B4.1**	The firmware must support the authentication of applications loaded onto the terminal consistent with B4. If the device allows software application and/or configuration updates, the device cryptographically authenticates updates consistent with B4.
PCI	**B5**	The device never displays the entered PIN digits. Any array related to PIN entry displays only non-significant symbols, e.g. asterisks.
PCI	**B6**	Sensitive data shall not be retained any longer, or used more often, than strictly necessary. Online PINs are encrypted within the device immediately after PIN entry is complete and has been signified as such by the cardholder, e.g. via pressing the enter button. 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.
EPC PLUS	**B6.a**	Requirement B6 is not intended to prevent PIN change for a proprietary Card scheme.
PCI	**B7**	Access to sensitive services requires authentication. Sensitive services provide access to the underlying sensitive functions. Sensitive functions are those functions that process sensitive data such as cryptographic keys, PINs, and passwords. Entering or exiting sensitive services shall not reveal or otherwise affect sensitive data.
PCI	**B8**	To minimize the risks from unauthorized 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.
PCI	**B9**	If random numbers are generated by the device in connection with security over sensitive data, the random number generator has been assessed to ensure it is generating numbers sufficiently unpredictable.
PCI	**B10**	The device has characteristics that prevent or significantly deter the use of the device for exhaustive PIN determination.

EPC PLUS	**B10.a**	The POI has characteristics that prevent the use of the device for exhaustive PIN determination.
PCI	**B11**	The key-management techniques implemented in the device conform to ISO 11568 and/or ANSI X9.24. Key-management techniques must support the ANSI TR-31 key derivation methodology or an equivalent methodology for maintaining the TDEA key bundle.
PCI	**B12**	The PIN-encryption technique implemented in the device is a technique included in ISO 9564.
PCI	**B13**	It is not possible to encrypt or decrypt any arbitrary data using any PIN-encrypting key or key-encrypting key contained in the device. The device must enforce that data keys, key-encipherment keys, and PIN-encryption keys have different values.
PCI	**B14**	There is no mechanism in the device that would allow the outputting of a private or secret clear-text key or clear-text PIN, the encryption of a key or PIN under a key that might itself be disclosed, or the transfer of a clear-text key from a component of high security into a component of lesser security.
PCI	**B15**	The entry of any other transaction data must be separate from the PIN-entry process, avoiding the accidental display of a cardholder PIN on the device display. If other data and the PIN are entered on the same keypad, the other data entry and the PIN entry shall be clearly separate operations.

Note: *If the POI device has a keypad that can be used to enter non-PIN data, the device must meet at least one of the following: A7, B16, or E3.4.*

- *A7 applies to any components or paths containing plaintext display signals between the cryptographic processor and display unit.*
- *B16 applies to devices that allow for updates of prompts or use cryptography to communicate with a display, whether performed by the vendor or the acquirer.*
- *E3.4 is appropriate for unattended devices that do not meet any of the aforementioned.*

PCI	**B16**	All prompts for non-PIN data entry are under the control of the cryptographic unit of the device and requiring an attack potential of at least 18 per device for identification and initial exploitation with a minimum of 9 for exploitation[7] to circumvent. If the prompts are stored inside the cryptographic unit, they cannot feasibly be altered without causing the erasure of the unit's cryptographic keys. If the prompts are stored outside the cryptographic unit, cryptographic mechanisms must exist to ensure the authenticity and the proper use of the prompts and that modification of the prompts or improper use of the prompts is prevented.
PCI	**B17**	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, but not limited to, modifying data objects belonging to another application or the OS.
PCI	**B18**	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.
PCI	**B19**	The vendor must provide adequate documented security guidance for the integration of any secure component into a PIN entry POI Terminal.
PCI	**B20**	A user-available security policy from the vendor addresses the proper use of the POI in a secure fashion, including information on key-management responsibilities, administrative responsibilities, device functionality, identification, and environmental requirements. The security policy must define the roles supported by the POI and indicate the services available for each role in a deterministic tabular format. The POI is capable of performing only its designed functions - i.e., there is no hidden functionality. The only approved functions performed by the POI are those allowed by the policy.

[7] As defined in Appendix B of the PCI PTS POI DTRs.

Section C - Online PIN Security Requirement		
Origin	**Number**	**Description of the requirement**
PCI	**C1**	If the device can hold multiple PIN-encryption keys and if the key to be used to encrypt the PIN can be externally selected, the device prohibits unauthorized key replacement and key misuse.
Section D - Offline PIN Security Requirements		
Origin	**Number**	**Description of the requirement**
PCI	**D1**	It is neither feasible to penetrate the ICC reader to make any additions, substitutions, or modifications to either the ICC reader's hardware or software, in order to determine or modify any sensitive data, without requiring an attack potential of at least 20 for identification and initial exploitation, with a minimum of 10 for exploitation[8], nor is it possible for both an ICC card and any other foreign object to reside within the card insertion slot. ***Note**: All attacks shall include a minimum of ten hours' attack time for exploitation.*
PCI	**D2**	The opening for the insertion of the IC card is in full view of the cardholder during card insertion so that any untoward obstructions or suspicious objects at the opening are detectable.
PCI	**D3**	The ICC reader is constructed so that wires running out of the slot of the IC reader to a recorder or a transmitter (an external bug) can be observed by the cardholder.

[8] As defined in Appendix B of the PCI PTS POI DTRs.

PCI	**D4**	PIN protection during transmission between the device encrypting the PIN and the ICC reader (at least two must apply): If the device encrypting the PIN and the ICC reader are not integrated into the same secure module, and the cardholder verification method is determined to be: • An enciphered PIN, the PIN block shall be enciphered between the device encrypting the PIN and the ICC reader using either an authenticated encipherment key of the IC card, or in accordance with ISO 9564. • A plaintext PIN, the PIN block shall be enciphered from the device encrypting the PIN to the ICC reader (the ICC reader will then decipher the PIN for transmission in plaintext to the IC card) in accordance with ISO 9564. If the device encrypting the PIN and the ICC reader are integrated into the same secure module, and the cardholder verification method is determined to be: An enciphered PIN, the PIN block shall be enciphered using an authenticated encipherment key of the IC card. • A plaintext PIN, then encipherment is not required if the PIN block is transmitted wholly through a protected environment (as defined in ISO 9564). If the plaintext PIN is transmitted to the ICC reader through an unprotected environment, the PIN block shall be enciphered in accordance with ISO 9564.

Evaluation Module 2: POS Terminal integration

Current desktop POIs used in face-to-face transactions can be characterised as devices where PIN entry functionality is a secure logical and physical perimeter. However it is also practical to evaluate the security of individual components or their combinations (card readers, display, keypads, or secure processors). The POS Terminal Integration Evaluation Module ensures that the integration of previously evaluated components does not impair the overall security as stated in the security requirements. This module also supports the cost effective maintenance of components and includes security management requirements applicable to the integrated device.

Note: *in the following requirements, the device under evaluation is referred as the "device."*

Section E - POS Terminal Integration Security Requirements

Origin	Number	Description of the requirement
Configuration Management		
PCI	**E1**	Any secure component integrated into a PIN entry POI terminal submitted for evaluation has a clearly identified physical and logical security perimeter (related to PIN entry and card-reading functions).

Integration of PIN Entry Functions		
PCI	**E2.1**	The logical and physical integration of a PCI-approved secure component (or components) into a PIN entry POI terminal must not impact the overall PIN protection level.
PCI	**E2.2**	The PIN pad (PIN entry area) and the surrounding area must be designed and engineered in such a way that the complete device does not facilitate the fraudulent placement of an overlay over the PIN pad. An overlay attack must require an attack potential of at least 18 for identification and initial exploitation, with a minimum of 9 for exploitation[9].
Integration into a POS Terminal		
PCI	**E3.1**	The logical and physical integration of an approved secure component into a PIN entry POI terminal does not create new attack paths to the PIN.
PCI	**E3.2**	The PIN entry POI terminal is equipped with mechanisms to prevent attacks aiming at retaining and stealing the payment card (e.g. Lebanese Loop attack).
PCI	**E3.3**	There is a clear logical and/or physical segregation between secure components and non-secure components integrated into the same device.

[9] As defined in Appendix B of the PCI PTS POI DTRs.

Note: *If the POI device has a keypad that can be used to enter non-PIN data, the device must meet at least one of the following: A7, B16, or E3.4.* • *A7 applies to any components or paths containing plaintext display signals between the cryptographic processor and display unit.* • *B16 applies to devices that allow for updates of prompts or use cryptography to communicate with a display, whether performed by the vendor or the acquirer.* • *E3.4 is appropriate for unattended devices that do not meet any of the aforementioned.*		
PCI	**E3.4**	The POI (application) must enforce the correspondence between the display messages visible to the cardholder and the operating state (i.e., secure or non-secure mode) of the PIN entry device, e.g. by using cryptographic authentication. If commands impacting the correspondence between the display messages and the operating state of the PIN entry device are received from an external device (e.g. a store controller), the commands enabling data entry must be authenticated. The alteration of the correspondence between the display messages visible to the cardholder and the operating state of the PIN entry device cannot occur without requiring an attack potential of at least 18 per POI for identification and initial exploitation with a minimum of 9 for exploitation[10].
PCI	**E3.5**	The PIN-accepting POI terminal must be equipped with only one payment card PIN-acceptance interface, e.g. a keyboard. If another interface is present which can be used as a keyboard, a mechanism must exist to prevent its use for PIN entry, e.g. it must not have numeric keys, or it is not possible to use it otherwise for numeric entry or it is controlled in a manner consistent with B16.

[10] As defined in Appendix B of the PCI PTS POI DTRs.

Removal Requirements		
PCI	**E4.1**	The device is protected against unauthorized removal. Defeating or circumventing this mechanism must require an attack potential of at least 18 per device for identification and initial exploitation, with a minimum of 9 for exploitation[11].
PCI	**E4.2**	The vendor documents, maintains and makes available to integrators details on how to implement the protection system against unauthorized removal.
PCI	**E4.3**	For each embedded device, the protection system against unauthorized removal is properly implemented as documented by the embedded device manufacturer.

Evaluation Module 3: Open Protocols

This set of requirements ensures that POI using open security protocols and open communications protocols to access public networks do not have public domain vulnerabilities. These security protocols can be used to provide additional security services to protect transaction data, i.e. transaction message integrity and authenticity between the POI and the host and POI device authenticity.

Section F – Discovery

Origin	Number	Description of the requirement
PCI	**F1**	**All** public domain protocols and interfaces available on the platform are clearly identified in the *Open Protocols Module*.

[11] As defined in Appendix B of the PCI PTS POI DTRs.

Section G – Vulnerability Assessment		
Origin	**Number**	**Description of the requirement**
PCI	**G1**	The platform vendor has vulnerability assessment procedures and documentation for each protocol and interface listed in F1 of the *Open Protocols Module*.
PCI	**G2**	The device has undergone a vulnerability assessment to ensure that the protocols and interfaces listed in F1 do not contain exploitable vulnerabilities. a. The vulnerability assessment is supported by a documented analysis describing the security of the protocols and interfaces. b. The vulnerability assessment is supported by a vulnerability survey of information available in the public domain. c. The vulnerability assessment is supported by testing.
PCI	**G3**	The platform vendor has vulnerability disclosure measures in place for the device. a. The vulnerability-disclosure measures are documented. b. The vulnerability-disclosure measures ensure a timely distribution of information about newly found vulnerabilities. This information includes identification, description, and assessment of the vulnerabilities. c. The vulnerability-disclosure measures ensure a timely distribution of mitigation measures.

Section H – Vendor Guidance		
PCI	**H1**	The device has security guidance that describes how protocols and services must be used for each interface that is available on the platform identified in the *Open Protocols Module*.
PCI	**H2**	The device has guidance that describes the default configuration for each protocol and services for each interface that is available on the platform.
PCI	**H3**	The device has guidance for key management describing how keys and certificates must be used. a. The key-management guidance is at the disposal of internal users, and/or of application developers, system integrators, and end-users of the platform. b. Key-management security guidance describes the properties of all keys and certificates that can be used by the platform. c. Key-management security guidance describes the responsibilities of the platform vendor, application developers, system integrators, and end-users of the platform. d. Key-management security guidance ensures secure use of keys and certificates.
Section I – Operational Testing		
PCI	**I1**	The device has **all** the security protocols that are available on the platform clearly identified in the Open Protocols Module.
PCI	**I2**	The device is able to provide confidentiality of data sent over a network connection. a. Encryption mechanism utilizes key sizes appropriate for the algorithm(s) in question. b. Encryption is provided by using keys that are established in a secure manner using appropriate key-management procedures, such as those listed in NIST SP800-21, Guidelines for Implementing Cryptography.

PCI	**I3**	The device is able to provide the integrity of data that is sent over a network connection. a. Integrity is provided by a MAC as defined in ISO 16609, or by a digital signature. b. Hashing can be provided by at least one of the following algorithms: SHA-224, SHA-256, SHA-384, and SHA-512. c. Examples of appropriate algorithms and minimum key sizes are stated in Appendix D of the PCI PTS POI DTRs.
PCI	**I4**	The device uses a declared security protocol to authenticate the server. a. Server authentication utilizes key sizes appropriate for the algorithm(s) in question. b. Hashing can be provided by at least one of the following algorithms: SHA-224, SHA-256, SHA-384, and SHA-512. c. The platform is able to verify the validity of the public keys it receives. d. The platform is able to verify the authenticity of the public keys it receives.
PCI	**I5**	The device is able to detect replay of messages, and enables the secure handling of the exceptions.
PCI	**I6**	The platform implements session management. a. The platform keeps track of all connections and restricts the number of sessions that can remain active on the platform to the minimum necessary number. b. The platform sets time limits for sessions and ensures that sessions are not left open for longer than necessary.

Section J – Maintenance		
PCI	**J1**	The platform vendor maintains guidance describing configuration management for the platform. a. The guidance is at the disposal of internal users, and/or of application developers, system integrators and end-users of the platform. b. The guidance covers the complete platform; including firmware, applications, certificates and keys. c. The guidance covers the complete life cycle of the platform from development, over manufacturing, up to delivery and operation. d. The security guidance ensures that unauthorized modification is not possible. e. The security guidance ensures that any modification of a PTS-approved platform that impacts platform security, results in a change of the platform identifier.
PCI	**J2**	The platform vendor has maintenance measures in place. a. The maintenance measures are documented. b. The maintenance measures ensure timely detection of vulnerabilities that apply to the device by periodical execution of a vulnerability assessment that includes activities such as: analysis, survey of information available in the public domain, and testing. c. The maintenance measures ensure timely assessment and classification of newly found vulnerabilities. d. The maintenance measures ensure timely creation of mitigation measures for newly found vulnerabilities that may impact platform security.
PCI	**J3**	Deployed platforms can be updated, and the platform vendor maintains guidance describing how the update mechanism is to be used.

PCI	**J4**	The update mechanism ensures confidentiality, integrity, server authentication, and protection against replay by using an appropriate and declared security protocol. If the device allows software and/or configuration updates, the device cryptographically authenticates the update and if the authenticity is not confirmed, the update is rejected and deleted.
Evaluation Module 4: Secure Reading and Exchange of Data (SRED) This module defines requirements for cardholder account data protection. The security services used to protect account data can also be used to protect transaction data (for example by providing transaction message confidentiality, integrity and authenticity). Specific controls to achieve this additional functionality are described in the table of applicability, later in this book.		
Section K – Account Data Protection		
PCI	**K1**	All account data is either encrypted immediately upon entry or entered in clear-text into a secure device and processed within the secure controller of the device.
PCI	**K1.1**	The device protects all account data upon entry (consistent with A10 for magnetic stripe data and D1 for Chip data), and there is no method of accessing the clear-text account data (using methods described in A1) without defeating the security of the device. Defeating or circumventing the security mechanism requires an attack potential of at least 16 for identification and initial exploitation, with a minimum of 8 for exploitation[12]. ***Note:*** *MSRs and ICCRs must meet the attack potentials stipulated in DTRs A10 and D1 respectively.*
PCI	**K1.2**	Failure of a single security mechanism does not compromise device security. Protection against a threat is based on a combination of at least two independent security mechanisms.

[12] As defined in Appendix B of the PCI PTS POI DTRs.

PCI	**K2**	The logical and physical integration of an approved secure card reader into a PIN entry POI terminal does not create new attack paths to the account data. The account data is protected (consistent with A2) from the input component to the secure controller of the device.
PCI	**K3**	Determination of any cryptographic keys used for account data encryption, by penetration of the device and/or by monitoring emanations from the device (including power fluctuations), requires an attack potential of at least 26 for identification and initial exploitation with a minimum of 13 for exploitation[12].
PCI	**K3.1**	Public keys must be stored and used in a manner that protects against unauthorized modification or substitution. Unauthorized modification or substitution requires an attack potential of at least 26 for identification and initial exploitation with a minimum of 13 for exploitation[12].
PCI	**K4**	All account data shall be encrypted using only ANSI X9 or ISO-approved encryption algorithms (e.g. AES, TDES) and should use ANSI X9 or ISO-approved modes of operation.
PCI	**K5**	If remote key distribution is used, the device supports mutual authentication between the sending key distribution host and receiving device.
PCI	**K6**	The device supports data origin authentication of encrypted messages.
PCI	**K7**	Secret and private keys that reside within the device to support account data encryption are unique per device.
PCI	**K8**	Encryption or decryption of any arbitrary data using any account data-encrypting key or key-encrypting key contained in the device is not permitted. The device must enforce that account data keys, key-encipherment keys, and PIN-encryption keys have different values.

PCI	**K9**	If the device may be accessed remotely for the purposes of administration, all access attempts must be cryptographically authenticated. If the authenticity of the access request cannot be confirmed, the access request is denied.
PCI	**K10**	The firmware, and any changes thereafter, have been inspected and reviewed consistent with B3.
PCI	**K11.1**	The firmware must confirm the authenticity of all applications loaded onto the terminal consistent with B4. If the device allows software application and/or configuration updates, the device cryptographically authenticates all updates consistent with B4.
PCI	**K11.2**	The vendor must provide clear security guidance consistent with B2 and B6 to all application developers to ensure: • That it is not possible for applications to be influenced by logical anomalies which could result in clear text data being outputted whilst the terminal is in encrypting mode. • That account data is not retained any longer, or used more often, than strictly necessary.
PCI	**K12**	If the device allows updates of firmware, the device cryptographically authenticates the firmware and if the authenticity is not confirmed, the firmware update is rejected and deleted.
PCI	**K13**	The device's functionality shall not be influenced by logical anomalies consistent with B2.
PCI	**K14**	If the device is capable of communicating over an IP network or uses a public domain protocol (such as but not limited to Wi-Fi or Bluetooth), then requirements specified in DTR Module 3: Open Protocols Requirements have been met.
PCI	**K15**	When operating in encrypting mode, there is no mechanism in the device that would allow the outputting of clear-text account data. Changing between an encrypting and non-encrypting mode of operation requires explicit authentication.

PCI	**K15.1**	When operating in encrypting mode, the secure controller can only release clear-text account data to authenticated applications executing within the device.
PCI	**K15.2**	Account data (in either clear-text or encrypted form) shall not be retained any longer, or used more often, than strictly necessary.
PCI	**K16**	If the device is capable of generating surrogate PAN values to be outputted outside of the device, it is not possible to determine the original PAN knowing only the surrogate value.
PCI	**K16.1**	If using a hash function to generate surrogate PAN values, input to the hash function must use a salt with minimum length of 64-bits.
PCI	**K16.2**	If using a hash function to generate surrogate PAN values, the salt is kept secret and appropriately protected. Disclosure of the salt cannot occur without requiring an attack potential of at least 16 per device for identification and initial exploitation with a minimum of 8 for exploitation[13].
PCI	**K17**	The key-management techniques implemented in the device are consistent with B11.
PCI	**K18**	The device has characteristics that prevent or significantly deter the use of the device for exhaustive PAN determination.
PCI	**K19**	Environmental or operational conditions cannot be altered to compromise the security of the device, or cause the device to output clear-text account data. (An example includes subjecting the device to temperatures or operating voltages outside the stated operating ranges.)

[13] As defined in Appendix B of the PCI PTS POI DTRs.

PCI	**K20**	If the device supports multiple applications, it must enforce the separation between applications consistent with B17.
PCI	**K21**	The following features of the device's operating system must be in place: • 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 unauthorized or unnecessary functions. API functionality and commands that are not required to support specific functionality must be disabled (and where possible, removed).
PCI	**K22**	Access to sensitive services requires authentication. Sensitive services provide access to the underlying sensitive functions. Sensitive functions are those functions that process sensitive data such as cryptographic keys, account data, and passwords. Entering or exiting sensitive services shall not reveal or otherwise affect sensitive data.
PCI	**K23**	Sensitive services are protected from unauthorized use consistent with B8.

Evaluation Module 5: Device Management Security Requirements *Note: in the following requirements, the device under evaluation is referred as the "device".*		
Section L – During Manufacturing		
EPC PLUS	**L0**	L requirements must be checked by the testing lab. This includes a periodic site visit regarding critical steps in the manufacturing process (excluding the key loading).[14]
PCI	**L1**	Change-control procedures are in place so that any intended security-relevant change to the physical or functional capabilities of the device causes a re-certification of the device under the Core PIN Entry and/or POS Terminal Integration Security Requirements of this document.
PCI	**L2**	The certified firmware is protected and stored in such a manner as to preclude unauthorized modification during its entire manufacturing life cycle–e.g. by using dual control or standardized cryptographic authentication procedures.
PCI	**L3**	The device is assembled in a manner that the components used in the manufacturing process are those components that were certified by the Core PIN Entry and/or POS Terminal Integration Security Requirements evaluation, and that unauthorized substitutions have not been made.
PCI	**L4**	Production software (e.g. firmware) that is loaded to devices at the time of manufacture is transported, stored, and used under the principle of dual control, preventing unauthorized modifications and/or substitutions.
PCI	**L5**	Subsequent to production but prior to shipment from the manufacturer's or reseller's facility, the device and any of its components are stored in a protected, access-controlled area or sealed within tamper-evident packaging to prevent undetected unauthorized access to the device or its components.

[14] The periodic site visit plan will be detailed by guidance.

PCI	**L6**	If the device will be authenticated at the key-loading facility or the facility of initial deployment by means of secret information placed in the device during manufacturing, then this secret information is unique to each device, unknown and unpredictable to any person, and installed in the device under dual control to ensure that it is not disclosed during installation.
PCI	**L7**	Security measures are taken during the development and maintenance of POI security related components. The manufacturer must maintain development security documentation describing all the physical, procedural, personnel, and other security measures that are necessary to protect the integrity of the design and implementation of the POI security-related components in their development environment. The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the POI security-related components. The evidence shall justify that the security measures provide the necessary level of protection to maintain the integrity of the POI security-related components.
PCI	**L8**	Controls exist over the repair process and the inspection testing process subsequent to repair to ensure that the device has not been subject to unauthorized modification.
EPC Plus	**L8a**	If tamper mechanisms can be reset during the repair process then for this repair process the requirements L1 till L7 and the M requirements are applicable.

Section M – Between Manufacturer and Initial Key Loading ***Note:*** *in the following requirements, the device under evaluation is referred as the "device".*		
PCI	**M1**	The POI should be protected from unauthorized modification with tamper-evident security features, and customers shall be provided with documentation (both shipped with the product and available securely online) that provides instruction on validating the authenticity and integrity of the POI. Where this is not possible, the POI is shipped from the manufacturer's facility to the initial key-loading facility or to the facility of initial deployment and stored en route under auditable controls that can account for the location of every POI at every point in time. Where multiple parties are involved in organizing the shipping, it is the responsibility of each party to ensure that the shipping and storage they are managing is compliant with this requirement.
PCI	**M2**	Procedures are in place to transfer accountability for the device from the manufacturer to the facility of initial deployment. Where the device is shipped via intermediaries such as resellers, accountability will be with the intermediary from the time at which they receive the device until the time it is received by the next intermediary or the point of initial deployment.
PCI	**M3**	While in transit from the manufacturer's facility to the initial key-loading facility, the device is: • Shipped and stored in tamper-evident packaging; and/or • Shipped and stored containing a secret that is immediately and automatically erased if any physical or functional alteration to the device is attempted, that can be verified by the initial key-loading facility, but that cannot feasibly be determined by unauthorized personnel.
PCI	**M4**	The device's development security documentation must provide means to the initial key-loading facility to assure the authenticity of the TOE's security relevant components.

EPC PLUS	**M4a**	In order to ensure ongoing key loading facility operational security and conformity, key loading audits must be conducted. Those entities carrying out such audits must be suitably qualified to certify conformity with the requirements of Secure key loading operations and Key management. The audit should at least cover: • The operational environment of the key loading; • The key management environment including conduct of any key ceremonies; • The configuration of the key loading; • Any changes relevant to pre- and post-operational security. The subject of the Audit should be allowed to communicate their report to the relevant bodies.
PCI	**M5**	If the manufacturer is in charge of initial key loading, then the manufacturer must verify the authenticity of the POI security-related components.
EPC PLUS	**M5a**	Requirement M4a also applies to Requirement M5.
PCI	**M6**	If the manufacturer is not in charge of initial key loading, the manufacturer must provide the means to the initial key-loading facility to assure the verification of the authenticity of the POI security-related components.
EPC PLUS	**M6a**	Requirement M4a also applies to Requirement M6.
PCI	**M7**	Each device shall have a unique visible identifier affixed to it.

PCI	**M8**	The vendor must maintain a manual that provides instructions for the operational management of the POI. This includes instructions for recording the entire life cycle of the POI security-related components and of the manner in which those components are integrated into a single POI, e.g.: • Data on production and personalization; • Physical chronological whereabouts; • Repair and maintenance; • Removal from operation; • Loss or theft.

2.6.2 Applicability of Requirements

To determine which of the above requirements need to be evaluated in order to assess the security of a product, the Vendor must utilize the table and matrix below to define the core functionalities, capabilities and therefore security of the product. For compound devices, it is possible that these requirements are met or exceeded by the relevant module(s), if the corresponding requirements are fully covered.

To determine which requirements apply to a device, the following steps must take place:

1. Identify which of the functionalities the device has the capability to support.
2. For each of the supported functionalities, report any marking "x" from the functionality column to the baseline column. "x" stands for "applicable," in which case the requirement must be considered for possible evaluation.

Functionality Description

PIN Entry	This is the functionality present for any device under test that captures the PIN from the cardholder and turns it into information. No assumption is made upon the format; this could be a PIN block, but also cover partial PIN information such as a digit, if this partial information is going to form a PIN during a legitimate transaction.
Keys	This functionality is considered whenever the device under evaluation contains-even temporarily-keys involved in PIN security. Under the scope of this functionality are the secret keys of symmetric algorithms, the private keys of asymmetric algorithms, and the public keys of asymmetric algorithms (with the limitation of scope to their integrity and authenticity).
Card Reader	This functionality applies whenever a device under evaluation has the capability to capture card data, irrespective of the technology being used (i.e., it encompasses both the magnetic stripe and smart card readers). This is further broken down into ICCR and MSR functionality.
Feedback to cardholder	Each time a device under evaluation implements any way of possibly giving feedback to the cardholder during its PIN-based transaction, it applies to this functionality. This includes but is not limited to auditory and visible feedback (i.e., displays).
Terminal is a module	If the device under evaluation is designed to be integrated into equipment, then it applies for "terminal is a module" functionality. Modules are also referred to as OEM equipment.
Terminal is compound	A device under evaluation is said to be compound whenever it incorporates one or more modules, in order to cover one or several of the aforementioned functionalities. Being a compound device does not preclude the applicability of "terminal is a module" functionality. Both functionalities are independent.
Terminal implements TCPIP stack	A device under evaluation implements a TCPIP stack and associated open protocols.

Chip only POI	The Chip only POI • does not allow fallback to magnetic stripe transactions. • does not use SDA as Offline Data Authentication method. • does not support Offline plaintext PIN.
Transaction Data Protection	POI has the capacity to protect communications over external communication channels, meaning that POI security components use cryptography: • To protect all transaction data sent or received by the POI against modification; • To protect all transaction data sent or received by the POI against disclosure; • For the POI to be uniquely authenticated by the external entity it communicates with. POI management data is provided to the POI in an authentic way and is protected against unauthorised change. The transaction data is handled with authenticity and integrity in the POI.

TABLE 6: FUNCTIONALITY DESCRIPTION

Requirement	PIN Entry	Keys	ICCR	MSR	Feedback to cardholder	Terminal is a module	Terminal is compound	Terminal Implements TCPIP stack	Protects account data	Chip only POI	Transaction Data Protection	Conditions
Core Requirements Modules												
Core Physical Security Requirements												
A1	x											For POI in purely chip based systems sensitive functions are protected by logical means only.
A2	x	x										
A3	x	x								x		
A4	x	x										For POI in purely chip based systems sensitive functions are protected by logical means only.
A5	x				x							
A6		x								x		For POI in purely chip based systems the attack potential is reduced. "…, requires an attack potential of at least 26 for identification and initial exploitation with a minimum of 13 for exploitation."
A7					x							
A8	x				x					x		
A9												
A10				x								
A11	x				x					**x**		
Core Logical Security Requirements												
B1	x	x						x	x	x		
B2	x	x								x		
B3	x	x								x		B3a applies as described in PCI DTR v4
B4	x	x								x		
B4.1	x	x								x		
B5	x									x		
B6	x									x		
B7	x	x								x		
B8	x	x								x		
B9		x						x	x	x		
B10	x									x		B10.a applies
B11		x								x		
B12	x	x								x		
B13		x								x		

Requirement	PIN Entry	Keys	ICCR	MSR	Feedback to cardholder	Terminal is a module	Terminal is compound	Terminal Implements TCPIP stack	Protects account data	Chip only POI	Transaction Data Protection	Conditions
B14	x	x								x		
B15	x									x		
B16					x					*x*		If keypad that can be used to enter non-PIN data.
B17	x									x		
B18	x									x		
B19			x	x		x				x		
B20	x	x	x	x	x	x	x	x		x		
Additional Online Requirement												
C1		x								x		
Additional Offline Requirements												
D1			x									
D2			x									
D3			x									
D4			x							x		
POS Terminal Integration Requirements												
E1	x	x	x		x	x	x	x	x	x		Always applicable
E2.1	x						x			x		
E2.2	x						x			x		
E3.1							x			x		
E3.2			x			x	x			x		
E3.3	x						x			x		
E3.4	x				x		x			*x*		If keypad that can be used to enter non-PIN data.
E3.5	x						x			x		
E4.1	x		x			x				x		
E4.2	x		x			x				x		
E4.3							x			x		
Open Protocols Security Module												
All								x	x	x		All requirements applicable
The following OP- requirements are applicable in case of protection of transaction data												
I2											x	Also for confidentiality of data received.
I3											x	Also for authenticity of data received

Requirement	PIN Entry	Keys	ICCR	MSR	Feedback to cardholder	Terminal is a module	Terminal is compound	Terminal Implements TCPIP stack	Protects account data	Chip only POI	Transaction Data Protection	Conditions
I4											x	Not only server authentication, also POI authentication must be in scope of this requirement
J4											x	
Secure Reading and Exchange of Data Module												
All			x	x					x			All requirements applicable, if card data are defined as assets to be detected
The following K-requirements are applicable for protection of transaction data												
K3										x	x	For protection against disclosure of any non-PIN secret key
K3.1											x	
K5											x	
K6											x	
K7											x	For all data encryption
K8											x	For all data encryption
K9											x	For POI management data
K10											x	To be evaluated at least based on documentation
K11.1											x	
K13											x	
K17											x	
K20											x	
Device Security Requirements												
During Manufacturing												
L1	x	x	x	x	x	x	x	x	x	x		
L2	x	x	x	x	x	x	x	x	x	x		
L3	x	x	x	x	x	x	x	x	x	x		
L4	x	x	x	x	x	x	x	x	x	x		
L5	x	x	x	x	x	x	x	x	x	x		
L6	x	x	x	x	x	x	x	x	x	x		
L7	x	x	x	x	x	x	x	x	x	x		
L8	x	x	x	x	x	x	x	x	x	x		
Between Manufacturing and Initial Key Loading												
M1	x	x	x	x	x	x	x		x	x		
M2	x	x	x	x	x	x	x		x	x		

Requirement	PIN Entry	Keys	ICCR	MSR	Feedback to cardholder	Terminal is a module	Terminal is compound	Terminal Implements TCPIP stack	Protects account data	Chip only POI	Transaction Data Protection	Conditions
M3	x	x	x	x	x	x	x		x	x		
M4	x	x	x	x	x	x	x		x	x		
M5	x	x	x	x	x	x	x		x	x		
M6	x	x	x	x	x	x	x		x	x		
M7	x	x	x	x	x	x	x		x	x		
M8	x	x	x	x	x	x	x		x	x		

TABLE 7: SUPPORTED FUNCTIONALITIES

2.7 Requirements for Hardware Security Modules

2.7.1 Introduction

This chapter defines the security requirements that apply to Hardware Security Modules (HSMs) which are widely used to manage and protect cryptographic keys in order to achieve the cryptographic protection required by the other chapters in Book 4.
HSMs are essential to provide security services in support of Card payment transactions. They contribute to the protection of cardholder data confidentiality, authenticity and integrity; for example protection of real-time messages such as PIN translation between security zones for online PIN, to cardholder and card data storage, and to terminal management - whether or not PINs are involved.
The following requirements must be adhered to for a stakeholder to call itself conformant with the Volume.

2.7.2 Hardware Security Modules

A HSM is a specialized hardware device designed to protect cryptographic keys and the use of those keys in executing cryptographic functions. It may also accelerate crypto processes.

Hardware Security Modules have three different types of security requirements that must be met:

1. The device itself must meet certain requirements for its hardware and software. The manufacturer or vendor must submit his product for certification against these requirements, which also extend to the production, any initial manufacturer key loading and transport of the specific product.
2. The usage of the HSMs in the card payment operational context. Here the focus is on how the owner and user of the HSM has protected and configured it, including the generation and loading and storage of operational keys

3. The interface between the two i.e. pre- and post-operational security, describing the secure handover from factory state to operational state and the secure removal of a HSM from service, ensuring e.g. that all operational keys are deleted.

2.7.3 Scope of Requirements

HSMs are widely used to protect cryptographic keys by all actors in the card payment infrastructure, be they Card Schemes, Issuers, Acquirers, Card Producers, Processors, Vendors, Banks, Merchants and others.

These requirements are therefore relevant wherever a HSM is used for any function relevant to the security of a Volume conformant solution.

These requirements apply anywhere where HSMs are used to provide hardware based cryptographic functionality or services needed to achieve conformance with Book 4.

However, they do not apply to cards and POI devices (which themselves provide this), or directly to card personalisation or Acquirer to Issuer links (which are assumed to be protected by the individual Card Payment Schemes themselves).

2.7.4 Security Zones

A security zone describes the entities sharing encryption keys and is effectively all those parties directly affected by the compromise of a key.

A security zone should be setup between two parties for one purpose. In the example of a Terminal to Acquirer protocol with several zones, there is a security zone between the POI and Interim Host, another between the Interim Host and Acquirer, etc. (This should not be read as meaning that an interim host is required however if there is one then a security zone between POI and Acquirer becomes two zones.)

Examples of HSM Use

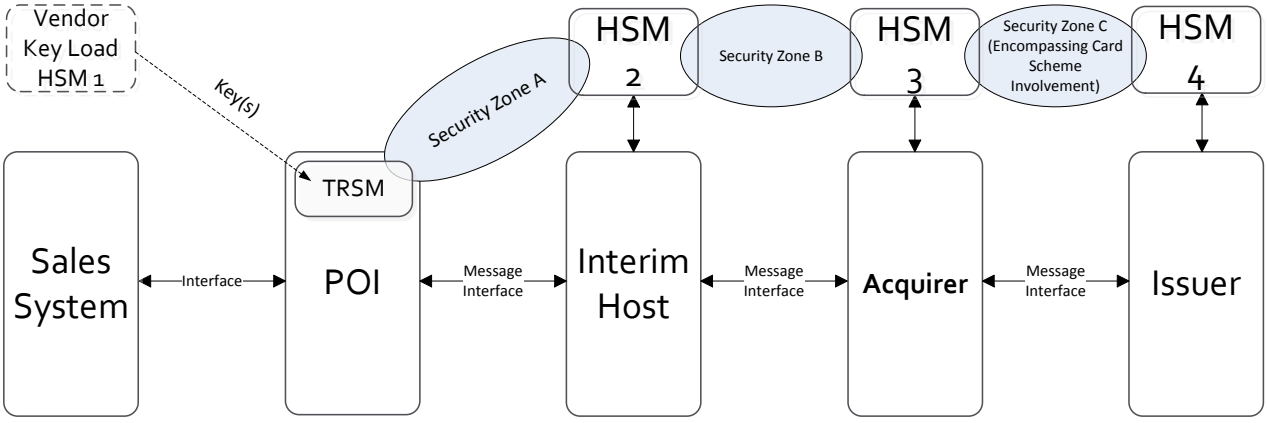

FIGURE 8: EXAMPLES OF HSM USE

2.7.5 HSM Product Certification

HSMs used in card payment solutions conformant to the Volume must be assured and evaluated against one of the following options:

- FIPS PUB 140-2 Level 3 currently approved version;
- PCI HSM currently approved version (v2.0);
- Common Criteria EAL 4.

Certification and approval of a POI does not constitute an approval as a HSM, but a POI may also have an additional certification and approval as a HSM.

Certification and approval to an equivalent standard may be considered provided that the standard is conformant with the processes defined in Book 5.

2.7.6 Operational Security

The PCI PIN Security Requirement is a baseline standard for the secure operation of HSMs.

This covers the minimum operational security requirement that must be complied with by a HSM installation for protecting PINs, but all Key Management requirements apply whether or not the HSM is used for PIN processing.

For example, HSMs used to provide integrity of real time messaging must therefore be operated in line with the PCI PIN requirements even for protocols that do not support online PIN.

2.7.7 Audits

In order to ensure ongoing HSM operational security and conformity, HSM audits must be conducted.

Those entities carrying out such audits must be suitably qualified to certify conformity with the requirements of Secure HSM operations and Key management.

The audit should at least cover:

- the operational environment of the HSM;
- the key management environment including conduct of any key ceremonies;
- the configuration of the HSM;
- any changes relevant to pre- and post-operational security.

The result of an Audit should be communicated to the relevant approval bodies.

2.7.8 Key Management

Management of cryptographic keys must satisfy a formal key management policy and key lifecycle requirements. In particular, the integrity and usage of keys must be assured and the usage of keys must be as restrictive as possible. PCI PIN Security Requirements and the other standards referenced therein for PIN protecting keys should be followed for all cryptographic keys.

2.7.9 Key Ceremonies

All management of keys in cleartext i.e. import, export, storage and destruction of key components must be carried out as a formal key ceremony.

Security sensitive changes to HSM configuration should also be performed as a formal key ceremony.

2.7.10 Test Systems

HSMs used solely in test systems are exempt from the requirements of this document.

Cryptographic keys used in test systems must never be used in operational systems and, conversely, operational keys must never be used in test systems, not even for error searching.

A HSM that has been used in a test system cannot be used as an operational HSM unless it is reconfigured in accordance with PCI PIN or any reference which is used therein. Alternatively it can be certified by its manufacturer as meeting the same requirements as a new or repaired HSM and satisfies the requirements for pre-operational security before it is taken into operations according to the provisions of this document.

An operational HSM may be used as a test HSM provided it has been decommissioned according to the requirements of this document.

2.7.11 Security Configuration

The security configuration of operational HSMs must be “hardened” in the sense that:

- all unused commands must be disabled;
- all unused PIN block formats must be disabled;
- all unnecessary security options must be disabled.

All operational HSMs (including back-up HSMs) used for the same purpose must have the same security configuration, which must be fully documented, including reasons why commands, PIN block formats and security options are enabled.

2.7.12 Changes to Security Configuration

Changes to the security configuration may only be carried out via a key ceremony, following a pre-defined and approved procedure. Commands or security options that need to be enabled for a specific purpose (for example, as part of a key import ceremony) must be enabled only for the minimum time necessary.

2.7.13 New Commands

The impact of any new command must be analysed to ensure that it does not introduce a weakness into the HSM's enabled command set, either by itself or in conjunction with other enabled commands.

The organisation utilising the HSM must have a formal process to approve new commands.

2.7.14 Software Loading

Loading of HSM software or firmware is subject to the principles of dual control and split knowledge and the authenticity of loaded software/firmware must be verified by cryptographic means.

The organisation utilising the HSM must have a formal process to approve and review new software commands.

2.7.15 Physical Access

Operational HSMs must be located in a physically secure environment and must be under dual control. To prevent tampering all equipment used for cleartext input and output must be stored securely when not in use and must also be managed under dual control.

Any equipment used to set the HSM into an authorised state where it is possible to alter the configuration or load a cleartext key must also be stored securely when not in use and must be managed under dual control.

A manual log of direct access to a HSM must be completed, including date/time, names and signatures of the personnel involved and the reason for access.

2.7.16 Network Access

Where operational HSMs may be accessed remotely this must only be via the host-machine and/or by special PED-like devices provided by the HSM manufacturer.

Any access should be authenticated by strong cryptographic processes. The cryptographic authentication process must be performed in secure memory that prevents MiTM attacks. Two-factor authentication must be required.

The minimum number of people necessary shall be granted such access and all access must be logged.

2.7.17 Pre-Operational Security

HSMs sent from the manufacturer must be sealed in tamper-evident packaging, which must be checked upon receipt for signs of tampering. The packaging shall only be opened at the time the HSM is to be installed. The opening and installation must be under dual control. Details of all HSMs installed must be logged including HSM make/model, serial number, location and date of installation. An affidavit attesting to the fact that the HSM was always under dual control until installation was completed must be created and stored for later inspection.

2.7.18 Post-Operational Security

A HSM that is no longer required for operational use must be returned to the factory-default state, via a formal key ceremony, before being removed from service. This procedure must be carried out under dual control. Thereafter, the HSM may be returned to the manufacturer for repair or to the manufacturer (or another approved party) for secure destruction.

In the event that a HSM cannot be returned to the factory-default state via command (i.e. via key ceremony) then a separate procedure must be invoked to ensure that all cryptographic keys and other sensitive data are deleted before repairs or destruction can take place. As above, this procedure must be carried out under dual control.

Under no circumstances shall a HSM that contains live keys or other sensitive data be sent for repair or destruction to a third party.

An affidavit attesting to the correct decommissioning of each HSM must be signed by all personnel involved and stored for possible future inspection.

3 FIGURES AND TABLES