ECSG

european cards stakeholders group

ECSG001-17 01.03.2017

(VOL REF. 8.4.00)

SEPA CARDS STANDARDISATION (SCS) "VOLUME"

STANDARDS' REQUIREMENTS

BOOK 4

SECURITY REQUIREMENTS

Payments and Cash Withdrawals with Cards in SEPA

Applicable Standards and Conformance Processes

Abstract	This document contains the work on SEPA cards standardisation to date
Document Reference	ECSG001-17
Issue	Book 4 - v8.4.00
Date of Version	1 March 2017
Reason for Issue	Publication
Reviewed by	Approved for publication by the ECSG Board of 9 February 2017
Produced by	ECSG Secretariat
Owned by	ECSG
Circulation	Public

Change History of Book 4		
6.4.0.x	2012-2013	Working version of Book 4
7.4.1.0	12.12.2013 (published 07.01.2014)	EPC Published version - Volume v7.0
7.4.1.0x	2014-2015	Working version 2014-2015
7.4.1.05	11.02.2015 (published 10.03.2015)	Consultation version 2015
7.4.2.1	08.12.2015	EPC Published version - Volume v7.1
7.4.2.11-7.4.2.99	16.12.2015-	Working Version 2015-2016
8.4.00	01.03.2017	ECSG Published version - Volume v8.0

Table of Contents

1. General

1.1. Book 4 - Executive summary

It is critical to ensure that security in card services is fully addressed in order to

- Maintain and enhance the cardholder's trust in card payment schemes,
- Enact the risk management of the different stakeholders (or actors) in the value chain in their respective domains,
- Ensure compliance with relevant regulations and security standards.

This book is focused on the security requirements for components of card payment systems regardless of whether the payment is performed in a local or remote environment. For other aspects such as functionality, interoperability and certification, readers shall consult the relevant books within the Volume.

To minimise the need to create new requirements unnecessarily, Book 4 references existing standards and requirements, where these adequately address a particular area. This marks a move towards alignment with Global Standards and expansion of the security requirements definition beyond that of the POI to include security requirements for other components involved in the card payment chain. Consequently, this Book specifies security requirements for components involved in the card payment chain such as:

- Contact and Contactless Cards irrespective of form factor
- Credential(s) Security
- CVM related security
- Data protection
- HSM (Hardware Security Module)
- Mail Order and Telephone Order [MOTO]
- Mobile Contactless Payment Application
- (Mobile) Remote Payment / Authentication Application Security
- POI security (Physical/Remote POI)
- Transaction security

In addition, it provides security guidelines for consumer devices.

The evolving regulatory developments in the field of security are addressed as described in Book 1 and this book will be further updated as appropriate as part of the maintenance process of the Volume.

1.2. Description of changes since the last version of Book 4

Following feedback received from previous consultations, this version includes:

- An overview and requirements for contactless payments (Sections 2 and 3).
- A restructuring of the security requirements for POI (Section 3) to simplify the requirements and make them more high level, in line with the other books of the Volume.
- Requirements for the POI Payment Application.
- Recognition of some new developments and technologies in the payments space.

2. Description of Security Features For Card Transactions

2.1. Introduction

This chapter provides a high level overview of different security aspects related to the transaction flows involved in Card Services. This is achieved either by including the appropriate references or by providing the description.

This Chapter differentiates between security aspects related to local transactions (see 2.2) and remote transactions (see 2.3) because the risk profiles differ in these environments with respect to who performs the card services, the technology used to process the card service, as well as where and which technologies are used to provide the card data. A detailed description of the different environments and technologies is provided in Book 2.

For e- & m- Commerce transactions it should be noted that the consumer device used for Card data entry is not under the control of the issuer, acquirer or their agent(s), and therefore its integrity may not be guaranteed. However, a consumer device may provide access to a secure environment in order to facilitate card authentication and/or cardholder verification to secure remote transactions.

2.2. Local Transactions

For local transactions, a number of well-established security features are implemented in the market and used by the stakeholders. In the context of this book, a distinction is made between whether a physical card (contact or contactless) or a mobile contactless payment application accessed via a mobile device is involved. The security features for both are specified in the relevant sections of the EMV books (see [EMV]).

2.2.1. Local Transactions - Contact

Reference is made to [EMV Book 2].

2.2.2. Local Transactions - Contactless

This document provides a high level overview of the different transaction scenarios possible in Contactless Payments. This includes on-line and off-line payments and the optional execution of a Cardholder Verification Method (CVM).

The mobile environment offers a number of additional features which can be exploited for mobile contactless card payments with respect to Cardholder Verification Methods (CVMs) compared to contactless card payments using physical cards. For mobile contactless, the EPC Mobile Contactless SEPA Card Interoperability Implementation Guidelines [EPC MCP IIG] may also be consulted for further guidance.

2.2.2.1. Card Authentication

For contactless payments, the Contactless / Mobile Contactless Card Application is authenticated by the POI (Offline Data Authentication) and/or by the Issuer (Online Mutual Authentication).

Different Data Authentication methods may be used for the authentication of the Contactless Application as follows:

- A Combined Data Authentication (CDA) (see EMVCo, Book 2, section 6.6)
- A fast Dynamic Data Authentication (fDDA) (See [EMV C3])

2.2.2.2. Cardholder Verification Methods

The CVM differs depending on whether a card or consumer device is used. With mobile contactless transactions additional features of the consumer device such as the keyboard and/or display could be used in the CVM process. The following CVM methods may be applied for contactless transactions based on:

Physical Cards:

- No CVM required
- Offline Encrypted PIN
- Online PIN
- Signature

Mobile Device:

- No CVM required.
- Offline Mobile Code
- Online PIN
- Signature

2.3. Remote Transactions

Remote transactions cover a wide variety of implementations, ranging from manual entry of credentials to a dedicated application on a Consumer Device. Each utilises different security features including Card Authentication (See section 2.3.2.1), CVM (2.3.2.2) and Risk Parameters (Annex 01), which may or may not be EMV based. Section 2.3.2.3 explains how these functions relate to strong customer authentication as defined by EBA (see [EBA]).

The key characteristics of the different types of Remote Payments, including their security features are covered in more detail below.

The Acquirer shall provide the capabilities for the transaction and/or the cardholder to be redirected to the issuer domain for further authentication to allow the issuer to confirm the authenticity and validity of the Card Data presented.

2.3.1. MOTO

Mail Order and Telephone Order (MOTO) are remote transactions where the cardholder provides credentials *(*PAN, expiration date and Card Security Code [CSC]), to pay for goods or services.

For Mail Order transactions the card data is provided in writing by the cardholder. The Acceptor uses a Physical POI or a Virtual Terminal to manually enter Card Data and the address data, as needed, for authorisation and clearing.

2.3.2. e- & m-commerce transactions

e- & m-commerce transactions are made up of a series of phases (such as contracting, shopping, ordering, delivery, payment, tax declaration, possible refund ...) to be presented to the cardholder. For the purpose of this document, card based payment is undertaken during the ordering process. Direct Debit, or Payment upon Delivery are not considered.

The cardholder shall be presented with a sequence of appropriate forms which will need to be completed manually or automatically via their consumer device, depending on the technology being used. In this document the focus is on the payment phase of the e- & m-commerce transaction and, more specifically, on how to guarantee the authenticity of the data exchanged.

When conducting e- or m-commerce transactions, the data security implications for the protection of data including card data when stored or processed in an acceptor’s environment, and the protection of data transmitted over open public networks is of paramount importance. It is therefore the responsibility of the acceptor to adopt appropriate data security measures to protect the data it stores, processes or transmits. Data transmitted over an open public network should always be protected by appropriate cryptography and security protocols, (see section 3.3).

A successful payment transaction requires the execution of protocols at different interfaces, which provide security services proportional to the assessed risks.

The selection of a particular payment instrument may depend, among others, on the amount of the transaction, the transaction environment and the applicable legislation. When registering the cardholder for remote card payment services. Acceptor websites shall also provide similar security information. It is assumed that the cardholder initiates and conducts the transaction using a consumer device such as an *electronic device* (e.g., PC) for use in e-commerce or a *mobile device* (e.g., mobile phone) for m-commerce, as defined in Book 1.

For e- & m-commerce transactions, Acceptors shall not place trust or reliance:

- in the inherent security of the consumer devices used, or

- in the degree to which cardholders may or may not implement their own measures to protect their environment as recommended by their issuer.

In conjunction with a Consumer Device, an Additional Authentication Device may be used by the Issuer to authenticate the cardholder, which could be integrated or connected to the Consumer Device.

As a general rule, the payment phase of an e- or m-commerce transaction shall:

- Be segregated from the ordering and negotiation phases for products and/or services. However, the protocol between the consumer device and the Virtual POI may convey transaction related data (order identifier, nature of the goods, contractual arrangements, delivery details ...).

- Protect the entities involved in the transaction by using security services of authentication, confidentiality, integrity and non-repudiation.

In this section, the different security mechanisms for e- & m-commerce transactions are described. It is assumed that the cardholder initiates and conducts the transaction using a consumer device, occasionally an additional authentication device may also be used (see section 2.3.2.1).

It should also be noted that a mobile device used by the cardholder offers a number of additional features compared to other card payments involving a consumer device, but also a number of additional risks. For example, Over the Air (OTA) is an additional channel available to the issuer to manage the Mobile Payment Application including risk parameters.

Compared to a physical [EMV] card, which possesses characteristics that make them highly suitable for protecting the assets required by payment transactions, the hardware and software in consumer devices are quite complex and typically comprise a number of independent modules developed by different providers.

A risk assessment on transactions involving a consumer device needs to take into consideration the threats to the assets and vulnerabilities in these devices. This also makes the integration of countermeasures more challenging.

There are many ways by which the acceptor will obtain card data from the cardholder and each comes with specific security threats which need to be appropriately addressed by the parties involved. Examples:

- Solutions where the acceptor outsources all the payment functionality to a hosted payment service provider. With this approach, the acceptor never stores, processes or transmits any card data. Total reliance is placed on the service provider hosting the payment page.

- Solutions where the acceptor starts the payment process by providing the cardholder with a payment page. When the payment page has been populated by the cardholder, the payment page is redirected/handed off to the acquirer, sometimes via the Third Party Service Provider. While with this approach card data is not returned to the acceptor, nonetheless, the web site providing the payment page to the cardholder could be a source of vulnerability.

- Solutions where the acceptor's payment page captures and processes card data before submitting it to the acquirer. With this approach, the acceptor shall follow more stringent security requirements for protecting card data across their entire architecture.

It is beyond the scope of this Book to define each and every method and the related security requirements. High level guidance for defining security requirements for e and m-commerce transactions can be found in Chapter 3.7 of this book.

For e- & m-commerce transactions different authentication mechanisms may be used in combination with a CVM. The figure below lists typical combinations ("X") of authentication methods with CVMs:

	Card authentication		
Cardholder verification	No authentication	Static authentication	Dynamic authentication
No CVM	X	X	X[1]
CVM		X	X[2]

Figure 1: Combination of authentication methods / CVMs for e- and m-commerce

2.3.2.1. Card Authentication Methods

In this book, "Card Authentication" refers to data authentication of the "payment instrument". The dedicated data stored on, or accessed through, the consumer device and used to perform an authentication may range from pure (card) payment credentials to a dedicated Authentication Application. The Authentication Application may be integrated in an (M)RP Application as described in Book 2.

[1] The usage of the consumer device as a personal device might allow this combination for certain scenarios (e.g., for low value payments).

[2] For dynamic authentication, the transaction data may be used to generate the challenge which, in combination with a CVM, will create a strong customer authentication method, as defined by the draft EBA RTS guidelines on the security of Internet payments, see *[EBA]*, as well as [PSD2]

To support card authentication by the issuer during an e or m-commerce transaction there are two common processes that are currently adopted, though other methodologies exist:

- In the first process authentication credentials supplied by the cardholder (static authentication), and captured during the payment process, can be carried in the body of the transaction and authenticated by the card issuer during transaction authorisation.

- In the second process, a redirection authentication request is made to the issuer, as the first step of the Authorisation process. The Issuer then executes an authentication directly with their cardholder using the authentication method specified by the Issuer in accordance with the Card Schemes rules. The results of this authentication are then passed by the Issuer to the Acceptor. This process may be utilised within 3 Domain Security.

Different card authentication methods are used for e- & m-commerce transactions:

- A static authentication method using a "*static authenticator*" such as a static Card Security Code (CSC) (e.g., CVV2, CVC2 or CID). The authentication is performed by the issuer validating the static authenticator. The authenticator may be provided by the (M)RP / Authentication Application or may be delivered by other means (e.g., manually entering into the consumer device by the cardholder).

- A dynamic authentication method where the "dynamic *authenticator*" may be

  - A One Time Password (OTP) generated by the issuer or its agent and sent by a different channel to the cardholder (e.g., SMS, e-mail, different device);

  - The result of a random challenge / response mechanism. This may be implemented in different ways:

    - An Additional *Authentication Device* may be involved. In this case, the cardholder inserts his/her payment card into the additional device; the issuer provides the cardholder with a "challenge" to be entered / transmitted (on) to the additional device, followed by the cardholder's PIN entry (CVM). The authentication device then generates a "response" which the cardholder is requested to enter at a given time during this process on his/her consumer device. The response is subsequently transmitted to the issuer via the authentication response for verification.

    - If a dedicated *Authentication Application* (independent or integrated with the (M) RP application) is accessible via the consumer device, a dynamic authentication method (e.g., challenge/response method) is initiated by the issuer or its agent and is handled automatically by the Authentication Application in a *secure environment*. The cardholder is requested to enter his/her personal/mobile code (CVM) only once during the transaction process.

2.3.2.2. Cardholder Verification Methods

The term "CVM" in an e- or m-commerce transaction refers to the method used by the issuer to verify the cardholder. Certain features of the consumer device such as the keyboard and/or display could be used in the CVM process.

Consumer devices such as mobile phones are less exposed to physical attacks, but are very vulnerable to logical attacks. Regardless, the impact of an attack is limited by the number of payment cards that will be processed by a cardholder on a personal device.

Wherever a consumer device is involved, the CVM security requirements differ from the security requirements for physical POIs.

If an offline CVM method (involving a *personal* or *mobile code*) is used with a consumer device, a *secure environment* may be required for the verification process.

Note that if an offline PIN is used in the CVM process, it should only be entered via a secured device (e.g., an additional authentication device) approved by the card scheme. The usage of a CVM is related to the transaction risk management and is currently for e- & m-commerce transactions at the contractual choice of the issuer in accordance to the card scheme license terms.

To perform an online cardholder verification during an e or m-commerce transaction, the cardholder may be redirected to the issuer - this process is known as 3 Domain Security - as the first step of the Authorisation process. The Issuer verifies the cardholder using the previously registered personal or mobile code. The result of this verification is then passed by the Issuer to the Acceptor.

The following CVM methods may be considered for e- and m-commerce:

- Personal / Mobile code verified off-line in a secure environment by the electronic / mobile device (e.g., by a dedicated (M)RP Application or Authentication Application);
- Personal / Mobile code verified on-line by the issuer. Here two different types on-line verification methods may be distinguished:
  - Checked by the issuer via the card network (standard authorisation message);
  - Checked by the issuer via internet using a secure channel (outside the card network);
- Offline PIN verification performed in combination with an authentication mechanism (e.g., using an additional authentication device).

	No CVM	On-line CVM	Off-line CVM
On-line transaction	X	X	X
Off-line transaction	X	C	X

FIGURE 2: TRANSACTION TYPES AND CVMS FOR E- AND M-COMMERCE

Where multiple e- or m-commerce transactions are performed consecutively by the same cardholder, it may be considered inconvenient to request a CVM for each of these transactions. The CVM could be considered valid for the subsequent transactions based on issuer pre-set parameters, but at acceptor's risk.

2.3.2.3. *Strong Customer Authentication*

The combination of a dynamic card authentication method (see section 2.3.2.1) with a CVM provided by the cardholder (see section 2.3.2.2) will create a "strong customer (cardholder) authentication method" as defined by the EBA Final guidelines on the security of internet payments (see *[EBA]]*).

2.3.2.4. *Passive Authentication*

Passive authentication is a complementary technique used by Issuers which does not require the direct involvement of the Cardholder. It may be composed of Consumer Device authentication and/or transaction specifics.

Consumer Device authentication may include:

- Verification of characteristics of the Consumer device being used,
- Verification of the location of the Consumer device, e.g., as per a geo-location facility on a mobile device,
- Verification of the true IP of the Consumer device being used.

Transaction specifics may include amount, date, acceptor name, etc.

To perform a passive authentication during an e or m-commerce transaction, the cardholder needs to be redirected to the issuer as the first step of the Authorisation process.

2.3.2.5. *Additional authentication considerations*

Additional considerations may be taken into account with respect to the authentication methods used such as:

- The Cardholder is a repeat customer and was authenticated on previous occasions
- The Cardholder is using the same payment card
- The Cardholder is requesting delivery of the goods or services to the same address.

3. SECURITY REQUIREMENTS

3.1. Introduction

This chapter defines security requirements for:

- Card Transactions including Card Authentication, CVMs and Risk Parameters
- Cardholder Environments
- POIs
- Mobile devices
- HSMs
- Communication protocols.

3.2. Security Requirements for Card Data

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

However, the degree to which PCI-DSS applies to a particular environment is to be determined by the different card schemes which will be supported in that payment context. Card schemes may accept equivalent security processes.

This applies throughout Book 4 where PCI-DSS is referred to.

The position will be reviewed on an on-going basis to cater for the global adoption and use of EMV approved chip cards, and also for the development of a robust authentication process for Card-Not Present (CNP) transactions that will keep card data secure.

In addition certain sections are currently optional to vendors:

- Section K covers Secure Read and Exchange of Data (SRED) relating to the encryption of cardholder data and message authentication within the POI device

- Section N covers Requirements for the POI Application.

3.3. Cryptography and Key Management

For encryption or key management, appropriate cryptographic algorithms and key lengths shall be employed. Guidance is given in EMV and [EPC Crypto].

3.4. Security Requirements for Card Transactions

3.4.1. Local transactions

3.4.1.1. Chip with Contact

For local contact transactions, the security requirements specified in [EMV B2] apply.

3.4.1.2. Chip and Mobile Contactless

For Contactless Transactions, the relevant Security Requirements defined by EMV shall apply. In addition the following requirements shall apply:

Req S1: For Card Authentication for contactless transactions, dynamic authentication as described in section 2.2.2 shall be performed.

Req S2: The risk parameters “Acquirer CVM Limit”, “Floor Limit” and “Transaction Limit” shall be supported by the Physical POI.

Req S3: The acquiring systems and protocols used shall be able to support the authentication methods and the CVM methods, as appropriate, described respectively in sections 2.2.2.1 and 2.2.2.2.

Req S4: If a PIN/Mobile Code is used for CVM, then they shall be used in conjunction with a PIN/Mobile Code Try Limit and with a PIN/Mobile Code Try Counter.

Req S5: Mechanisms shall be made available by the Card and the POI to safeguard against relay attacks.

3.4.2. e- and m-commerce

This section focuses on the security requirements of the following:

- The virtual POI.
- The communication protocols used between components.
- The (M)RP related data, (M)RP Application including personalisation data, Authentication Application and (M)RP credentials, that may be hosted on the consumer device (electronic or mobile device);
- The consumer devices and the secure environments used in conjunction with those devices, typically an SE/TPM located in the device, a secure environment located on a secured server and remotely accessed via the electronic device as the carrier of the (M)RP related data, with the potential presence of an additional TEE;

For e- and m-commerce, authentication may take place at any phase of the transaction. However, it is assumed that authentication (see section 2.3.2.1) will take place during the payment phase.

A particular security protocol is not enforced during the payment phase of the e- or m-commerce transaction. As a consequence, this chapter assumes that different trade-offs may be applied in terms of simplicity, performance and security. Implementations conformant with this Book may therefore feature different levels of security.

For e- & m-commerce transactions, the following security requirements apply:

Req S6: The usage of static or dynamic authentication is at the discretion of the Issuer provided that the Issuer complies with [PSD2] as well as the EBA RTS [EBA1] and national regulations.

Req S7: Strong customer authentication shall be performed in accordance with the [PSD2] and the EBA RTS. See section 2.3.2.3.

Req S8: On-line authorisation shall be supported unless a dedicated (M)RP application is used.

Req S9: The risk parameters “Acquirer CVM limit” and “Floor limit” shall be supported by the virtual POI.

Req S10:The acquiring systems and protocols used shall be able to support the authentication methods and the CVM methods, as appropriate, described respectively in sections 2.3.2.1 and 2.3.2.2

3.4.3. MOTO

For MOTO transactions the following security requirements apply:

Req S11: The floor limit for all MOTO transactions shall be set to zero.

Req S12:

1. The PAN number shall be entered first. If initial PAN validation takes place off-line, the following checks shall be performed:

   a) valid IIN

   b) the PAN number entered is the correct length

   c) valid LUHN check digit

   Otherwise the PAN shall be validated during authorisation immediately after step 3.

2. The expiry date is entered and checked to ensure the month is in a range of 01 - 12 and within 20 years, to mitigate against errors when entering Card Data.

3. The CSC shall be entered.

Req S13:

1. The PAN shall be protected.

   The full PAN should not be displayed on operator screens. The first 6, last 4 digits may be displayed.

2. Only the last 4 digits of the PAN shall be printed on the cardholder receipt.

3. Access to card data shall be limited to those who have a business need to view the data.

Req S14: Card Data shall be encrypted when transmitted across open public networks as required by card schemes.

Req S15: Sensitive card data shall be appropriately protected.

Req S16: Static Authentication as described in section 2.3 shall be performed at a minimum which involves the Issuer verifying the data presented.

Req S17: The static authenticator (CSC) shall be securely deleted by the Acceptor after authorisation, which means it shall never be stored post-authorisation.

Req S18: For Telephone Order, the Card Data shall not be included in call recordings, even if encrypted[3].

3.5. Security Requirements for Cardholder Verification

This section provides security requirements for the following CVMs: PIN, Personal and Mobile Code.

Biometrics is recognised as a technology which may be used for CVM purposes. However, the ECSG considers that, as Biometrics as a CVM is still evolving, this version of the Volume is not identifying specific requirements for this technology. The ECSG will continue to analyse Biometrics in the context of Card Services.

It is proposed that future versions of the Volume will provide Security requirements for the use of Biometrics as a CVM as well as CDCVM.

3.5.1. PIN Security Requirements

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

[3] This would involve the storage of the CSC, which is in contradiction with the mandatory requirements of the Payment Card Industry Data Security Standard (PCI DSS).

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

Req S19: For online transactions, PINs shall be formatted according to ISO 9564-1 PIN block formats 0, 1, 3 or 4 prior to encryption and shall be encrypted using a dynamic encryption method like DUKPT (Derived Unique Key Per Transaction) or UKPT (Unique Key Per Transaction). Format 1 should be avoided when the PAN is available.

Req S20: Format 2 shall 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.

Req S21: PIN translation from one ISO PIN block format into another shall follow the PIN block format translation restrictions defined in ISO 9564-1.

Req S22: If random values are not used for key derivation, unique key methods shall be applied. Such methods may involve the use of uni-directional, dynamic session keys (i.e. shall 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:

Req S23: The PIN shall be encrypted inside a TRSM (PIN pad or PED) where the PIN is entered by the cardholder at the POI.

Req S24: The PIN shall be translated from one cryptographic zone to another, inside an approved hardware security module (HSM) at a non-issuer host system, e.g. acceptor and acquiring host.

3.5.2. Personal and Mobile Code Security Requirements

Req S25: If Personal or Mobile Code is used and processed, then it shall be protected using appropriate security standards. These will be assessed for a later release of Book 4.

3.6. Security Requirements for Card Environments

3.6.1. Security Requirements for Physical Chip Cards

This section describes the generic security requirements for Physical Chip Cards. It details the following:

- Scope of Evaluation, outline what parts and functions of the Chip Card are to be evaluated;
- Security Objectives and 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 Physical Chip Card, refer to Book 5, which describes the requirements for an Evaluation and the Certification Methodology.

3.6.1.1. 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, as clarified within figure 5.

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

- Application Selection (at card level);
- Initiate Application Processing;
- Off-line communication with the POI;
- Off-line Data Authentication;
- On-line Authentication and communication with the issuer;
- Cardholder Verification;
- 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 in table 6 can be used to evaluate any Chip 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. Chip Card functionality is therefore modelled on the typical EMV transaction flow. The figure below shows the architecture and components on a typical multi-application Chip Card.

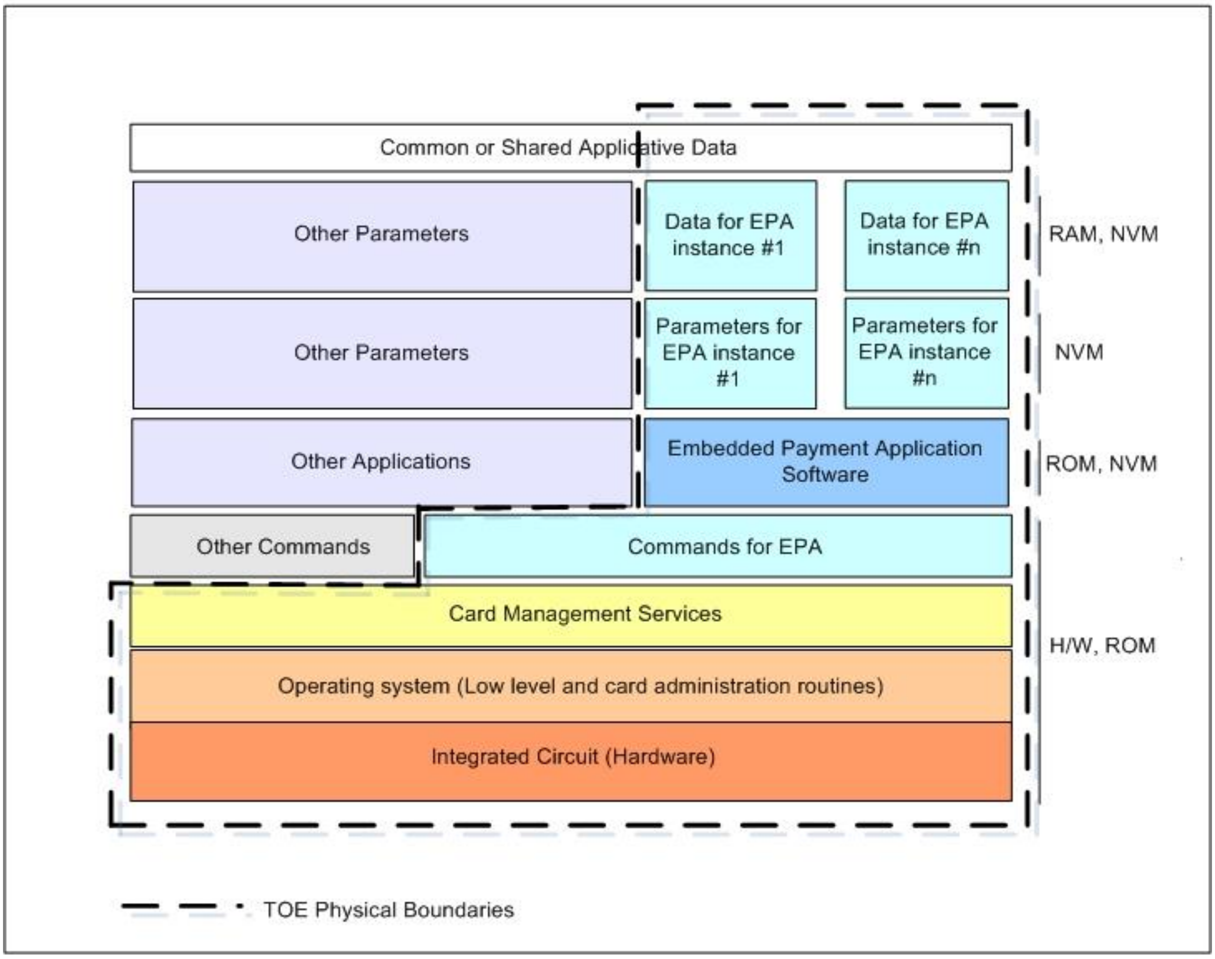

Common or Shared Applicative Data
Other Parameters
Data for EPA instance #1
Data for EPA instance #n
RAM, NVM
Other Parameters
Parameters for EPA instance #1
Parameters for EPA instance #n
NVM
Other Applications
Embedded Payment Application Software
ROM, NVM
Other Commands
Commands for EPA
Card Management Services
H/W, ROM
Operating system (Low level and card administration routines)
Integrated Circuit (Hardware)
TOE Physical Boundaries

FIGURE 3: ARCHITECTURE AND COMPONENTS ON A TYPICAL MULTI-APPLICATION CHIP CARD

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 Chip Card encompasses all layers and embedded resources contributing to Payment Application functionality. Most banking chip cards may operate more than one application. In this case, all other applications (payment and non-payment) fall outside the chip card perimeter, but stay within the chip card environment, so the evaluator can assess their impact on Payment Application security, e.g. an appropriate implementation of firewalls.

There is no restriction on card technology (single- 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.

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.

3.6.1.2. Security objectives

The following Security Objectives have to be met:

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

SUA2	O.CH_VER	When required by the transaction flow, the Chip card 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 Chip 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 Chip Card enforces protection of its services against service denial or corruption.**	
EP1	O.OPERATE	The Chip Card shall 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 Chip Card.
EP2	O.ISOLATION	The Chip 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 Chip Card protects sensitive data from corruption and disclosure when required.**	
DP1	O.SECRECY	The Chip 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 Chip Card shall ensure that sensitive information managed or manipulated by the Chip 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 Chip Card
DP3	O.CRYPTO	The Payment Application keys and Payment Application reference PIN shall be protected from potential exploitation of implementation security weaknesses that would lead to their values being determined and obtained.

SP	**SERVICES PROTECTION** **The Chip Card enforces its own security policy to prevent provided services from being attacked.**	
SP1	O.RISK_MNGT	The Chip 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 Chip Card shall ensure that the issuer of the Payment Application is the only external user able to access the services for Chip Card parameter modification: – Payment Application Reference PIN, – Payment Application Keys, – Payment Application Selection Parameters, – Payment Application Card Transaction Parameters
SP3	O.DETECTION	The Chip Card shall administrate the detection of security violations: corruption of sensitive card content, access to restricted area, or improper conditions of use of the Chip Card. *Application note: the Chip 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 4: SECURITY OBJECTIVES

3.6.1.3. 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 Chip Cards shall be equivalent to the assurance package defined as EAL4 in the Common Criteria methodology[4]. Nevertheless an EAL4 set of assurance requirements shall be augmented taking in to consideration the following criteria:

Type of assurance augmentation	**Description**
Life Cycle Support _ Sufficiency of security measures.[5]	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.[6]	It is the highest possible level for vulnerability analysis and penetration testing. It requires the card to resist all CC-referenced attacks on Chip Cards, either through software, hardware or combination of both. It is traditionally labelled as "*highly resistant*"

TABLE 5: EAL4 ASSURANCE CRITERIA

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

3.6.1.4. Contactless Card Security Requirements

For Contactless Cards the Security Objectives from paragraph 3.6.1.4 apply. In addition, the following Security Objectives are defined for Contactless Cards.

[4] 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.

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

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

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

TABLE 6: 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.

3.6.2. Security requirements for Mobile Contactless Payment Applications residing in a Secure Element

This section describes the generic security requirements for an MCP Application residing within a secure element on a mobile device, performing the payment functions related to an MCP, as dictated by the MCP issuer. It details the following:

- Scope of Evaluation, outline what parts and functions of the SE and MCP Application are to be evaluated;
- Security Objectives and Assurance Level, outline of main security requirements.

The ECSG recognises that new technical solutions for Mobile Contactless Payments are continuously being introduced into the market which may come with different security risks (e.g. TEE implementations based on HCE, presenting a different risk model). Future releases of the

Volume will cover those as the technologies further mature and will reflect relevant industry standards.

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

3.6.2.1. Scope of the Evaluation

The Target of Evaluation includes all hardware and software parts of the SE and MCP application needed to perform the payment functionality and to enforce its security.

SE and MCP application functionality, can consist of transactions and possibly also card management functions, as specified by each payment scheme. In this respect, it is assumed that the following basic capabilities are supported:

- Application Selection (at SE level);
- Initiate Application Processing;
- Off-line communication with the POI;
- Off-line Data Authentication (as described in *[EPC1]*);
- On-line authentication and communication with the issuer (as described in *[EPC1]*);
- CVM (see section 2.3.2.2);
- MCP risk management;
- Transaction Certification;
- Script processing (to update MCP 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 for ny MCP applications on an SE that provides contactless payments via the NFC interface by supporting the basic capabilities listed above. It is an assumption that Secure Elements are either Chip cards (e.g. UICCs) or share common technology with Chip cards (secure micro SD card or embedded SE) such that evaluation services used for Chip cards (e.g. payment cards) can be utilised.

The SE encompasses all layers and embedded resources contributing to MCP application functionality. SEs may operate next to the MCP other applications. In this case, the latter applications fall outside the MCP application perimeter, but stay within the SE environment, so the evaluator can assess their impact on the MCP application security.

There is no restriction on SE technology provided that all security requirements expressed, and mainly focusing on MCP application functionality, are met.

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

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

3.6.2.2. *Security Objectives*

TP	**TRANSACTION PROTECTION** **The SE and the MCP application enforce generation of unique certificates binding their users, following the transaction flow as defined by the MCP application specifications**	
TP1	O.GENUINE_ TRANSACTION_ONCE	The probability that two transaction certificates generated by a genuine MCP application, including authentication certificates, transaction certificates, and authorisation certificates are equal shall be very low. This is related to having genuine "unique" transactions.
TP2	O.TRANSACTION_BINDING	Transactions using offline Mobile Code verification shall bind the cardholder. Transactions cannot be modified at the advantage of an attacker; certified terms of the transactions shall not be modified, and transactions shall not be modified such they can be denied.
TP3	O.INTENDED_TRANSACTION_FLOW	The normal transaction flow as defined by the MCP application specifications shall be followed and any attempt at bypassing expected transaction steps shall be detected.
TP4	O.EXHAUSTIVE_PARAMETERS	The SE and the MCP application shall be secure for all the possible values of parameters.
SUA	**MCP APPLICATION AND USER AUTHENTICATION** **The MCP application provides means for its authentication and enforces authentication of some users in order to prevent forgery and identity usurpation.**	
SUA1	O.AUTH	The SE services shall be protected from transaction forgery by ensuring MCP application authentication during the processing of each payment transaction.
SUA2	O.CH_VER	When required by the transaction flow, the MCP application shall verify the Cardholder. For Mobile Code verification by the MCP Application, the following apply: – Systematic counting to identify verification failure.

		– Secure authentication invalidation when Mobile code is blocked. – Secure authentication validation when Mobile Code comparison succeeds.
SUA3	O.ISSUER_AUTH	The MCP application shall ensure the authentication of the MCP 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 MCP Application Card Manager.
EP	**EXECUTION PROTECTION** **The SE and the MCP application enforce protection of their services against service denial or corruption.**	
EP1	O.OPERATE	The SE and the MCP application shall ensure the continued operation of their services: the MCP application and embedded payment application resources shall be available under normal conditions of use of the SE.
EP2	O.ISOLATION	The SE and the MCP application shall ensure MCP application isolation through a secure data sharing mechanism. This means that no other application within this SE shall be able to access or modify MCP application data without authorisation by the data sharing mechanism.
DP	**DATA PROTECTION** **The SE and the MCP application protect sensitive data from corruption and disclosure when required.**	
DP1	O.SECRECY	The SE and the MCP application shall ensure that the storage and the manipulation of their sensitive information are protected against unauthorised disclosure: – SE Management Keys;

		– MCP Management Keys;
		– MCP Transaction Mobile Code;
		– MCP Reference Mobile Code;
		– MCP Application Keys.

DP2	O.INTEGRITY	The SE and the MCP applications shall ensure that sensitive information managed or manipulated by the SE or MCP applications is securely protected against any corruption or unauthorised modification:
		– SE configuration and management data;
		– MCP Application PAN;
		– MCP Application Keys;
		– MCP Application Risk Parameters;
		– MCP Reference Mobile Code;
		– MCP Application Selection Parameters;
		– MCP Application Transaction Parameters;
		– MCP Application Transaction Data;
		– POI Transaction Data when operated by the MCP application.

DP3	O.CRYPTO	Cryptographic services, including keys, shall be protected from exploitation that would lead to confidential information being revealed or to incorrect operation of the cryptographic mechanism.
SP	**SERVICES PROTECTION** **The SE and the MCP application enforce their own security policy to prevent provided services from being attacked.**	
SP1	O.RISK_MNGT	The SE and the MCP application shall ensure that MCP application Risk Management features cannot be corrupted or manipulated: – System and security counters (e.g. ATC). – Risk parameters (limits and counters).
SP2	O.EPA_ISSUER	The SE shall ensure that the issuer of the SE is the only external user able to read and modify SE management features and data. The SE and the MCP application shall ensure that the issuer of the MCP application is the only external user able to read and modify MCP application features and data.

SP3	O.DETECTION	The SE and the MCP application shall administrate the detection of security violations: corruption of sensitive content, access to restricted area or improper conditions of use of the SE.
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 7: SECURITY REQUIREMENTS FOR SECURE ELEMENTS AND MCP APPLICATIONS

3.6.2.3. 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 take a greater evaluation effort, through a broader scope, a greater attention to fine details or a more formal evaluation process.

The assurance level to be associated with the Security Objectives listed for SEs and MCP Applications shall be equivalent to the assurance package defined as EAL4+ in the Common Criteria methodology[7]. Nevertheless an EAL4+ set of assurance requirements shall be augmented regarding the following criteria:

Type of assurance augmentation	**Description**
Life Cycle Support _ Sufficiency of security measures[8]	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, SE Issuer, MCP application loader).

[7] 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.

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

Vulnerability Analysis _ Advanced Methodical Vulnerability Analysis[9]	It is the highest possible level for vulnerability analysis and penetration testing. It requires the SE to resist all Common Criteria referenced attacks on chip cards, either through software, hardware or combination of both. It is traditionally labelled as "*highly resistant*".

TABLE 8: TYPE OF ASSURANCE AUGMENTATION

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 recognised.

3.6.3. Security requirements for Applications and Credentials for e- & m-commerce

This section refers to what comprises the generic security requirements for Authentication Applications, (Mobile) Remote Payment Applications and Credentials hosted on or accessed via a consumer device (an electronic or mobile device).

3.6.3.1. (M)RP related data types and locations

The figure below lists a number of categories[10] that might be considered to help define generic security requirements for the (M)RP related data. These categories have been identified, based on the type of (M)RP related data (applications or credentials), their location for storage and processing, and the possible presence of a TEE, next to an SE / TPM or a Secured Server. The categories where a secure environment is not involved are not covered in this document.

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

[10] This list is not meant to be exhaustive; other categories may involve components such as a mobile wallet.

Category	(M)RP related data Type	(M)RP related data Access	SE/TPM on consumer device	Secured Server	TEE on consumer device
1	Credentials	Manually entered by cardholder	N	-	N
			N	-	Y
2a	Credentials	Stored on the consumer device	N	-	N
			N	-	Y
			Y	-	N
			Y	-	Y
2b	Credentials	Stored outside the consumer device	-	Y	N
			-	Y	Y
3a	(M)RP / Authentication Application	Stored on the consumer device	Y	-	N
			Y	-	Y
3b	(M)RP / Authentication Application	Stored outside the consumer device	-	Y	N
			-	Y	Y

FIGURE 9: TYPICAL EXAMPLES OF LOCATIONS FOR STORAGE AND PROCESSING OF (M)RP RELATED DATA

The figure shall be interpreted as follows:

- For category 1, if credentials are manually entered, there is no storage on the secure device but TEE may be present.
- For category 2a, the credentials may be stored on the consumer device, in a SE/TPM or not and each comes with the possible presence of a TEE.

The security requirements for the categories 1, 2a and 2b, 3a and 3b are covered respectively in sections 3.6.3.2, 3.6.3.3 and 3.6.3.4.

3.6.3.2. Security Requirements for (M)RP Credentials Manually Entered by Cardholder

In the first two entries listed under category 1 in Figure 11, the (M)RP related data used at the time of the e- or m-commerce transaction are the credentials of a physical card.

- In the first entry whereby a TEE is not present, no additional security requirements need to be defined since (M)RP related data are not stored in or accessed via the electronic / mobile device and the security requirements for physical cards apply.

- In the second entry whereby a TEE is present, the reader is referred to section 3.6.3.5 for more details.

3.6.3.3. *Security Requirements for Secure Environments and (M)RP Credentials residing on a Consumer Device*

This section refers to what comprises the generic security requirements for a secure environment with (M)RP Credentials. It details the following:

- Scope of evaluation, what parts & functions of the secure environment and (M)RP related data are to be evaluated;

- Security Objectives & Assurance Level, an outline of the main security requirements.

In order to provide an understanding of how this section can be used and what is required for a security evaluation, the reader is referred to Book 5, describing the Evaluation and Certification Methodology.

Security Requirements for secure environments residing on a Secured Server may be handled in a future release.

3.6.3.3.1. *Security objectives*

The following Security Objectives apply for a secure environment storing (M)RP credentials.

DP_S	**DATA PROTECTION** **The secure environment protects sensitive data from corruption and disclosure when required.**	
DP_S1	O.SECRECY	The secure environment shall ensure that the storage and the manipulation of their sensitive information are protected against unauthorised disclosure: • Secure environment Management Keys.
DP_S2	O.INTEGRITY	The secure environment shall ensure that sensitive information managed or manipulated by the secure environment is securely protected against any corruption or unauthorised modification: • Secure environment configuration and management data; • Data, such as PAN, expiry date …

FIGURE 10: SECURITY REQUIREMENTS FOR SECURE ENVIRONMENTS AND (M)RP CREDENTIALS

3.6.3.3.2. Assurance Level

The same assurance level as in section 3.6.2.3 shall be met.

3.6.3.4. Security Requirements for Secure Environments and (M)RP / Authentication Applications

This section includes the generic security requirements for a secure environment with an (M)RP / Authentication Application. It details the following:

Scope of evaluation, what parts & functions of the secure environment and (M)RP related data are to be evaluated;

Security Objectives & Assurance Level, an outline of the main security requirements.

In order to provide an understanding of how this section can be used and what is required for a security evaluation, the reader is referred to Book 5, describing the Evaluation and Certification Methodology.

3.6.3.4.1. Scope of the Evaluation

The Target of Evaluation covers all security aspects and data types (as per Figure1). It includes all hardware and software parts of the secure environment and (M)RP related data needed to perform the payment functionality and to enforce its security.

While each payment scheme will specify its own requirements for (M)RP data type, access and environments, it is assumed that the following capabilities may be supported:

- CVM;
- (M)RP risk management;
- On-line authentication and communication (e.g. authorisation) with the (M)RP issuer;
- Off-line authentication/authorisation in a secure environment by the electronic / mobile device (e.g. by a dedicated (M)RP Application or Authentication Application);
- Transaction completion;
- (M)RP risk parameters update.

The security requirements specified in the following sections can be used by any (M)RP or Authentication Application that supports all or a subset of the functionalities listed above.

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

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

3.6.3.4.2. Security objectives

The following Security Objectives apply for remote e- or m-commerce transactions whereby a secure environment including a dedicated (M)RP or Authentication Applications is involved.

TP	**TRANSACTION PROTECTION** **The secure environment and the (M)RP / Authentication Application enforce generation of unique certificates binding their users, following the transaction flow as defined by the (M)RP Application specifications**	
TP1	O.GENUINE_ TRANSACTION_ONCE	The probability that two transaction certificates generated by a genuine (M)RP / Authentication Application, including authentication certificates, transaction certificates, and authorisation certificates are equal shall be very low. This is related to having genuine "unique" transactions.
TP2	O.TRANSACTION_BINDING	Transactions using offline CVM shall bind the cardholder. Transactions cannot be modified at the advantage of an attacker; and certified terms of the transactions shall not be modified, and transactions shall not be modified such they can be denied.
TP3	O.INTENDED_TRANSACTION_FLOW	The normal Transaction flow as defined by the (M)RP / Authentication Application specifications shall be followed and any attempt at bypassing expected transaction steps shall be detected.
TP4	O.EXHAUSTIVE_PARAMETERS	The secure environment and the (M)RP / Authentication Application shall be secure for all the possible values of parameters.
SUA	**(M)RP / AUTHENTICATION APPLICATION AND USER AUTHENTICATION** **The (M)RP / Authentication Application provides means for its authentication and enforces authentication of some users in order to prevent forgery and identity usurpation.**	
SUA1	O.AUTH	The secure environment services shall be protected from transaction forgery by ensuring the authentication of the (M)RP / Authentication Application during the processing of each payment transaction.
SUA2	O.CH_AUTH	The (M)RP / Authentication Application shall ensure the authentication of the cardholder while processing any transaction: • Authentication failure systematic counting;

		• Secure authentication invalidation when CVM (including personal / mobile code) is blocked; • Secure authentication validation when CVM (including personal / mobile code) execution succeeds.
SUA3	O.ISSUER_AUTH	The (M)RP / Authentication Application shall ensure the authentication of the issuer for any (M)RP / Authentication Application management process (e.g. update of risk parameters) involving the issuer.
SUA4	O.CARD_MANAGER	Card[11] Management processing is authorised to the authenticated (M)RP / Authentication Application Card Manager.
EP	**EXECUTION PROTECTION** **The secure environment and the (M)RP / Authentication Application enforce protection of their services against service denial or corruption.**	
EP1	O.OPERATE	The secure environment and the (M)RP / Authentication Application shall ensure the continued operation of their services: the application and embedded application resources shall be available under normal conditions of use of the secure environment.
EP2	O.ISOLATION	The secure environment and the (M)RP / Authentication Application shall ensure application isolation between the (M)RP / Authentication Application and all other application(s), such that no other application can read or modify application data within this secure environment.
DP	**DATA PROTECTION** **The secure environment and the (M)RP / Authentication Application protect sensitive data from corruption and disclosure when required.**	
DP1	O.SECRECY	The secure environment and the (M)RP / Authentication Application shall ensure that the storage and the manipulation of their sensitive information are protected against unauthorised disclosure: • Secure environment Management Keys; • Application Management Keys;

[11] In this case, the card should be interpreted as the secure environment where the application resides.

		• Application Reference CVM; • Application Transaction CVM.
DP2	O.INTEGRITY	The secure environment and the (M)RP / Authentication Application shall ensure that sensitive information managed or manipulated by the secure environment or application is protected against any corruption or unauthorised modification: • Secure environment configuration and management data; • Application data, such PAN, expiry date, static authentication data …; • Application Keys; • Application Risk Parameters; • Application Reference CVM; • Application Transaction Parameters; • Application Transaction Data • POI (Transaction) Data when operated by the (M)RP / Authentication Application
DP3	O.CRYPTO	The (M)RP / Authentication Application keys and Payment Application reference CVM shall be protected from potential exploitation of implementation security weaknesses that would lead to their values being determined and obtained.
SP	**SERVICES PROTECTION** **The secure environment and the (M)RP / Authentication Application enforce their own security policy to prevent provided services from being attacked.**	
SP1	O.RISK_MNGT	The secure environment and the (M)RP / Authentication Application shall ensure that (M)RP / Authentication Application Risk Management features cannot be corrupted or manipulated: • System and security counters; • Risk parameters (limits and counters).
SP2	O.EPA_ISSUER	The secure environment shall ensure that the supplier of the secure environment is the only external user able to read and modify secure environment management features and data. The secure environment and the (M)RP / Authentication Application shall ensure that the issuer of the (M)RP / Authentication Application is the only external user able to read and modify (M)RP / Authentication Application features and data.

SP3	O.DETECTION	The secure environment and the (M)RP / Authentication Application shall administrate the detection of security violations: corruption of sensitive content, access to restricted area or improper conditions of use of the secure environment.
MP	**(M)RP / AUTHENTICATION APPLICATION PROTECTION** **The application is adequately protected from corruption.**	
MP1	APP.CERTIFICATION	Combined certification of the platform (secure environment) + the (M)RP / Authentication Application residing on it shall be executed.
MP2	APP.INTERFERENCE	Verification of all other basic applications that are residing on the platform (secure environment) shall be executed.

FIGURE 11: SECURITY REQUIREMENTS FOR SECURE ENVIRONMENTS AND (M)RP / AUTHENTICATION APPLICATIONS

3.6.3.4.3. Assurance level

Assurance forms the basis 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. Greater assurance results from a greater evaluation effort, through a broader scope, a greater attention to fine details or a more formal evaluation process.

The assurance level to be associated with the above Security Objectives for secure environments shall be equivalent to the assurance package defined as EAL4+ in the Common Criteria methodology[12]. Nevertheless an EAL4+ set of assurance requirements shall be augmented by using the following criteria:

[12] 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.

Type of assurance augmentation	**Description**
Life Cycle Support _ Sufficiency of security measures[13]	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 secure environment manufacturer, secure environment issuer, (M)RP / Authentication Application loader).
Vulnerability Analysis _ Advanced Methodical Vulnerability Analysis[14].	It is the highest possible level for vulnerability analysis and penetration testing. It requires the secure environment to resist all Common Criteria referenced attacks on chip cards, either through software, hardware or combination of both. It is traditionally labelled as "*highly resistant*".

FIGURE 12: TYPE OF ASSURANCE AUGMENTATION

It is the responsibility of the secure environment and 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, as for instance specified by GlobalPlatform (see *[GP1]*) is recognised. 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/TPM suppliers are encouraged to resort to it.

3.6.3.5. Security Requirements for TEE and (M)RP Related Data

In a consumer device, applications typically are executed in an environment provided and managed by a Rich OS, the so-called REE (Rich Execution Environment) which is outside the Trusted Execution Environment (TEE). This environment and applications running on it are considered un-trusted.

A TEE can be defined as a dedicated execution environment providing security features such as isolated execution, integrity of applications along with confidentiality of their assets for the deployment of sensitive services. It complements SEs / TPMs for handling sensitive assets, brings security to interaction with the cardholder and has the potential to control data flows in the consumer device.

The TEE runs alongside the Rich OS and provides security services to that rich environment and applications running inside the environment. A set of TEE APIs allows the communication from the REE to run Trusted Applications within the TEE.

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

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

The interfaces between the main components are represented in Figure 13.

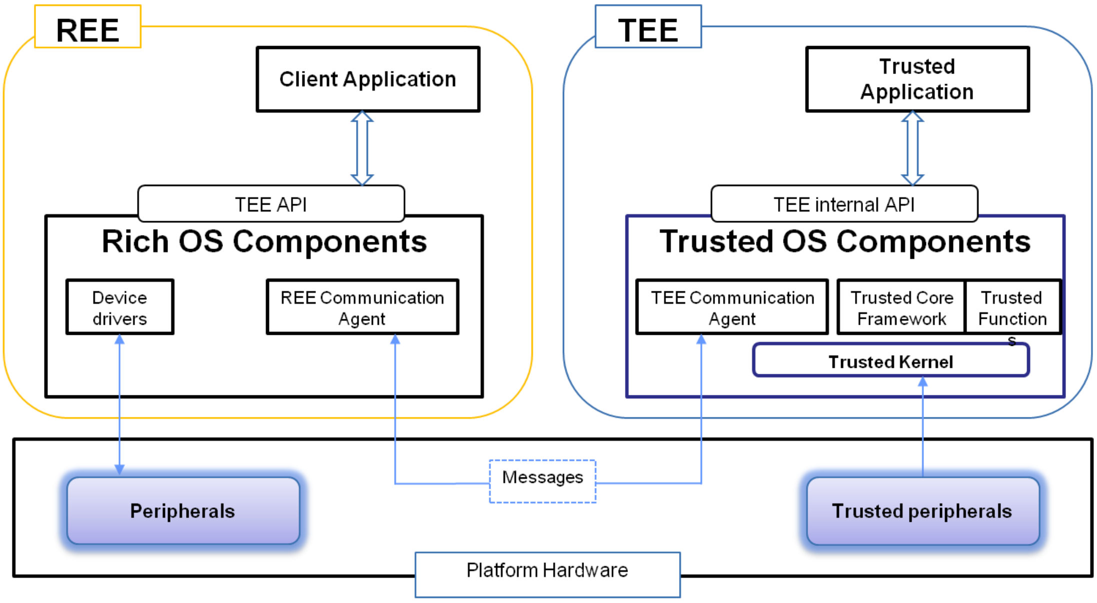


FIGURE 13: EXAMPLE OF A TEE MODEL

The model identifies API interfaces and a communication agent within the REE:

- These APIs allow access to some TEE services, such as cryptography or trusted storage and enable the execution of a Client Application in the Rich OS to access and exchange data with a Trusted Application running inside a TEE. The TEE API in the REE enables the standard communication with the TEE and is used by the Client Application.

- The REE Communication Agent provides REE support for messaging between the Client Application and the Trusted Application.

Note: A mobile device has a set of peripherals that may be controlled either by the REE or by the TEE but not by both at the same time. Therefore, when a peripheral is under the control of the TEE and cannot receive a request from the REE, it is referred to as a trusted peripheral (sometimes also referred to as a peripheral in “Trusted User Interface (TUI) mode[15]).

3.6.3.5.1. Security objectives

The following Security Objectives apply for e- or m-commerce transactions whereby a TEE is involved.

DPTEE	**DATA PROTECTION** **The TEE protects sensitive data from corruption and disclosure when required.**

[15] More information on the TUI is provided in [GP4].

DPTEE1	TEE.SECRECY	The TEE shall provide a safe area[16] (a trusted storage) on the consumer device to protect sensitive information from unauthorised access. The TEE shall ensure that the storage of the sensitive information are protected against unauthorised access: • TEE configuration and management data; • Data, such as PAN, expiry date … This trusted storage shall be bound to the consumer device such that no unauthorised internal or external attacker may access, copy or modify the data contained.
DPTEE2	TEE.INTEGRITY	The TEE shall ensure that sensitive information managed or manipulated by the TEE is securely protected against any corruption or unauthorised modification by notifying any corruption: • "Trusted" screen on the consumer device that securely displays (M)RP credentials and transaction data; • A keyboard not accessible through the REE that may be used to securely enter credentials, mobile code …
SUATEE	**(M)RP / AUTHENTICATION APPLICATION AUTHENTICATION** **The (M)RP / Authentication application provides means for its authentication to be eligible for an execution within the TEE.**	
SUATEE1	TEE_MANAGER	TEE processing is authorised to the authenticated (M)RP / Authentication Applications.
EPTEE	**EXECUTION PROTECTION** **The TEE and the (M)RP / Authentication Application enforce protection of their services against service denial or corruption.**	
EPTEE1	O.OPERATE	The TEE and the (M)RP / Authentication Application shall ensure the continued operation of their services: the application and application resources shall be available under normal conditions of use of the TEE.
EPTEE2	O.ISOLATION	The TEE and the (M)RP / Authentication application shall ensure application isolation through a secure data sharing mechanism between the TEE and the rest of the consumer device (including the REE). This means that no other application shall be able to access or modify (M)RP / Authentication

[16] Note that a TEE "trusted storage" is not considered hardware tamper resistant such as an SE and offers a level of security between a Rich OS and a typical SE. A TEE may complement the SE by providing a TUI.

		Application data without authorisation by the data sharing mechanism.

Figure 14: SECURITY REQUIREMENTS FOR A TEE AND (M)RP RELATED DATA

3.6.3.5.2. Assurance Level

Assurance is ground 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. Greater assurance results from a greater evaluation effort, through a broader scope, a greater attention to fine details or a more formal evaluation process.

The assurance level to be associated with the above Security Objectives for secure environments shall be equivalent to the assurance package defined as EAL2+ in the Common Criteria methodology (see ISO 15408), whereby AVA_VAN.2 is refined to increase the attack potential from Basic to Enhanced-Basic.

3.7. POI Security Requirements

This section specifies the security requirements for POIs: physical POI for local transactions, virtual POI for e- & m- commerce and physical POI and virtual terminal for MOTO.

3.7.1. Physical POI (for local transactions)

3.7.1.1. Introduction

This section defines the applicable security requirements for all POI devices. These requirements are derived from PCI PTS, and additional European Card Stakeholder Group requirements, referred to in the table as “ECSG+”. 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.

Vendors wishing to submit a POI device for certification against these high level requirements will need to ensure that the product conforms to the detailed requirements of the relevant Specification Provider, (PCI PTS, CSEC-C, PCI PTS with ECSG+ or CSEC-C with ECSG+). Approval to use a certified product in a particular market remains with the relevant Approval Body or Card Payment Scheme, the process for which is detailed in Book 5 e.g. UKCA and girocard follow CSEC-C, global Schemes follow PCI PTS. Other Schemes may require PCI or CSEC-C with additional ECSG+ requirements.

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 Card Data, transaction data and POI management data.
- DEVICE MANAGEMENT - requirements addressing the life cycle of the POI

Verb usage: The auxiliary verb *shall* which is presented in *italic* letters is used when the provided security requirement is mandatory. The auxiliary verb *should* which is presented in *italic* letters is used when the provided method is strongly recommended.

Within the specified Security Requirements detailed below and depending upon the solution and proposed usage, not all requirements are applicable. This is defined in the Table 18.

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

Number	**Description of the requirement**
A1	The POI shall use tamper-detection and response mechanisms such that it becomes infeasible to recover or obtain the sensitive data. These mechanisms shall protect against physical penetration of the device and there is not any demonstrable way to disable or defeat the mechanism. 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 is required. **Note:** All attacks shall include a minimum of ten hours' attack time for exploitation.
A2	Protection against a threat shall be based on a combination of at least two independent security mechanisms.
A3	The security of the POI shall not be compromised by altering: ▪ Environmental conditions ▪ Operational conditions
A4	Sensitive functions or data shall only be used in the protected area(s) of the device. Sensitive data and functions dealing with sensitive data are protected from modification. An attack potential of at least 26 for identification and initial exploitation, with a minimum of 13 for exploitation is required. Exclusive of the IC card reader
A5	There *shall* be no feasible way to determine any entered and internally transmitted PIN digit. An attack potential of at least 26 for identification and initial exploitation with a minimum of 13 for exploitation

A6	For determination of any PIN-security-related cryptographic key resident in the device an attack potential of at least 35 for identification and initial exploitation with a minimum of 15 for exploitation is required. **Note**: If the POI device has a keypad that can be used to enter non-PIN data, the device shall meet at least one of the following: A7, B16, or E3.4. as appropriate.
A7	The unauthorized alteration of prompts for non-PIN data entry into the PIN entry key pad such that PINs are compromised *shall* not occur. An attack potential of at least 18 per device for identification and initial exploitation with a minimum of 9 for exploitation is required.
A8	The POI *shall* provide a means to deter the visual observation of PIN values as they are being entered by the cardholder.
A8.ECSG+	The POI *should* have a privacy shield. However if a privacy shield is in place then it *shall* be in accordance with [EPC Guidelines on Privacy Shields.].
A9	It *shall* not be feasible to penetrate the device and associated hardware or software, in order to determine or modify magnetic-stripe track data. An attack potential of at least 16 per device, for identification and initial exploitation, with a minimum of 8 for exploitation is required.
A10	Secure components intended for unattended devices *shall* contain an anti-removal mechanism. Defeating or circumventing this mechanism *shall* require an attack potential of at least 18 per device for identification and initial exploitation, with a minimum of 9 for exploitation.
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	
Number	**Description of the requirement**
B1	The POI *shall* perform a regular self-test, which includes integrity and authenticity tests to check whether the POI is in a compromised state. In the event of a failure, the POI and its functionality fail in a secure manner. The POI *shall* reinitialize memory at least every 24 hours
B2	The POI's functionality *shall* not be influenced by logical anomalies which could result in the POI outputting the clear-text PIN or other sensitive data.
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.
B3.ECSG+	The vendor's processes in Requirement B3 *shall* be evaluated by the testing laboratory.
B4	If the POI allows updates of firmware, the POI *shall* cryptographically authenticate the firmware. All firmware updates *shall* be cryptographically authenticated by the device or rejected and deleted
B4.1	If the POI allows software application and/or configuration updates, the firmware *shall* use state of the art authentication mechanisms consistent with B4.
B5	The device never displays the entered PIN digits in clear text, and it *shall* not be possible to determine the PIN from any displayed characters or digits

B6[17]	Sensitive data *shall* not be retained any longer, or used more often, than strictly necessary. The POI *shall* automatically clear its internal buffer after sensitive data e.g. the PIN was processed, or after a determined period of inactivity. Online PINs *shall* be encrypted within the device immediately after PIN entry is complete
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. Entering or exiting sensitive services *shall* not reveal or otherwise affect sensitive data.
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 POI is forced to return to its normal mode.
B9	If random numbers are generated by the POI in connection with security over sensitive data, the random number generator be assessed to ensure it is generating numbers sufficiently unpredictable.
B10	The POI shall have characteristics that prevent or significantly deter the use of the device for exhaustive PIN determination.
B10.ECSG+	The POI shall have characteristics that prevent the use of the POI for exhaustive PIN determination.
B11	The key-management techniques implemented in the POI *shall* conform to ISO 11568 and/or ANSI X9.24. Key-management techniques *shall* support the ANSI X9. TR-31 key derivation methodology or an equivalent methodology.
B12	The PIN-encryption technique implemented in the POI *shall* be a technique included in [ISO 9564].
B13	It *shall* not be possible to encrypt or decrypt any random data using a key stored within the device. The encryption or decryption of data *shall* only be possible using dedicated keys. The device *shall* enforce that all dedicated keys have different values.

[17] Requirement B6 is not intended to prevent PIN change for a proprietary Card scheme.

B14	There *shall* be no mechanism in the device that would allow the outputting of a private or secret clear-text key from a given security component into a component of lesser security.
B15	The entry of any other transaction data *shall* be separate from the PIN-entry process. 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 shall 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.	
B16	All prompts for non-PIN data entry *shall* be 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[18] 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 *shall* 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.
B17	If the POI supports multiple applications, it *shall* enforce the separation between applications. It *shall* not be possible that one application interferes with or tampers with another application or the OS of the device
B18	The operating system of the POI *shall* contain only the software necessary for the intended operation. The operating system *shall* be configured securely and run with least privilege.
B19	The vendor *shall* provide adequate documented security guidance for the integration of any secure component into the POI.

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

B20	A security policy addressing the proper use of the device in a secure fashion *shall* be available for the user. This security policy *shall* define the roles supported by the device and indicate the services available for each role. 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 *shall* be those allowed by the policy.
Section C - Online PIN Security Requirement	
Number	**Description of the requirement**
C1	The POI *shall* be protected against and prohibits unauthorised key replacement and key misuse.
Section D - Offline PIN Security Requirements	
Number	**Description of the requirement**
D1	It *shall* neither be feasible to penetrate the ICC reader 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 nor *shall* it be possible for both an ICC card and any other object to reside within the card insertion slot. **Note**: All attacks shall include a minimum of ten hours' attack time for exploitation.
D2	The opening for the insertion of the IC card *shall* be in full view of the cardholder during card insertion.
D3	The ICC reader *shall* be constructed in a manner that objects not belonging to it can be observed by the cardholder.
D4	PIN protection during transmission between the device encrypting the PIN and the ICC reader shall apply to both integrated and non-integrated combinations, according to the relevant sections of [ISO 9564-1] and [EMV Book 2].

Evaluation Module 2: POS Terminal integration

Current desk 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 - POI Integration Security Requirements

Number	Description of the requirement
	Configuration Management
E1	Any secure component integrated into a device submitted for evaluation *shall* have a clearly identified physical and logical security perimeter.
	Integration of PIN Entry Functions
E2.1	The logical and physical integration of a PCI-approved secure component (or components) into a PIN entry POI terminal *shall* not impact the overall PIN protection level.
E2.2	The design of the PIN entry area of the POI *shall* not facilitate fraudulent placement of an overlay over the PIN entry area and its environment. An overlay attack *shall* require an attack potential of at least 18 for identification and initial exploitation, with a minimum of 9 for exploitation[19].

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

Integration into a POS Terminal	
E3.1	The logical and physical integration of an approved secure component into the POI *shall* not create new attack paths to the PIN.
E3.2	The POI *shall* be equipped with mechanisms to prevent attacks aiming at retaining and stealing the payment card.
E3.3	There *shall* be a clear logical and/or physical separation between secure components and non-secure components integrated into the same POI.
Note: If the POI device has a keypad that can be used to enter non-PIN data, the device shall 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.	
E3.4	The POI *shall* enforce cryptographic authentication of the correspondence between the display messages visible to the cardholder and the operating state of the POI. Where commands for data entry are from an external device, these commands shall be authenticated The alteration of the correspondence between the display messages visible to the cardholder and the operating state of the PIN entry device *shall* not occur without requiring an attack potential of at least 18 per POI for identification and initial exploitation with a minimum of 9 for exploitation[20].

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

E3.5	The PIN-accepting device *shall* 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 *shall* exist to prevent its use for PIN entry or it is controlled in a manner consistent with B16.
Removal Requirements	
E4.1	The POI *shall* be protected against unauthorized removal. Defeating or circumventing this mechanism *shall* require an attack potential of at least 18 per device for identification and initial exploitation, with a minimum of 9 for exploitation[21].
E4.2	The vendor documents, maintains and makes available to customers or integrators *shall* detail on how to implement the protection system against unauthorized removal.
E4.3	For each embedded device, the protection system against unauthorised removal *shall* be properly implemented as documented by the manufacturer.
Evaluation Module 3: Open Protocols This set of requirements ensures that the 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 the POI authenticity.	
Section F - Discovery	

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

Number	Description of the requirement
F1	**<u>All</u>** public domain protocols and interfaces available on the POI *shall* be clearly identified in the *Open Protocols Module.* All protocols and interfaces available on the POI *shall* be accurately identified and described.
Section G - Vulnerability Assessment	
Number	**Description of the requirement**
G1	The POI vendor *shall* have internal policies and procedures that ensure that the vendor maintains an effective process for detecting vulnerabilities that may exist within their device. This process is expected to be robust enough to include all interfaces defined in the *Open Protocols Module*. This process *shall* be effective enough to detect vulnerabilities which may have not been publicly known during the last vulnerability assessment.
G2	The POI *shall* undergo a vulnerability assessment to ensure that the protocols and interfaces listed in the *Open Protocols Module* do not contain exploitable vulnerabilities.
G3	The platform vendor *shall* have vulnerability disclosure measures in place for the POI.
Section H - Vendor Guidance	
H1	The POI *shall* have security guidance that describes how protocols and services shall be used for each interface that is available on the platform identified in the *Open Protocols Module*.
H2	The POI *shall* have guidance that describes the default configuration for each protocol and services for each interface that is available on the platform.
H3	The POI *shall* have has guidance for key management accurately describing how all keys and all certificates shall be used.
Section I - Operational Testing	

I1	The POI *shall* have **all** the security protocols that are available on the POI clearly identified in the *Open Protocols Module.*
I2	The POI *shall* implement appropriate cryptography to be able to provide confidentiality of data sent over a network connection, in accordance with [EPC Crypto].
I3	The POI *shall* implement appropriate cryptography to be able to provide integrity of data that is sent over a network connection, in accordance with [EPC Crypto].
I4	The POI *shall* implement appropriate authentication mechanisms to be able to authenticate the server, in accordance with [EPC Crypto].
I5	The POI *shall* be able to detect replay of messages, and *shall* enable the secure handling of the exceptions.
I6	The POI *shall* implement session management. a. The POI *shall* keep track of all connections and *shall* restrict the number of sessions that can remain active on the platform to the minimum necessary number. b. The POI *shall* set time limits for sessions and *shall* ensure that sessions are not left open for longer than necessary.
Section J - Maintenance	

J1	The device vendor *shall* provide and maintain guidance describing configuration management for the device. a. The guidance *shall* be 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 *shall* cover the complete life cycle of the platform d. The guidance *shall* ensure that unauthorised modification is not possible. e. The guidance *shall* ensure that any modification of an approved platform that impacts security, results in a change of the platform identifier.
J2	The platform vendor *shall* have maintenance measures in place. a. The maintenance measures *shall* be documented. b. The maintenance measures *shall* ensure timely detection of vulnerabilities that apply to the platform by periodical execution of a vulnerability assessment. c. The maintenance measures *shall* ensure timely assessment and classification of newly found vulnerabilities. d. The maintenance measures *shall* ensure timely creation of mitigation measures for newly found vulnerabilities that may impact platform security.
J3	Deployed devices can be updated, and the platform vendor provides and maintains guidance describing how the update mechanism *shall* be used.
J4	The update mechanism *shall* ensure confidentiality, integrity, authentication, and protection against any attack. If the device allows software and/or configuration updates, the device *shall* cryptographically authenticate the update. If the authenticity is not confirmed, the update *shall* be rejected and deleted.
Evaluation Module 4: Secure Reading and Exchange of Data (SRED)	

<table>
<tr><td colspan="2">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.</td></tr>
<tr><td colspan="2"><b>Section K - Protection of Card Data during Data Retrieval</b></td></tr>
<tr><td><b>K1</b></td><td>All account data <i>shall</i> either be encrypted immediately upon entry or <i>shall</i> be entered in clear-text into a secure device and processed within the secure controller of the POI.</td></tr>
<tr><td><b>K1.1</b></td><td>The POI <i>shall</i> protect all account data upon entry and there <i>shall</i> be no method of accessing the clear-text account data without defeating the security of the POI. 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[22].
<b><i>Note:</i></b> <i>MSRs and ICCRs shall meet the attack potentials stipulated in A10 and D1 respectively.</i></td></tr>
<tr><td><b>K1.2</b></td><td>Failure of a single security mechanism <i>shall</i> not compromise the POI security. Protection against a threat <i>shall</i> be based on a combination of at least two independent security mechanisms.</td></tr>
<tr><td><b>K2</b></td><td>The logical and physical integration of an approved secure card reader into a PIN entry device <i>shall</i> not create new attack paths to the account data. The account data <i>shall</i> be protected from the input component to the secure controller of the POI.</td></tr>
<tr><td><b>K3</b></td><td>Determination of any cryptographic keys by penetration of the POI and/or by monitoring emanations from the device, requires an attack potential of at least 26 for identification and initial exploitation with a minimum of 13 for exploitation[23].</td></tr>
</table>

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

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

K3.1	Public keys *shall* be stored and used in a manner that protects against unauthorized modification or substitution. Unauthorised modification or substitution requires an attack potential of at least 26 for identification and initial exploitation with a minimum of 13 for exploitation[24].
K4	All account data *shall* be encrypted using only appropriate encryption algorithms and modes of operation in accordance with [EPC Crypto]
K5	If remote key distribution is used, the POI *shall* support mutual authentication between the sending key distribution host and receiving device.
K6	The POI *shall* support data origin authentication of encrypted messages.
K7	Keys that reside within the POI to support data encryption *shall* be unique per device.
K8	Encryption or decryption of any arbitrary data using any account data-encrypting key or key-encrypting key contained in the POI *shall* not be permitted. The POI *shall* enforce that all different keys for different purposes have different values.
K9	If the POI may be accessed remotely for the purposes of administration, all access attempts *shall* be cryptographically authenticated. If the authenticity of the access request cannot be confirmed, the access request *shall* be denied.
K10	The firmware, and any changes thereafter, *shall* be inspected and reviewed consistent with B3.
K11.1	The firmware *shall* confirm the authenticity of all applications loaded onto the terminal consistent with B4. If the POI allows software application and/or configuration updates, the POI *shall* cryptographically authenticate all updates consistent with B4.
K11.2	The vendor *shall* provide clear security guidance consistent with B2 and B6 to all application developers to ensure:

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

	- That it is not possible for applications to be influenced by logical anomalies. - That account data is not retained any longer, or used more often, than strictly necessary.
K12	If the POI allows updates of firmware, the POI *shall* cryptographically authenticate the firmware and if the authenticity is not confirmed, the firmware update *shall* be rejected and deleted.
K13	The device's functionality *shall* not be influenced by logical anomalies consistent with B2.
K14	If the POI is capable of communicating over a network or uses a public domain protocol, then requirements specified in Open Protocols Requirements *shall* be met.
K15	When operating in encrypting mode, there *shall* be no mechanism in the POI that would allow the outputting of clear-text account data. Changing between an encrypting and non-encrypting mode of operation *shall* require explicit authentication.
K15.1	When operating in encrypting mode, the secure controller *shall* only release clear-text account data to authenticated applications executing within the POI.
K15.2	Account data *shall* not be retained any longer, or used more often, than strictly necessary.
K16	If the POI is capable of generating surrogate PAN values to be outputted outside of the device, it *shall* not be possible to determine the original PAN knowing only the surrogate value.
K16.1	If using a hash function to generate surrogate PAN values, input to the hash function *shall* use appropriate random data.
K16.2	If using a hash function to generate surrogate PAN values, the random data *shall* be 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[25].

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

K17	The key-management techniques implemented in the device *shall* be consistent with B11.
K18	The POI *shall* have characteristics that prevent or significantly deter the use of the POI for exhaustive PAN determination.
K19	Environmental or operational conditions *shall* not be altered to compromise the security of the device, or cause the device to output clear-text data.
K20	If the POI supports multiple applications, it *shall* enforce the separation between applications consistent with B17.
K21	The following features of the POI's operating system *shall* be in place: • The operating system of the device *shall* contain only the software necessary for the intended operation. • The operating system *shall* be configured securely and run with least privilege. • The security policy enforced by the device *shall* not allow unauthorized or unnecessary functions. API functionality and commands that are not required to support specific functionality *shall* be disabled (and where possible, removed).
K22	Access to sensitive services *shall* require authentication. Entering or exiting sensitive services *shall* not reveal or otherwise affect sensitive data.
K23	Sensitive services *shall* be 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	
L0 ECSG+	L requirements *shall* be checked by the testing lab. This includes a periodic site visit regarding critical steps in the manufacturing process (excluding the key loading).
L1	Change-control procedures *shall* be in place so that any intended security-relevant change to the physical or functional capabilities of the POI causes a re-certification of the POI under the Core PIN Entry and/or POI Integration Security Requirements of this document.
L2	The certified firmware *shall* be 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.
L3	The POI *shall* be 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 POI Integration Security Requirements evaluation, and that unauthorized substitutions have not been made.
L4	Production software (e.g. firmware) that is loaded to devices at the time of manufacture *shall* be transported, stored, and used under the principle of dual control, preventing unauthorized modifications and/or substitutions.
L5	Subsequent to production but prior to shipment from the manufacturer's or reseller's facility, the POI and any of its components *shall* be stored in a protected, access-controlled area or sealed within tamper-evident packaging to prevent undetected unauthorized access to the POI or its components.
L6	If the POI will be authenticated at the key-loading facility or the facility of initial deployment by means of secret information placed in the POI during manufacturing, then this secret information *shall* be unique to each device, unknown and unpredictable to any person, and *shall* be installed in the POI under dual control to ensure that it is not disclosed during installation.

L7	Security measures are taken during the development and maintenance of the POI security related components. The manufacturer *shall* 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.
L8	Controls *shall* exist over the repair process and the inspection testing process subsequent to repair to ensure that the POI has not been subject to unauthorized modification.
L8 ECSG+	If tamper mechanisms can be reset during the repair process then for this repair process the requirements L1 till L7 and the M requirements *shall* be applicable.
Section M - Between Manufacturer and Initial Key Loading ***Note:*** *in the following requirements, the device under evaluation is referred as the "device".*	
M1	The POI *shall* be protected from unauthorized modification and customers *shall* be provided with documentation in a secure way that provides instruction on validating the authenticity and integrity of the device. Where this is not possible, the POI *shall* be shipped from the manufacturer's facility to the initial key-loading facility or to the facility of initial deployment and *shall* be stored and 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 *shall* be the responsibility of each party to ensure that the shipping and storage they are managing is compliant with this requirement.
M2	Procedures *shall* be in place to transfer accountability for the POI from the manufacturer to the facility of initial deployment. Where the POI is shipped via intermediaries such as resellers, accountability *shall* be with the intermediary from the time at which they receive the POI until the time it is received by the next intermediary or the point of initial deployment.

M3	While in transit from the manufacturer's facility to the initial key-loading facility, the device is shipped and stored containing a secret that is immediately and automatically erased if any physical or functional alteration to the device is attempted. Any attempt of alteration shall be detectable by the key loading facility.
M4	The POI's development security documentation *shall* provide means to the initial key-loading facility to assure the authenticity of the TOE's security relevant components.
M4 ECSG+	In order to ensure ongoing key loading facility operational security and conformity, key loading audits *shall* be conducted. Those entities carrying out such audits *shall* be suitably qualified to certify conformity with the requirements of Secure key loading operations and Key management. The audit *shall* 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 *shall* be allowed to communicate their report to the relevant bodies.
M5	If the manufacturer is in charge of initial key loading, then the manufacturer *shall* verify the authenticity of the POI security-related components.
M5 ECSG+	Requirement M4 **ECSG+** also applies to Requirement M5.
M6	If the manufacturer is not in charge of initial key loading, the manufacturer *shall* provide the means to the initial key-loading facility to assure the verification of the authenticity of the POI security-related components.
M6 ECSG+	Requirement M4 **ECSG+** also applies to Requirement M6.

<table>
<tr><td><b>M7</b></td><td>Each device <i>shall</i> have a unique visible identifier affixed to it.</td></tr>
<tr><td><b>M8</b></td><td>The vendor <i>shall</i> 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.</td></tr>
<tr><td colspan="2"><b>Section N- Requirements for the POI payment application</b>
<b>Note: All section N are ECSG+ requirements</b></td></tr>
<tr><td><b>N1 ECSG+</b></td><td>The POI provides security functions. These security functions <i>shall</i> be called by the payment application according to a secure process flow as defined by the payment application.
The following security functions <i>shall</i> be considered as part of the secure process flow.
a) PIN entry
b) Confirmation of the amount
c) Verification of the online and offline result
d) Prompting of the transaction result
e) Maintaining security related transaction data</td></tr>
</table>

N1.1 ECSG+	The secure process flow *shall* be controlled by the POI in order that it cannot be bypassed by logical means. POI and payment application *shall* control the secure process flow.
N1.2 ECSG+	Online and offline process order *shall* not be allowed to be manipulated. A state machine (or other solutions) that controls the online and offline process steps and the final status screen prompt in the application *shall* be present.
N1.3 ECSG+	A state machine *shall* control the secure process flow even if the POI is cut from the message exchange or from power supply. If there is no response on a request or keys are not pressed according to expected time outs the secure process flow *shall* react in an adequate way. • Transport layers are provided by the firmware. • The application layer is part of the payment application.
N2 ECSG+	Security functions of the firmware implementing authentication and integrity for the online messages, including transaction data, *shall* be called by the payment application according to the secure process flow. For a firmware not covering all security functions for key derivation the missing functions *shall* be part of the payment application. The usage of cryptographic signature/ authentication code key management and signature/ authentication code key *shall* be part of the firmware. The calls for the calculation and verification of signatures/ authentication codes of online messages (requests, responses) *shall* be part of the payment application.
N3 ECSG+	Any secure process flow *shall* only use random numbers generated by the random number generator which have been assessed and verified in the firmware evaluation. The random number generator *shall* be provided by the firmware. Both the payment application as well as the EMV kernel *shall* use the (assessed) random number generator provided by the firmware.
N4 ECSG+	The EMV related part of the secure process shall provide for authenticity and integrity of the code and relevant security data, e.g. keys and management data.

N5 ECSG+	It *shall* not be possible to bypass the display of the transaction amount by logical means. The cardholder *shall* not be deceived about the secure process flow showing him another amount than the amount being authorised. This *shall* also hold for the key the cardholder is pressing to confirm or to cancel a transaction. The execution of functions depending on the user authentication *shall* only be allowed, e.g. the authorisation of a transaction, if the user authentication has been performed successfully.

3.7.1.2. *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 shall utilise 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 shall 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 shall be considered for possible evaluation.

3. Full Volume compliant products shall conform to all baseline requirements AND additional ECSG+ requirements.

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 contains-even temporarily-keys involved in PIN security. Under the scope of this functionality are the secret keys of symmetric algorithms, the private and public keys of public key algorithms (with the limitation of scope to their integrity and authenticity).
Card Reader	This functionality applies whenever a device has the capability to capture card data, irrespective of the technology being used (i.e., it encompasses both the magnetic stripe and chip card readers). This is further broken down into ICCR and MSR functionality.
Feedback to cardholder	If a device gives feedback to the cardholder during its PIN-based transaction, this functionality applies. This includes but is not limited to auditory and visible feedback (i.e., displays).
Terminal is a module	If the device 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 is said to be compound if it incorporates one or more modules, 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 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.
POI Payment Application	The POI payment application • uses security related functionalities e.g. cryptographic mechanisms provided by the platform to the extent possible; • uses the random number generator provided by the platform; • provides a secure process flow.

TABLE 15: 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	POI Payment Application	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 ECSG+	x				x					x			Depends upon AB/CPS
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
B3 ECSG+	x	x								x			Depends upon AB/CPS
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
B10 ECSG+	x									x			Depends upon AB/CPS

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**	**POI Payment Application**	**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**	**POI Payment Application**	**Conditions**
I4											x		Not only server authentication, also POI authentication shall be in scope of this requirement
J4											x		
Secure Reading and Exchange of Data Module (optional)													
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	x		For protection against disclosure of any non-PIN secret key
K3.1									x		x		
K5									x		x		
K6									x		x		
K7									x		x		For all data encryption
K8									x		x		For all data encryption
K9									x		x		For POI management data
K10									x		x		To be evaluated at least based on documentation
K11.1									x		x		
K13									x		x		
K17									x		x		
K20									x		x		
Device Security Requirements													
During Manufacturing													
L0 ECSG+	x	x	x	x	x	x	x	x	x	x			Depends upon AB/CPS
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			
L8 ECSG+	x	x	x	x	x	x	x	x	x	x			Depends upon AB/CPS
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**	**POI Payment Application**	**Conditions**
M3	x	x	x	x	x	x	x		x	x			
M4	x	x	x	x	x	x	x		x	x			
M4 ECSG+	x	x	x	x	x	x	x		x	X			Depends upon AB/CPS
M5	x	x	x	x	x	x	x		x	x			
M5 ESCG+	x	x	x	x	x	x	x		x	X			Depends upon AB/CPS
M6	x	x	x	x	x	x	x		x	x			
M6 ECSG+	x	x	x	x	x	x	x		x	x			Depends upon AB/CPS
M7	x	x	x	x	x	x	x		x	x			
M8	x	x	x	x	x	x	x		x	x			
Requirements for the POI payment application (optional)													
N1 ECSG+												x	Depends upon AB/CPS
N1.1 ECSG+												x	Depends upon AB/CPS
N1.2 ECSG+												x	Depends upon AB/CPS
N1.3 ECSG+												x	Depends upon AB/CPS
N2 ECSG+												x	Depends upon AB/CPS
N3 ECSG+												x	Depends upon AB/CPS
N4 ECSG+												x	Depends upon AB/CPS
N5 ECSG+												x	Depends upon AB/CPS

TABLE 16: SUPPORTED FUNCTIONALITIES

3.7.2. Security Guidelines for Virtual POI (for e- & m- commerce)

Acceptors choosing to sell their goods and services online have a number of options to consider, for example:

- Use a third-party solution, develop their own e- or m-commerce payment software, or use a combination of both.
- Use a variety of technologies to implement e- or m-commerce functionality, including hosted payment pages, inline frames (iFrames), application-programming interfaces (APIs), or payment-processing applications.
- Choose to maintain different levels of control and responsibility for managing the supporting information technology infrastructure. For example, an acceptor may choose to outsource management of all systems and infrastructure to hosting providers and/or e-commerce payment processors, manage some components in house while outsourcing other components to third parties, or manage all networks and servers in house.

No matter which option an acceptor may choose, key considerations need to be kept in mind regarding the security of card data:

- Regardless of the extent of outsourcing to third parties, the acceptor shall retain responsibility for ensuring that payment card data is protected. Connections and redirections between the acceptor and the third party can be compromised, and the acceptor shall monitor its systems to ensure that no unexpected changes have occurred and that the integrity of the connection/redirection is maintained.
- Virtual POI Applications for E- and M-commerce which utilise the PAN as the authenticator can be validated according to *[PCI PA-DSS]* and confirmed to be included on PCI SSC's list of "Validated Payment Applications". For in-house developed Virtual POI Applications, *[PCI PA-DSS]* can be used as a best practice during development.
- Third-party relationships and the responsibilities of the acceptor and each third party can be clearly documented in a contract or service-level agreement as defined in PCI DSS, to ensure that each party understands its responsibilities and implements the appropriate security requirements.

Further information on e- or m-commerce security may be found in the "PCI DSS E-commerce Guidelines" (see *[PCI3]*).

PCI DSS describes a way that acceptors and PSPs can secure their systems. PCI DSS applies to all acceptors of e- and m-commerce. The number of technical requirements that apply depend on the way the acceptor configures the website to accept card payments. PCI DSS applies to all acceptor's web servers, even if a web server does not itself store, process or transmit Card Data because the acceptor's web server determines how Card Data is processed and so can impact the security of the transaction.

Three options may be considered by the Acceptor as described below. Different validation of the security requirements for e- & m-commerce will apply depending on how the Acceptor handles card data as the different options carry different risks:

- The entire payment page is received from and returned to a third party processor.
- The acceptors website does not store, process or transmit card data, but controls how the card data is collected from the cardholder.
- The acceptor website stores, processes or transmits card data.

An overview of typical configurations for accepting card data is given below. A distinction is made between the following:

- the redirection process;
- the iFrame
- the direct post
- the JavaScript created form
- the API (sometimes called the merchant gateway).

For each of the configurations a stepwise description is provided below for the transmission of the card data in the case of E- and M- Commerce with static authentication.

3.7.2.5 *The redirect process*

The following figure illustrates the different steps involved in the configuration whereby the cardholder's customer device is redirected to a TPP to request a payment page. This configuration imposes the lowest risk for the acceptor.

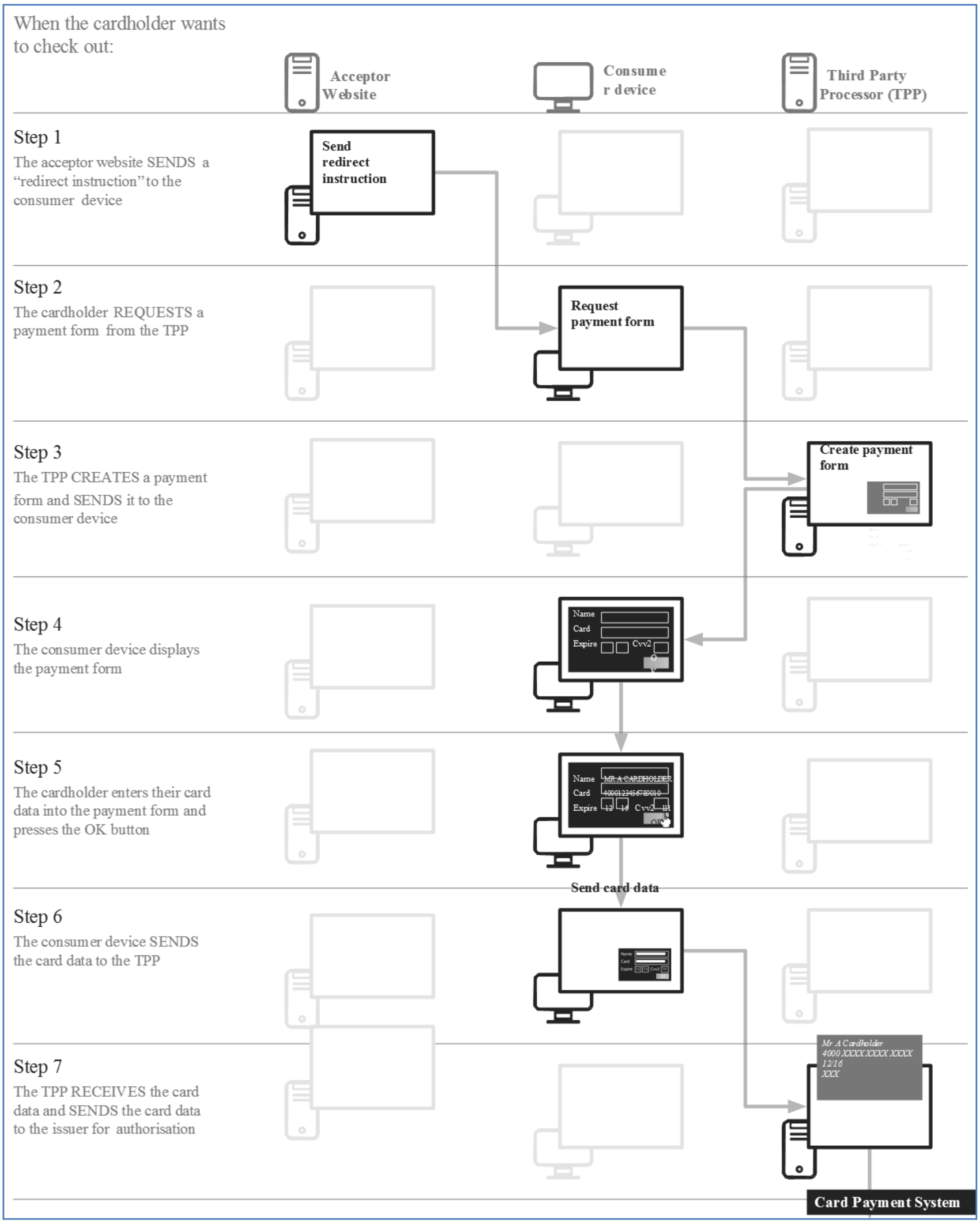
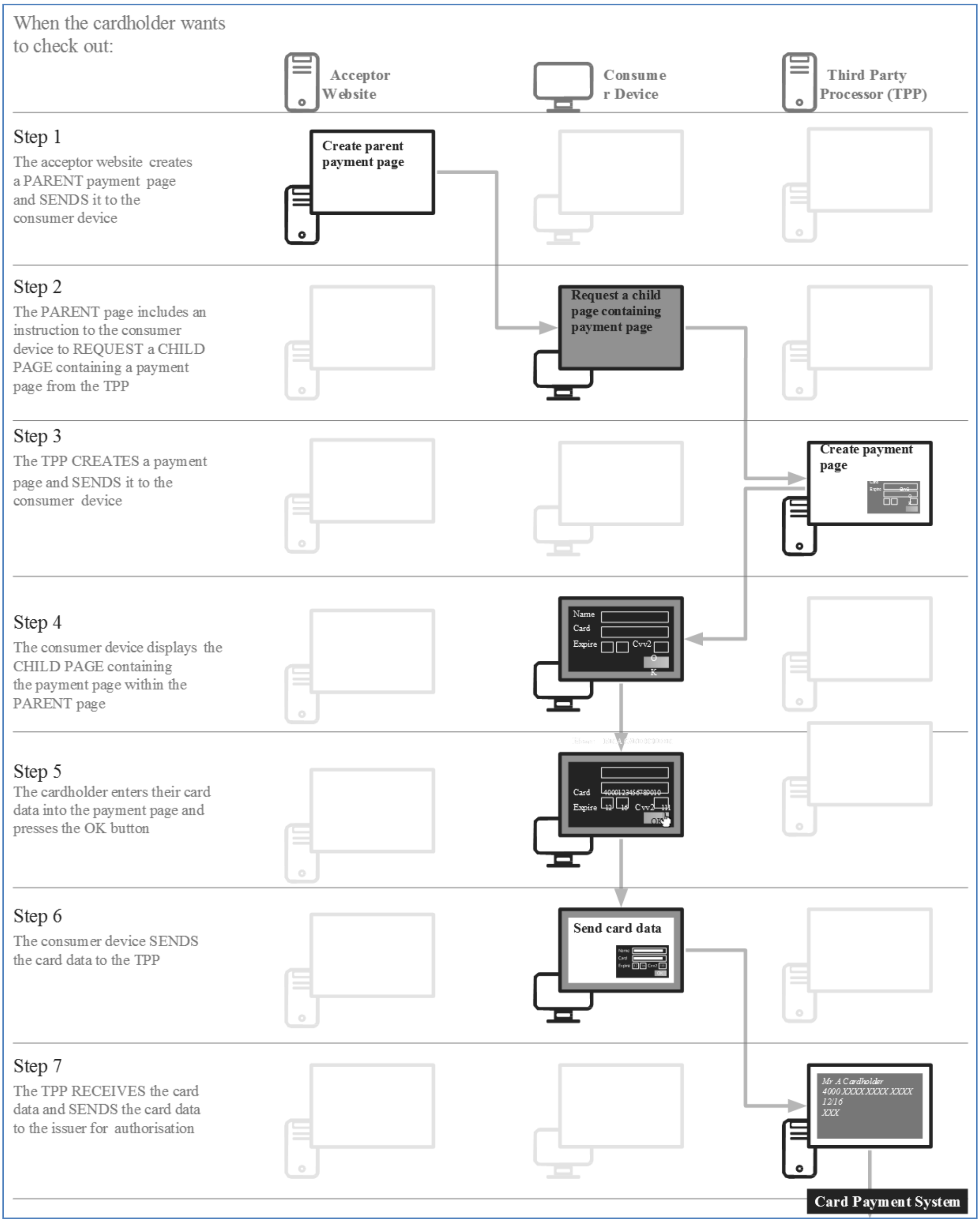

When the cardholder wants to check out:
Acceptor Website
Consume r device
Third Party Processor (TPP)
Step 1
The acceptor website SENDS a "redirect instruction" to the consumer device
Send redirect instruction
Step 2
The cardholder REQUESTS a payment form from the TPP
Request payment form
Step 3
The TPP CREATES a payment form and SENDS it to the consumer device
Create payment form
Step 4
The consumer device displays the payment form
Name
Card
Expire
Cvv2
OK
Step 5
The cardholder enters their card data into the payment form and presses the OK button
Name MR A CARDHOLDER
Card 4000123456789010
Expire 12 16 Cvv2 111
OK
Send card data
Step 6
The consumer device SENDS the card data to the TPP
Step 7
The TPP RECEIVES the card data and SENDS the card data to the issuer for authorisation
Mr A Cardholder
4000 XXXX XXXX XXXX
12/16
XXX
Card Payment System

FIGURE 17: THE REDIRECT CONFIGURATION

3.7.2.6 *The IFRAME*

The following figure illustrates the different steps involved in the configuration whereby the cardholder’s customer device is redirected to a TPP to request a payment page via a so-called parent payment page obtained from the acceptor’s website.



When the cardholder wants to check out:

Step 1
The acceptor website creates a PARENT payment page and SENDS it to the consumer device

Step 2
The PARENT page includes an instruction to the consumer device to REQUEST a CHILD PAGE containing a payment page from the TPP

Step 3
The TPP CREATES a payment page and SENDS it to the consumer device

Step 4
The consumer device displays the CHILD PAGE containing the payment page within the PARENT page

Step 5
The cardholder enters their card data into the payment page and presses the OK button

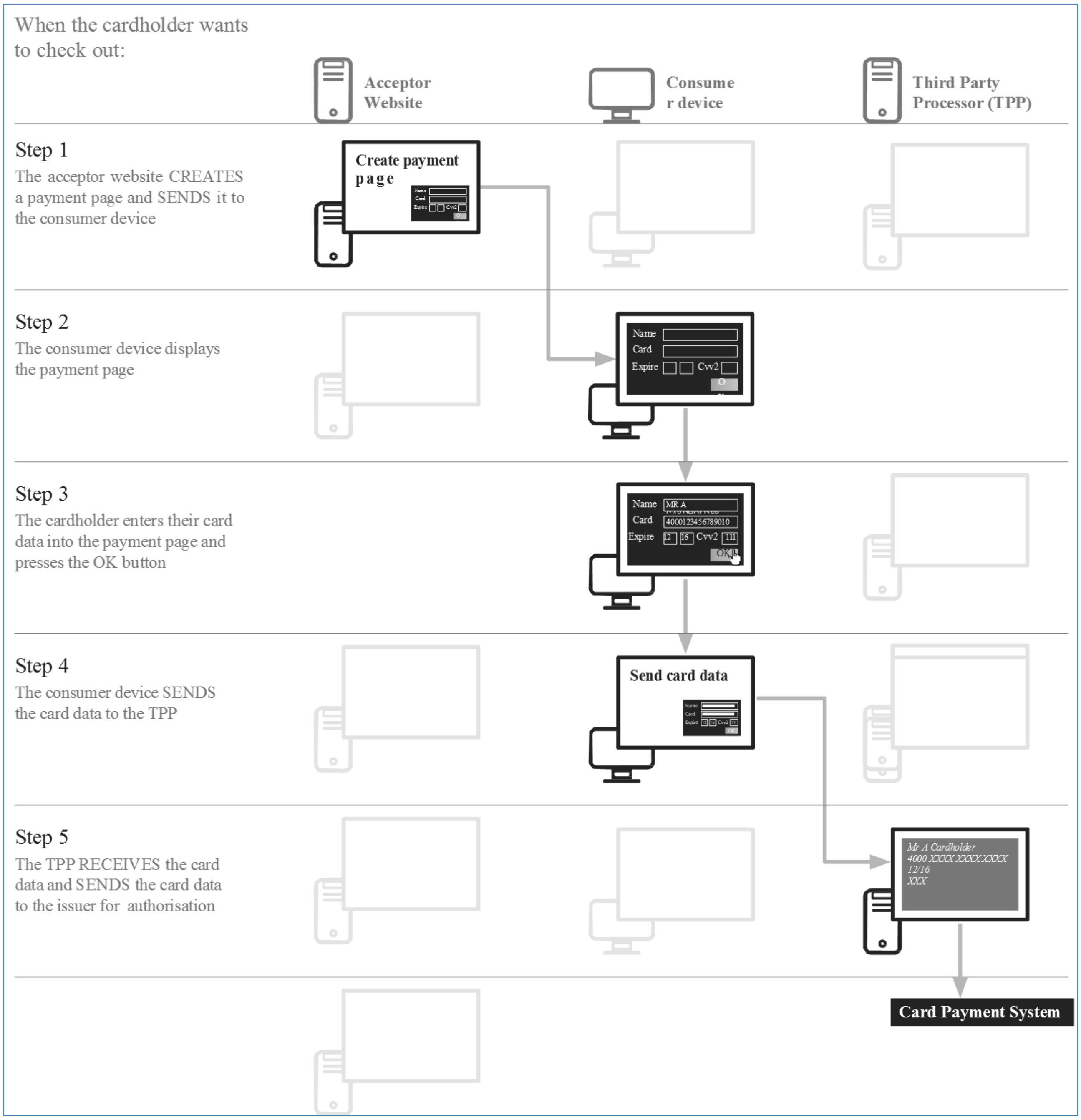
Step 6
The consumer device SENDS the card data to the TPP

Step 7
The TPP RECEIVES the card data and SENDS the card data to the issuer for authorisation

FIGURE 18: THE IFRAME

3.7.2.7 *The direct post*

The following figure illustrates the different steps involved in the configuration whereby the cardholder's customer device is displaying the payment page. This configuration is also sometimes referred to as "browser API" or "silent post".



When the cardholder wants to check out:

Step 1
The acceptor website CREATES a payment page and SENDS it to the consumer device

Step 2
The consumer device displays the payment page

Step 3
The cardholder enters their card data into the payment page and presses the OK button

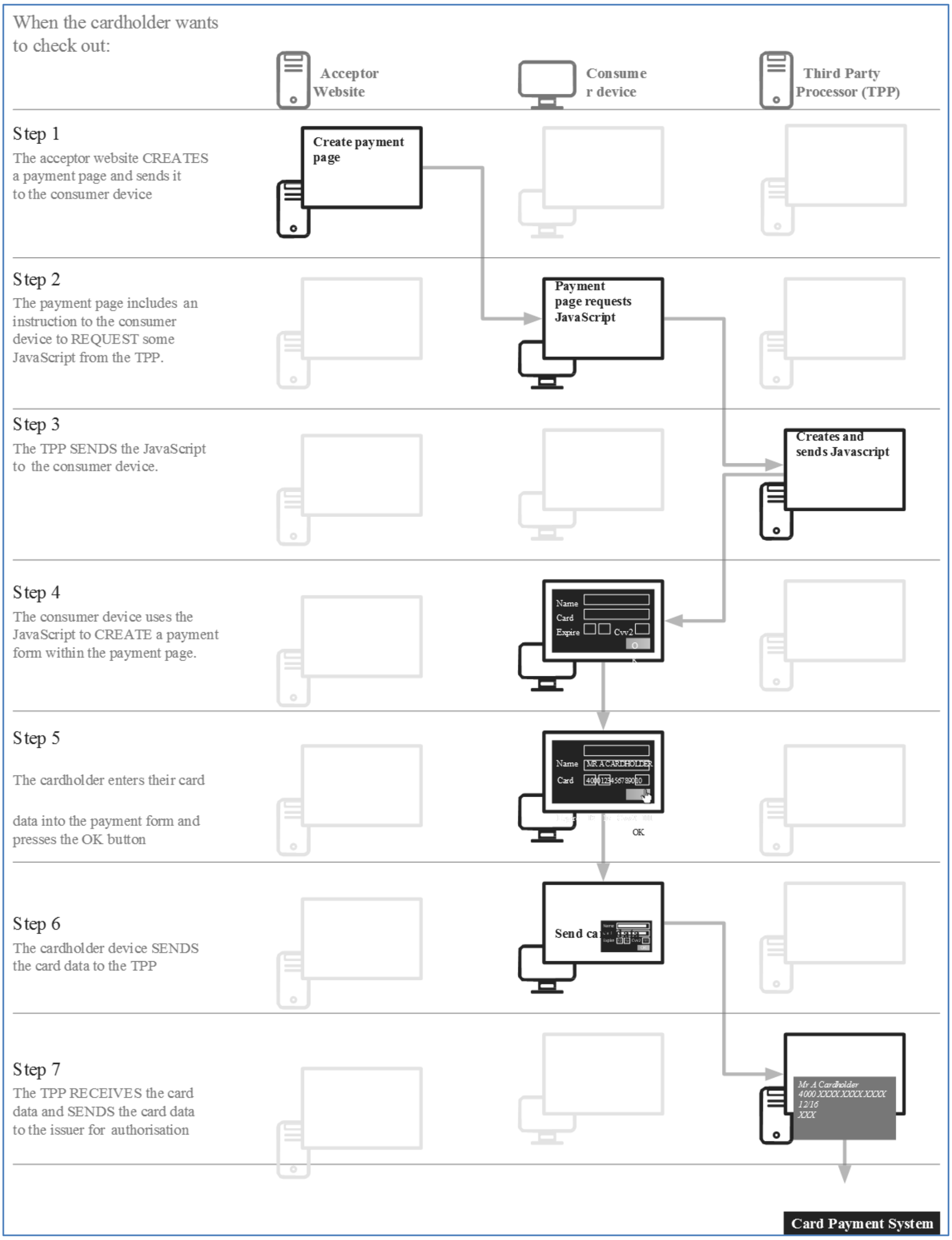
Step 4
The consumer device SENDS the card data to the TPP

Step 5
The TPP RECEIVES the card data and SENDS the card data to the issuer for authorisation

FIGURE 19: THE DIRECT POST

3.7.2.8 *The JavaScript created form*

The following figure illustrates the different steps involved in the configuration whereby the cardholder is presented with a form created in JavaScript within the payment page.



When the cardholder wants to check out:

Step 1
The acceptor website CREATES a payment page and sends it to the consumer device

Step 2
The payment page includes an instruction to the consumer device to REQUEST some JavaScript from the TPP.

Step 3
The TPP SENDS the JavaScript to the consumer device.

Step 4
The consumer device uses the JavaScript to CREATE a payment form within the payment page.

Step 5
The cardholder enters their card

data into the payment form and presses the OK button

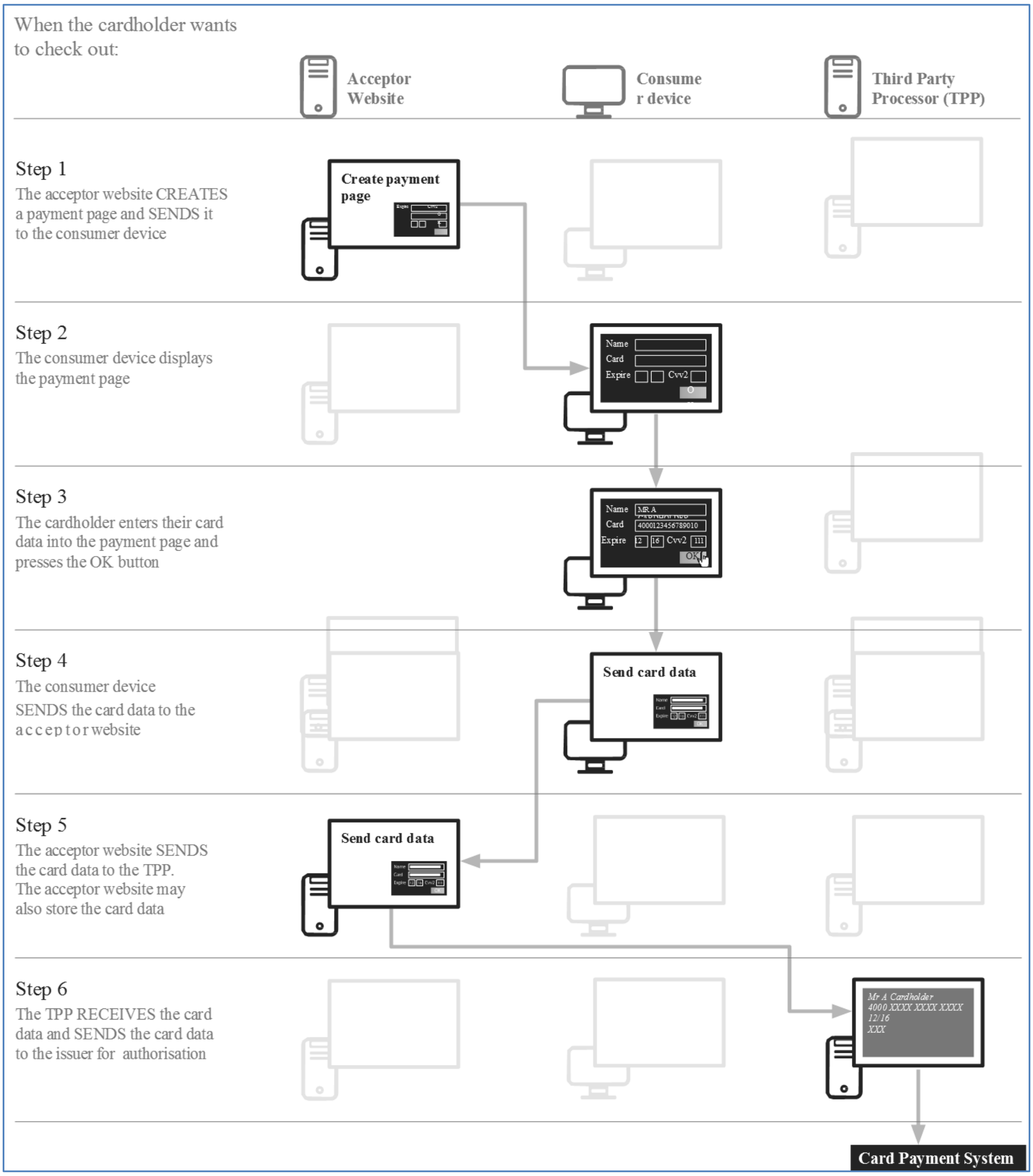
Step 6
The cardholder device SENDS the card data to the TPP

Step 7
The TPP RECEIVES the card data and SENDS the card data to the issuer for authorisation

FIGURE 20: JAVASCRIPT CREATED FORM

3.7.2.9 *The API*

The following figure illustrates the different steps involved in the configuration whereby a so-called acceptor gateway is sending data from the acceptor to the TPP in a specific format (e.g., XML).



When the cardholder wants to check out:

Step 1
The acceptor website CREATES a payment page and SENDS it to the consumer device

Step 2
The consumer device displays the payment page

Step 3
The cardholder enters their card data into the payment page and presses the OK button

Step 4
The consumer device SENDS the card data to the acceptor website

Step 5
The acceptor website SENDS the card data to the TPP.
The acceptor website may also store the card data

Step 6
The TPP RECEIVES the card data and SENDS the card data to the issuer for authorisation

FIGURE 21: THE API

3.7.3. Physical POI (for MOTO)

When a physical POI is configured and used to process MOTO transactions, the relevant Security Requirements specified in section 3.7.1 apply.

3.7.4. Virtual Terminal (for MOTO)

A virtual terminal is web-browser based access to an acquirer, processor or third party service provider website, to facilitate the authorisation and the submission of a payment card transaction to an Acquirer, whereby the acceptor manually enters Card data via a securely connected web browser. In addition, if the Acceptor supports Touch Tone facilities using Dual-Tone-Multi-Frequency-encoded technology (DTMF), the cardholder may use their phone keypad to manually enter the card data. The virtual terminal does not read data directly from a payment card.

Acceptors who process card data via a virtual terminal, do not store card data on any computer system. The Acceptor connects to a virtual terminal over a secure network connection to access a third party that hosts the virtual POI payment processing function (payment gateway). This third party may be a processor, acquirer, or other third-party service provider who stores, processes, and/or transmits Card Data to authorise and/or settle the Acceptors MOTO transactions.

Req S26:A Virtual Terminal shall meet all the relevant requirements of PCI DSS (see [PCI1]) to ensure the protection of the Card Data throughout the transaction process.

Req S27:In addition, the installation of the virtual terminals shall be correctly undertaken meaning that:

- All default settings including but not limited to Passwords and Simple Network Management Protocols shall be changed,
- All network and firewall security settings shall be validated after installation,
- All services and protocols not directly needed to perform the device’s specified functions shall be disabled and shall only be enabled, as required by the Card Service.

Req S28:The Acceptor shall only use the Virtual Terminal to process Card Data, consequently Card data shall not be processed or stored anywhere else within the Acceptor environment.

3.8. Security Guidelines for Consumer Devices

The following security guidelines apply for consumer (electronic or mobile) devices.

CD	Consumer Device
CD1	Only authorised applications (including POI applications)/entities should be able to access and communicate to the MCP / (M)RP / Authentication Application or Credentials residing in a secure environment on the consumer device.
CD2	There should be generic enablers for a secure environment (e.g. for controlled access to sensitive peripherals, secure storage, flexible secure boot to verify the integrity of the consumer device firmware, run-time integrity checking, firewalls and anti-virus software (for further guidance, see for instance *[OMTP1]*, *[OMTP2]* and *[OMTP3]*).
CD3	There should be a mechanism to: • Prevent unauthorised capture of data • Prevent unauthorised use of the consumer device (e.g. a lock function).
CD4	It is recommended that the issuer educates and informs the Cardholder on the risks associated with the use of Consumer Devices and how to protect themselves against the risks associated with e.g., • Rooting / jailbreaking a phone • App Downloading from untrusted sources. When feasible, it is recommended that the issuer provides antivirus products/regular updates to be downloaded and installed onto the consumer device.
CD5	It is recommended that stronger rules are put in place to ensure verification of Card Application codes and the origin of the Card Application, when distributed via an application store.
CD6	It is recommended that Card Application developers incorporate best practices such as • Clearer messaging of permissions requested by given Card Application • Reduce set of permissions to only the necessary ones.

Figure 22: SECURITY GUIDELINES FOR A CONSUMER DEVICE

3.9. Security Requirements for Hardware Security Modules

Hardware Security Modules (HSMs) are widely used to manage and protect cryptographic keys and to support secure processing in order to achieve the cryptographic protection required when data is encrypted by remote payments.

3.9.1. Introduction

This chapter defines the security requirements that apply to Hardware Security Modules (HSMs) 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 Card 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 shall be adhered to for a stakeholder to call itself conformant with the Volume.

3.9.2. Hardware Security Modules

An HSM is a specialised 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 shall be met:

1. The device itself shall meet certain requirements for its hardware and software. The manufacturer or vendor shall 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.

3.9.3. 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, Acceptors 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).

3.9.4. 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.)

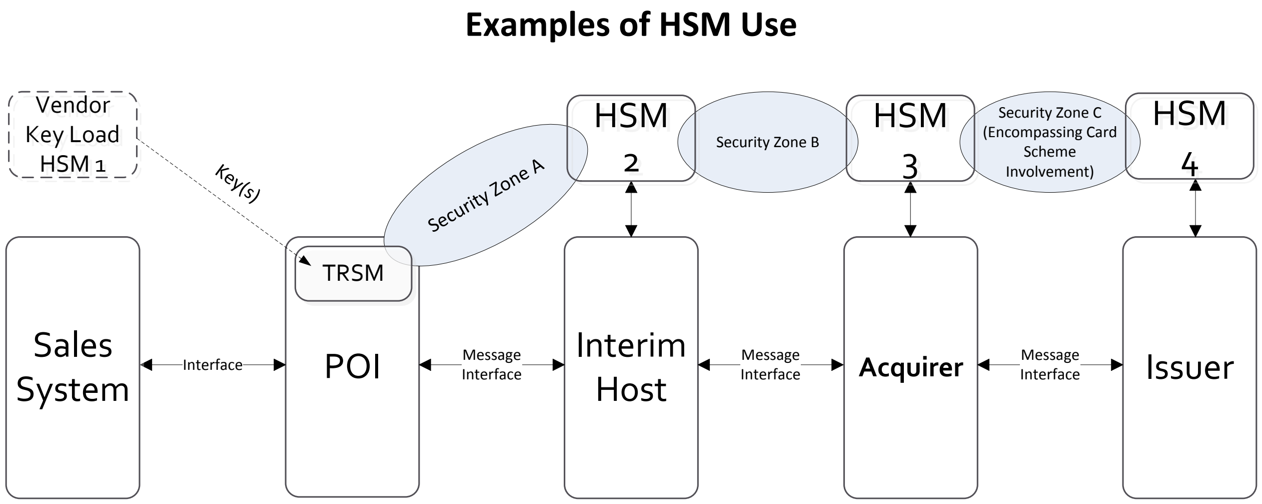


FIGURE 23: EXAMPLES OF HSM USE

3.9.5. HSM Product Certification

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

- FIPS PUB 140-2 Level 3 currently approved version;
- PCI HSM currently approved version;
- 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.

3.9.6. 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 shall 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 shall therefore be operated in line with the PCI PIN requirements even for protocols that do not support online PIN.

3.9.7. Audits

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

Those entities carrying out such audits shall 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.

3.9.8. Key Management

Management of cryptographic keys shall satisfy a formal key management policy and key lifecycle requirements. In particular, the integrity and usage of keys shall be assured and the usage of keys shall 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.

3.9.9. Key Ceremonies

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

Security sensitive changes to HSM configuration should also be performed as a formal key ceremony, i.e. a process in which operations are executed on cryptographic keys following a written approved procedure defined by the security policies of the company managing the HSM.

3.9.10. Test Systems

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

Cryptographic keys used in test systems shall never be used in operational systems and, conversely, operational keys shall 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 used in operational systems, as described in this document.

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

3.9.11. Security Configuration

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

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

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

3.9.12. 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) shall be enabled only for the minimum time necessary. All changes shall be logged. The records shall be precise, recording the versions of HSM (HW and SW), the changes made, the reason for the changes, the date, the time and dual signatures.

3.9.13. New Commands

The impact of any new command shall 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 shall have a formal process to approve new commands.

3.9.14. 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 shall be verified by cryptographic means. When new software is loaded on the HSM, all the keys in the HSM shall be automatically and effectively deleted.

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

3.9.15. Physical Access

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

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

3.9.16. Network Access

Where operational HSMs may be accessed remotely this shall 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 shall be performed in secure memory that prevents MiTM attacks. Two-factor authentication shall be required.

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

3.9.17. Pre-Operational Security

HSMs sent from the manufacturer shall be sealed in tamper-evident packaging, which shall 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 shall be under dual control. Details of all HSMs installed shall 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 shall be created and stored for later inspection.

3.9.18. Post-Operational Security

A HSM that is no longer required for operational use shall be returned to the factory-default state, via a formal key ceremony, before being removed from service. This procedure shall 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 shall 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 shall 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 shall be signed by all personnel involved and stored for possible future inspection.

3.10. Security Requirements for Communication Protocols

3.10.1. Security Requirements for POI to Acquirer Protocols

Authenticity and integrity of data and its confidentiality (as appropriate) in all card payment messages are required to protect the financial system. The mechanism for this is to use cryptographic techniques[26]. 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 POI management. The protocol specification providers and POI management suppliers will define the appropriate security requirements for their messages within their protocols, to provide authenticity and integrity in accordance with this Book. Card schemes may choose to accept the security provided by a POI to acquirer protocol that meets their specific risk requirements.

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

3.10.2. Security Requirements for Consumer Device to POI protocol

Req S29: The protocol shall establish a secure channel between the consumer device and the virtual POI, to protect the transmitted data (authentication, integrity and confidentiality as appropriate). The protected transmitted data may include EMV commands and responses, in the event that a Card Application is used.

Req S30: The initial protected exchange between the consumer device and the virtual POI shall include an indication of the protocol version being used, as the usage of old insecure versions of a protocol should not be permitted.

Req S31: The protocol shall support messages to enable the authentication of both the consumer device and the virtual POI.

Req S32: The consumer device (e.g. through the browser) shall display an icon or similar graphical information to enable the cardholder to recognise that a secure channel has been established with the virtual POI.

Req S33: During the payment stage, the protocol shall convey information to the cardholder on the status of the transaction.

4. Figures and Tables