

EPSG035-26

25.09.2026

VERSION 11.0

SEPA PAYMENTS STANDARDISATION (SPS) “VOLUME”
STANDARDS’ REQUIREMENTS

BOOK 4

SECURITY REQUIREMENTS

Payments and Cash Withdrawals in SEPA
Applicable Standards and Conformance Processes

© European Payments Stakeholders Group AISBL.
Any and all rights are the exclusive property of
EUROPEAN PAYMENTS STAKEHOLDERS GROUP AISBL.

Abstract	This document contains the work on SEPA payment standardisation to date
Document Reference	EPSG035-26
Issue	Book 4 – v11.0
Date of Version	25.09.2026
Reason for Issue	Publication
Reviewed by	15 th EPSG Board
Produced by	Book 4 Expert Team
Owned by	EPSG
Circulation	Public

*The EPSG's Payments Standardisation Volume is dedicated to the memory and legacy of **Jeremy Massey** and **Patrice Hertzog**, whose commitment, leadership and vision have left a lasting mark on our community.*

Jeremy Massey, in his roles as Co-Chair of the informal CSG first, becoming Vice Chair of the registered association ECSG when it was established, exemplified dedication, professionalism and a spirit of collaboration that inspired all those who had the privilege to work with him. Patrice Hertzog, through his skillful guidance as Chair of the ECSG, provided steady leadership and invaluable insight, strengthening both the work and the cohesion of the group.

Beyond their institutional responsibilities, both Jeremy and Patrice are remembered for their generosity, integrity and the meaningful personal connections they fostered. Their contributions continue to resonate in the progress achieved and in the values upheld by this community.

This dedication stands as a tribute to their enduring impact and as a sign of our deep gratitude.

Change History of Book 4		
6.4.0	2012-2013	Working version of Book 4
7.4.1.0	12.12.2013 (published 07.01.2014)	EPC Published version - Volume v7.0
7.4.1.0	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
8.4.40	08.11.2018	Board Approval version for Consultation as 8.5
8.4.50	14.12.2018	Public Consultation Release v8.5
8.5.1	28.02.2019- 28.08.2019	Working version 2019
9.0	15.01.2020	ECSG Published version - Volume v9.0
9.01- 9.13	28.05.2020- 04.11.2021	Working Version 2020-2021
9.13	15.12.2021	Public Consultation Release v9.5
10.0	01.10.2022	ECSG Published version - Volume v10.0
10.01- 10.18	2023-2025	Working Versions towards v10.5
10.5	27.11.2025 (published in December 2025)	Public Consultation Release 10.5
10.5.01	18.05.2026	Validation by the B6ET for submission to Volume-Subgroup review
10.5.02	25.05.2026 (sent to the Board on 27.05.2026 for approval)	Validation by the Volume-Subgroup for submission to legal review

10.5.02	31.08.2026	Legal review
10.5.03	03.09.2026	VOLSG Sanity Check
10.5.04	24.09.2026	Board approval

Table of Contents

1. GENERAL.....	8
1.1. Book 4 - Executive summary	8
1.2. Description of changes since the last version of Book 4.....	10
2. DESCRIPTION OF SECURITY FEATURES FOR PAYMENT TRANSACTIONS.....	11
2.1. Introduction	11
2.2. Local Transactions – Contact and Contactless	11
2.2.1. Card Authentication, Data Protection and Cardholder Verification Methods.....	11
2.2.2. Strong Customer Authentication (SCA)	13
2.2.3. Mobile Contactless architectures	14
2.2.4. Card Based Payments using Commercial Off-the-Shelf Devices.....	18
2.3. Remote Transactions	19
2.3.1. MOTO	19
2.3.2. e- & m-commerce transactions	20
2.4. Instant Credit Transfer (ICT).....	25
2.4.1. Security Considerations specific to ICT Transactions.....	26
2.4.2. Reinforcing SCA for ICT	26
2.4.3. Security Controls for ICT not directly based on SCA	28
2.4.4. The QR Code Security Case	29
2.4.5. Approaches for ICT authentication in distributed contexts	29
3. SECURITY REQUIREMENTS.....	31
3.1. Introduction	31
3.2. Security Requirements for Data related to Payment Services	31
3.3. Cryptography and Key Management	31
3.4. Authentication	32
3.4.1. Possession	32
3.4.2. Knowledge.....	33
3.4.3. Inherence	34

3.5. Acceptance Environments	35
3.5.1. Local Card Transactions	35
3.5.2. e- and m-Commerce Card Transactions.....	36
3.5.3. MOTO Transactions.....	36
3.5.4. Local Instant Credit Transfer Transactions	37
3.5.5. Remote Instant Credit Transfer Transactions	40
3.6. Security Requirements for Card Environments	41
3.6.1. Security Requirements for Physical Chip Cards	41
3.6.2. Security requirements for Mobile Contactless Payment Applications residing in a Secure Element.....	48
3.6.3. Security requirements for Mobile Applications (MA) for HCE-Based systems	55
3.6.4. Security requirements for Applications and Credentials for e- & m- Commerce.....	60
3.7. Security Requirements for Consumer Device used for ICT Transactions	72
3.7.1. Security Objectives for ICT Transactions.....	72
3.7.2. Common Security Requirements for ICT Transaction models and flows	73
3.7.3. Security Requirements for ICT Transaction initiated by NFC/Contactless	74
3.7.4. Security Requirements for ICT Transactions in an e-Commerce context.....	74
3.8. POI Security Requirements	75
3.8.1. Physical POI (for local transactions).....	75
3.8.2. Commercial Off-the-Shelf Devices (COTS)	103
3.8.3. Security Requirements for the Capture of Biometrics by the POI.....	173
3.8.4. Security Guidelines for Virtual POI (for e- & m- commerce)	174
3.8.5. Physical POI (for MOTO)	175
3.8.6. Virtual Terminal (for MOTO)	175
3.9. Security Guidelines for Consumer Devices	176
3.10. Security Requirements for Automated Teller Machines ATMs	176
3.11. Security Requirements for Hardware Security Modules	177
3.11.1. Introduction	177
3.11.2. Hardware Security Modules	177
3.11.3. Scope of Requirements.....	178
3.11.4. Security Zones.....	178

3.11.5. HSM Product Certification	179
3.11.6. Operational Security	179
3.11.7. Audits	179
3.11.8. Key Management	180
3.11.9. Key Ceremonies	180
3.11.10. Test Systems	180
3.11.11. Security Configuration	181
3.11.12. Changes to Security Configuration	181
3.11.13. New Commands	181
3.11.14. Software Loading	181
3.11.15. Physical Access	182
3.11.16. Network Access	182
3.11.17. Pre-Operational Security	182
3.11.18. Post-Operational Security	182
3.12. Security Requirements for Communication Protocols	183
3.12.1. Security Requirements for POI to Acquirer Protocols	183
3.12.2. Security Requirements for Consumer Device to Virtual POI Protocols	183
3.12.3. Security Requirements for Instant Credit Transfer Protocols	184
4. FIGURES AND TABLES	185

1. GENERAL

1.1. Book 4 - Executive summary

It is critical to ensure that security in Payment Services is fully addressed in order to

- Maintain and enhance trust in 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 Payment Systems regardless of the environment as defined in Book 2. 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, 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 payment chain. Consequently, this Book specifies security requirements for components involved in the payment chain such as:

- Application Programming Interface (API)
- Contact and Contactless Payments Instruments, Cards and non-Card irrespective of form factor
- Credential(s) Security
- Customer Authentication 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/COTS)
- 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.

Note that no updates to the MOTO sections with respect to [PSD2] have been performed, in view of recital (95) of PSD 2 as well as the “Final Report On Draft RTS Amending The RTS On SCA&CSC”.

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

Within the continuing update of Book 4, this version includes:

-
- the integration of Security Requirements for Instant Credit Transfer,
- the integration of PCI PTS v7,
- the integration of Commercial Off-the-Shelf (COTS) Devices with PIN entry, and
- editorial updates across the whole Book 4

2. DESCRIPTION OF SECURITY FEATURES FOR PAYMENT TRANSACTIONS

2.1. Introduction

This chapter provides a high-level overview of different security aspects related to the transaction flows involved in Payment 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 payment services, the technology used to process the payment service, as well as where and which technologies are used to provide the e.g. 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 Account 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.

Recommendations for the security of payment account access services can be found within [ECB 2].

2.2. Local Transactions – Contact and Contactless

For local transactions, a number of well-established security features are implemented in the market and used by the stakeholders. This includes

- Card Authentication
- Cardholder Verification
- Data protection using a secure channel
- Security measures against relay attacks.

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]).

The following considerations apply to ICT Transactions initiated by the Card performed via EMV technology.

2.2.1. Card Authentication, Data Protection and Cardholder Verification Methods

This document provides a high level overview of the different Card Authentication and Cardholder Verification Methods (CVMs) for local transactions.

The mobile environment offers a number of additional features which can be utilised for mobile contactless card payments with respect to 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.

	Contact	Contactless	
Card Authentication			
DDA*	X		
fDDA**		X	
CDA*	X	X	
XDA*	X		
BDHLA****		X	
Data Protection			
BDH****		X	
CVMs	Card	Card	Mobile
Physical POI CVM			
Online PIN	X	X	X
Offline PIN	X	X	
Offline Biometrics	X	(see definition in Book1)	
Signature*****	X	X	
No CVM Required	X	X	X
Consumer Device CVM (CDCVM)			
Biometrics			X
Mobile code***			X
Other Methods			
Biometrics via Sensor on Card	(see definition in Book1)	X	

FIGURE 1: OVERVIEW OF CARD AUTHENTICATION AND CARDHOLDER VERIFICATION METHOD

*See [EMV B2] sections 6 and 12

**See [EMV C3]

*** Mobile code¹: entered on the mobile device.

- The verification of the mobile code is done by the MCP application in the SE on the mobile device;
- or
- Implicit validation of the correct entry of the mobile code through a cryptographic derivation, verified on-line by the MCP issuer, typically used for HCE-Based systems (see 2.2.3.2).

**** See [EMV E]

***** Although Signature is not recognised as a valid authentication factor in the context of SCA, it is listed here for implementations that rely on Signature with Chip Cards.

One approach to a “mobile payment using a Consumer Device User/Cardholder Verification Method” (refer to as CDCVM Solution) is described in [1].

A **CDCVM Solution** may be provided at application level (Card / Authentication Application), and/or at device or OS level as a mobile platform authentication mechanism for use by mobile applications on the device (“shared CDCVM”).

It has to be ensured that the CDCVM Solution cannot be maliciously abused, disabled or bypassed; and that its assets are adequately protected. The key security goals and objectives for the steps involved in CDCVM processing (e.g. biometry, mobile code) are:

- **Capture:** Secure processing of the (raw) entry data, secure channel for transfer of CVM data
- **Feature extraction:** Secure extraction / conversion of input into a format suitable for matching with a reference; secure channel for transfer of sample (if applicable).
- **Match:** Secure channel for transfer of stored reference data, secure matching process; and secure channel for transfer of the result of the matching process through the Authenticator APIs

A number of **CDCVM Assets** must be protected, depending on the CDCVM solution. Assets can be categorized as requiring one or more security services: Confidentiality (e.g. Biometric Image), Integrity (e.g. Verification Result), and Integrity with the addition of accountability/authentication (e.g. Biometric Processing Firmware).

2.2.2. Strong Customer Authentication (SCA)

When the European Commission created the [PSD2], within article 97 it mandated the usage of SCA for all electronic payment transactions. However, within article 98 of the [PSD2] the European Commission acknowledged that there are some circumstances, referred to as exemptions, where

¹ For security reasons, in case of a mobile code, this is a dedicated mobile code (also referred to as mobile PIN, mobile passcode, etc.) which differs from the “classic” card PIN.

SCA may not be required and mandated the EBA to specify these exemptions. Chapter 3 of the [RTS SCA/CSC] provides details and definitions of these exemptions.

The combination of Card Authentication with a Cardholder Verification Method (see [Figure 1](#)) is a means to enable SCA. An example of these combinations to achieve SCA could be the usage of an EMV smart card creating an application cryptogram and PIN whereas an exemption is a low value contactless transaction not using a CVM (ref. Art.11 of RTS SCA).

For further details on the exemptions see the documents issued by EBA.

2.2.3. Mobile Contactless architectures

This section provides an overview of the technical and security infrastructure needed to support an MCP transaction (see [Figure 2](#)).

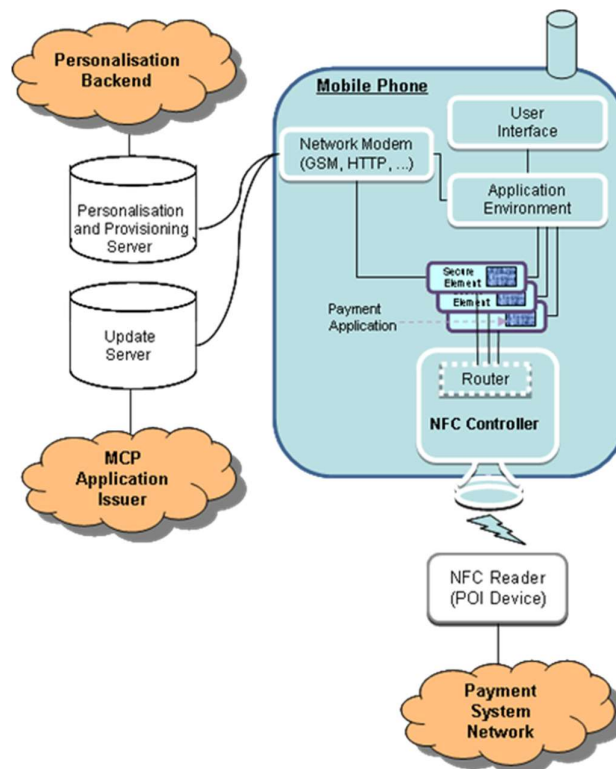


FIGURE 2: THE MCP SYSTEM ARCHITECTURE

Using this architecture MCP transactions are implemented in two different approaches:

- SE-Based,
- HCE-based.

The following table provides for a short overview of the different approaches:

SE in the mobile device	HCE
More complex business model, because a third party must be involved as the provider of the security module SE.	Implementation also possible via an own HCE-Platform; the involvement of a third party can be avoided. A simpler business model can be achieved.
A security level comparable to smartcard and PIN is achievable.	Lower security level compared to the SE approach, while risks can be limited by specific measures, e.g. monitoring and authentication capabilities of the cloud and backend systems.
Experiences available	New innovative approach

Table 3: THE MCP SYSTEM ARCHITECTURE – DIFFERENT APPROACHES

2.2.3.1. SE-Based

To be eligible to conduct an SE-based MCP transaction, the mobile equipment should have the following components:

- An Application Environment in which applications may be loaded and run. This application environment may host User Interface applications which allow for communication between a MCP application and the user.
- A User Interface which displays necessary information and provides the input mechanism for user selection and payment functions.
- One (or more) Secure Element(s) which host one or more MCP applications.
- A NFC Controller which provides contactless capabilities.
- A Network Modem (standard networking protocols issued by ETSI and GSMA, or application-specific protocols built on top of standard Internet access protocols) which provides network connectivity for the Application Environment and for provisioning and personalisation of MCP application onto a Secure Element.

The MCP application is to be installed on a Secure Element by a personalisation and provisioning server which communicates with the Secure Element via the mobile network connection (e.g. OTA). This implies that dedicated processes need to be defined for the provisioning and management of the payment application, which may vary depending on the Secure Element form factor.

An SE is a tamper-resistant module capable of hosting applications in a secure manner. The SE provides a protection of the applications including separation of the applications. The SE may appear in different form factors in the mobile equipment, commonly referred to as:

- An UICC
- An eSE or iSE
- An eUICC

These form factors are mentioned for completeness but are not considered further in the Volume. More information may be obtained from [EPC MCP IIG].

Regardless of the form factor, a Secure Element shall contain:

- An Operating System which supports the secure execution of applications and secure storage of application data. The operating system may also support the secure loading of applications.
- Two communication interfaces:
 - A device (contact) interface which enables commands and responses to be exchanged between the SE and authorised mobile applications in the mobile equipment.
 - An antenna interface (contactless) interface which enables the exchange of commands and responses between an application in the SE and a contactless Point of Interaction via the NFC Controller of the mobile equipment.
- A Manager to maintain a list of contactless applications on the SE, the status of the applications and the associated data. The status of an application indicates if the application is available for selection on the contactless interface.

The Personalisation and Provisioning Server is connected to a personalisation backend, which allows the issuing bank to issue the MCP application to the mobile equipment.

2.2.3.2. HCE-Based

An alternative approach to SE-based MCP Applications has been the introduction of Cloud-Based Payments (CBP) using Host Card Emulation (HCE) supported by the Android mobile phone operating system. Other mobile phone operating systems may also support HCE.

For cloud-based MCPs, the following components are involved:

- A Cloud-Based Payments Platform (CBPP) performs core functions that provision and manage consumer accounts according to issuer predefined preferences.
- A Mobile Application (MA), residing on the Mobile Device, that provides consumers with the tools necessary to manage the cloud-based payments experience including enrolment, provisioning, lifecycle management, and payment
- A Mobile Application Cloud Platform (MACP) securely brokers messages in support of enrolment, provisioning, active account management, and other use cases between the CBPP and the MA.

For these models, the MCP application consists of a part referred to as the Mobile Application (MA) residing on the mobile device and a part implemented in the Mobile Application Cloud Platform (MACP) (see Figure 4).

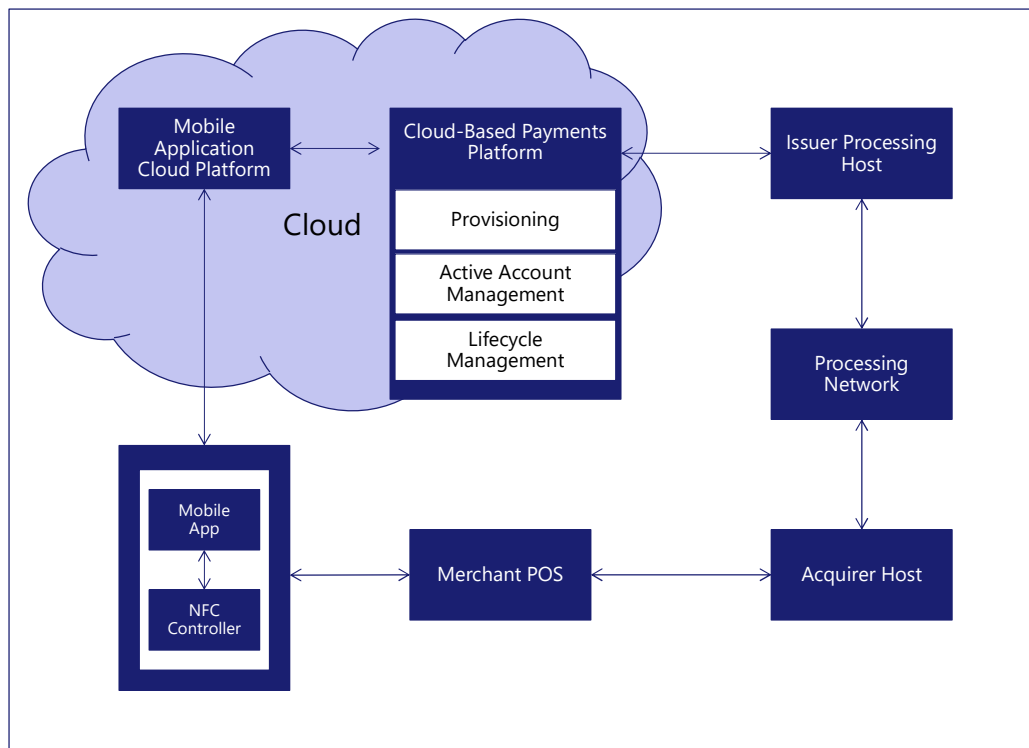


FIGURE 4: THE MOBILE APPLICATION AND MOBILE APPLICATION CLOUD PLATFORM

Cloud-based MCPs require a process to replenish account parameter dynamic data based on the MCP issuer preferences, a process which is referred to as Active Account Management (AAM)

AAM Scenarios:

- **Scenario 1 – Processing Host – Initiated**
 1. Consumer initiates the payment;
 2. Business as usual transaction processing flow;
 3. Transaction flows from the acquirer to the issuer processing host who checks if account parameters (dynamic data) need to be replenished;
 4. AAM will generate new account parameters and push to the MA on the mobile device.
- **Scenario 2 – Cloud-based payments platform – Initiated**
 1. Based on account parameters, the cloud-based payments platform initiates AAM;
 2. The cloud-based payments platform pushes new account parameters to the MA on the mobile device.
- **Scenario 3 – Mobile Application – Initiated**
 1. On-device account thresholds indicate account parameter replenishment is needed; the MA sends a request to cloud-based payment platform via the MACP;

2. The cloud-based payment platform will either replenish account parameters or deny request. If honouring request, it sends new account parameters to the MA on the mobile device.

To enhance the security, HCE-based solutions may be offered in combination with Payment Tokenisation. For further information on Payment Tokenisation, please refer to the EMVCo Tokenisation Specification – Technical Framework [EMVCo-FW v2]. The EPSG work on this subject is ongoing.

2.2.4. Card Based Payments using Commercial Off-the-Shelf Devices

Background

In traditional merchant payment scenarios, a PIN entry device (PED) that has been independently tested and validated against detailed security requirements is used to enable Contact, (Chip and PIN) or Contactless, (Tap and go) transactions to be performed. Traditional PEDs rely on hardware security as the primary protection mechanism to ensure the security of PIN data entered into the device.

Mobile payment acceptance introduces a new method for Card Based Payment Transactions to be accepted by merchants in remote, non-fixed locations. This new payment acceptance method utilizes Commercial Off-the-Shelf, (COTS) devices considered a COTS Solution consisting of the following key components:

- COTS Device as Front-End including Payment Application on the COTS and SCRP (where necessary)
- Back-end monitoring system

The assurance of the COTS Solution moves away from the reliance on physical security to be based upon an initial security evaluation and the continuous monitoring by the Back-end system of the Front-End.

Note that the COTS Device is assumed not to contribute to the security of the COTS Solution.

There are three different acceptance methods for Mobile Payment Acceptance:

- Contact with Pin on COTS
- Contactless on COTS without PIN
- Contactless on COTS with PIN

Ensuring the security of Customer data for all three options is essential and utilizes new concepts for providing security of the PIN and Customer data.

For each acceptance method there are some common core aspects and some security mechanisms specific to the acceptance and authentication method used.

All three methods rely on a secure payment application running on the COTS Device that is the core of the payment acceptance process. This application will enable the transaction to take place

and where necessary allows for software-based PIN entry, encrypting the PIN immediately in software upon entry.

Supporting the secure payment application is a back end monitoring system. The secure payment application will be in communication with a back-end monitoring system such that it will:

- Monitor and provision security controls to detect, alert and mitigate suspected or actual threats and attacks against the secure payment application, and the COTS Device
- Perform regular health-check on data from the secure payment application and enforces pre-established security policies
- Provides the Processing environment that receives encrypted Customer and PIN data (for online PIN validation and authentication).

For a Contact with PIN solution it is necessary to have a separate Secure Card Reader PIN, (SCRPN) that supports the solution and enables the transaction to be undertaken whilst performing any necessary PIN functions. The SCRPN is Secure Read and Exchange of Data (SRED)-enabled and connected to the COTS Device. The SCRPN provides:

- a. Protection of Customer data sourced from the payment instrument
- b. Decryption of encrypted PIN data received from the PIN CVM application
- c. Translation of PIN data into required PIN-block format (This would only apply to online PIN verification processing.)
- d. Re-encryption of PIN data

Detailed and specific security requirements for all these options can be found in Section 3.7.2

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, 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 PSD2 (see [PSD2]).

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

The Acquirer shall have the capability to enable further authentication of the transaction and/or the Customer 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 Customer 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 Customer. 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 Customer. For the purpose of this document, the payment is undertaken during the ordering process. Direct Debit, or Payment upon Delivery are not considered.

The Customer 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 Customer for remote payment services, Acceptor websites shall also provide similar security information. It is assumed that the Customer 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
- the degree to which Customers 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 Customer, 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 Customer 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 Customer offers a number of additional features compared to other 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 Account Data from the Customer and each comes with specific security threats which need to be appropriately addressed by the parties involved. Examples:

- Acceptor not involved in the payment phase: Solutions where the acceptor outsources all the payment functionality to a payment service provider. With this approach, the acceptor never stores, processes or transmits any Account Data. Total reliance is placed on the service provider hosting the payment page.
- Acceptor partially involved in the payment phase: Solutions where the acceptor starts the payment process by providing the Customer with a payment page. When the payment page has been populated by the Customer, the payment page is redirected/handed off to the acquirer, sometimes via the Third Party Service Provider. While with this approach Account Data is not returned to the acceptor, nonetheless, the website providing the payment page to the Customer could be a source of vulnerability.
- Acceptor fully controls the payment phase: Solutions where the acceptor's payment page captures and processes Account Data before submitting it to the acquirer. With this approach, the acceptor shall follow more stringent security requirements for protecting Account 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 all of the above described solutions, on completion of shopping the Customer confirms the transaction amount and provides Account Data to the payment page either by

- manually entering their Account Data on the payment page, or
- confirming previously stored Account Data.

For e- & m-commerce transactions different authentication mechanisms may be used in combination with a CVM. The following sections describe these in more detail.

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.

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 Customer (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, either directly with their Customer or indirectly using Risk Based Authentication in accordance with [PSD2]. 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 Customer).
- 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 Customer (e.g., SMS, e-mail, different device);
 - The result of a random challenge / response mechanism. For card payments, 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 Customer is requested to enter their CDCVM only once during the transaction process.

For further details on implementation of a dedicated *Authentication Application* refer to [FIDO] standards for example.

The dynamic authenticator is typically linked to a specific transaction and the transaction amount

2.3.2.2. Cardholder Verification Methods (CVM)

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 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 secure device (e.g., an additional authentication device) approved by the 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 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 code / CDCVM 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).

The figure below lists typical combinations (“X”) of Card Authentication Methods with CVMs:

Cardholder verification	Card authentication		
	No authentication	Static authentication	Dynamic authentication
No CVM	X	X	X ²
CVM		X	X ³

FIGURE 5: COMBINATION OF AUTHENTICATION METHODS / CVMs FOR E- AND M-COMMERCE

2.3.2.3. Strong Customer Authentication with Dynamic Linking

For remote transactions, if the issuer applies Strong Customer Authentication, the “Dynamic linking” as specified in art 97.2 of [PSD2] and art. 5 of [RTS] shall be applied. This requires that:

- “...The authentication code generated shall be specific to the amount of the payment transaction and the payee agreed to by the payer when initiating the transaction.
- the authentication code accepted by the payment service provider corresponds to the original specific amount of the payment transaction and to the payee agreed to by the payer.
- Any change to the amount or the payee shall result in the invalidation of the authentication code generated.” (article 5 of [RTS])

² The usage of the consumer device as a personal device might allow this combination for certain scenarios (e.g., for low value payments).

³ For dynamic authentication, the transaction data may be used to generate the challenge which, in combination with a CVM, could create a Strong Customer Authentication method, as defined by the RTS guidelines on the security of Internet payments, see [RTS SCA/CSC], as well as [PSD2]

The combination of a dynamic card authentication method (see section 2.3.2.1) with a CVM provided by the Customer (see section 2.3.2.2) is a means to enable “strong customer authentication method” with Dynamic Linking.

2.3.2.4. Risk-Based Authentication

Risk-Based Authentication is the use of statistical models via transaction, location, device and profile data to make a Customer authentication decision without active Customer participation in the decision-making process (see also Articles 18 and 19 of the EC Delegated Regulation 2018/389).

Risk-Based 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 Risk-Based Authentication during an e or m-commerce transaction, the Customer needs to be redirected to the issuer/acquirer as the first step of the Authorisation process.

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

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

2.4. Instant Credit Transfer (ICT)

Appropriate security services shall be implemented by the devices and associated processing services for ICT.

Key security services are confidentiality, SCA as well as authentication, and integrity of the exchanged messages. Such services shall be implemented by means of security mechanisms (i.e. cryptographic primitives) by the parties interacting at each stage of the ICT Transaction. These security mechanisms require the use of certified hardware and software components for cryptographic calculations (generation and verification of cryptograms), management of cryptographic keys and protection of authentication data.

When properly implemented, these security services shall reduce the ICT system vulnerabilities and the feasibility and impact of the threats on the business interests of the parties involved in the ICT Transaction execution.

2.4.1. Security Considerations specific to ICT Transactions

With ICT Transactions, the risk that the funds become immediately available to fraudsters should be addressed. Appropriate security measures shall be in place to mitigate this risk, both in the Payee enrolment phase and during the transaction.

Security services should be implemented by devices and associated processing services involved in ICT Transactions. The security services of the ICT Transaction environment provide security properties to the messages exchanged during the ICT Transaction to comply with the requirements for ICT set out in section 3. When appropriate, sensitive data should be protected not only in-transit, but also at rest or when being processed in any computing operation during the ICT Transactions execution.

Notice that a diversity of security strategies can be put into place by PSPs to detect ICT fraud. Basically there are two types of complementary security controls put in practice by PSPs to minimize the fraud risk for ICT Transactions:

1. Those using trusted technology to reinforce the explicit consent provided by a Payer to initiate an ICT Transaction, using trusted payment devices and cryptographic mechanisms. That's the "reinforced" SCA strategy, especially in an Open Banking model through dedicated secure interfaces. They are insufficient to mitigate "social engineering" attacks typical of ICT Transactions. Refer to 2.4.2. Notice that the distributed nature of the ICT Transaction processing circuits is a driver for innovation on authentication mechanisms. This point is introduced in 2.4.5.
2. Those don't relying directly in cryptography but (1) using real-time risk analysis of the ICT Transactions (ICT scoring, Customer behaviour) and/or (2) through the implementation of additional security controls, such as the EPC Verification of Payee or Request to Pay to protect the ICT users. Refer to 2.4.3

2.4.2. Reinforcing SCA for ICT

2.4.2.1. Specific risks for ICT

Compared with card payments, ICT Transactions show up a higher risk profile for different reasons:

1. The amount that can be paid using an ICT is much higher than for card payments
2. The nature of the ICT makes it more complex to be paid back in case of involuntary mistake or fraudulent transaction
3. The diversity of Data Flows involving multiple intermediaries

4. The broad use of QR-Codes whose security has just been standardized but not still been endorsed to initiate a payment. Refer to 2.4.4
5. Social engineering attacks specialising in ICT Transactions difficult to counter by technical means
6. The fact that PSPs only have some seconds for filtering suspicious transactions. In a card transaction the analysis of the risk takes place before the authorization of the transaction. In ICTs the analysis of the risk takes usually place after the ICT Transaction has been authorised by the PSP of the payer

All the above reasons push PSPs to reinforce technologies used to confirm the explicit consent of the ICT Transaction payer to pay a fixed amount.

Central security services for ICTs include data confidentiality, message (data) and user authentication, integrity and not repudiation when a message conveys a confirmation by the user. These services will protect the messages against the identified ICT threats. When properly designed, these security services will reduce the ICT system vulnerabilities and the level of fraud.

Security services shall be implemented by means of security mechanisms making use of cryptographic primitives and biometric mechanisms. The implementation of these security mechanisms requires the use of certified hardware and software components to (1) compute cryptographic calculations (generation and verification of cryptograms), (2) support the secure management of cryptographic keys and (3) ensure the protection of authentication data used for SCA in the ICT context.

2.4.2.2. ICT Transactions initiating channels and SCA

Card payment channels may be used to initiate an ICT Transaction: NFC/Contactless, Scan of QR-Codes and Remote Transactions. Yet in each scenario the processing circuit and therefore the threats for the ICT Transaction differ. For instance, the ability of an attacker to intercept and modify a legitimate ICT order depends on the channel used.

- In the current ICT market, solutions based on the scan with a mobile device of a QR-Code presented by the merchant prevail. The ICT application is then redirected to a remote server using an @ Internet encoded in the QR-Code. The ICT application should however proceed to the verification of this QR-Code prior to accept any redirection. The remainder of the ICT Transaction is remote and therefore dynamic linking SCA applies
- When the ICT Transaction is initiated using a NFC/Contactless interface the EBA (refer to Q&A 2020_5247) considers that the transaction should be considered as a proximity payment requiring SCA but not dynamic linking
- When the ICT is generated for a remote transaction, dynamic linking applies according to Article 97(2) of the PSD2

2.4.3. Security Controls for ICT not directly based on SCA

2.4.3.1. Use of artificial intelligence (AI) and machine learning (ML) to counter ICT Fraud

Traditionally PSPs have made use of AI technologies to detect payments and customer enrolment fraud as well as to comply with KYC requirements. Yet the use of AI to improve the security of payments has not been discussed so far in the EPSG.

Use AI machine learning (Deep) to anticipate fraud patterns and improve filtering of suspicious ICT Transactions. AI algorithms are useful to reduce false positives (fraudulent ICT Transactions considered good) and false negatives (legitimate ICT Transactions mistakenly blocked) especially for online payments and ICT Transactions initiated via a TPPSP.

Another use case for AI and ML could be adding new beneficiaries (white list), which is for regular ICTs a usual target for social engineering attacks.

2.4.3.2. Verification of the Payee and Request-to-Pay in the ICT context

As outlined by the EBA in recent years, many consumers have been tricked into transferring money to fraudulent accounts, and little chance for reimbursement. In the short term, Verification of Payee and Request to Pay appear as solutions to prevent fraud in the field of ICT Transactions.

- **EPC Verification Of Payee (VOP) scheme**

VOP is the EPC solution for the IP Regulation requirement that mandates all the Banks in the EU/EEA to implement a mechanism to verify the payee (i.e., beneficiary) of an ICT. The scheme provides PSPs with a messaging functionality. It is not a payment means or a payment instrument but it allows the payer to verify certain data about a Payee. VOP terminology is particular. For instance, the “The VOP Requester” is the Payer.

The VOP scheme allows the payer’s PSP (the Requesting PSP) to instantly send to the PSP of the payee (the Responding PSP), a request to verify the IBAN and the name of the payee as given by the payer (the Requester), and potentially in addition, an unambiguous identification code (e.g., Value-Added Tax (VAT) number, an Legal Entity Identifier (LEI), social security code) about that payee. The reason for this request is that the payer intends to initiate a SEPA Credit Transfer (SCT) or a SEPA Instant Credit Transfer (SCT Inst) transaction to the payee. The Responding PSP will then instantly verify whether the received data match with the concerned data registered for that payee at the Responding PSP. The Responding PSP immediately provides the Requesting PSP with a VOP response (e.g., match, no match, close match with the name of the payee, match/verification check not possible). The Requesting PSP then immediately passes on the response to the payer.

The EPC has published a first version VOP v1.0. It can be seen as a kind of ID Management System for Beneficiaries (Merchants, Individuals) of ICTs. Thus, the VOP Scheme has created

a new Role of Routing and Verification Mechanisms (RVM) in the context of the EPC Verification Of Payee (VOP) scheme. Organizations can apply to become a “EPC-compliant” RVM and provide the service to the Banks or TPP initiating an ICT.

The technical Interbank domain specifications for the VOP scheme will be based on API technology and ISO 20022 messages.

- **SRTP (SEPA Request-to-Pay)**

The new SRTP Scheme Rulebook v4.0 has been just released in November 2024. It follows a Public Consultation on v3.0 that concluded in December 2023. Since then a specific EPC Task Force has tried to solve the Comments submitted during the Consultation and has released this v4.0.

In the SRTP there is no Broker. The merchant initiates directly a Request-to-Pay transaction with its own Merchant Bank or RTP Service Provider. Before, the Payer and the Merchant agree on the RTP conditions (how the Payer’s Debt with the merchant will be paid. For instance in three times) and the Payer provides a RTP mandate to the Merchant.

2.4.4. The QR Code Security Case

ISO 5201 (2024) is the only standard available for the security of QR-Code used by the financial industry.

This standard provides a complete set of recommendations to improve the security of transactions initiated with a QR Code covering the whole range of QR Code payment scenarios even if ISO 5201 is not specific to ICTs.

Due to the short term after publication ISO 5201 has not been widely endorsed for ICT QR Code solutions by the payments industry.

2.4.5. Approaches for ICT authentication in distributed contexts

ICT Transactions may be processed over distributed contexts, meaning open networks involving multiple independent entities (e.g., ASPSPs, PISPs, Scheme hubs, Merchants), which may not share direct contractual relationships. Beyond SCA requirements, additional authentication approaches are used to ensure mutual trust among participants and to protect the integrity of the transaction flow. The following approaches are commonly used to support Customer authentication in ICT Transactions involving a TPP PISP:

Redirection:

The Customer initiates the transaction with the PISP and is then redirected to the ASPSP to perform SCA. Once authentication is completed, the Customer is redirected back to the PISP. This model does not use the PSD2 API for the SCA process itself.

It is compatible with modern authentication protocols such as FIDO2/WebAuthn, often combined with authorisation frameworks like OAuth 2.0 or OpenID Connect, enabling strong cryptographic authentication without relying on shared secrets.

Embedded:

The PISP handles the Customer interface for the full authentication process, while communicating with the ASPSP through the PSD2 API. The ASPSP generates an authentication challenge that is passed to the Consumer Device, where the Customer responds using a biometric or knowledge-based factor. The response is then transmitted back to the ASPSP for verification.

This challenge-response flow is supported by specifications such as the Berlin Group's OpenAPI.

Decoupled:

The PISP initiates the transaction via the PSD2 API, and the ASPSP performs authentication through a separate channel — typically a mobile banking app. The Customer completes the SCA outside the PISP interface, while the browser session remains active with the PISP.

This model enhances user experience by eliminating redirections while maintaining strong authentication via a trusted ASPSP application.

Delegated:

The ASPSP delegates the execution of SCA to a third party, such as a wallet provider or a PISP, while remaining fully responsible for compliance. The third party performs the authentication, and the result is transmitted to the ASPSP via the PSD2 API.

This delegation may include partial SCA execution, such as relying on device biometrics provided by the third party. The EBA has issued guidance clarifying the conditions under which such delegation is permitted under PSD2.

Offline:

Authentication occurs locally between the Consumer Device and a POI using EMV standards. The resulting cryptogram is transmitted to the PISP, who uses it to initiate the ICT Transaction via the PSD2 API.

The PISP also relays necessary merchant identifiers (e.g., IBAN or tokenised ID) to complete the transaction. This approach entails API support to process the offline-generated authorisation request securely.

3. SECURITY REQUIREMENTS

3.1. Introduction

This chapter defines security requirements for:

- Payment Transactions including Authentication, CVMs and Risk Parameters
- Payment Devices
- POIs
- Mobile devices
- ATMs
- HSMs
- Communication protocols.

3.2. Security Requirements for Data related to Payment Services

Req S1: All Customer and Acceptor Personal Data and Sensitive Payment Data related to Payment Services shall be protected strictly in accordance with the respective legal and regulatory requirements such as [PSD2] and [GDPR] and used solely for the purposes explicitly allowed by those regulatory standards.

Req S2: Customer data and sensitive authentication data shall be protected in all Acceptance environments. Scheme Rules will define whether this is achieved by:

- Compliance to PCI DSS where relevant,
- Compliance to a Scheme defined equivalent Security Framework, dependant on the particular environment.

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

The protection of Card Data in the Cards Environment is handled in Section 3.6

3.3. Cryptography and Key Management

For encryption or key management, appropriate cryptographic algorithms and key lengths according to the state of the art shall be employed.

- For Payment Transactions, guidance for the usage of cryptography and key lengths is given in [EPC Crypto].
- For Key Management, guidance can be found in [ISO 11568]. For specific key transport mechanisms, reference is [ISO 20038].
- For ICT Transactions, guidance is given in several RFC standards, i.e. [RFC5652] and [ETSI TS 119 312].
- [BSI TR-02102-1] provides guidance for both Payment Services.

3.4. Authentication

The distinction between 'Cardholder Verification' and 'Card Authentication' used in previous versions of this Book is due to the EMV standard, which defines these two functions and their related methods separately. From a more abstract perspective, 'Cardholder Verification' and 'Card Authentication' together form a method for performing Strong Customer Authentication (SCA). Both functions thus are part of methods for strong customer authentication based on different factors.

In the context of ICT Transactions, only the concept of Authentication applies, whereas 'Cardholder Verification' and 'Card Authentication' are specific to the EMV® standard and Card Transactions.

Therefore, 'Cardholder Verification' and 'Card Authentication' are merged into one function called 'Authentication', which in general also covers 'Authentication' for Instant Credit Transfers.

Customer Authentication is performed according to the rules defined by the ASPSP including SCA mechanism according to [PSD2] and the [RTS SCA/CSC]. This applies to both, the onboarding process and the transaction processing. The security requirements for the onboarding process are out of scope of this Book.

The Authentication of the Acceptor is performed by the Acceptor PSP. This Authentication process is out of the scope of this document. This section provides security requirements for the Authentication methods as described in Table 4 of Book 2.

3.4.1. Possession

The Authentication methods SDA, DDA, CDA, fDDA, XDA, BDHLA, EMV Online Authentication, fulfilling Possession factor under SCA are defined by EMVCo. Therefore, security requirements shall be implemented according to [EMV B2] and [EMV E].

The Dynamic Authentication methods fulfilling Possession factor under SCA shall align with standardised secure algorithms (e.g. [ISO/IEC 18033]) and key management (e.g. [ISO 11568]).

Static Authentication, while it is not an SCA-compliant method, continues to be used in the card environment for legacy reasons and is thus retained in the Volume.

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

Req S10: 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 [RTS SCA/CSC], [EBA 1], and national regulations.

Req S11: Strong customer authentication shall be performed in accordance with the [PSD2] and the RTS. See section 2.3.2.3.

Req S12: For the purposes of generating an Authentication Code to satisfy the requirements on Dynamic Linking, (as specified in [PSD2] and [RTS]) Payment Service Providers shall include in the authentication process, elements which dynamically link the transaction to a specific amount and a specific Acceptor.

3.4.2. Knowledge

In Table 4 of Book 2 the PIN, and Online/Offline Personal or Mobile Code have been identified as Knowledge factors for SCA.

3.4.2.1. 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.

Req S8: If a PIN/CDCVM is used for CVM or One Time Password, then they shall be used in conjunction with a Try Limit and with a Try Counter⁴.

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

Req S24: 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 one of the algorithms of [ISO 9564]-2. A dynamic encryption method like DUKPT (Derived Unique Key Per Transaction) or UKPT (Unique Key Per Transaction) should be used to enforce unique keys per transaction for the PIN block protection. Format 1 should be avoided when the PAN is available.

Req S25: 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 S26: PIN translation from one ISO PIN block format into another shall follow the PIN block format translation restrictions defined in ISO 9564-1.

Req S27: 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 S28: The PIN shall be encrypted inside a TRSM (PIN pad or PED) where the PIN is entered by the Cardholder at the POI.

Req S29: 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.

⁴ Where there are a number of applications on a single device using the same CVM reference data, there should be a common Try Counter.

For PIN transmission from the POI to the Card the following requirement applies:

Req S43: The PIN shall always be transmitted encrypted.

3.4.2.1. *Online/Offline Personal or Mobile Code Security Requirements*

Req S30: If Personal or Mobile Code is used and verified online by the Issuer or offline by the Payment Device, then it shall be protected using appropriate security requirements.

Req S34: If the Personal or Mobile Code is used as a knowledge factor for a SCA method according to PSD2/RTS the requirements of the RTS have to be fulfilled.

3.4.3. Inherence

3.4.3.1. *CDCVM Security Requirements*

In [EMV CDCVM SR], dedicated Security Requirements for controls are listed, which should be followed in the design of the CDCVM Solution, for a dedicated Card / Authentication Application and its architecture. Further best practices may also be consulted in [EMV CDCVM BP].

Req S33: If CDCVM is used and verified on the mobile device, then it shall be protected using appropriate security requirements, as defined in [EMV CDCVM SR].

Req S35: If the biometric is used as an inherence factor for a SCA method according to PSD2/RTS the requirements of the RTS have to be fulfilled.

3.4.3.1. *Biometrics via Sensor on Card*

For the usage of Biometrics for physical card, the following security requirements apply:

Req S31: If a biometric method is used as CVM, then it shall be used in conjunction with a Biometric Try Counter Limit and with a Biometric Try Counter on the Physical Card. This Counter and Limit should be distinct from the ones used for Offline PIN.

False Acceptance Rate (FAR) and False Rejection Rate (FRR) of a biometrics verification method implementation should not exceed a value set according to the payment industry security best practises and/or technology state-of-the-art. Higher values of FRR will result in a need to set the respective Biometric Try Counter Limit to a relatively higher value that will affect the security of the method. Therefore, FRR should be at an optimal security versus convenience ratio.

Req S32: If a biometric method is used as CVM, then the threshold for the FAR shall be less or equal to 10^{-4} ($= 1:10.000 = 0.01\%$). 5

3.5. Acceptance Environments

This section defines requirements for Payment transactions conducted in various Acceptance Environments.

3.5.1. Local Card Transactions

Req S3: For local contact transactions, the requirements on Strong Customer Authentication specified in [PSD2] and [RTS] shall apply.

3.5.1.1. Chip with Contact

Req S4: For local contact transactions, SCA shall be implemented according to the relevant Security Requirements specified in [EMV B2].

3.5.1.2. Chip and Mobile Contactless

Req S5: For Contactless Transactions, SCA shall be implemented according to the relevant Security Requirements specified in [EMV B2] and, when ECC is used, according to [EMV E].

In addition, the following requirements shall apply:

Req S6: For Card Authentication for contactless transactions, dynamic authentication as described in section 2.2 shall be performed.

Req S7: The risk parameters “Acquirer CVM Limit”, “Floor Limit” and “Transaction Limit” shall be supported by the Physical POI.

Req S8: The acquiring systems and protocols used shall be able to support the authentication methods and the CVM methods, as appropriate, described in section 2.2.1.

Req S9: Mechanisms may be made available by the Card and the POI to safeguard against relay attacks as defined by EMV in [EMV C8].

3.5.2. e- and m-Commerce Card Transactions

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 global authentication standard currently in use is the [EMV 3DS].

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 S13: On-line authorisation shall be supported unless a dedicated (M)RP application is used.

Req S14: The risk parameters “Acquirer CVM limit” and “Floor limit” shall be supported by the virtual POI.

Req S15: The acquiring systems and protocols used shall be able to support the authentication methods and the CVMs, as appropriate, described respectively in sections 2.3.2.1 and 2.3.2.2

3.5.3. MOTO Transactions

For MOTO transactions the following security requirements apply:

Req S16: The floor limit for all MOTO transactions shall be set to zero.

Req S17:

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 S18:

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 S19: Card Data shall be encrypted when transmitted across open public networks as required by card schemes.

Req S20: Sensitive card data shall be appropriately protected.

Req S21: Static Authentication as described in section 2.3 shall be performed at a minimum which involves the Issuer verifying the data presented.

Req S22: The static authenticator (CSC) shall be securely deleted by the Acceptor after authorisation, which means it shall never be stored post-authorisation.

Req S23: For Telephone Order, the Card Data shall not be included in call recordings, even if encrypted⁶.

3.5.4. Local Instant Credit Transfer Transactions

For Local ICT Transactions the requirements listed in section 3.4.1 "Possession" apply.

In addition, tokenisation mechanisms are often used to encrypt user data.

⁶This 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).

3.5.4.1. *Merchant-presented or Consumer-presented QR Code*

[ISO 5201] and “CSN EN 18184 Financial services — Specification of QR codes for mobile initiated (instant) credit transfers” are listing relevant security requirements for QR code usage for Local ICT Transactions.

The following requirements summarise the most relevant security aspects from ISO and EPC work to mitigate the risks related to QR Code usage for ICT Transactions.

3.5.4.1.1. Common Security Requirements

Req S44: The request to generate QR-Code data shall be subject to the authentication by the CSP or the requester entity (mobile device of the payer or merchant POI)

Req S45: The CSP, Mobile Payment Applications and POI software processing QR-code data shall be subject to a security certification program

Req S46: PSPs shall assess the potential risks on displayed QR-Codes attacks and when feasible use physical control measures to mitigate this threat

Req S47: PSPs shall assess the risks of the unauthorized disclosure, alteration and misuse of the individual data fields of the payload

Req S48: Based on the above risk analysis, PSPs shall decide which data fields can be transmitted as plain text or ciphertext

Req S49: Upon the request of the payment service user (Customer or Acceptor) the QR-code data generated by the CSG shall be protected by an integrity cryptographic mechanism (digital signature or MAC-based)

Req S50: A mobile device application or POI processing software shall have the capability to verify a digital signature or MAC on a scanned QR-Code

Req S51: A payload field carrying privacy sensitive data shall be encrypted

Req S52: It shall be possible to allow a mobile device application or merchant POI to append and apply an additional signature or MAC to an authentication code originated from the CSP

Req S53: An anti-phishing policy shall be set up, that defines methods and processes to protect personal and transaction data from being compromised or misused.

Req S54: The integrity of data generated by the CSP, as appropriate, shall be checked before any transaction information is displayed to the payer on their mobile device or the merchant POI.

Req S55: The CSP shall be able to establish a secure channel with either the mobile device application or the POI or processing equipment of the merchant.

Req S56: The CSP shall be able to establish a secure channel with PSPs.

3.5.4.1.2. Security requirements specific for Merchant-presented QR Code

- Req S57: The data encoded in the QR-Code shall be designed to activate a properly developed and certified application resident in the payer's mobile device.
- Req S58: The payer's mobile device application and/or its PSP and CSP shall verify the integrity and authenticity of the payment QR-code presented by the merchant.
- Req S59: The PSP and/or the CSP shall implement anti-phishing mechanisms to be executed prior to any redirection of the payer's mobile device to a web site designated by the code URL.
- Req S60: Any merchant or other web site with which a payer's mobile payment application interacts after scanning the QR Code shall be protected against all well-known internet originated attacks.
- Req S61: Any merchant or other web site with which a payer's mobile payment application interacts after scanning the QR Code shall present no malware injection or other threats to an authorized connecting mobile payment application.
- Req S62: The POI processing software shall avoid having sensitive clear-text information (such as IBAN_merchant) in the QR Code presented to the mobile device of the payer.
- Req S63: The merchant requester of a QR Code to the CSP shall be authenticated.
- Req S64: The web site to which the mobile device is redirected shall protect the payer's sensitive information.
- Req S65: The POI equipment shall implement a mechanism to identify that the same presented QR Code designed for a single payment is being scanned repeatedly and reject subsequent payments associated to the same QR Code.

3.5.4.1.3. Security requirements specific for Consumer-presented QR Code

- Req S66: If the payer presented code is dynamic it shall be valid only for a defined period of time and the payer shall be informed that he has to insure a valid QR Code is available. h
- Req S67: If the Consumer-presented code is designed for multiple payments, the Customer shall be informed of the number of presentations still available.
- Req S68: Encryption shall always be applied to all confidential data such as the following data:
- o account holder verification data such as authentication factors of the category knowledge,
 - o PSP personal information,

- o Payment Account IBANs/PANs.

Req S69: A field carrying a payer's IBAN or equivalent which has not been cryptographically tokenised shall be encrypted.

Req S70: Prior to the QR-Code presentation, sensitive payer's data such as the identifier e.g. the e-mail address or mobile number shall be protected by a certified mobile application.

Req S71: After scanning by the POI, access to confidential data like IBAN shall after decryption only be possible within a Secure Cryptographic Device compliant with ISO 13491-1 requirements.

3.5.4.2. NFC-based ICT Transaction

For NFC-based ICT Transactions the following requirements apply:

Req S72: For Contact and Contactless Transactions, SCA shall be implemented according to the relevant Security Requirements specified in [EMV B2] and, when ECC is used, according to [EMV E].

Req S73: Dynamic authentication as described in section 2.2 shall be performed.

Req S74: The intermediary payment systems (e.g., Scheme platform, PISP) and protocols used shall be able to support the authentication methods and the CVM methods, as appropriate, described in section 2.2.1.

3.5.5. Remote Instant Credit Transfer Transactions

3.5.5.1. Merchant-presented QR Code

[ISO 5201] and "CSN EN 18184 Financial services — Specification of QR codes for mobile initiated (instant) credit transfers" are listing relevant security measures for QR Code usage for Local ICT Transactions.

Refer to security requirements for Merchant-presented QR Code described in Section 3.5.4.1.

3.5.5.2. NFC-based ICT Transaction

NFC-based ICT Transactions are not applicable to Remote Transactions. Refer to Book 2 Table 4 for further information.

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.

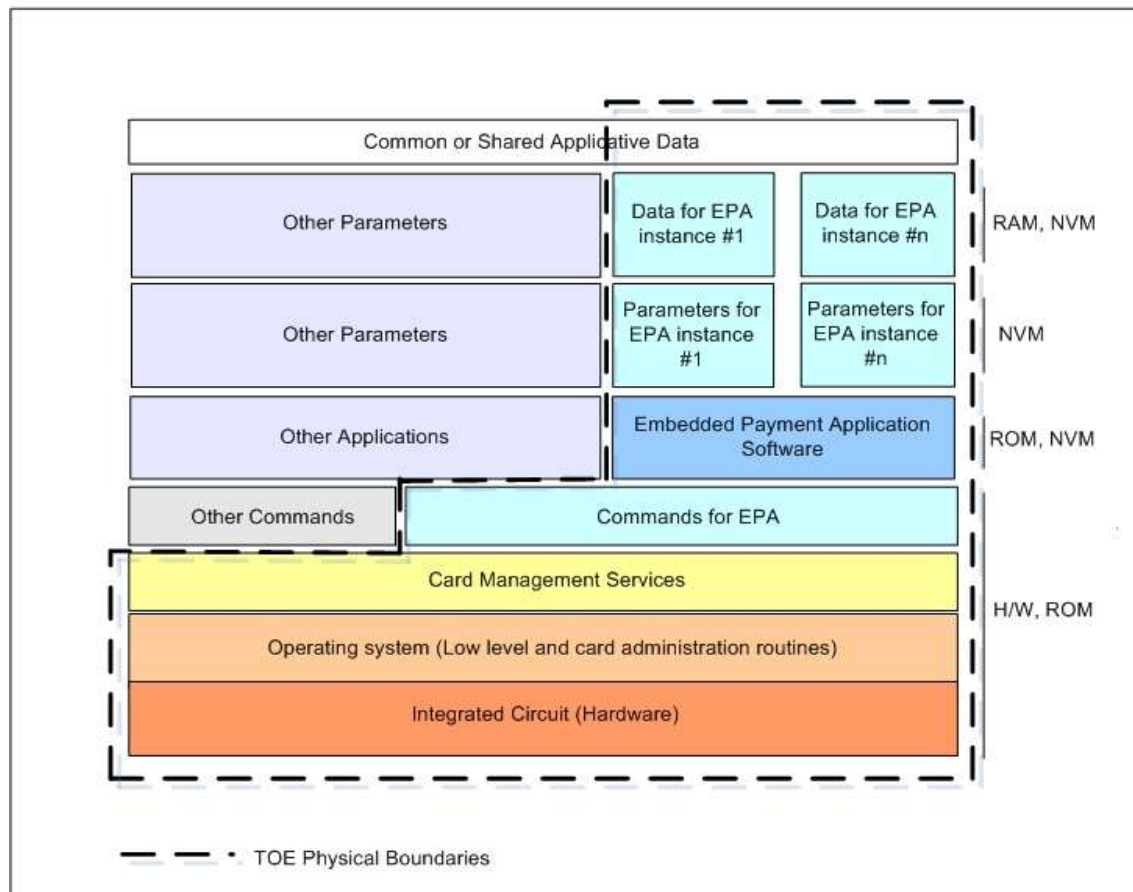


FIGURE 6: ARCHITECTURE AND COMPONENTS ON A TYPICAL MULTI-APPLICATION CHIP CARD

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 Payment 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 Customer. 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 – Biometric Data reference template (if present) when operated by the Chip Card
DP3	O.CRYPTO	The Payment Application keys, Payment Application reference PIN and Biometric Reference Template 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 Payment 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. <i>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.</i>

TABLE 7: 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 methodology⁷. Nevertheless, an EAL4 set of assurance requirements shall be augmented taking in to consideration the following criteria:

Type of assurance augmentation	Description
<i>Life Cycle Support _ Sufficiency of security measures.</i> 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, card initialiser, card personaliser...)
<i>Vulnerability Analysis Advanced Methodical Vulnerability Analysis.</i> ⁹	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 8: 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.

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)

⁹ 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 only be exchanged encrypted using a session key established for a Secure Channel through contactless transactions. If such a Secure Channel cannot be established, these relevant personal data 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 9: 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.

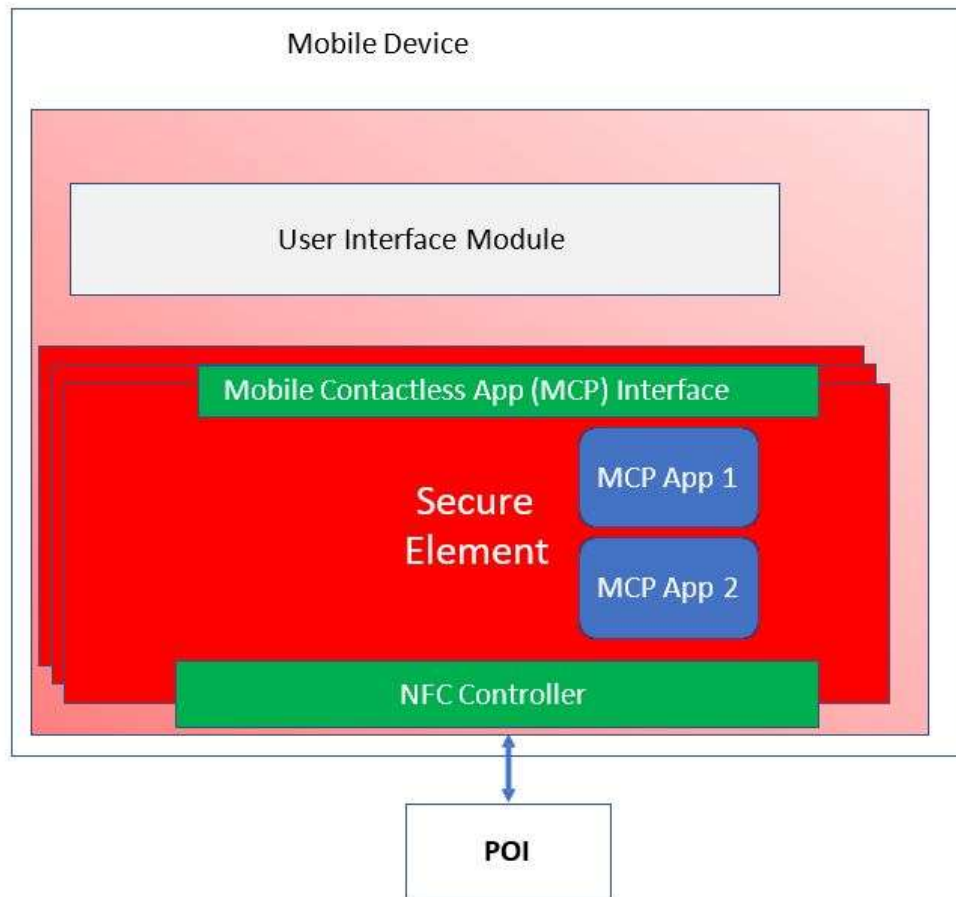


FIGURE 10: MCP APPLICATION RESIDING WITHIN A SECURE ELEMENT ON A MOBILE DEVICE

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.

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;
- On-line authentication and communication with the issuer;
- 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 any 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 Customer. 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 Customer. For CDCVM¹⁰ verification by the MCP Application, the following apply: – Systematic counting to identify verification failure. – Secure authentication invalidation when CDCVM is blocked. – Secure authentication validation when CDCVM comparison succeeds.
SUA3	O.ISSUER_AUTH	The MCP application shall ensure the authentication of the MCP issuer while processing any on-line transaction

¹⁰ This is only valid for not shared CDCVM.

		– 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 CDCVM; – MCP Reference CDCVM; – 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 CDCVM; – 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 11: 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 methodology¹¹. Nevertheless an EAL4+ set of assurance requirements shall be augmented regarding the following criteria:

Type of assurance augmentation	Description
<i>Life Cycle Support _ Sufficiency of security measures¹²</i>	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).
<i>Vulnerability Analysis _ Advanced Methodical Vulnerability Analysis¹³</i>	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 “ <i>highly resistant</i> ”.

TABLE 12: 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.

¹¹ 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.

¹² ALC_DVS.2 (Life Cycle Support up to level 2)

¹³ AVA_VAN.5 (vulnerability analysis up to level 5)

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 Mobile Applications (MA) for HCE-Based systems

This section describes the generic security requirements for an MA for Cloud-Based Payments (CBP) using Host Card Emulation (HCE). This version of the book focuses on the security relevant components of the MA on the mobile device.

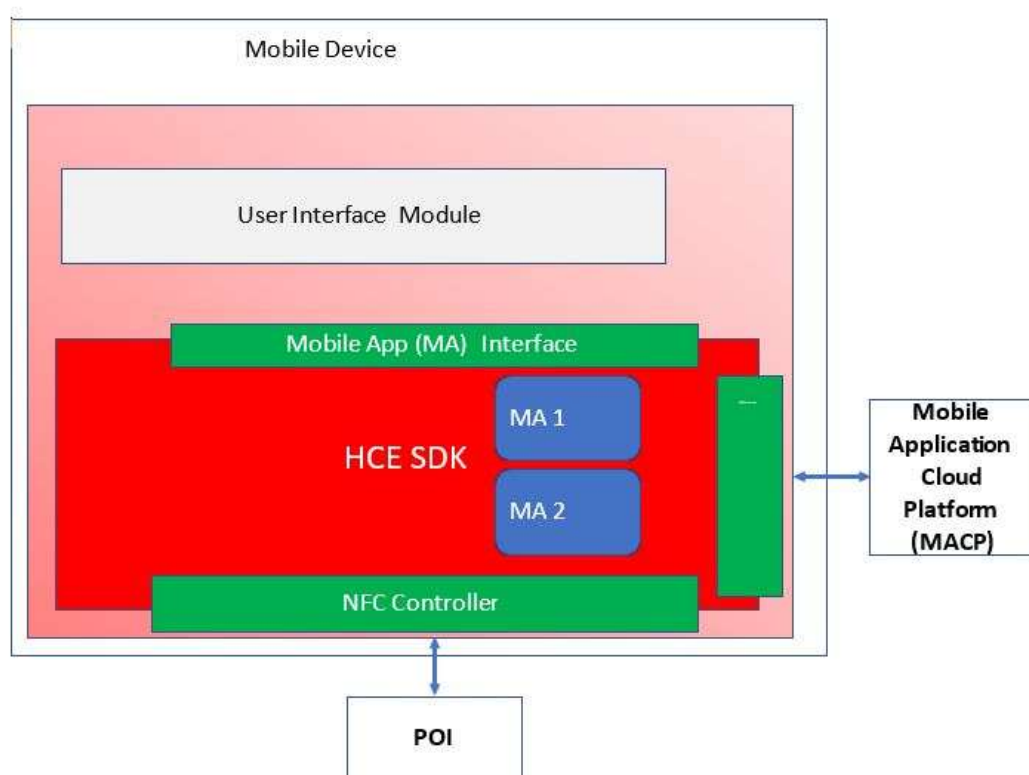


FIGURE 13: COMPONENTS FOR HCE-BASED MOBILE APPLICATION USED IN MCPs

Figure 13 identifies the following components for HCE-based Mobile Application:.

- The Mobile Application MA
- Software Development Kit SDK supporting one or several Mobile Apps, also called digital or software cards
- Interfaces to the POI and the MACP.

Depending on the HCE implementation components involved shall meet the security objectives.

3.6.3.1. Security Objectives

In the following table the security objectives are defined which shall be met by the HCE implementation on the mobile device (see [EMV SBMP]). The implementation is called MA in the table.

DP	DOCUMENTATION The assets of the MA shall be documented and monitored as the basis for the evaluation.	
DP1	O.USAGE	The MA must be provided with a security guidance document which describes its secure usage.
DP2	O.VERSIONS	The security guidance must identify all supported mobile devices, e.g. all versions of the supported platforms/OS.
DP3	O.ASSETS	The security guidance must list all security assets of the MA and the relevant protection mechanisms including the authenticity, integrity and confidentiality of the security relevant data.
AP	ASSET PROTECTION All defined MA assets shall be protected.	
AP1	O.PROTECTION	All defined MA assets must be protected according to the defined security objectives.
AP2	O.CONF_DATA	Confidential data shall be securely removed from the Consumer Device when no longer needed.
AP3	O.SENS_DATA	Sensitive data while stored, transmitted and processed shall be protected to meet its defined security requirements
AP4	O.EVAL	The security mechanisms used by the MA to protect the assets shall be evaluated, including underlying components, if the MCP Application security relies on the security of these components.
UA	USER AUTHENTICATION The MA and the MACP provide means for mutual authentication and enforces authentication of some users in order to prevent forgery and identity usurpation.	

UA1	O.ENTI	The MA shall have a list of defined entities and interfaces it is allowed to communicate with.
UA1	O.AUTH	The MA shall be protected from transaction forgery by being able to securely authenticate each of the entities listed under UA1.
SUA2	O.CH_VER	When required by the transaction flow, the MA shall verify the Customer. For CDCVM verification by the MA, the following apply: – Systematic counting to identify verification failure. – Secure authentication invalidation when CDCVM is blocked. – Secure authentication validation when CDCVM comparison succeeds.
UA3	O.MCPA_AUTH	The MA shall ensure the authentication of the MACP while processing any on-line transaction to trust the credentials provided to it.
UA4	O.MACP_AUTH	The MACP shall be able to authenticate the MA in order to be certain that credentials are not provided to an untrusted application.
UA5	O.DISCLO	The MA shall not disclose sensitive information when queried by an unauthorized entity.
MAP	MA PROTECTION The MA shall be protected against unauthorized modification and usage	
MAP1	O.INST_UPD	The MA shall be securely installed and updated.
MAP2	O.BIND	The MA shall be securely binded with the Consumer Device once the MCP Application is installed.
MAP3	O.MOD	The MA shall be protected against unauthorized modification and update.
MAP4	O.UPD	The MA shall have the ability to check and to force a secure update of its last version.
MAP5	O.ROLL_BACK	The MA shall not allow a Customer initiated roll back to an earlier version.
MAP6	O.INT	The integrity of the MA shall be verified at and/or during run time

MAP7	O.RUN	The MA shall not run on non-supporting platforms or devices.
MAP8	O.RUN_MODE	The MA shall not run in audit, debug or test mode.
MAP9	O.LOG	The MA shall not log sensitive data in plain mode.
MAP10	O.DEACT	The MA shall have the capability to be deactivated and to securely remove all Sensitive Payment Data, if the MA or the MACP detects any compromise.
MAP11	O.ISOLATION	The MA must protect itself within the execution environment of the mobile device according to state-of-the-art technology against any impact of other application.
CA	CUSTOMER AUTHENTICATION The MA provides suitable Customer Authentication and Verification	
CA1	O.VERIF	The MA shall provide or integrate an approved functionality to verify the Customer whenever applicable to the transaction.
CA2	O.CVM_INT	The MA shall ensure the integrity of the result of the CVM processing and shall ensure authenticity of the Customer intent/consent status that is presented to the MA.
REP	REPORTING and Attestation The MA shall provide reliable and secure reporting information to the MACP	
REP1	O.SEC	Information used for security reporting shall be protected from unauthorized disclosure and modification.
REP2	O.ATTACK	Any reporting communications shall not reveal information that would aid an attacker in obtaining sensitive information.
REP3	O.COMP	The MA shall have the capability to report to the MACP and the Customer if any compromises are detected.

REP4	O.ATT_Prot	If the MA relies on a server-side attestation reporting model, the attestation protocol must implement mechanisms for • Source and data integrity and • Timely reporting, to ensure that actions and responses delivered between the MCP Application and the server result from, and reflect, the current state of the system.
REP5	O.ATT_INT	If the MA relies on a server-side attestation reporting model, file integrity protection must be applied to configuration files, executables, and public keys/certificates used for security services on any back-end components of the attestation system.
REP6	O.ATT_RUN	Any reporting or attestation mechanisms must not interrupt payment transaction processing.
C	CRYPTOGRAPHIC KEYS, METHODS AND RANDOM NUMBERS Secure and industry accepted cryptographic protocols and methods shall be used.	
C1	O.Crypto	Industry standardized cryptographic algorithms, methods and protocols shall be used and securely configured.
C2	O.KEY_PROTECT	Cryptographic keys shall be protected as specified in the security objectives for the MA
C3	O.KEY_USE	Cryptographic keys shall be used only for their intended purpose.
C4	O.KEY_HIE	The cryptographic key hierarchy shall be defined.
C5	O.MANAGE	Arrangements shall be in place for the distribution, administration and regular change of keys. There shall be measures to limit the damage in case of keys or Customer component being compromised.
C6	O.RND	Random numbers shall have sufficient entropy for the required security level within the MA
DES	SECURE MA DESIGN and DEVELOPMENT	

	MA shall be developed at a secure site with configuration management, version control and secure coding practices.	
DES1	O.DEV	The MA shall be developed with proper configuration and source code control
DES2	O.SITE	The MA development site shall be properly protected from a physical, logical, and organizational security perspective.
DES3	O.PRACT	The MA shall be developed with secure design and security coding practices.

TABLE 14: SECURITY OBJECTIVES FOR MAs BASED ON HCE

3.6.3.2. Assurance level

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

For physical cards and hardware security modules like SEs or HSMs established processes and assurance levels are defined. For MCP transactions based on HCE technology no industry agreed processes nor an industry agreed assurance level currently exist. This is due to a different risk model linked to HCE based MCP transactions and due its innovative character. The only common denominator applies to the architecture of HCE based MCP transactions which implies that the security crucially relies on the effectiveness of the cloud and backend systems. The current assurance ratings do not take into account the issuer risk management in these systems but rely solely on the robustness of the payment device.

Therefore, this version of the book does not define an assurance level. The EPSG will however monitor the future development of this topic.

3.6.4. 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).

3.6.4.1. (M)RP related data types and locations

The figure below lists a number of categories¹⁴ 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.

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 Customer	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 15: 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.

¹⁴ This list is not meant to be exhaustive; other categories may involve components such as a mobile wallet.

- 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 3.6.4.2, 3.6.4.3 and 3.6.4.4.

3.6.4.2. Security Requirements for (M)RP Credentials Manually Entered by Customer

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 3.6.4.5 for more details.

3.6.4.3. 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.

3.6.4.3.1. *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 16: SECURITY REQUIREMENTS FOR SECURE ENVIRONMENTS AND (M)RP CREDENTIALS

3.6.4.3.2. Assurance Level

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

3.6.4.4. 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.

3.6.4.4.1. 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.

3.6.4.4.2. 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 Customer. 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 Customer while processing any transaction: • Authentication failure systematic counting; • Secure authentication invalidation when CVM (including personal / CDCVM) is blocked;

		Secure authentication validation when CVM (including personal / CDCVM) 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 ¹⁵ 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; - Application Reference CVM; - Application Transaction CVM.

¹⁵ In this case, the card should be interpreted as the secure environment where the application resides.

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 (e.g. counters, limits, etc.) 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 17: SECURITY REQUIREMENTS FOR SECURE ENVIRONMENTS AND (M)RP / AUTHENTICATION APPLICATIONS

3.6.4.4.3. 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 methodology¹⁶. Nevertheless an EAL4+ set of assurance requirements shall be augmented by using the following criteria:

¹⁶ 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
<i>Life Cycle Support _ Sufficiency of security measures¹⁷</i>	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).
<i>Vulnerability Analysis _ Advanced Methodical Vulnerability Analysis¹⁸.</i>	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 “ <i>highly resistant</i> ”.

FIGURE 18: 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.

3.6.4.5. 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 Customer 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.

The interfaces between the main components are represented in [Figure 19](#).

¹⁷ ALC_DVS.2 (Life Cycle Support up to level 2)

¹⁸ AVA_VAN.5 (vulnerability analysis up to level 5)

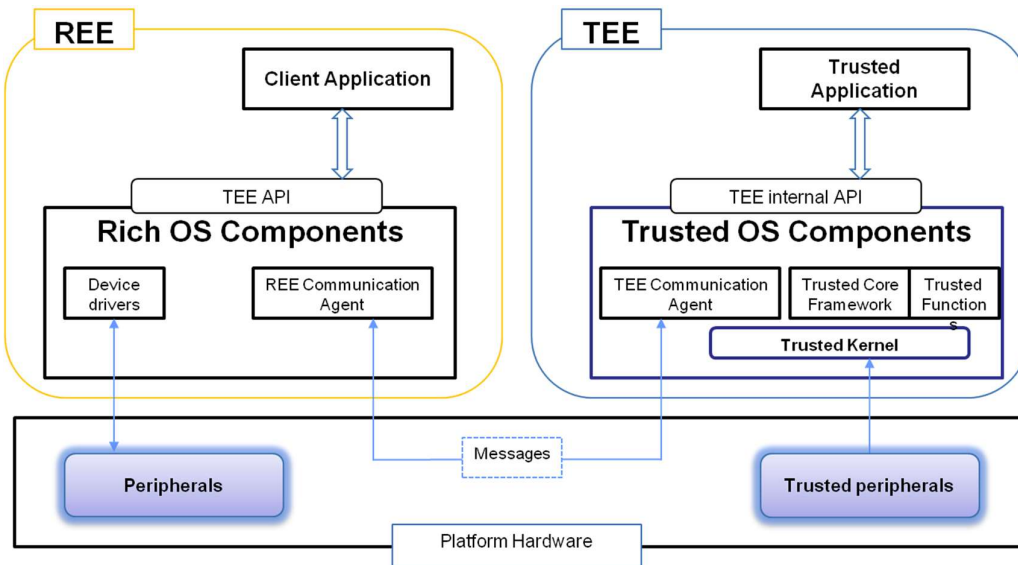


FIGURE 19: EXAMPLE OF A TEE MODEL

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) mode¹⁹).

3.6.4.5.1. 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.
-------	--

¹⁹ More information on the TUI is provided in [GP4].

DPTEE1	TEE.SECRECY	The TEE shall provide a safe area²⁰ (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, CDCVM ...
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

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

3.6.4.5.2. 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. Security Requirements for Consumer Device used for ICT Transactions

3.7.1. Security Objectives for ICT Transactions

Security objectives are intended to protect financial assets (e.g. payment account balance) from fraud, with a focus on the integrity of the Customer's bank account. They refer to an ideal highly desirable functioning for systems based on ICT from the security point of view. The proposed approach is that "we go on the right direction" to achieve these security objectives if we conform to the security requirements as set out in section 3.6.3.

O1: An ICT Transaction can only result in the credit of Payment Account of the beneficiary designated by the Customer and by an amount approved by the Customer except for any pre-agreed fee. This beneficiary can be either a legitimate enrolled payee or a fraudster.

O2: An ICT Transaction can only result in the debit of the Payment Account of the Customer associated with the ICT at the time the Customer was enrolled and by an amount approved by the Customer except for any pre-agreed fee. Otherwise the payment can be revoked.

O3: The ICT functionality ensures the same level of security even if the number of users escalates.

O4: The ICT functionality is designed to minimise the risk of misuse for financial crime purposes.

O5: The ICT functionality protects effectively sensitive ICT-related data even in case of a significant security incident.

O6: The level of risk for an ICT Transaction must be the same regardless the applied payment flow.

O7: The ICT functionality is resilient against known cyberattacks and even in case of compromise it is able to ensure a minimum level of Quality of Service.

O8: The level of the security controls to be executed (SCA, encryption) are proportional to the level of risk of an individual transaction. Nevertheless the selected level has to be in any case compliant with regulatory requirements.

O9: Ensure the confidentiality of sensitive data related to ICT Transactions even in case of a technical incident.

O10: The individual components and processing environment of the ICT may coexist with other Payment Instruments without any adverse impact in terms of additional security vulnerabilities for the ICT Transactions and/or other retail Payment Instruments available for selection.

O11: The ICT functionality is able to produce evidence enough for dispute resolution mechanisms. This evidence has to be accessible for a reasonable period of time after an ICT Transaction has been performed.

3.7.2. Common Security Requirements for ICT Transaction models and flows

Req S75: ICT shall implement security mechanisms that ensures the impossibility to replay a legitimate ICT Transaction order without detection.

Req S76: ICT shall implement security mechanisms that minimises the possibility for a Customer to deny successfully an ICT Transaction order if the Customer effectively authorised the payment.

Req S77: ICT shall implement security mechanisms that makes unfeasible in practice for an Acceptor to contest an amount credited in his account if the amount paid was authorised by a legitimate payer.

Req S78: An ICT Transaction shall only be executed if there is a proof of the explicit consent of the legitimate payer to pay a pre-agreed amount.

Req S79: An ICT Transaction shall only be initiated using an authentic ICT.

Req S80: Evidence data for an ICT Transaction shall be accessible for a reasonable period of time after the transaction was executed.

Req S81: Entity and data authentication mechanisms shall be implemented to protect the messages exchanged between the sender and the receiver at any interface in the ICT so that:

1. No other entity than the intended recipient will finally receive the ICT Transaction message sent by the sender.
2. A third party should not be able to modify the ICT Transaction messages exchanged without being detected.
3. The received messages should be generated by the sender in such a way that the intended recipient can verify that the messages are authentic and fresh.
4. If the sender receives an acknowledge message from the recipient, then the verification of this message should lead the sender to the conclusion that the previous ICT Transaction message was successfully received by the intended recipient.

When the ICT Transaction is intermediated by a PISP in an Open Banking model:

Req S82: The PISP shall be authenticated by the ASPSP through the PSD2 API against a Certificate issued by a recognised Certification Authority.

Req S83: The ASPSP and the PISP shall exchange transaction data through the PSD2 API using a Secure Channel established using a recognised Security Protocol (e.g. TLS v3.0).

Req S84: The ASPSP (Issuer) shall be responsible for compliance with SCA, as defined in point (30) of Article 4 of PSD2.

Req S85: The application of SCA can be delegated to the PISPs or other third parties having a contract with ASPSP, provided that the ASPSP complies with the applicable legal requirements as defined in point (30) of Article 4 of PSD2.

Req S86: When the PSD2 API can be accessed directly by the ASPSP customers as well, mechanisms shall be implemented to differentiate between a customer, a PISP and an unauthorised third-party request.

When the ICT Transaction is operated by a Scheme

Req S87: An ICT Scheme shall establish a documented security certification framework including the responsibilities for their effective implementation by members of the scheme.

3.7.3. Security Requirements for ICT Transaction initiated by NFC/Contactless

Req S88: If the ICT Transaction is initiated locally using an NFC interface to communicate with a Physical POI, requirements for using SCA similar to Card Transactions apply. Meaning:

1. The payment shall be initiated by an authentic ICT.
2. The payment shall be initiated under exclusive control of the Customer the payment instrument was issued to.

3.7.4. Security Requirements for ICT Transactions in an e-Commerce context

3.7.4.1. Merchant-presented QR Code for Remote Transactions

At a minimum, the security requirements applicable to Merchant-presented QR Codes shall also apply in this context. The Merchant-presented QR Code shall be encrypted to ensure authentication, integrity, and confidentiality. The ICT shall support SCA for Remote Transactions in accordance with PSD2. For further details, refer to Sections 3.5.4.1.1 and 3.5.4.1.3.

3.7.4.2. Other scenarios

When QR Codes are not used, then the security requirements for e- and m-Commerce, as defined in section 3.5.2, shall apply.

3.8. 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.

3.8.1. Physical POI (for local transactions)

3.8.1.1. Introduction

This section defines the applicable security requirements for all POI devices being custom made or commissioned specifically for the purpose of card payments. These POI devices in particular rely on hardware/firmware protection for defined security assets like the PIN.

These requirements are derived from PCI PTS and Common.SECC, with 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, Common.SECC, PCI PTS with ECSG+ or Common.SECC 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. UK Finance and girocard follow Common.SECC, global Schemes follow PCI PTS. Other Schemes may require PCI or Common.SECC 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
- COMMUNICATION AND INTERFACES - requirements for POI's connected to open networks
- LIFE CYCLE - 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 [Figure 18](#).

3.8.1.2. Life Cycle

Life Cycle covers how the POI device is produced, controlled, transported, stored, and used throughout its life. If the device is not properly managed, unauthorized modifications might be made to its physical or logical security characteristics.

Where Keys are loaded in order to protect the POI device from Initial Manufacture to Initial Key Loading and where Schemes consider this activity to be the “initial key load” then clear terminology must exist, defined by the Schemes, to enable easy identification of the Life Cycle to meet the requirements of Section F.

3.8.1.3. Requirements

Evaluation Module 1: Core Requirements

Note: in the following requirements, the device under evaluation is referred as the “POI.”

Section A - Core Physical Security Requirements

Number	Description of the requirement
A1	The POI <i>shall</i> use tamper-detection and response mechanisms that cause it to become immediately inoperable and result in the automatic and immediate erasure of any sensitive data that may be stored in the POI, such that it becomes infeasible to recover the sensitive data. These mechanisms protect against physical penetration of the device by means of (but not limited to) drills, lasers, chemical solvents, opening covers, splitting the casing (seams), and using ventilation openings.
A2	There is no demonstrable way to disable or defeat the tamper mechanism/s and insert a sensitive key-press-disclosing bug. Keypads used for PIN entry require an attack potential of at least 26 per device for identification and initial exploitation, with a minimum of 13 for initial exploitation, exclusive of the integrated circuit (IC) card reader. Keypads used for manual PAN entry, but not PIN entry e.g., a non-PED require an attack potential of at least 16 per POI for identification, with a minimum of 8 points for exploitation
A3	The security of the POI <i>shall</i> not be compromised by altering: ▪ Environmental conditions ▪ Operational conditions
A4	Sensitive functions or data are only used in the protected area(s) of the device. Sensitive data, and functions dealing with sensitive data, are protected from unauthorized modification without requiring an attack potential of at least 26 for identification and initial exploitation, with a minimum of 13 for initial exploitation, exclusive of the IC card reader or the biometric reader, for identification and initial exploitation.
A5	There is no practical way to determine any entered and internally-transmitted PIN digit by monitoring sound, electro-magnetic emissions, power consumption, or any other external characteristic available for monitoring—even with the cooperation of the device operator or

	sales clerk—without requiring an attack potential of at least 26 for identification and initial exploitation, with a minimum of 13 for initial exploitation.
A6	Determination of any PIN-security-related secret or private cryptographic keys resident in the device by penetration of the device requires an attack potential of at least 35 for identification and initial exploitation, with a minimum of 15 for initial exploitation. For an SRED-enabled device, determination of any account-data-security-related secret or private cryptographic keys resident in the device by penetration of the device requires an attack potential of at least 26 points for identification and initial exploitation, with a minimum of 13 for initial exploitation.
A7	Determination of any PIN security-related secret or private cryptographic keys resident in the device by monitoring of emanations from the device (including power fluctuations) requires an attack potential of at least 35 for identification and initial exploitation, with a minimum of 15 for initial exploitation. For an SRED-enabled device, determination of any account-data-security-related secret or private cryptographic keys resident in the device by monitoring of emanations from the device requires an attack potential of at least 26 points for identification and initial exploitation, with a minimum of 13 for initial exploitation.
A8	The unauthorized alteration of prompts for non-PIN data entry into the PIN entry keypad such that PINs are compromised—i.e., by prompting for the PIN entry when the output is not encrypted—cannot occur without requiring an attack potential of at least 18 per device for identification and initial exploitation, with a minimum of 9 for initial exploitation.
A9	The device provides a means to deter the visual observation of PIN values as they are being entered by the cardholder.
A9.ECSG+	The POI <i>should</i> have a privacy shield. However if a privacy shield is in place then it <i>shall</i> be in accordance with the EPC Guidelines on Privacy Shields [EPC PS].
A10	The device <i>shall</i> protect all account data upon entry for magnetic-stripe or contactless data, and there is no method of accessing the cleartext account data to determine or modify the data (using methods described in Requirement A2) without defeating the security of the device. Defeating or circumventing the security mechanism requires an attack potential of at least 16 for identification and initial exploitation, with a minimum of 8 for initial exploitation.
A11	All account data is either encrypted immediately upon entry or entered in clear text into a secure POI and processed within the secure controller of the device.

A12	The logical and physical integration of an approved secure card reader into a PIN entry POI <i>does</i> not create new attack paths to the account data. The account data is protected from the input component to the secure controller of the POI—i.e., it is not possible to insert a bug that would disclose sensitive data
A13	It is neither feasible to penetrate the ICC reader to make any additions, substitutions, or modifications to either the ICC reader’s hardware or software, in order to determine or modify any sensitive data, without requiring an attack potential of at least 20 for identification and initial exploitation, with a minimum of 10 for exploitation, nor is it possible for both an IC card and any other foreign object to reside within the card insertion slot. SCRP’s <i>shall</i> require an attack potential of at least 26 for identification and initial exploitation, with a minimum of 13 for exploitation
A14	The opening for the insertion of the IC card is in full view of the Cardholder during card insertion so that any untoward obstructions or suspicious objects at the opening are detectable. The ICC reader is constructed so that wires running out of the slot of the IC reader to a recorder or a transmitter (an external bug) can be observed by the Cardholder.
A15	It is impractical to make any additions, substitutions, or modifications to either the biometric reader’s hardware or software in order to determine or modify any sensitive data. “Impractical” is defined as requiring an attack potential of at least 20 for identification and initial exploitation, with a minimum of 10 for initial exploitation.

Section B - Core Logical Security Requirements

Note: All Firmware must be regularly tested and validated by a Test Laboratory to ensure on-going Security.

Number	Description of the requirement
B1	The device <i>shall</i> perform a self-test, which includes integrity and authenticity tests upon start-up and at least once per day to check whether the device is in a compromised state. In the event of a failure, the device and its functionality fail in a secure manner. The device must reinitialize memory at least every 24 hours.
B2	The device <i>shall</i> support firmware updates. The device <i>shall</i> cryptographically authenticate the firmware and if the authenticity is not confirmed, the firmware update is rejected and deleted. The update mechanism ensures security i.e., integrity, mutual authentication, and protection against replay by using an appropriate and declared security protocol when using a network connection
B2.1	The firmware <i>shall</i> enforce the authentication of payment applications loaded onto the terminal security processor and must support authentication of applications loaded onto the application processors for non-third-party applications, consistent with Requirement B2.
B2.2	The vendor <i>shall</i> provide a defined and documented process containing specific details on how any signing mechanisms <i>shall</i> be implemented. This <i>shall</i> include any “turnkey” systems required for compliance with the management of display prompts, or any mechanisms used for authenticating any application code. This <i>shall</i> ensure: ▪ The signing process is performed under dual control. ▪ All executable files are signed. ▪ Software is only signed using a secure cryptographic POI (e.g., smartcard) provided by the terminal vendor.
B2.3	Third-party applications must not be able to be loaded or executed in execution environments that have access to cleartext account data. Third-party applications must be signed.
B3	The device neither displays nor otherwise provides an indication of the value of the entered PIN digits. Any array related to PIN entry displays only non-significant symbols—e.g., asterisks. 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.

B4²¹	Sensitive data shall not be retained any longer, or used more often, than strictly necessary. Online PINs are encrypted within the device immediately after PIN entry is complete and has been signified as such by the cardholder—e.g., via pressing the Enter button. The device must automatically clear its internal buffers of full track data (or chip equivalent), and sensitive authentication data is cleared when either: ▪ The transaction is completed, or ▪ The device has timed out waiting for the response from the cardholder or merchant.
B5	Access to sensitive services requires authentication. Sensitive services provide access to the underlying sensitive functions. Sensitive functions are those functions that process sensitive data such as cryptographic keys, PINs, and passwords/authentication codes. Entering or exiting sensitive services <i>shall</i> not reveal or otherwise affect sensitive data.
B6	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.
B7	If random numbers are generated by the POI in connection with security over sensitive data, the random number generator <i>shall</i> be assessed by the Test Laboratory to ensure it is generating numbers sufficiently unpredictable.
B8	The POI <i>shall</i> have characteristics that prevent or significantly deter the use of the POI for exhaustive PIN determination.
B9	The key-management techniques implemented in the POI <i>shall</i> conform to ISO 11568 and/or ANSI X9.24. Key-management techniques <i>shall</i> support the ANSI X9. TR-31 key derivation methodology or an equivalent methodology. POIs <i>shall</i> support key blocks as specified by ISO 20038 and/or the ANSI TR-31 key-derivation method. Equivalent methods may be supported where required by legal or regulatory requirements. When equivalent methods are used, these methods <i>shall</i> be subject to an independent expert review and validated by the Test Laboratory.

²¹ Requirement B6 is not intended to prevent PIN change for a proprietary Card scheme.

B10	All account data <i>shall</i> be encrypted using only ANSI X9 or ISO approved encryption algorithms (e.g., AES, TDES) and should use ANSI X9 or ISO-approved modes of operation.
B11	The PIN-encryption technique implemented in the POI <i>shall</i> be a technique included in [ISO 9564].
B12	It <i>shall</i> not be possible to encrypt or decrypt any random data using a key stored within the POI. The encryption or decryption of data <i>shall</i> only be possible using dedicated keys. The POI <i>shall</i> enforce that all dedicated keys have different values.
B13	There <i>shall</i> be no mechanism in the POI that would allow the outputting of a private or secret clear-text key or cleartext PIN, the encryption of a key or PIN under a key that might itself be disclosed, or the transfer of a cleartext key from a component of high security into a component of lesser security.
B14	The entry of any other transaction data <i>shall</i> be separate from the PIN-entry process, avoiding the accidental display of a cardholder PIN on the device display. If other data and the PIN are entered on the same keypad, the other data entry and the PIN entry <i>shall</i> be clearly separate operations.
Note: If the POI has a keypad that can be used to enter non-PIN data, the POI <i>shall</i> meet at least one of the following: A8, B15, or C2.4. • A8 applies to any components or paths containing plaintext display signals between the cryptographic processor and display unit. • B15 applies to POIs that allow for updates of prompts or use cryptography to communicate with a display, whether performed by the vendor or the acquirer. • C2.4 is appropriate for unattended POIs that do not meet any of the aforementioned.	
B15	Cryptographic mechanisms must exist to ensure the authenticity and proper use of the display, and that modification of the prompts or improper use of the device display is prevented. All prompts for non-PIN data entry <i>shall</i> be under the control of the cryptographic unit of the POI. 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 <i>shall</i> 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.
B16	If the POI supports multiple applications, it <i>shall</i> enforce the separation between applications. It <i>shall</i> not be possible that one application interferes with or tampers with another application or the OS of the device including, but not limited to, modifying data objects belonging to another application or the OS.
B16.1	If the POI supports software with lesser security requirements or that is not developed by the vendor e.g., applications, it <i>shall</i> enforce segregation at least between different software security domains.
B16.2	The vendor <i>shall</i> provide clear security guidance consistent with D1 and B4 to all application developers to ensure: ▪ That it <i>shall</i> not be possible for applications to be influenced by logical anomalies which could result in clear-text data being outputted whilst the terminal is in encrypting mode. ▪ That account data <i>shall</i> not be retained any longer, or used more often, than strictly necessary. ▪ That SRED functions, where provided, are correctly implemented.
B17	The operating system of the POI <i>shall</i> contain only the software necessary for the intended operation. The operating system <i>shall</i> be configured securely and run with least privilege.
B18	If the POI can hold multiple PIN-encryption keys and if the key to be used to encrypt the PIN can be externally selected, the POI shall prohibit unauthorized key replacement and key misuse.
B19	The vendor <i>shall</i> provide adequate documented security guidance for the integration of any secure component into the POI.
B20	A user-available security policy from the vendor addresses the proper use of the POI in a secure fashion, including information on key-management responsibilities, administrative responsibilities, device functionality, identification, and environmental requirements. The security policy must define the roles supported by the POI and indicate the services available for each role in a deterministic tabular format. The POI is capable of performing only its designed functions—i.e., there is no hidden functionality. The only approved functions performed by the POI are those allowed by the policy.
B21	PIN protection during transmission between the POI encrypting the PIN and the ICC reader (at least two <i>shall</i> apply):

	If the POI encrypting the PIN and the ICC reader are not integrated into the same secure module, and the Cardholder verification method is determined to be: ▪ An enciphered PIN, the PIN block <i>shall</i> be enciphered between the POI encrypting the PIN and the ICC reader using either an authenticated encipherment key of the IC card, or in accordance with ISO 9564. ▪ A plaintext PIN, the PIN block <i>shall</i> be enciphered from the POI encrypting the PIN to the ICC reader (the ICC reader will then decipher the PIN for transmission in plaintext to the IC card) in accordance with ISO 9564. If the POI encrypting the PIN and the ICC reader are integrated into the same secure module, and the Cardholder verification method is determined to be: ▪ An enciphered PIN, the PIN block <i>shall</i> be enciphered using an authenticated encipherment key of the IC card. ▪ A plaintext PIN, then encipherment is not required if the PIN block is transmitted wholly through a protected environment (as defined in ISO 9564). If the plaintext PIN is transmitted to the ICC reader through an unprotected environment, the PIN block <i>shall</i> be enciphered in accordance with ISO 9564.
Secure Read and Exchange of Data (SRED)	
B22	If the POI can be accessed remotely for the purposes of administration, all access attempts must be cryptographically authenticated. If the authenticity of the access request cannot be confirmed, the access request is denied.
B23	When operating in encrypting mode, there is 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 requires explicit authentication. Cleartext account data must never be available to execution environments that are able to execute third-party applications, even through the use of whitelists.
B23.1	When operating in encrypting mode, the secure processor can only release clear-text account data to authenticated applications executing within the POI. Devices supporting third-party applications must not pass cleartext account data to the execution environment executing the third-party application, even through the use of whitelists.
B24	If the POI is capable of generating surrogate PAN values to be outputted outside of the POI, it is not possible to determine the original PAN knowing only the surrogate value. Where a hash function is used to generate surrogate PAN values: ▪ Input to the hash function must use a salt with minimum length of 64 bits. ▪ The salt is kept secret and appropriately protected.

	▪ Disclosure of the salt cannot occur without requiring an attack potential of at least 16 per POI for identification and initial exploitation with a minimum of 8 for exploitation, as defined in Appendix B.
B25	The POI has characteristics that prevent or significantly deter the use of the POI for exhaustive PAN determination.
B26	Secure enablement tokens are required from the monitoring system for operation of the SCRP to accept and/or process payments.
Evaluation Module 2: POI Terminal integration	
Section C – Integration of PIN Entry Functions	

Number	Description of the requirement
C1.1	The logical and physical integration of an approved secure component (or components) into a PIN entry POI terminal <i>shall</i> not impact the overall PIN protection level.
C1.2	The PIN pad (PIN entry area) and the surrounding area <i>shall</i> be designed and engineered in such a way that the complete POI does not facilitate the fraudulent placement of an overlay over the PIN pad. An overlay attack <i>shall</i> require an attack potential of at least 18 for identification and initial exploitation, with a minimum of 9 for exploitation
Integration into a POI terminal	
C2.1	The logical and physical integration of an approved secure component into a PIN entry POI terminal <i>shall</i> not create new attack paths to the PIN.
C2.2	The PIN entry POI terminal is equipped with mechanisms to prevent attacks aiming at retaining and stealing the payment card (e.g., Lebanese Loop attack).
C2.3	There is a clear logical and/or physical segregation 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 POI must meet at least one of the following: A8, B15, or C2.4. ▪ A8 applies to any components or paths containing plaintext display signals between the cryptographic processor and display unit. ▪ B15 applies to POIs that allow for updates of prompts or use cryptography to communicate with a display, whether performed by the vendor or the acquirer. ▪ C2.4 is appropriate for unattended POIs that do not meet any of the aforementioned. If numerical key input is enabled, the display prompts should be controlled by the cryptographic processor

C2.4	The POI (application) must enforce the correspondence between the display messages visible to the Cardholder and the operating state (i.e., secure or non-secure mode) of the PIN entry device, e.g., by using cryptographic authentication. If commands impacting the correspondence between the display messages and the operating state of the PIN entry device are received from an external device (e.g., a store controller), the commands enabling data entry must be authenticated. The alteration of the correspondence between the display messages visible to the Cardholder and the operating state of the PIN entry device cannot occur without requiring an attack potential of at least 18 per POI for identification and initial exploitation with a minimum of 9 for exploitation
C2.5	The PIN-accepting POI terminal must be equipped with only one payment card PIN-acceptance interface, e.g., a keyboard. If another interface is present which can be used as a keyboard, a mechanism must exist to prevent its use for PIN entry—e.g., it must not have numeric keys, or it is not possible to use it otherwise for numeric entry, or it is controlled in a manner consistent with B15
Evaluation Module 3: Communications and Interfaces	
Section D – Communications and Interfaces	
Number	Description of the requirement
D1	All protocols and all interfaces available on the POI are accurately identified by the POI vendor. The vendor has a complete and comprehensive understanding of how all protocols and interfaces present on the POI interact. All public domain protocols and interfaces available on the POI are clearly identified in the Open Protocols – Protocol Declaration Form
D2	The POI's functionality <i>shall</i> not be influenced by logical anomalies such as (but not limited to) unexpected command sequences, unknown commands, commands in a wrong POI mode, and supplying wrong parameters or data, which could result in the POI outputting the clear-text PIN or other sensitive data
D3	The POI has security guidance that describes how protocols and services <i>shall</i> be used for each interface that is accessible by the POI applications.
D4	The POI has guidance that describes the default configuration for each protocol and services for each interface that is available on the POI. Each interface and protocol on the POI <i>should</i> be configured with secure default settings.

D5	The POI has guidance for key management describing how keys and certificates <i>shall</i> be used. a) The key-management guidance is at the disposal of internal users and/or of application developers, system integrators, and end-users of the POI. b) Key-management security guidance describes the properties of all keys and certificates that can be used by the POI. c) Key-management security guidance describes the responsibilities of the POI vendor, application developers, system integrators, and end-users of the POI. d) Key-management security guidance ensures secure use of keys and certificates, including certificate status (e.g., revoked), secure download, and roll-over of keys.
D6	The POI has all the security protocols that are available on the POI clearly identified. The POI vendor provides documentation that describes the implementation and use of the security protocols that are available on the POI.
D7	The POI is able to provide confidentiality of data sent over a network connection. a) Encryption mechanism utilizes key sizes appropriate for the algorithm(s) in question. b) Encryption is provided by using keys that are established in a secure manner using appropriate key-management procedures, such as those listed in NIST SP800-21, Guidelines for Implementing Cryptography in the Federal Government and ISO 11568 Banking – Key Management (Retail).
D8	The POI is able to provide the integrity of data that is sent over a network connection. a) Integrity is provided by a MAC as defined in ISO 16609, or by a digital signature. b) Hashing can be provided by at least one of the following algorithms: SHA-224, SHA-256, SHA-384, and SHA-512. c) Examples of appropriate algorithms and minimum key sizes are stated within [EPC Crypto].
D9	The POI uses a declared security protocol to authenticate the server. a) Server authentication utilizes key sizes appropriate for the algorithm(s) in question. b) Hashing can be provided by at least one of the following algorithms: SHA-224, SHA-256, SHA-384, and SHA-512. c) The POI is able to verify the validity of the public keys it receives. d) The POI is able to verify the authenticity of the public keys it receives. e) The POI's trusted root certificate store <i>shall</i> contain only public key certificates from trusted CAs or else self-signed certificates verified by the acquirer.
D10	The POI is able to detect replay of messages and enables the secure handling of the exceptions.

D11	The POI implements session management. a) The POI keeps track of all connections and restricts the number of sessions that can remain active on the POI to the minimum necessary number. b) The POI sets time limits for sessions and ensures that sessions are not left open for longer than necessary
D12	Bluetooth communications <i>shall</i> be secured against eavesdropping and man-in-the-middle attacks.
D13	Wi-Fi communications <i>shall</i> be securely configured. Protocols with known vulnerabilities must be disabled.
D14	Wireless communication interfaces which do not have specific security requirements, or have not met those requirements as listed, must be physically and cryptographically isolated. Note: Where the applicable security Requirements D12 and/or D13 for Bluetooth or Wi-Fi are not met, D14 must be used.

Evaluation Module 4: Life Cycle Security Requirements

The POI manufacturer confirms the compliance to following requirements. The Test Laboratories will validate compliance via documentation reviews, and by means of evidence that procedures are properly implemented and used.

Note: in the following requirements, the device under evaluation is referred as the “POI.”

Section E – During Manufacturing

Number	Description of the requirement
E0 ECSG+	Section E requirements <i>shall</i> be checked by the Test Laboratory. This includes a periodic site visit regarding critical steps in the manufacturing process (excluding the key loading).
E1	Change-control procedures are in place so that any intended change to the physical or functional capabilities of the POI causes a recertification of the POI under the impacted security requirements of this document. Re-certification is not required for changes that purely rectify errors and faults in software in order to make it function as intended and do not otherwise remove, modify, or add functionality that impacts security. Approval of delta submissions is contingent on evidence of the ongoing change control and vulnerability management process.
E2	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.
E3	The certified firmware is protected and stored in such a manner as to preclude unauthorized modification during its entire manufacturing life cycle—e.g., by using dual control or standardized cryptographic authentication procedures.
E4	The POI is assembled in a manner that the hardware components used in the manufacturing process are those hardware components evaluated by the Test Laboratory, and that unauthorized substitutions have not been made.
E5	Production software (e.g., firmware) that is loaded to POI’s at the time of manufacture is transported, stored, and used under the principle of dual control, preventing unauthorized modifications and/or substitutions

E6	Subsequent to production but prior to shipment from the manufacturer's or reseller's facility, the POI and any of its components are stored in a protected, access-controlled area or sealed within tamper-evident packaging to prevent undetected unauthorized access to the POI or its components.
E7	The POI <i>shall</i> be authenticated at the key-loading facility or the facility of initial deployment by means of secret information placed in the POI during manufacturing. This secret information is unique to each POI, unknown and unpredictable to any person, and installed in the POI. Secret information is installed under dual control to ensure that it is not disclosed during installation, or the POI may use an authenticated public-key method. Authentication by secret information is mandatory
E8	Security measures are taken during the development and maintenance of POI security-related components. The manufacturer must maintain development-security documentation describing all the physical, procedural, personnel, and other security measures that are necessary to protect the integrity of the design and implementation of the POI security-related components in their development environment. The development-security documentation <i>shall</i> provide evidence that these security measures are followed during the development and maintenance of the POI security-related components. The evidence <i>shall</i> justify that the security measures provide the necessary level of protection to maintain the integrity of the POI security-related components.
E9	Controls exist over the repair process at all POI vendor-authorized repair facilities, including the resetting of tamper mechanisms and the inspection/testing process subsequent to repair, to ensure that the POI has not been subject to unauthorized modification.
E10	The POI vendor has internal policies and procedures that ensure the vendor maintains an effective process for detecting vulnerabilities that may exist within its POI. This process is expected to be robust enough to include all interfaces defined in Requirement D1 and to detect vulnerabilities which may have not been publicly known during the last vulnerability assessment.
E11	The POI has undergone a vulnerability assessment to ensure that the protocols and interfaces list in D1 do not contain exploitable vulnerabilities. a) The vulnerability assessment is supported by a documented analysis describing the security of the protocols and interfaces. b) The vulnerability assessment is supported by a vulnerability survey of information available in the public domain. c) The vulnerability assessment is supported by testing.
E12	The POI vendor has vulnerability disclosure measures in place for the POI. a) The vulnerability-disclosure measures are documented.

	b) The vulnerability-disclosure measures ensure a timely distribution of information about newly found vulnerabilities. This information includes identification, description, and assessment of the vulnerabilities. c) The vulnerability-disclosure measures ensure a timely distribution of mitigation measures
Section F - Between Manufacturer and Facility of Initial Key Loading or Facility of Initial Deployment	
Approved Test Laboratories will validate this information via documentation reviews and by means of evidence that procedures are properly implemented and used and this information <i>shall</i> be included in the evaluation report.	
Number	Description of the requirement
F0 ECSG+	Section F requirements <i>shall</i> be checked by the Test Laboratory. This includes a periodic site visit regarding critical steps in the manufacturing process.

F1	The POI <i>shall</i> be protected from unauthorized modification with tamper-detection security features, and customers <i>shall</i> be provided with documentation (both shipped with the product and available securely online) that provides instruction on validating the authenticity and integrity of the POI. Where this is not possible, the POI is shipped from the manufacturer’s facility to the initial key-loading facility or to the facility of initial deployment and stored en-route under auditable controls that can account for the location of every POI at every point in time—such as the use of serialized tamper-evident packing for all POIs with no tamper detection, in conjunction with thorough physical inspection (possibly including sampling of HW internals) upon reception. Where multiple parties are involved in organizing the shipping, it is the responsibility of each party to ensure that the shipping and storage they are managing is compliant with this requirement. In the absence of defined agreements stipulating otherwise, the POI vendor remains responsible.
F2	Procedures are 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 will 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. In the absence of defined agreements stipulating otherwise, the POI vendor remains responsible.
F3	While in transit from the manufacturer’s facility to the initial key loading facility, the POI is shipped and stored containing a secret that: ▪ Is immediately and automatically erased if any physical or functional alteration to the POI is attempted, and ▪ Can be verified by the initial key-loading facility but cannot feasibly be determined by unauthorized personnel.
F4	The POI’s development-security documentation <i>shall</i> provide means to the initial key-loading facility to assure the authenticity of the TOE’s security-relevant components.
F5	If the manufacturer is in charge of initial key loading, the manufacturer <i>shall</i> verify the authenticity of the POI security-related components.
F6	If the manufacturer is not in charge of initial key loading, the manufacturer <i>shall</i> provide the means to the initial key-loading facility to assure the verification of the authenticity of the POI security-related components.
F7	Each POI <i>shall</i> have a unique visible identifier—i.e., model name and hardware version—affixed to it. This information <i>shall</i> also be retrievable by a query.

F8	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
F9 ECSG+	In order to ensure ongoing key loading facility operational security and conformity, key loading audits <i>shall</i> be conducted. Those entities carrying out such audits <i>shall</i> be suitably qualified to certify conformity with the requirements of secure key loading operations and key management. The audit <i>shall</i> 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 <i>shall</i> be allowed to communicate their report to the relevant bodies.
Section G- Requirements for the POI payment application Note: All section G are ECSG+ requirements	
G1 ECSG+	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) Establishing and using the Secure Channel, if supported by both POI, and Card b) Confirmation of the amount c) PIN entry d) Prompting of the transaction result e) Verification of the online and offline result f) Maintaining security related transaction data Note: This ECSG+ requirement is covered within the PCI PTS standard by multiple requirements including requirements A4, A7, B2, B14 and B15. This ECSG+ is retained for ease of adoption by other schemes.
G1.1 ECSG+	The secure process flow <i>shall</i> be controlled by the POI in order that it cannot be bypassed by logical means. POI and payment application <i>shall</i> control the secure process flow.
G1.2 ECSG+	Online and offline process order <i>shall</i> 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 <i>shall</i> be present.
G1.3 ECSG+	A state machine <i>shall</i> 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 <i>shall</i> react in an adequate way. • Transport layers are provided by the firmware. • The application layer is part of the payment application.
G2 ECSG+	Security functions of the firmware implementing authentication and integrity for the online messages, including transaction data, <i>shall</i> 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 <i>shall</i> be part of the payment application.

	The usage of cryptographic signature/ authentication code key management and signature/ authentication code key <i>shall</i> be part of the firmware. The calls for the calculation and verification of signatures/ authentication codes of online messages (requests, responses) <i>shall</i> be part of the payment application.
G3 ECSG+	Any secure process flow <i>shall</i> only use random numbers generated by the random number generator which have been assessed and verified in the firmware evaluation. The random number generator <i>shall</i> be provided by the firmware. Both the payment application as well as the EMV kernel <i>shall</i> use the (assessed) random number generator provided by the firmware.
G4 ECSG+	The EMV related part of the secure process <i>shall</i> provide for authenticity and integrity of the code and relevant security data, e.g. keys and management data.
G5 ECSG+	It <i>shall</i> not be possible to bypass the display of the transaction amount by logical means. The Customer <i>shall</i> not be deceived about the secure process flow showing him another amount than the amount being authorised. This <i>shall</i> also hold for the key the Customer is pressing to confirm or to cancel a transaction. The execution of functions depending on the user authentication <i>shall</i> only be allowed, e.g. the authorisation of a transaction, if the user authentication has been performed successfully.

3.8.1.4. 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 audible 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.
Open Protocol	The protocols in the Internet stack are open so that the device can follow the protocol to join the global network, e.g. Bluetooth, Wifi, TLS. These must be validated against the requirements marked. Devices implementing

	SRED must be validated against the requirements in the Transaction Data Protection.
Secure Card Reader PIN, (SCRIP)	This applies to a specific device that contains a secure card reader,(ICC, Magnetic stripe or contactless) and is SRED enabled. In addition the SCRIP also has the capability to manage a PIN securely.
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 21: FUNCTIONALITY DESCRIPTION

Requirement	PIN Entry	Keys	ICCR	MSR	Feedback to Cardholder	Terminal is a module	Terminal is compound	open protocol	SCRIP	Chip only POI	Transaction Data Protection	POI Payment Application	Conditions
Module 1 - Core Requirements Modules													
Core Physical Security Requirements													
A1	x	x	x	x					x		x		For POI in purely chip based systems sensitive functions are protected by logical means only.
A2	x												
A3	x	x							x	x	x		
A4	x	x							x		x		For POI in purely chip based systems sensitive functions are protected by logical means only.
A5	x									x			
A6		x							x	x	x		Invasive Attacks – Determining Keys Analysis – For SCRIP applicable whenever reader handles PINs, either offline or online, and has plaintext secret or private PIN-security-related cryptographic keys resident in the device. 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							x		x		Non-Invasive Attacks – Determining Keys Analysis – For SCRIP applicable whenever reader handles PINs, either offline or online, and has plaintext secret or private PIN-security-related cryptographic keys resident in the device.
A8					x								Physical Security of Display Prompts – If keypad can be used to enter non-PIN data
A9	x												Visual Observation Deterrents
A9 ECSG +	x				x					x			Depends upon AB/CPS
A10				x					x		x		
A11									x		x		
A12									x		x		
A13			x						x				
A14			x						x				
A15			x						x				
Core Logical Security Requirements													
B1	x	x						x	x	x	x		

B2	x	x							x	x	x		
B2.1	x	x							x	x	x		
B2.2	x	x							x	x	x		
B2.3		x								x			
B3	x									x			
B4	x								x	x	x		
B5	x	x							x	x	x		
B6	x	x							x	x	x		
B7		x						x	x	x	x		
B8	x									x			
B9		x							x	x	x		
B10									x	x	x		
B11	x								x	x			
B12		x							x	x	x		
B13	x	x							x	x			
B14	x									x			
B15					x					x			
B16	x								x	x	x		
B16.1	x								x	x	x		
B16.2	x								x	x	x		
B17	x								x	x	x		
B18		x								x			
B19			x	x		x				x			
B20	x	x	x	x	x	x	x	x	x	x	x		
B21			x						x	x			
B22									x		x		
B23									x		x		
B23.1									x		x		
B24									x		x		
B25									x		x		
B26									x				

Requirement	PIN Entry	Keys	ICCR	MSR	Feedback to Cardholder	Terminal is a module	Terminal is compound	Implements open protocol	SCRIP	Chip only POI	Transaction Data Protection	POI Payment Application	Conditions
Module 2: POI Terminal integration													
Integration of PIN Entry Functions													
C1.1	x					x				x			
C1.2	x					x				x			
C2.1						x				x			
C2.2			x			x				x			
C2.3	x					x				x			
C2.4	x				x	x				x			
C2.5	x					x				x			
Module 3: Communications and Interfaces													
Communications and Interfaces													
D1								x	x				
D2	x	x							x		x		
D3								x	x				
D4								x	x				
D5								x	x				
D6								x	x				
D7								x	x		x		
D8								x	x				
D9								x	x				
D10								x	x				
D11								x	x				
D12								x	x				
D13								x	x				
D14								x	x				
Module 4: Life Cycle Security Requirements													
During Manufacturing													
E0 ECSCG +	x	x	x	x	x	x	x	x	x	x	x		Depends upon AB/CPS
E1	x	x	x	x	x	x	x	x	x	x	x		

E2	x	x	x	x	x	x	x	x	x	x	x		
E3	x	x	x	x	x	x	x	x	x	x	x		
E4	x	x	x	x	x	x	x	x	x	x	x		
E5	x	x	x	x	x	x	x	x	x	x	x		
E6	x	x	x	x	x	x	x	x	x	x	x		
E7	x	x	x	x	x	x	x	x	x	x	x		
E8	x	x	x	x	x	x	x	x	x	x	x		
E9	x	x	x	x	x	x	x	x	x	x	x		
E10	x	x	x	x	x	x	x	x	x	x	x		
E11	x	x	x	x	x	x	x	x	x	x	x		
E12	x	x	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	Implements open protocol	SCRIP	Chip only POI	Transaction Data Protection	POI Payment Application	Conditions
Between Manufacturer and Facility of Initial Key Loading or Facility of Initial Deployment													
F0 ECSG +	x	x	x	x	x	x	X		x	X	X		Depends upon AB/CPS
F1	x	x	x	x	x	x	x		x	X	x		
F2	x	x	x	x	x	x	x		x	X	x		
F3	x	x	x	x	x	x	x		x	X	x		
F4	x	x	x	x	x	x	x		x	X	x		
F4 ECSG +	x	x	x	x	x	X	x		X	X	X		Depends upon AB/CPS
F5	x	x	x	x	x	x	x		x	X	x		
F6	x	x	x	x	x	x	x		x	X	x		
F7	x	x	x	x	x	x	x		x	X	x		
F8	x	x	x	x	x	x	x		x	x	x		
Requirements for the POI payment application (optional except G1 ECSG+)													
G1 ECSG +												x	Depends upon AB/CPS
G1.1 ECSG +												x	Depends upon AB/CPS
G1.2 ECSG +												x	Depends upon AB/CPS

G1.3 ECSG +													x	Depends upon AB/CPS
G2 ECSG +													x	Depends upon AB/CPS
G3 ECSG +													x	Depends upon AB/CPS
G4 ECSG +													x	Depends upon AB/CPS
G5 ECSG +													x	Depends upon AB/CPS

TABLE 22: SUPPORTED FUNCTIONALITIES

3.8.2. Commercial Off-the-Shelf Devices (COTS)

The following figure shows a generic example of a COTS solution and its environment.

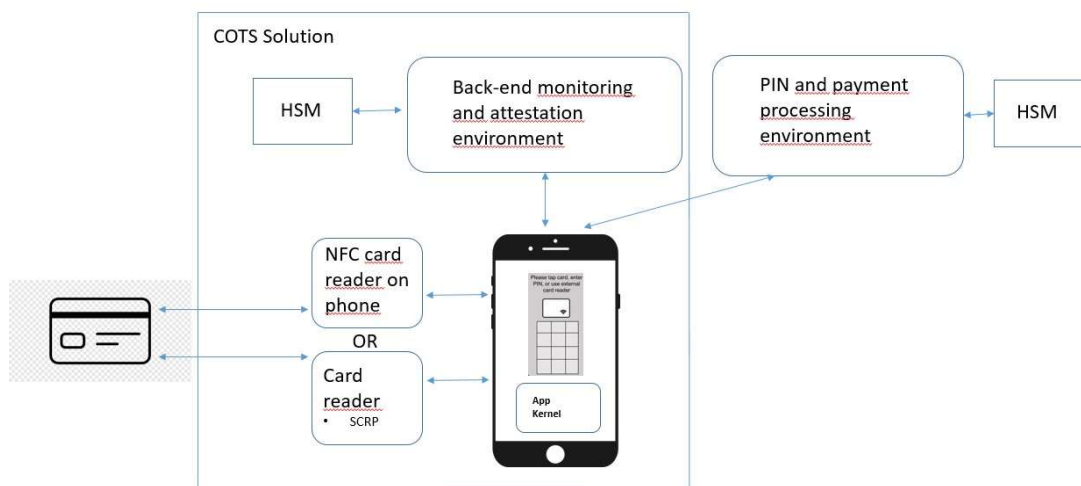


FIGURE 23: EXAMPLE OF COTS USE

This section defines the applicable security requirements for different options of payments using Commercial Off-the-Shelf Devices. In contrast to dedicated card payment devices for which security requirements are defined in section 3.8.1, COTS Devices are publicly available and not commissioned specifically for the purpose of card payments (see section 2.2.4).

The use of COTS Devices introduces additional risks as it relates to privacy, unauthorized disclosure and exposure to vulnerabilities. The risk model for a COTS device is fundamentally different from the one applied to traditional PTS POI compliant POS device, the latter based on both the physical and logical security of the POI device to secure sensitive data.

The COTS device does not have any physical security features and instead relies upon the constant review and alert from the various functions and features of the COTS Device; the Payment App, OS,

(where applicable, an embedded a TEE) and the effectiveness of the backend system in detecting and reacting to a potential compromise and attack.

The security requirements listed in this section pay dedicated attention to these additional risks by e.g. requiring

- additional hardware components to compensate the processing of security functions in software,
- continuous monitoring of the software processing security relevant functions,
- a proper design of the COTS application, and
- continuous risk assessments and risk policies from the COTS Solutions providers and Acceptors.

Beyond these security requirements listed in this Book, Acceptors using COTS Devices should consider the following risk mitigating factors

- Know the location of the COTS Device to prevent the criminal from stealing, modifying and returning the COTS Device without the merchants being aware.
- Ensure it is not possible for a criminal to correlate personal Customer information contained within the COTS Device to account takeover.
- Ensure that software must not be loaded on the COTS Device from untrusted sources like unofficial app-stores.

The requirements listed in this section are derived from PCI SSC and European Card Stakeholders Group requirements. They apply to all COTS Solutions. The 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 optimise evaluation costs and time, particularly when laboratories are reviewing non-conventional architectures.

Vendors wishing to submit a COTS Solution 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 SSC or local European Scheme). 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.

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.

3.8.2.1. Contact Payment with PIN and a Secure Card Reader

Contact Payment with PIN and a Secure Card Reader, (SCR) is a specific option of a COTS Solution where the Cardholder enters their card into a separate Secure Card Reader. The payment application is running on the COTS Device, and the Cardholder uses the COTS Device to enter their PIN.

This solution utilises the following key components:

- COTS Device
- Secure Card Reader SCRP
- Secure application on COTS Device, called App Kernel in the following requirements list
- Back-end monitoring-system

The requirements defined in this section of Book 4 have been grouped into the following modules:

- CORE REQUIREMENTS - General requirements that define security controls applicable to the overall COTS Solution
- PIN CVM APPLICATION – Requirements that apply to the software application(s) that reside on the COTS device
- BACK-END SYSTEMS – MONITORING/ATTESTATION – Requirements supporting the management of the COTS Solution and ensuring security controls and mitigation mechanisms
- SOLUTION INTEGRATION - Requirements necessary for overall oversight, governance and responsibility of the COTS Solution
- BACK-END SYSTEMS – PROCESSING – requirements for the processes/environments that perform and complete PIN and payment processing.
- SECURE CARD READER SRCP

- **Module 1: Core Requirements** applicable to the overall COTS Solution

- **1.1 Protection of Sensitive Services**

Requirements

1. Documentation detailing all sensitive services implemented by the components and COTS Solution must exist and be updated regularly. At a minimum, this must include key loading (for all in-scope areas), signing of applications and SCRPs, firmware and signing of updates to the monitor services or configuration.
2. A dual-control process must exist for the generation of cryptographic keys used for digital signatures to verify the authenticity and integrity of security assets.

- **1.2 Random Numbers**

Requirements

1. Documentation to identify all random number generation functions and reliance on random data used in the solution must exist and be maintained.
2. Any random numbers used on the COTS Device for security purposes must be seeded from a value provided from the RNG on the SCRPs that has been evaluated through POI scheme evaluation.

Note: This excludes the establishment of secure communication protocols where the use of the native OS RNG is out of the control of the PIN CVM application.

3. Random number generation used by the PIN CVM application must utilize a PRNG that was originally seeded by a random seed provided by the evaluated SCRPs. It must not be possible to replay or reuse the same seed except by chance.
4. The PIN CVM application must use an evaluated RNG where cryptographic algorithms require the use of random numbers.
5. Any random numbers used on a back-end system for security purposes must be seeded from a value provided initially from the RNG on at least an HSM certified according to a scheme recognized standard according to section 3.10.5 of this Book.

Note: Random numbers that are not directly relied upon for security of the Cardholder PIN, Cardholder data, or monitoring/attestation data—e.g., random values used in TLS sessions, where the data being transmitted is otherwise protected using application level cryptography—do not need to meet this requirement.

• 1.3 Acceptable Cryptography

Requirements

1. Documentation must exist to identify cryptographic processes and operations used by the solution for security services.
At a minimum, documentation must include the following:
 - Cryptographic algorithms used and where
 - Identification of all keys, the complete key hierarchy, their purposes and crypto periods
 - Key-generation or key-agreement processes
2. All security services provided by the solution must adhere to scheme requirements on minimum and equivalent key sizes and strengths for approved algorithms.
3. Where key-derivation methods are used for creating a unique key, the method must not be reversible (e.g., using XOR operations only) and provide perfect forward secrecy.
4. Hash functions must be implemented in accordance with scheme requirements on minimum and equivalent key sizes and strengths for approved algorithms.
5. Encryption used to protect PIN data or tamper-detection data must be performed using a key that is unique per transaction/communication session and per PIN CVM application instance.
6. All messages that are communicated between components in the COTS Solution must use a unique key per session.
7. Security must not be provided to any key by a key of lesser strength.
8. Public keys/certificates used by the solution must be signed or MAC'd. The integrity and authenticity of the key must be ensured.
Mechanisms must be in place to identify expired certificates and prevent continued processing when certificates are expired.
9. Each key must have a single unique purpose, and no keys may be used for multiple purposes (such as both signing and encrypting data).
10. Keys used to validate authenticity must be unique to each end point so that an HMAC or signature generated at one end would always be different if generated by the other end point.
11. Any key "signature" or "fingerprint" values returned by the system must not reveal any details about the key itself.
12. KCVs must be limited to five bytes or less, and hash algorithms used for key fingerprints (on secret or private keys) must implement SHA256 or stronger (or be truncated to no more than five bytes).

• 1.4 Key Management

Requirements

1. Documentation, including procedures, must exist to support all key lifecycle management functions used by the solution.
2. Key-management techniques must protect the integrity and purpose of symmetric cryptographic keys.
3. Cryptographic key-management processes must conform to recognized national or international key-management standards.
4. Key-loading methods must enforce dual control to ensure that no one person is solely responsible for key-loading operations.
5. Secret and/or private cryptographic keys must be unique per devices and/or applications.
6. Generation and loading of clear-text secret and/or private keys or key components must ensure split-knowledge principles are enforced.
7. Secret and/or private cryptographic keys must be maintained in one or more of the following approved forms:
 - a. Encrypted by a key of equal or greater strength
 - b. Stored within a SCD
 - c. Managed as two or more full-length components

Note: These approved methods do not apply when storing secret and/or private cryptographic keys within the PIN CVM application. For the PIN CVM application (e.g., white-box cryptography) refer to Module 2.

8. Methods and procedures to revoke compromised public/private key pairs and certificates must be documented and implemented.
9. All key-generation functions must implement one-way functions or other irreversible key-generation processes.
10. Keys must be generated with equivalent entropy (e.g., a 128-bit key is generated with 128 bits of entropy input).

- **1.4 Key Management**

Requirements

11. Audit logs must be maintained for all key-management activities and all activities involving clear-text key components. The audit log includes:
--

- | |
|---|
| <ul style="list-style-type: none">a. Unique identification of the individual that performed each functionb. Date and timec. Function being performedd. Purposee. Success or failure of activity |
|---|

Controls must be established to protect logs from unauthorized modifications or deletion.

Retention of key-management audit logs must conform to industry accepted practices and the organization's record retention policies.

12. Incident response procedures must exist and include activities for reporting and responding to suspicious or confirmed key-related issues, including key compromises.

- **1.5** *Secure Software Development Practices*

Requirements

1. All software must be developed according to the development process and to the development requirements outlined by cards schemes. Card schemes shall require the software development to be carried out according to recognized techniques and standards.

• **Module 2: PIN Cardholder Verification Method (CVM) Application**

• **2.1 Development**

Requirements

1. Software that handles, secures or otherwise affects the security of the PIN entry and processing on the COTS Device must be logically separated from code that is used for other purposes (such as general merchant UI).
2. Documentation must exist and be maintained to detail the following:
 - Protections provided to the application to protect against tampering, side-channel attacks, fault injection and reverse engineering for the various supported platform and protection methods (such as TEE, white-box cryptography).
 - Details of all areas where functions provided by the application are executed. This should include the main processing environment of the COTS Device but may also include other local execution environments (such as a TEE or embedded security processor).
 - Data-flow diagrams that show how the PIN is entered, processed, encrypted and validated within the application, where the data is transmitted outside of the scope of the application and any assumptions made about these external connections.
 - Block diagram that indicates where all sensitive data is available in clear text on the merchant-side systems. This includes, but may not be limited to, the SCRP, the COTS OS, any TEE or physically separate security-processing elements used. This diagram must indicate the flow of sensitive data through the various elements.
 - Guidance for merchants regarding how to ensure the PIN is entered in a way that it cannot be observed.
 - Identification of where internal buffers are used and cleared when collecting sensitive data.
 - Process that is demonstrably in use for the discovery and remediation of bugs and vulnerabilities in the system.
 - A policy on how to manage vulnerabilities and perform security testing.
3. Mechanisms must exist to uniquely identify each instance of the PIN CVM application to the back-end monitoring system and the back-end attestation component.
4. The PIN CVM application must only communicate with known and trusted POI approved SCRPs.

• 2.1 *Development*

Requirements

5. The PIN CVM application must prevent against attacks designed to expose data in storage or memory and deploy appropriate controls including minimizing such storage post transaction completion or application timeout.
6. The PIN CVM application must be securely developed to prevent screen captures.
7. The PIN CVM application must be resistant to reverse engineering.
8. Correlatable data that may be supplied by the Customer—e.g., e-mail addresses and/or mobile phone numbers required for receiving virtual receipts—must only be viewed in clear text during its initial entry for the purposes of error correction by the Customer. Thereafter, any re-presentation of this data by the PIN CVM application must be masked to prevent exposure of the information.
9. Establishing a new session or refreshing a secure session between the PIN CVM application and the back-end monitoring system and back-end attestation component must require successful attestation between the PIN CVM application and monitoring environment.
10. The PIN CVM application must automatically clear the internal buffers it controls when any one of the following occurs:
 - The transaction terminated for any reason (including success or failure), or
 - The PIN CVM application has timed out waiting for the response from the Customer or merchant or
 - A tamper-detection event has been signaled by the back-end monitoring system, or the PIN CVM application is halted, loses focus or otherwise is moved to background processing.

• 2.2 *Secure Provisioning*

Requirements

1. There must be a clear definition of all platforms—including device types, hardware and OSs—on which the PIN CVM application can be executed.
2. PIN CVM applications must be developed only for supported platforms.

• 2.2 Secure Provisioning

Requirements

3. The PIN CVM application must only support platforms that, at a minimum, provide the following features:
 - An enforcing mandatory access control framework
 - A “trusted boot” mechanism that validates the OS’s authenticity
 - Ability to prevent all applications other than the foreground application from accessing touch-event details
 - Validation of an application signature upon loading and execution of that application. This signature must be calculated with cryptography, and no known bypass measures may exist for the acceptable baseline systems.
 - Isolation of touch-event data such that only the application currently in focus can receive or otherwise identify the location of touch events
4. The PIN CVM application must be installed and updated using methods that ensure its integrity and authenticity, using only the OS store implementing cryptographic validation of this store and any loaded applications.

The OS store must not have publicly disclosed vulnerabilities that have not been patched or otherwise remediated by other features of the overall solution.
5. Any required cryptographic keys or other data necessary for first execution must be securely provided to the PIN CVM application and securely stored.
 - Where an external SCRP is used, this must include the use of cryptographic keys stored within the SCRP to provide security to the provisioning process.
 - Where white-box cryptography is used white-box keys must be unique per PIN CVM application instance. The reliance and use of common white-box keys must be minimized after the secure provisioning process.
 - Secure provisioning must implement the principles of perfect forward secrecy.
6. The PIN CVM application executables and scripts must be digitally signed and a signature provided to confirm the software author and guarantee that the application from the OS store (and any other updates) has not been altered or corrupted since it was last signed.

The digital signatures must be checked prior to use of the application and at required attestation intervals.
7. The process to generate digital signatures must be performed using dual control, based on cryptographic keys that are secured within an HSM formally approved by card scheme recognized certification schemes according to section 3.10.5 of this Book.

• 2.2 *Secure Provisioning*

Requirements

8. A security policy must exist for acceptable use of the PIN CVM application and be provided to all users of the PIN CVM application.

• 2.3 *Tamper Checks*

Requirements

1. The PIN CVM application must offer tamper-resistance measures around the handling of code, application/monitor interface code and any code that is involved in the use or security of cryptographic keys (both public and private/secret keys) for all the supported platform and protection methods (such as TEE, white-box cryptography).
2. Documentation must exist and be maintained on how tamper resistance is achieved for each of the supported platforms, including but not limited to:
 - Code obfuscation
 - Protections provided by specific platforms
 - Reliance on TEE, security processor, or other security feature of the COTS Devices used
3. The PIN CVM application must implement methods for detecting and reporting to the monitoring system if any COTS Devices have been rooted or jailbroken, including but not limited to:
 - When the PIN CVM application is executed
 - As requested by the monitoring system
 - Whenever white-box cryptography or obfuscation methods, implementations, or instantiations are updated

The monitoring system must detect when the PIN CVM application has been “side loaded” outside of normal channels and treat this as a tamper-detection event.

Applications that fail this check should be prohibited from use to accept PINs.

• 2.4 PIN Entry

Requirements

1. The PIN CVM application must not display the PIN entry screen if it detects that it is being run in developer or emulator mode.
 2. The following events during a PIN entry session must be detected by the PIN CVM application and result in termination of the PIN entry session and deletion of all data collected during the transaction, including PIN data, and not limited to:
 - Switching between applications (e.g., PIN CVM application and any other application on the COTS Device)
 - Stealing focus during PIN entry
 - Stealing focus at any other time during the foreground execution of the PIN CVM application to maliciously prompt for (and thereby capture) PIN entry
 - Screen capture during PIN entry
 - Not using “full screen mode”
 - Activating sensors or pooling sensor data
 - Enablement or access of the NFC interface by any other application
 3. The PIN CVM application must not allow PIN entry to be triggered unless the transaction is EMV-based. All transactions must be processed online.
- Note:** *This does not prohibit the use of offline PIN verification.*
4. PIN display in the PIN CVM application must be fully masked so as not to display any digit of the PIN value.
 5. The PIN entry keyboard must not rely on the COTS Device OS keyboard, and it must be securely rendered by the PIN CVM application.
 6. During PIN entry, any signal or event (visual, audible, etc.) must be uncorrelated to the touch event position and the PIN digit being selected. In addition, this must account for other leakage factors—e.g., local haptic feedback, numeric key animation when pressed, on device sensors, etc.
 7. The PIN CVM application must not cache PINs.

• 2.5 PIN Encryption

Requirements

1. PIN data must be encrypted upon entry into the PIN CVM application and remain encrypted when transmitted by the PIN CVM application through a trusted and secure interface to the SCRP.
2. Encrypted PIN data must be protected from malicious activity, attacks and attempts to extract masked PIN values.
3. The PIN-encryption keys and algorithms in the PIN CVM application used to initially encrypt the PIN must adhere to scheme requirements on minimum and equivalent key sizes and strengths for approved algorithms.
4. PIN-encryption keys must be established in the PIN CVM application in a secure manner.
5. Secret keys associated with PIN encryption must be protected to ensure their confidentiality as well as their integrity.
6. Where white-box cryptography is used, the white-box cryptography keys must be changed periodically, e.g. monthly.
7. The customer PIN data must be encrypted using ISO format 4 for transport between the PIN CVM Application and the SCRP.

• 2.6 Audit Logs

Requirements

1. The PIN CVM application must ensure logs exist and are communicated securely to the back-end monitoring system. The logs must not contain correlatable data or PIN data.
2. The audit trail generated by the PIN CVM application must support reconstructing the following events:
 - All user access to correlatable or PIN data.
 - All activity that impacts security functions of the PIN CVM application (e.g., changes to cryptographic functions, changes to application permissions, failure or success to establish secure channel with monitoring system, etc.)
 - All access to the audit trail managed by or within the PIN CVM application.
 - Use of and changes to the PIN CVM application's identification and authentication mechanisms.
 - Initialization, stopping or pausing of the PIN CVM application logs.

- 2.6 *Audit Logs*

Requirements
3. All recorded events must capture at least the following information: • User identification • Type of event • Date and time • Success or failure • Origination of event • Identity or name of affected data, system component or resource

- **Module 3: Back-end Systems – Monitoring/Attestation** supporting the management of the COTS Solution and ensuring security controls and mitigation mechanisms

• 3.1 COTS System Baseline

Requirements

1. Documentation must exist and be maintained for the following:
 - Implemented processes to determine the COTS System Baseline for acceptance of COTS Devices (for example whitelist, blacklist, or hybrid approach)
 - How these processes account for known and potential vulnerabilities in systems
 - Clear identification of roles and responsibilities for which aspects of the COTS System Baseline validation process are performed by the PIN CVM application itself, and which are performed by other systems or execution environments.
 - Process that is demonstrably in use for the discovery and remediation of bugs and vulnerabilities in the system.
2. Documentation must exist and processes be demonstrably in use that identify methods used for updating the COTS System Baseline as new threats are identified.
3. The COTS System Baseline must be validated by the attestation process upon provisioning of the PIN CVM application.
4. The COTS System Baseline must not include rooted or jailbroken devices.
5. Validation of the COTS System Baseline must be performed during each attestation check performed by the back-end attestation component.
6. COTS Devices that use unsupported COTS System Baselines must be prohibited from processing transactions.

• 3.2 Attestation Mechanism

Requirements

1. A documented attestation policy that defines health-check rules for the SCRP, COTS Device, and PIN CVM application attestation mechanisms must exist.
 - The policy must include detailed response procedures for successful and non-successful results.
 - The policy must be maintained and strictly controlled including reviews and updates as necessary, regularly, e.g. at least annually.
2. The attestation system must manage attestation parameters and measurements securely and maintain their integrity wherever they are stored or processed. (Note that measurement parameters can be static or behavior-based, privileges, intents, system calls).
 - Attestation data must be cryptographically signed.

Note: *If no assurance is available, any security dependence on the proxy is a residual risk.*
3. Attestation must be performed at a minimum:
 - a. At initialization/initial installation of the PIN CVM application initiated by the attestation system, back-end systems, or other trusted non-local execution environment.
 - b. At least every five minutes (if not otherwise activated by one of the events above during that time).
 - c. As indicated in following sections.
4. For any attestation response, The solution provider must be able to identify:
 - a. Where the process is implemented (in the PIN CVM application, in a server-based attestation component, remotely or locally to the consumer device, etc.).
 - b. Whether the process was developed by the attestation vendor.
 - c. Whether the process is managed by a third-party provider that provides an API to the attestation vendor but no other privileged access.
5. Escalation procedures must be defined for undocumented and unknown attestation responses.
6. Attestation code implemented in the PIN CVM application must be protected by the tamper-resistance features implemented in the PIN CVM application.

• 3.2 Attestation Mechanism

Requirements

7. If the attestation system tamper response involves a manual process—e.g., a potential tamper event, it must be escalated to vendor staff to validate:
 - a. Written procedures for manually processed events must exist and be demonstrably in use.
 - b. These procedures must cover events where staff relied upon for such determinations are unavailable.
 - c. Events must be immediately escalated for manual review and then actioned within 48 hours.
 - d. Automated systems must be in place to disable any further payment processing from systems when an event has not been actioned for 48 hours.
8. Requisite skilled staff must be provided to implement and interpret attestation health-check rules, associated controls and findings, along with the associated training.
9. Retention requirements must be defined and implemented for attestation results.
- 10 Retained attestation findings must have a unique ID, date and time stamp and description.
- 11 Attestation mechanism changes must be performed using authorized processes.
- 12 Attestation mechanism changes must adhere to formal change-control procedures.
- 13 For manual updates of the attestation system:
 - There must be documented procedures.
 - Deployment of changes to the production environment must require dual control.

- **3.3 Type 1 – Attestation of Secure Card Reader PIN SCRP**

Requirements

- | |
|--|
| <ol style="list-style-type: none">1. The PIN CVM application attestation component must be able to determine that the connected SCRP is valid. At a minimum verify the following:<ol style="list-style-type: none">a. Firmware version is acceptableb. SCRP is in a secure state and supports SRED functionalityc. Correct unique identifier of the SCRP <hr/> <ol style="list-style-type: none">2. Attestation of the SCRP must be performed in accordance with the specified attestation policy. At a minimum the attestation must occur:<ol style="list-style-type: none">a. At system initializationb. Before business processing commences (prior to first transaction)c. If initiated by a monitoring environment requestd. Polled at unpredictable intervals during an online sessione. Whenever the SCRP is physically or logically disconnected and reconnected to the COTS Device. <hr/> |
|--|

• 3.4 Type 2 – Attestation of COTS Devices

Requirements

1. Attestation through verification of the COTS System Baseline must be performed at PIN CVM application provisioning.
2. Attestation must include comprehensive configuration information of the COTS Device.
3. Mechanisms must be in place to validate the integrity of the attestation results.
4. Attestation mechanisms must not be vulnerable to TOCTOU (time-of-check, time-of-use) attacks.
5. Information about the platform state must be accessible to measurement tools.
6. Attestation mechanisms must not interrupt payment-transaction processing.
7. Attestation responses must not leak information about the attestation mechanism.
8. Attestation responses must be unclonable.
9. Attestation responses must complete within an expected timeframe as defined in the attestation policy. If not, the monitoring environment must be notified.
10. Attestation mechanisms must be provided and maintained with up-to-date information about known vulnerabilities to detect at a minimum:
 - a. Modifications to the COTS Device OS firmware
 - b. COTS Device OS firmware tamper
 - c. PIN CVM application execution in developer mode
 - d. PIN CVM application execution in debug mode
 - e. Emulator use
 - f. Use of a hooking framework
 - g. PIN CVM application modification
 - h. PIN CVM application tamper
 - i. Use of PIN CVM application code, or part thereof, within another (valid and/or invalid) operational environment—e.g., through “code lifting” of the entire, or partial, application to another platform after initialization and personalization
 - j. Asynchronous rooting and un-rooting of the COTS Device OS
 - k. Relay attacks on PIN entry
11. Implement controls to protect the attestation mechanism from reverse engineering.

- **3.4 Type 2 – Attestation of COTS Devices**

Requirements
12 The COTS Device attestation must be performed in accordance with the specified attestation policy. At a minimum, the attestation must occur:
a. At PIN CVM application startup
b. Before business processing commences (first transaction of the day)
c. If initiated by a monitoring environment request
d. At unpredictable intervals, polled during an online session
e. After changes have been made to the solution or to major configuration files
f. When the “Application” loses “focus” and regains “focus”
g. Continuously, polled at periodic, unpredictable intervals

• 3.5 *Type 3 – Monitoring Environment Attestation of PIN CVM application*

Requirements

1. The PIN CVM application's attestation must meet requirements of Type 2 attestation.
2. The PIN CVM application must support a set of attestation criteria that meet the attestation baseline.
3. A set of rules must be defined for analyzing the attestation responses and assign a risk-severity rating for the attestation responses that aligns with the attestation policy.
4. Establish detailed procedures or automated responses for attestation responses. Procedures must include, at a minimum:
 - a. Send an alert to the monitoring environment support personnel based on attestation-response severity.
 - b. Conduct corrective actions (e.g., modify a hash of a configuration file) for false positives.
 - c. Completely block transaction processing in the most significant cases as defined in the attestation policy.
 - d. Temporarily stop transaction processing to update obsolete solution components (either internal or third-party dependencies).
5. Maintain up-to-date configuration measurements to support attestation criteria.
6. Establish controls to defend against attestation abuses to subvert the prover—e.g., defend against DoS through malicious verifier attacks.
7. Establish controls to defend against attestation abuses that exploit system automation such as data poisoning attacks.
8. The monitoring environment-based attestation must be performed in accordance with the specified attestation policy. At a minimum the attestation must occur:
 - a. At system startup
 - b. Before business processing commences (first transaction of the day)
 - c. At unpredictable intervals, polled during an online session
 - d. If triggered by the PIN CVM application attestation component
 - e. If initiated by a monitoring environment request
 - f. After changes have been made to the solution or to major configuration files

• 3.5 Type 3 – Monitoring Environment Attestation of PIN CVM application

Requirements

9. A documented policy and procedure for assessing these changes to the COTS System Baseline must exist and provide details on how:
 - Decisions are made to remove previously acceptable platforms from the COTS System Baseline.
 - Such changes will affect the parties using these platforms, so the documentation must also include how communication is handled in these cases.

10. The solution provider must have a documented risk-assessment policy and procedures that provide details on:
 - The methods used to assess on-going risk of the solution;
 - How and when updates to the system baseline are performed; and
 - How such changes are communicated to affected merchants.

The risk-assessment policy and procedures must be reviewed at least annually.

It is not considered acceptable for the policy to require a minimum number of PIN CVM applications to be using a vulnerable platform before it is removed from the system baseline.

11.
 - Thresholds for minimum acceptable PIN CVM application versions must be maintained by the solution provider.
 - A risk-assessment methodology must exist, be documented and followed to ensure that merchants are using the most current acceptable version of the PIN CVM application.
 - In instances where a merchant is using an acceptable version, but it is not the current, there must be notifications sent to the merchant to require them to update it. PIN CVM applications using a version that is not within the version threshold must not be permitted to accept PIN data.
 - Installation of previous versions of the PIN CVM application must not be permitted.

- **3.6 Basic Protections**

Requirements

- | |
|--|
| <ol style="list-style-type: none">1. When the back-end monitoring system and back-end attestation component reside in an organization's Customer data environment, each of these must adhere to security requirements for data as defined in section 3.2 of this book. |
| <ol style="list-style-type: none">2. If PAN is not present in the back-end monitoring and attestation systems' environment and it is not part of an organization's existing Customer data environment, the environment must comply with the logical and physical security requirements for monitoring and attestation environment basic protections. |
| <ol style="list-style-type: none">3. All traffic to/from back-end monitoring and attestation systems must be strictly controlled. |
-

- **3.7 Operational Management**

Requirements

1. Documented procedures to support the operation of the monitoring environment must exist and be demonstrably in use.
2. Staff responsible for monitoring environment duties must be provided up-to-date security training upon hire and at least annually in order to support monitoring, alerting and response responsibilities.
3. Reviews must be performed at least quarterly to verify operational procedures are being followed.

Reviews must be performed by personnel assigned to the security governance and include the following:

- Confirmation that all operation-management processes are being performed
 - Confirmation that personnel are following security policies and operational procedures—for example, daily log reviews, firewall rule-set reviews, configuration standards for new systems, etc.
-

- **Module 4: Solution Integration Requirements**

- **4.1 *Pairing of Disparate Components***

Requirements
1. Mechanisms must exist to identify and validate the SCRP and PIN CVM application as authorized prior to communication of any sensitive data between the SCRP and PIN CVM application.
2. The monitoring system must be able to associate the PIN-based transaction to a specific merchant, COTS Device and SCRP combination for tracking. If not successful, the transaction must fail.
3. The back-end monitoring system must be able to accept and process attestation data from the SCRP and PIN CVM application and take appropriate action based on predefined rules (for example, suspending transactions).
4. The back-end monitoring system must establish mechanisms to ensure attestation data is refreshed and up to date.

• 4.2 Secure Channels

Requirements

1. A secure channel must exist between each of the physically and logically disparate components of the COTS Solution.
2. Each secure channel must provide mutual authentication to uniquely identify each component prior to exchanging sensitive data, as well as protect against MITM and replay attacks.

Mutual authentication between the communicating components must be based on cryptography that aligns with scheme requirements on minimum and equivalent key sizes and strengths for approved algorithms.
3. Cryptographic keys used to establish secure channels between components and for data encryption must be unique, except by chance.
4. Documentation must exist and be maintained to identify logical connections between the PIN CVM application and other components of the COTS Solution.

Documentation must identify how data confidentiality and authenticity is maintained.
5. Use of standard protocols must prevent against downgrade attacks.

• 4.3 PIN CVM Solution Requirements

Requirements

1. A user guide that provides information about the solution, including identifying control points and security responsibilities for the merchant(s) must exist and be made available to the merchant.
2. The security assets of the solution must be identified and managed. At a minimum, the solution provider must ensure identification of authorized SCRPs, linking SCRPs to the PIN CVM application and back-end monitoring environment and verification that firmware/application updates are current.
3. The solution must be “online,” connected to the back-end systems (monitoring, attestation component and processing) and in an operational state before initiating any PIN entry functions.
4. The SCRP and PIN CVM application (including the attestation component) must have the ability to be identified as authorized and validated to the monitoring environment, by cryptographic means, before initiating a PIN entry session.

• **4.3 PIN CVM Solution Requirements**

Requirements

5. The solution must incorporate a detection system or feed other detection systems capable of detecting anomalous and potentially fraudulent activity, including suspicious transactions.
6. Plans and procedures must be defined to address interruptions to the solution due to unplanned business disruption, major disaster or failure of services.
Testing to ensure viability of such plans and procedures must be performed annually at a minimum.
7. The solution provider must have a documented risk-assessment policy and procedure, which is reviewed at least annually.
This policy must include the methods used to assess on-going risk of the solution as well as how and when updates to the COTS System Baseline are performed and how such changes are communicated to affected merchants.
8. A threat-management process must be established to monitor for newly discovered vulnerabilities that may impact the security of the solution.
A risk assessment of these vulnerabilities must be performed against currently implemented security and attestation controls to:
 - *Determine the residual risk and*
 - *Ensure that the vulnerability does not change the baseline integrity of the solution.*
9. The solution configuration and release management process must be integrated with the threat management process. The firmware- and software-release process must take input from the threat-management process on the development of the minimum viable product.
10. The solution Provider must provide the approved lab with a test platform to evaluate the solution.
This test platform must be developed in a manner that provides full accessibility and visibility into the solution. The test platform must provide an interface or a report that would enable an external company to validate the detection of potential vulnerabilities present on systems used in the testing.
11. All encryption keys associated with the SCRP must be injected by a key-injection facility that meets the PIN Security Requirements defined within section 3.4.2.1 of this document.

- **Module 5: Back-end Systems – Processing** applying to the processes/environments that perform and complete PIN and payment processing.

- **5.1 Security of Customer Data and PIN Processing Environment**

Requirements

1. Decryption of all Customer data and PIN data received from the SCRP must only occur in back-end payment and PIN-processing environments, respectively.
2. The processing environment that performs the decryption of the Customer data must maintain and comply with security requirements for data as defined in section 3.2 of this book.
3. PIN processing performed in the processing environment must meet the PIN Security Requirements defined within section 3.4.2.1 of this document.

Module 6: Secure Card Reader (SCRP)

- **6.1 Use of a Secure Card Reader**

Requirements

1. The SCRCP must include all Physical and Logical requirements as defined in Section A and B of section 3.8.1.3 of this document, except those specific to PIN entry, display prompt control, unattended usage, and use of magnetic-stripe readers.

3.8.2.2. Contactless Payment without PIN

Contactless Payment without PIN is a specific option of a COTS Solution which enables the Customer to use their (mobile) contactless payment application to make a payment by tapping onto the contactless antenna of the merchants COTS Device. The payment application is running on the COTS Device, and for this solution there is no PIN entry device.

This solution utilises the following key components:

- COTS Device
- Payment application on the COTS Device, called App Kernel in the following requirements list
- Back-end monitoring system

The requirements defined in this section of Book 4 have been grouped into the following modules:

- CORE REQUIREMENTS - General requirements that define security controls applicable to the overall COTS Solution
- CONTACTLESS PAYMENTS ON COTS APPLICATIONS - The App Kernel requirements apply to the software applications that reside on the COTS device and communicate with attestation components, back-end monitoring systems, and back-end processing systems. The App Kernel is responsible for initial and any subsequent encryption of the NFC read account data and collecting and reporting attestation information.
- BACK-END SYSTEMS – MONITORING/ATTESTATION – Requirements supporting the management of the COTS Solution and ensuring security controls and mitigation mechanisms
- BACK-END SYSTEMS – PROCESSING – requirements for the processes/environments that perform and complete PIN and payment processing.
- CONTACTLESS KERNEL

Module 1: Core Requirements

• 1.1 Protection of Sensitive Services

Requirements

1. Documentation detailing all sensitive services implemented by the solution and its components must exist, be reviewed regularly and be updated as necessary. This must include, but is not limited to, key management, signing of applications, and signing of updates to the attestation services or configuration.

Note: This includes sensitive services on the COTS Device and the back-end monitoring systems.

2. All sensitive services must be protected against unauthorized modification (i.e., integrity protection) and against unauthorized access (i.e., access control).

• 1.2 Random Numbers

Requirements

1. Documentation to identify all random number generation functions and reliance on random data used in the solution must exist and be maintained.
2. Any random numbers used on the COTS Device for security purposes must be seeded from a value provided from a trusted source combined with input from the Random Number Generator (RNG) on the COTS Device or within the App Kernel, and at least two other sources of non-deterministic data (such as user input timing and values collected from lowest bits of on-device analog sensors).

Note: Random numbers that are not relied upon directly for security of the account data or attestation data, such as random values used in TLS sessions where the data being transmitted is otherwise protected using application level cryptography, are exempt from this requirement.

3. The deterministic random number generator must be reseeded each time the App Kernel launches.
4. The seed value must never be stored in non-volatile memory.
5. The App Kernel must use an assessed RNG where cryptographic algorithms require the use of random numbers.
6. Any random numbers used on a back-end system for security purposes must be seeded from a value provided initially from the NRNG on at least a HSM certified according to a scheme recognized standard according to section 3.10.5 of this Book.

• 1.3 Acceptable Cryptography

Requirements

1. Documentation must exist that identifies cryptographic processes and operations used by the solution for security services. Documentation must include, but not be limited to, the following:
 - Cryptographic algorithms used and where they are used
 - Identification of all keys, the complete key hierarchy, their purposes, and their crypto periods
 - Key-generation or key-agreement processes
 - Description of cryptographic key protection mechanisms
 2. All cryptographic processes provided by the COTS Solution must adhere to scheme requirements on minimum and equivalent key sizes and strengths for approved algorithms.
 3. Hash functions must be implemented in accordance with scheme requirements on minimum and equivalent key sizes and strengths for approved algorithms.
 4. Security to any cryptographic key must not be provided by a key of lesser strength.
 5. Public keys and certificates used by the solution must be authenticated up the entire chain to the root certificate authority at install.
 6. Self-signed certificates are prohibited.
- Note:** *Self-signed certificates that exist as part of the base COTS Device are excluded from this requirement.*
7. Mechanisms must be in place to identify expired and revoked certificates, and to prevent continued processing when certificates have expired or been revoked.
 8. Each key must have a single unique purpose, and no keys may be used for multiple purposes, such as both signing and encrypting data.
 9. Keys used to validate message authenticity must be unique to each endpoint so that signature generated at one end would always be different if generated at the other endpoint.
 10. Any key signature or digital fingerprint values must not reveal any bits of the key itself.
 11. Key Check Values (KCVs) must be limited to five bytes (10 hexadecimal digits). In addition, hash algorithms used for key fingerprints on secret or private keys must implement SHA256 or stronger, or be truncated to no more than five bytes.

• 1.4 Key Management

Requirements

1. All key lifecycle management functions and procedures used by the COTS Solution must be documented.
2. Cryptographic key-management processes must conform to industry-accepted key-management standards.

Note: *White-box cryptographic keys are covered in Module 2.*

3. Key-management techniques must protect the integrity and purpose of all keys used in the COTS Solution.
4. Secret cryptographic keys and private cryptographic keys that are used as part of account data security must be maintained in one or more of the following approved forms:
 - Encrypted by a key of equal or greater strength
 - Stored within a secure cryptographic device
 - Managed as two or more full-length components
 - Managed as an M-of-N secret-sharing scheme

Note: *These approved methods do not apply when storing secret and/or private cryptographic keys within the App Kernel. For the App Kernel (white-box cryptography), refer to [Section 2.2 Software-Protected Cryptography of this requirements list](#). These requirements do not apply to TLS-negotiated sessions.*

5. Both secret cryptographic keys and private cryptographic keys must be unique per COTS Device and/or App Kernel.

Note: *White-box cryptographic keys are covered in Module 2: Contactless Payments on App Kernel.*

6. Key management processes for cleartext secret or private keys or key components must ensure split knowledge and dual control principles are enforced.

Note: *White-box cryptographic keys are covered in Module 2: Contactless Payments on App Kernel.*

7. Methods and procedures to revoke compromised public/private key pairs must be documented and implemented.

8. All symmetric key derivation functions must implement one-way functions or other irreversible processes.

• 1.4 Key Management

Requirements

9. Audit logs must be generated and maintained for all key-management activities and all activities involving cleartext key components. The audit log includes:
 - Unique identification of the entity that performed each function
 - Date and time
 - Function being performed
 - Purpose
 - Success or failure of the activity
10. Key-management audit logs must be retained for two years subsequent to key destruction.
11. The integrity of audit logs containing key-management activities must be protected from unauthorized modifications or deletion.
 Key management audit logs that are retained by a solution provider must be stored in accordance with PCI DSS. Otherwise, the environment must comply with the logical and physical security requirements for monitoring and attestation environment basic protections.
12. Incident response procedures must exist and include activities for reporting and responding to suspicious or confirmed key-related issues, including key compromises.

• 1.5 Secure Channels

Requirements

1. Connections between different physical and logical components of the solution must be secured.
2. Each secure channel must provide mutual authentication to uniquely identify each component prior to exchanging sensitive data and protect against MITM and replay attacks.
Note: *Mutual authentication between the communicating components must be based on cryptography that aligns with industry standards recognized by card schemes.*
3. Cryptographic keys used to establish secure channels between the solution components and for data encryption must be unique, except by chance.
4. Use of standard protocols must prevent downgrade attacks.

• 1.6 Correlatable Data

Requirements

1. COTS Solution provider must maintain documentation that includes any data elements created or accepted as input that the COTS Solution provider reasonably believes could be used for correlation of account data to App Kernel transactions.
2. COTS Solution provider must document the countermeasures incorporated in the solution to minimize the potential for correlatable data.

• 1.7 Operational Management

Requirements

1. Documented procedures to support the operation of the back-end environments must exist and be demonstrably in use.
2. The COTS Solution provider must have documented risk-assessment policy and procedures that are demonstrably in use and that provide details on:
 - Methods used to assess on-going risk of the COTS Solution
 - Thresholds for minimum acceptable App Kernel versions
 - How and when updates to the COTS System Baseline are performed
 - How such changes are communicated to affected merchants

The risk-assessment policy and procedures must be reviewed at least annually and when there are significant changes to the COTS Solution.
3. A threat-management process must be established to monitor newly discovered vulnerabilities that may impact the security of the COTS Solution. A risk assessment of these vulnerabilities must be performed against currently implemented security and attestation controls to:
 - Determine the residual risk
 - Ensure that the vulnerability does not change the baseline integrity of the COTS Solution
4. The COTS Solution provider vulnerability management process must be integrated with the threat-management process.
5. The COTS Solution must be tested regularly.
6. A public vulnerability-management program must be securely implemented and provide confidentiality of the reported vulnerability.
7. Plans and procedures must be defined, and tested regularly, to address interruptions to the solution due to unplanned business disruptions, major disasters or failures of service.

• 1.7 *Operational Management*

Requirements

8. Changes and updates of any of the solution components, such as the back-end monitoring system, attestation system, or a remote component of contactless kernel, must follow a formal change-control process.
9. Reviews must be performed at least quarterly to verify that operational procedures are being followed. Reviews must be performed by personnel assigned to security governance and include the following:
 - Confirmation that all operation-management processes are being performed
 - Confirmation that personnel are following security policies and operational procedures, such as daily log reviews, firewall rule-set reviews, and configuration standards for new systems

• 1.8 *Secure Software Development Practices*

Requirements

The App Kernel software should be developed and maintained in accordance with security standards and best practices to reduce the risk of vulnerabilities that result from poor coding techniques.

All software must be developed in accordance with the development process and to the development requirements described by cards schemes.

• 1.9 *Development, Maintenance and Dissemination of Solution User Manual*

Requirements

1. A user manual that provides information about the solution, including identifying control points and security responsibilities for the merchants, must exist and be made available to the merchant.
2. The COTS Solution user manual must be disseminated to merchants who are using the solution at the time of onboarding or upon request.
3. The COTS Solution user manual must be reviewed regularly and upon changes to the COTS Solution, including the COTS Device, the App Kernel, and the back-end systems. Any changes to the manual must be disseminated to merchants.

Module 2: Contactless Payments on COTS Applications

• 2.1 *Tamper and Reverse Engineering Protection*

Requirements

1. Documentation must exist and be maintained on how tamper resistance is achieved for each of the supported COTS Devices, including, but not limited to:

- Code obfuscation
- Protections provided by specific platforms
- Reliance on TEE, security processor, or other security features of the COTS Devices used

2. The App Kernel on must be protected by tamper-resistance measures to protect its code, application, attestation interface code, and any code involved in the use or security of cryptographic keys (both public and private/secret keys) for all the supported COTS Devices and protection methods (such as TEE, secure enclave, and white-box cryptography).

Note: *Tamper-resistant measures can be implemented in the App Kernel, provided by the COTS Device, or a combination of both.*

3. The attestation component must have the least privilege required to access proprietary APIs to determine the COTS Device state.

4. Attestation code implemented in the App Kernel must be protected by tamper-resistance features.

5. The contactless kernel, including any configuration files, optional settings, or payment brands public keys embedded or associated with App Kernel, must be protected by tamper-resistant methods to guarantee its integrity.

6. The contactless kernel operation must be immutable, such that transaction processing cannot be interfered by other applications or users on the COTS Device.

7. The App Kernel must implement methods for detecting and reporting the following to the back-end monitoring system:

- COTS Devices that have been rooted, jailbroken, or in developer mode.
- App Kernel that has been “side loaded” outside normal channels.
- Status of COTS Device sensors and hardware, as allowed by the COTS OS, that can be used to leak sensitive data.

All these events must be reported under conditions that include, but are not limited to:

- When the App Kernel is executed
- As requested by the App Kernel and back-end attestation components
- When white-box cryptography or obfuscation methods, implementations, or instantiations are updated

- **2.1 Tamper and Reverse Engineering Protection**

Requirements

8. An App Kernel that fails tamper checks must be prohibited from accepting account data.

- **2.2 Software-Protected Cryptography**

Requirements

1. Cryptographic methods protected primarily by software-based methods must be protected against analysis and abuse.
2. The robustness of the software-based protection mechanisms must be evaluated regularly, against current attack scenarios and vectors.
3. The cryptographic material used in software-based protection mechanisms, such as white-box keys, entropy seeds and nonces, must be changed periodically to prevent cryptographic key compromise.
4. Retired cryptographic material used in software-based protection mechanisms must be securely deleted soon after initial deployment of App Kernel versions using those keys.
5. The cryptographic material used in software-based protection mechanisms must not be used directly for account data or attestation data encryption.
6. Cryptographic keys that are protected primarily with software-based methods must be unique per App Kernel version and instance of the OS store.
7. Cryptographic algorithms and keys used in software-based protection mechanisms must meet security requirements in Section 1.3 [Acceptable Cryptography of this requirements list](#).
8. Cryptographic keys used in software-based protection mechanisms must meet the key management requirements described in Section 1.4 Key Management of this requirements list.

- **2.3 Online Processing**

Requirements

1. All payment processing must be performed online.
2. All components of the COTS Solution must be online and in an operational state before initiating any contactless transactions.

• 2.4 App Kernel Authenticity

Requirements

1. The App Kernel must include methods to allow for the merchant to validate the authenticity of the application through separate channels.
2. Mechanisms must exist to uniquely identify and authenticate each instance of the App Kernel to the back-end monitoring system and the back-end attestation component.
3. The App Kernel must be able to display the current version of the App Kernel software on startup and upon request.

• 2.5 Secure App Kernel

Requirements

1. Documentation must exist and be maintained to detail the following:
 - Protections provided to the App Kernel against tampering, side-channel attacks, fault injection, and reverse-engineering for the various supported COTS Devices and protection methods, such as TEE and white-box cryptography.
 - Details of all areas where functions provided by the App Kernel are executed. This should include the *rich* execution environment of the COTS Device, but may also include other local execution environments, such as a TEE or embedded security processor.
 - Data-flow diagrams that show how the account data is entered, processed, encrypted, and validated within the App Kernel, where the data is transmitted outside of the scope of the App Kernel and any assumptions made about these external connections.
 - Block diagram that indicates where all sensitive data is available in cleartext on the merchant COTS Device. This includes, but may not be limited to, the COTS OS and any TEE or physically separate security-processing elements used. This diagram must indicate the flow of sensitive data through the various elements.
 - Identification of where internal buffers are used and cleared when collecting sensitive data.
2. Documentation must exist and be maintained to identify logical connections between the App Kernel and other components of the COTS Solution.

• 2.5 Secure App Kernel

Requirements

3. The App Kernel must clear sensitive data automatically from the internal buffers and working memory it controls when any one of the following occurs:
 - The transaction completes
 - The transaction terminates for any reason during its normal execution
 - The App Kernel times-out waiting for the response from the Customer or merchant
 - The App Kernel or back-end monitoring system signals a tamper-detection event
 - The App Kernel pauses or stops executing
 - The App Kernel loses its foreground focus.
4. The COTS Devices supported by the App Kernel must provide for secure compilation and/or execution of software applications.
5. The App Kernel must use a validated RNG function.
6. The App Kernel must access only those COTS Device resources required to perform its transaction processing.
7. The App Kernel must access only those information repositories required for transaction processing.
8. The App Kernel must not disable or interfere with any security features provided by the COTS Device.
9. The App Kernel must initiate only those inbound and outbound network communications required to support the application's functions.
10. The App Kernel must encrypt all sensitive data before transmission.

Note: A secure channel cannot be used as the sole security and encryption mechanism. Protocol-level encryption, such as TLS, does not meet this requirement, which is asking for application level encryption.
11. Implementations must ensure that neither cleartext secret nor private cryptographic keys are exposed as cleartext in the COTS OS memory, except for the shortest feasible time while used for a cryptographic operation.
12. The App Kernel must not support PIN or customer biometric entry on the merchant's COTS Device.

• 2.6 Secure Provisioning

Requirements

1. There must be a clear definition of all COTS Devices, including device types, hardware, and operating systems, on which the App Kernel can be executed. See definition of COTS System Baseline in Book 1.
 2. App Kernels must be developed only for supported COTS Devices —the COTS System Baseline.
 3. The App Kernel must be installed and updated only through the OS store.
 4. App Kernel must be protected from unauthorized COTS OS or App Kernel rollback.
 5. Methods must be implemented to protect the OS store interface used to upload the App Kernel and deployed App Kernels from malicious alteration or misappropriation.
- Note:** Security of the OS store themselves are beyond the scope of these requirements.
6. Any required cryptographic keys or other data necessary for first execution must be securely provided to the App Kernel and securely stored.
 7. Secure provisioning must implement the principles of perfect forward secrecy.
 8. App Kernel executables and scripts must be digitally signed, and a signature must be provided to confirm the software author and to guarantee that the application (and any updates) from the OS store have not been altered or corrupted since it was last signed.
 9. Digital signatures used to sign App Kernel executables and scripts must be verified cryptographically prior to use of the application and at required attestation intervals.
 10. The process to generate digital signatures used to sign App Kernel executables and scripts must be performed using dual control on cryptographic keys that are secured within a HSM certified according to a scheme recognized standard.
 11. The App Kernel must be packaged such that its removal results in the deletion of the application and all associated data from the COTS Device.
 12. Code that handles, secures, or otherwise affects the security of the account data read through the NFC interface and processing on the COTS Device must be separated logically from code that is used for other purposes, such as general merchant UI.
 13. Where third-party libraries are used, the App Kernel must be packaged with only those libraries that are used by the App Kernel. The libraries used must not have known and unpatched security vulnerabilities.

• 2.7 *Audit Logs*

Requirements

1. The App Kernel must communicate securely the generated audit logs to the back-end monitoring system.
2. Audit logs generated by the App Kernel must not contain sensitive data.
3. Audit logs generated by the App Kernel must support reconstructing the following events:
 - All user access to sensitive data.
 - All activity that impacts security functions of the App Kernel, such as changes to cryptographic functions, changes to application permissions, and failure or success to establish secure channel with back-end monitoring system.
 - All access to the audit trail managed by or within the App Kernel.
 - Use of and changes to the App Kernel identification and authentication mechanisms.
 - Initialization, stopping, or pausing of the App Kernel logs.
4. All recorded events must capture at least the following information:
 - User identification
 - Type of event
 - Date and time
 - Success or failure
 - Origination of event
 - Identity or name of affected data, system component, or resource
5. All application audit logs must be time-synchronized with the back-end systems.

• 2.8 *Contactless Read of Account Data*

Requirements

1. The App Kernel must reside and execute on the same COTS Device as the NFC interface that is accessed to accept customer account data.
2. The App Kernel must attempt to lock the NFC interface to make sure it cannot be used by other applications during the contactless read from a consumer card or device.
3. The App Kernel must attempt to lock the COTS Device camera to ensure that it cannot be used by other applications during the contactless payment transaction.
4. If the App Kernel detects that it is being run in developer or emulator mode, the application must not be permitted to initiate a contactless payment transaction from a consumer card or device.

• 2.8 Contactless Read of Account Data

Requirements

5. The following events must be detected by the App Kernel during contactless payment transaction , and must result in termination of the session and deletion of all data collected during the transaction, including account data:
 - The App Kernel or back-end attestation component signals a tamper-detection event.
 - The App Kernel detects that it is executing in developer or emulator mode.
 - Another application obscures the App Kernel.
 - The App Kernel pauses or stops executing.
 - The App Kernel loses its foreground focus.
6. The App Kernel must not store account data in persistent storage.
7. The App Kernel must truncate PAN when providing customer receipts, either printed, electronic, or both using methods compliant with requirements defined in section 3.2 of this book.

Note: The NFC interface is to be physically contained within the COTS Device. This standard does not allow for the use of external contactless readers or antennas.

• 2.9 Account Data Encryption

Requirements

1. Account data must be encrypted within the App Kernel as soon as it is received by the application and always prior to transmission outside of the COTS Device. Account data must remain encrypted when transmitted through a secure channel.

Note: A secure channel cannot be used as the sole security and encryption mechanism. Protocol-level encryption, such as TLS, does not meet this requirement, which requires for application-level encryption.

2. Encryption used to protect account data must be performed using a key that is unique for each transaction/communication session.
3. Encrypted account data must be protected from malicious activity.
4. The integrity and confidentiality of the account data must be cryptographically protected wherever they are stored or processed.

Module 3: Back-end Systems — Monitoring/Attestation

• 3.1 COTS System Baseline

Requirements

1. Documentation must exist and be maintained for the following:
 Implemented processes to determine the COTS System Baseline for acceptance of COTS Devices, such as whitelist, blacklist, or hybrid approach.
 How implemented processes account for known and potential vulnerabilities in the COTS Device.
 Clear identification of roles and responsibilities for which aspects of the COTS System Baseline validation process are performed by the App Kernel itself and which are performed by other COTS Device components or execution environments.
 Processes that are demonstrably in use for the discovery and remediation of bugs and vulnerabilities in the COTS Device.
2. Documentation must exist and processes must be demonstrably in use that identify methods used for updating the COTS System Baseline as new threats are identified.
3. The initial COTS System Baseline must include only COTS OS versions that are supported by the OS vendor with security patches.
4. The COTS System Baseline must only include COTS Devices that allow applications to maintain control over NFC interface, hardware, and sensors that can be used to read account data while in foreground.
5. The COTS System Baseline must include only COTS Devices that, at minimum, provide the following features:
 An enforcing mandatory access control framework.
 A trusted boot mechanism that validates the operating system's authenticity.
 Validation of an application cryptographic signature upon loading and execution of that application.
6. The COTS System Baseline must not include "rooted" or "jailbroken" devices.
7. The COTS System Baseline must only include COTS Devices that support secure distribution of the applications.
8. The COTS System Baseline must include only COTS Devices that support secure compilation and execution of the applications.
9. The COTS System Baseline must be validated by the attestation process upon initial startup of the App Kernel.
10. Validation of the COTS System Baseline must be performed during each attestation check performed by the back-end attestation component.

• 3.1 COTS System Baseline

Requirements

11. A documented policy and procedure for assessing changes to the COTS System Baseline must exist and provide details on how:
COTS Devices are added to the COTS System Baseline.
Decisions are made to remove previously acceptable COTS Devices from the COTS System Baseline.
Such changes will affect the parties using these Devices. Therefore, the documentation must also include how communication is handled in these cases.

• 3.2 Attestation Mechanism

Requirements

1. A documented attestation policy that defines health-check rules for the COTS Device and App Kernel attestation component must exist and support the following:
 - Detailed response procedures for health-check results.
 - Health-check rules are maintained and strictly controlled.
 - Health-check rules are reviewed and updated as necessary, at least annually.
2. Implement controls to protect the attestation components and attestation system from reverse-engineering.
3. The attestation component must not be interrupted by payment-transaction processing by the App Kernel.
4. The integrity of the attestation data must be cryptographically protected wherever they are stored or processed.
5. For any attestation data, the solution provider must be able to identify:
 - Where the attestation data originates (in the App Kernel, in a server-based attestation component, remotely, or locally to the consumer device)
 - Identification of the responsible entity or process that is to take action on the attestation data
 - Whether the process to address the attestation data is managed by a third-party provider API with no other privileged access

Note: *If no action is available for any given attestation data, any security dependence on that attestation is considered a residual risk and must be accounted for by the solution provider.*
6. The attestation system must establish mechanisms to ensure attestation data is refreshed and up to date.

• 3.2 Attestation Mechanism

Requirements

7. A set of rules must be defined for analyzing the attestation data and assigning a risk-severity rating for the attestation data that aligns with the attestation policy.
8. Document and establish detailed procedures or automated responses for attestation data. Procedures must accommodate the following, at a minimum:
 - Send an alert to the monitoring system support personnel based on attestation-response severity.
 - Conduct corrective actions for false positives, such as modifying a configuration file hash.
 - Completely block transaction processing in the most significant cases as defined in the attestation policy.
 - Temporarily stop transaction processing.
9. Maintain up-to-date configuration measurements to support attestation criteria.
10. Establish controls to defend against attestation abuses to subvert the prover.
11. Escalation procedures must be defined for undocumented, unexpected, and unknown attestation data.
12. If the attestation system triggers a response in the monitoring system which involves a manual process, such as for a potential tamper event, it must be escalated to the back-end monitoring staff to validate:
 - Written procedures for manually processed events must exist and be demonstrably in use.
 - These procedures must cover events when staff who are relied upon for such determinations are unavailable.
 - Events must be escalated immediately for manual review and then actioned within a short timeframe.
 - Automated systems must be in place to disable any further payment processing from systems when an event has not been actioned for a pre-defined time frame.
13. Requisite qualified staff must implement and interpret attestation health-check rules, associated controls and findings, and the associated training.
14. Retention policy and associated procedures must be defined, documented and implemented for attestation results.
15. Retained attestation results must have a unique ID, date and time stamp and sufficient description to identify the information, attestation component, and attestation system used at that time.
16. Attestation components and attestation system changes must adhere to formal change-control procedures.

• 3.2 *Attestation Mechanism*

Requirements

17. Automated attestation component and attestation system changes must be performed using authorized processes.
18. For manual updates of the attestation system:
 - There must be documented procedures.
 - Deployment of changes to the production environment must adhere to formal change control procedures with evidence that changes were performed as intended.
19. The disabling of the attestation system or a significant loss of its function must result in the disabling of all transaction processing on all solutions that rely on that attestation component and attestation system.

• 3.3 *Type 1 – Attestation of COTS Device*

Requirements

1. Controls must be in place to validate the integrity of the attestation results.
2. Attestation components and the attestation system must not be vulnerable to time-of-check, time-of-use (TOCTOU) attacks.
3. Attestation data must not leak information about attestation components and the attestation system.
4. Attestation data must be unclonable.
5. The back-end monitoring system must be capable of detecting all failures of COTS Device attestation components.
6. The Type 1 attestation component must be provided and maintained to provide up-to-date information about the state of the COTS Device and known vulnerabilities. At a minimum, attestation must check and report the following:
 - Rooted or jailbroken devices, or devices in developer mode
 - Asynchronous rooting and unrooting of the COTS OS
 - COTS platforms support for secure compilation and execution of the applications
 - Modifications or tampering of the COTS OS
 - COTS OS or App Kernel rollback
 - Details on the access and use of the NFC interface for operating systems that allow for the collection of such data
 - Emulator use
 - Use of a hooking framework

• 3.3 Type 1 – Attestation of COTS Device

Requirements

7. The COTS Device attestation must be performed in accordance with the specified attestation policy. At a minimum, the attestation must occur:
 - Initial execution of the App Kernel
 - At App Kernel startup
 - If initiated by the back-end monitoring system or App Kernel attestation component
 - At unpredictable intervals, polled during an online session
 - After changes have been made to the solution or to major configuration files
 - When the App Kernel loses and then regains its Foreground focus

• 3.4 Type 2 – Attestation of the App Kernel

Requirements

1. Controls must be in place to validate the integrity of the attestation results.
2. Attestation components and the attestation system must not be vulnerable to time-of-check, time-of-use (TOCTOU) attacks.
3. Attestation data must not leak information about attestation components and the attestation system.
4. Attestation data must be unclonable.
5. The back-end attestation components must be capable of detecting all failures of App Kernel attestation components.
6. Type 2 attestation components must be provided and maintained to provide up-to-date information about the state of the App Kernel on the COTS device. At a minimum, attestation must include and report on the following:
 - COTS Devices and version
 - Instance of App Kernel
 - Current version of App Kernel
 - App Kernel and configuration modification
 - App Kernel and configuration tamper
 - App Kernel public key modification or tamper
 - App Kernel execution in developer mode
 - App Kernel execution in debug mode

• 3.4 Type 2 – Attestation of the App Kernel

Requirements

- Use of App Kernel code, or part thereof, within either another valid or invalid execution environment, such as through “code lifting” of the entire or partial application to another platform after initialization and personalization
 - State of contactless kernel
 - DRNG function health-check
 - Accessible hardware resources and information repositories
 - Number of transactions performed since the last attestation process
7. Attestation must be performed in accordance with the specified attestation policy. At a minimum, the attestation must occur:
- At initial execution of the App Kernel
 - At App Kernel startup
 - At unpredictable intervals polled during an online session defined by scheme rules
 - If initiated by the back-end monitoring system or App Kernel attestation component
 - After changes have been made to the solution or to major configuration files

• 3.5 Identification and Validation of Components

Requirements

1. The back-end monitoring system must identify all components of the solution.
2. The App Kernel and the attestation component must be identified as authorized and validated by the back-end monitoring system through cryptographic means.
3. The COTS Solution must be able to associate the contactless transaction to a specific merchant/COTS device combination for tracking. If this association is not successful, the transaction must fail.
4. The solution must be able to accept and process attestation data from the App Kernel and take appropriate action based on predefined rules (for example, suspending transactions).
5. The COTS Solution must incorporate a detection system (or feed other detection systems) capable of detecting anomalous and potentially fraudulent activity, including suspicious transactions.

- **3.6 Security of Monitoring and Attestation Environment**

Requirements

1. The back-end monitoring system and attestation system held by an organization, must adhere to PCI DSS according to section 3.2 of this Book.
2. The back-end monitoring system and attestation system must comply with the logical and physical security requirements for scheme defined monitoring and attestation environment basic protections.

Module 4: Back-end Systems — Processing

- **4.1 Security of Account Data Processing Environment**

Requirements

1. Decryption of all account data must occur only in back-end payment processing environments.
2. The back-end payment processing environment must maintain and comply with the requirements outlined in section 3.2 of this Book.

Module 5: Contactless Kernel

- **5.1 Contactless Kernel Functionality**

Requirements

1. The COTS Solution must use a payment brand-approved contactless kernel implementation.
2. The contactless kernel must use a suitable entropy source through an approved RNG or by using the EMV Unpredictable Number (UN) algorithm.

- **5.2 Contactless Kernel Security Requirement**

Requirements

1. Contactless kernel implementation must include security controls to protect its integrity and confidentiality.

- **5.2 Contactless Kernel Security Requirement**

Requirements

2. The remote component of contactless kernel environment must maintain and comply with the requirements according to section 3.2 of this Book.

3.8.2.3. Contactless Payment with PIN entry

Contactless Payment with PIN is a specific option of a COTS Solution which enables the Customer to use their Contactless Payment Application to make a Payment by tapping the Chip Card onto the contactless antenna of the Acceptor's COTS Device by entering their PIN when prompted directly on the COTS Device. No separate component is used as a PIN Entry Device.

This Solution utilises the following key components:

- COTS Device,
- Secure Payment Application on the COTS Device, called App Kernel in the following requirements list,
- Back-end monitoring system.

3.8.2.3.1. Domain 1: App Kernel Core Requirements

Module 1A: Core

• 1A.1 CORE
Requirements
1. App Kernel Software is developed by an entity that either: Meets the requirements of the PCI Secure Software Lifecycle (SLC) standard, (...) 2. A public security-flaw-reporting program is implemented to encourage the finding and reporting of vulnerabilities. 3. A vulnerability assessment has been performed on the App Kernel Software prior to initial assessment and at least once per year thereafter. 4. The App Kernel Software implements chip-based acceptance utilizing the COTS platform for the entry of at least one form of account data. 5. An App Kernel SDK does not pass cleartext sensitive assets to another App Kernel SDK or an App Kernel Application. 6. Where an App Kernel SDK integrates another App Kernel SDK: • The App Kernel SDKs do not share payment acceptance channel resources (such as a COTS-native NFC interface, or connection to an external card reader). • The App Kernel SDKs do not share sensitive assets in a way that assets collected in one App Kernel SDK could be exposed in cleartext within another App Kernel SDK. • - The App Kernel SDK to be integrated does not itself integrate any other App Kernel SDK. • The App Kernel SDK to be integrated is approved and listed as an Isolating SDK, meeting all relevant App Kernel requirements. • The App Kernel SDK to be integrated is provided with clear guidance on how it can be securely integrated into another App Kernel SDK. • The integration guidance to be followed by an App Kernel Application is complete, and includes all security relevant details for all of the App Kernel SDKs to be integrated into the App Kernel Application. • There is no negative impact on the security of either App Kernel SDK. 7. All cleartext card-based payment functionality has been included in the scope of the App Kernel Software assessment. 8. The COTS-based App Kernel Software provides a mechanism to validate its version number.

• 1A.2 *Random Numbers*

Requirements

1. Software development documentation provides details about how the App Kernel Software generates secure random numbers, as required, on all deployed platforms.
2. The App Kernel Software uses an assessed source for the generation of random numbers where the security of assets requires the use of random numbers.
3. When use of a hardware based true Random Number Generator (RNG) on the COTS device cannot be assured, the COTS-based App Kernel Software implements a secure DRNG based on industry standards.
4. DRNGs used by the COTS-based App Kernel Software are regularly (re)seeded with unpredictable values of sufficient entropy, which are protected for confidentiality and integrity.
5. The DRNG used by the COTS- based App Kernel Software uses more than one source of entropy to obtain its seed. Entropy sources include at least one external trusted source, as well as at least one trusted source from the COTS device.
6. The reseeding method used by the App Kernel must add entropy to the DRNG state instead of replacing the existing entropy.

• 1A.3 *Acceptable Cryptography*

Requirements

1. Software-development documentation provides details about acceptable cryptographic processes and operations to be used for security services.
2. All cryptographic processes including hash functions, used security to the solution adhere Appendix C Minimum and Equivalent Sizes and Strengths for Approved Algorithms.
3. Public keys used by the App Kernel Software are protected for integrity and authenticity and are authenticated before they are relied upon for providing security services.
4. Each key has a single unique purpose, and no keys are used for multiple purposes.
5. Key derivation and key check functions are implemented securely.

• 1A.4 Key Management

Requirements

1. Depending on scheme an inventory of all keys used by the App Kernel Software is maintained.
2. Secret or private keys imported to the App Kernel Software that protects their confidentiality integrity and does not solely protections provided by any channel(s) being used.
3. Secret or private keys embedded into COTS-based App Kernel Software implement software protection methods and are not exposed in cleartext.
4. Certificates that exist on the COTS device as part of the COTS OS are considered in scope if used for security purposes.
5. Cryptographic keys are established using a process that ensures the entropy and confidentiality of the key
6. The App Kernel Software supports the use of HSMs for storage and operation of secret and private cryptographic keys in the back-end environments. The App Kernel Software design ensures that cryptographic keys used for PIN-related security functions, and all keys which are not unique per session, will never be exposed outside of a HSM in cleartext.
7. The App Kernel Software implements methods to revoke or otherwise cease the use of compromised cryptographic keys or certificates.
8. Cryptographic keys are not protected with a key of lesser strength.
9. Secret or private cryptographic keys related to account data protection are never stored as cleartext in non- volatile storage within the REE of the COTS device.
10. Cryptographic keys used to encrypt account data on the COTS device are unique per installation of COTS-based App Kernel Software.
11. Secret and private account data encryption keys exposed in the rich execution environment of the COTS device are unique per transaction and implement forward secrecy.
12. The disclosure of a secret or private key used for account data encryption does not leak any sensitive information of the key values for past keys.

• 1A.5 Secure Channels

Requirements

1. Secure channels established by the App Kernel Software are documented.

• 1A.5 *Secure Channels*

Requirements

2. Connections between different physical elements of the implementation are secured through use of a secure channel.
3. Secret or private cryptographic keys used to establish and maintain secure channels between the elements of the App Kernel Software are unique per session except by chance.
4. Logical secure channels implement cryptographic controls for confidentiality, integrity, and authenticity
5. Each secure channel provides mutual authentication to uniquely identify each component prior to the exchange of sensitive assets and protect against MITM and replay attacks.
6. The secure channels supported by the App Kernel Software prevent downgrade attacks.
7. Assets are encrypted and authenticated at the data level during transport, and do not solely rely on the protections provided by any secure channel being used.

• 1A.6 *Third-Party APIs*

Requirements

1. Documentation of any API exposed to third parties exists.
2. APIs exposed by the App Kernel Software do not introduce vulnerabilities to the App Kernel Solution and provide only the defined functionality.
3. APIs exposed by the App Kernel Software secure assets according to their required protection type.

Module 1B: App Kernel Protection

• 1B.1 *Software Security Mechanisms*

Requirements

1. The security mechanisms implemented in the COTS-based App Kernel Software are documented.
2. All assets managed by the App Kernel Software are identified.

• 1B.1 Software Security Mechanisms

Requirements

3. Platform based security mechanisms relied upon by the COTS- based App Kernel Software to protect the assets have been evaluated.
4. Storage locations used by the COTS-based App Kernel Software, including temporary buffers and caches, containing cleartext sensitive assets are cleared immediately after use. The time where a sensitive asset is available as cleartext in memory is limited to the shortest period of time possible.
5. The COTS-based App Kernel Software, including all sensitive assets, is resistant to reverse engineering and covers all security-sensitive areas and sensitive assets.
6. Code and data provisioned to the COTS-based App Kernel Software after installation is transmitted, managed, and stored securely.
7. The COTS-based App Kernel Software prevents the use of compromised platforms which may impact the security of sensitive assets.
8. After initial download and execution, the COTS-based App Kernel Software installation is securely bound to the COTS device on which it is installed.
9. The COTS-based App Kernel Software is developed such that the removal of the COTS-based App Kernel Software results in the deletion of all sensitive assets from the COTS device.
10. The COTS-based App Kernel Software does not contain or expose functionality that may compromise the security of the App Kernel Product, such as a developer or debug mode.
11. When any part of the COTS- based App Kernel Software functionality is implemented outside the REE, that code is also protected against tampering and handles input data securely.
12. Where an Isolating App Kernel SDK is claimed, the App Kernel SDK is implemented in a way that secures the memory and sensitive assets of that SDK from an integrating App Kernel Application.
13. Payment transaction data is securely deleted from the COTS device once it has been transmitted to the payment back-end.
14. The COTS-based App Kernel Software assets and code stored on the COTS device is protected to an attack rating of 25 points using the attack- costing framework in Appendix B.

• 1B.2 Software-Protected Cryptography

Requirements

1. Cryptography protected with software-only means is documented.
2. The software-protected cryptography implementation does not implement operations that expose, or provide access to, cleartext cryptographic keys, key components/shares, or the intermediate results of a cryptographic operation.
3. The software-protected cryptography implementation does not implement unnecessary operations.
4. The software-protected cryptography implementation, where it is used for the protection of secret or private keys embedded into the COTS-based App Kernel Software, is required to be replaced before the estimated time needed to break the implementation. Replacement must include changing of any cryptographic keys, or other assets, within the software protected cryptographic implementation.
5. The software-protected cryptography implementation supports secure key management processes, including secure key generation where key generation is implemented.
6. Cryptographic keys deployed within a software-protected cryptography implementation is not used for encryption of account data or secret/private cryptographic keys during transmission.
7. The software-protected cryptography prevents the extraction of partial or complete cryptographic material to an attack rating of 25 points using the attack-costing framework in Appendix B.

Module 1C: Attestation and Monitoring Software

• 1C.1 Coverage

Requirements

1. Documentation on the coverage of the attestation and monitoring (A&M) exists.
2. The A&M functionality covers the complete lifecycle of the COTS-based App Kernel Software, starting from installation through to decommissioning.
3. The attestation and monitoring (A&M) checks cover the entire security- sensitive COTS-based App Kernel Software code and execution flows that handle assets.
4. The A&M system attests the security of the COTS platform and COTS- based App Kernel Software.

• 1C.2 *Measurements/Detection*

Requirements

1. The information that is collected for the purposes of attestation and monitoring is documented.
2. The A&M data reflects the current state of the COTS-based App Kernel Software, COTS platform, and peripheral devices, in addition to any security relevant changes or measurements that have occurred since the last communication to the A&M back-end.
3. The A&M data sent to the back- end implements methods to ensure the freshness and authenticity of the data.
4. The A&M functionality includes an aspect within the COTS-based App Kernel Software, which performs continual monitoring.

• 1C.3 *Response*

Requirements

1. Documentation exists that describes the actions that can be taken if the attestation and monitoring (A&M) indicates that the COTS-based App Kernel Software, or COTS platform is potentially compromised.
2. Potential tampering events detected by the COTS-based App Kernel Software are reported to the attestation and monitoring (A&M) back-end.
3. It is possible for the COTS-based App Kernel Software to disable processing in the event of tamper indications.
4. The COTS-based App Kernel Software performs an attestation with the A&M back-end upon start up and at least every 60 minutes of continuous operation or suspends further payment processing until such attestation is performed.
5. The COTS-based App Kernel Software that has been suspended or otherwise halted performs an A&M attestation prior to any payment processing.
6. A&M results that may require the cessation of payment acceptance are protected against manipulation during transmission to the payment back-end.

• 1C.4 *Anti-Tampering*

Requirements

1. The protections provided to the attestation and monitoring (A&M) are documented.

- **1C.4 Anti-Tampering**

Requirements

2. The local time source used by the COTS-based App Kernel Software is secured against tampering or alteration.
3. The A&M back-end is able to detect failures in the A&M functions within the COTS-based App Kernel Software.
4. The A&M used by the App Kernel must be resistant to tampering to a pre-defined attack rating.

- **1C.5 A&M Integration Guidance**

Requirements

1. A&M back-end operation security guidance information that explains how the attestation and monitoring (A&M) is securely configured and operated exists.
2. The security guidance information details how to securely integrate the A&M software component into the App Kernel Application.
3. Security guidance information details what A&M features are configurable, the processes for setting or changing these configurations, and how the applicable settings may affect the security and functionality of the overall App Kernel Solution.

Module 1D: Secure Entry and Processing of Account Data

- **1D.1 Account Data Entry and Encryption**

Requirements

1. Documentation exists that details how account data is entered and secured.
2. Account data is encrypted at the earliest possible point.
3. Account data provided from acceptance devices external to the COTS device (such as from a PCI PTS POI or non-PTS approved MSR device) must be provided encrypted and not be decrypted on the COTS platform.
4. The COTS-based App Kernel Software truncates or masks the PAN, using methods compliant to relevant PCI DSS FAQs, when outputting or displaying PAN data that is not encrypted.

- **1D.1 Account Data Entry and Encryption**

Requirements

5. The COTS-based App Kernel Software is able to detect and respond to events that may impact the security of the account data-entry process.
6. The COTS-based App Kernel Software does not store account data beyond the completion of the current transaction process for any purposes other than offline payment processing.

- **1D.2 Use of POI-approved Devices**

Requirements

1. The security guidance document details the secure card readers supported by the App Kernel Software.
2. Any chip accepting devices are approved to the PCI PTS POI requirements.
3. The PCI PTS POI devices are attested as part of the COTS-based App Kernel Software attestation system including validation that the device is operating in an encrypting mode that prevents transmission of cleartext account data to the COTS device.App Kernel
4. Whitelists allowing for the exposure of cleartext data from a PCI PTS POI device are:
 - Cryptographic authentication by the PCI PTS POI device's firmware.
 - Only allow for the output of non-PCI payment brand card data.
 - Documented and justified.

- **1D.3 Magnetic Stripe Data**

Requirements

1. The security guidance document details the MSRs supported by the App Kernel Software.
2. Magnetic-stripe cards are accepted only through readers listed as PCI PTS POI devices or are validated as a Non-PTS Approved MSR.
3. The MSR devices must be attested as part of the COTS-based App Kernel Software attestation system.App Kernel
4. MSR data captured in an App Kernel Solution is not made available in cleartext on the COTS device.App Kernel

- **1D.4** *COTS-Native NFC Interface*

Requirements

1. Information that details the implementation of the COTS-native NFC acceptance method, including the implementation for any contactless kernels, exists.
2. The COTS-based App Kernel Software ensures that the COTS-native NFC interface is not accessed by other applications during a payment transaction.
3. The COTS-based App Kernel Software ensures that the COTS device camera(s) are not accessed by other applications during a payment transaction where presentment of the card may be captured on the COTS camera.
4. When part of the kernel functionality is implemented remotely the connection between the COTS-based App Kernel Software and the remote component must be protected using a secure channel, and relevant requirements of Domain 4 and Domain 5 are met.

- **1D.5** *Manual entry*

Requirements

1. Documentation exists that details the manual entry process and protection methods.
2. Manually entered account data is used only for the purposes of transaction processing.
3. Manually entered account data is protected during entry.
4. The COTS-based App Kernel Software is able to detect events that could impact the security of the entry process.

Module 1E: PIN Entry on COTS Device

- **1E.1** *COTS-native PIN Entry*

Requirements

1. Documentation exists that describes the secure capture and processing of the cardholder PIN.
2. PIN entry is supported only for chip-based transactions.

• **1E.1** *COTS-native PIN Entry*

Requirements

3. The COTS-based App Kernel Software does not leak complete or partial PIN digits. The COTS-based App Kernel Software protects against side channels that use sensors present in the COTS device - e.g., accelerometers and gyroscopes - and screen capture.
4. The COTS-based App Kernel Software protects the PIN digits during entry.
5. The PIN is encrypted into an ISO format 4-PIN block as soon as it is captured, and prior to export from the COTS-based App Kernel Software and COTS device.
6. Attestation functions detecting indications of potential compromise are executed prior to each PIN entry process.
7. The COTS-based App Kernel Software detects when another application overlays, shares the screen during PIN capture, or otherwise could impact the security of the PIN entry process. In case of positive detection of events that could impact the security of PIN entry, the COTS-based App Kernel Software cancels any transaction currently in progress and provides notification of this event to the back-end A&M system.
8. PIN-related data (PIN, PIN related values such as touch locations, PIN block, PIN key) are not stored in the persistent storage and are erased once no longer required.
9. Offline PIN verification is supported only through the use of PCI PTS POI devices which are approved for this purpose.
10. Accessible PIN entry modes are implemented securely.
11. Where PIN entry is performed on a device other than the COTS device:
 - That device is listed as validated to the PCI PTS POI requirements.
 - An approved PIN entry function of the device is used, ensuring the PIN is encrypted into an ISO 9564 compliant PIN block before leaving the PCI PTS POI device.
 - The PIN is not exposed in cleartext on the COTS device.
12. PAN tokens, where used, are cryptographically bound to the PAN.

Module 1F: Offline Payment Transactions

- **1F.1** *Offline Payment Transactions*

Requirements

1. Stored assets, such as account data and transaction results, needed to process offline Payment transactions are encrypted in such a way that the cleartext values cannot be recovered on the COTS device after encryption.
 2. Payment transactions are only accepted in offline mode for a maximum period of 48 hours.
 3. Data stored for offline transaction processing is not accessible to other applications.
 4. Transactions currently underway during a transition to offline processing are either failed in a secure manner or managed in compliance with the requirements of this Section.
-

- **1F.2** *Offline Monitoring*

Requirements

1. The initiation of the offline mode is not available immediately after COTS device reboot. The COTS-based App Kernel Software only works offline after being connected to the A&M back-end.
 2. The COTS-based App Kernel Software A&M component supports a separate attestation policy for offline operation.
 3. The A&M back-end implements controls to mitigate attacks attempting to delete the COTS-based App Kernel Software during offline processing.
 4. The COTS-based App Kernel Software disables payment acceptance after 24 hours without receiving a response from the A&M back-end allowing for the continued processing of transactions.
 5. The results of the A&M security checks that are not dependent on the back-end are resistant to tampering to an attack rating of 25 points using the attack- costing framework in Appendix B. The verification/assessment of these security check results is not delayed until connection to the A&M back-end is re-established.
-

Module 1G: App Kernel Security Guidance

• 1G.1 Security Guidance

Requirements

1. The App Kernel Software is provided with a security guidance document that describes how the App Kernel SDK can be integrated with an App Kernel. The security guidance document is made available to potential integrators and assessment laboratories.
2. The App Kernel Software security guidance document defines the type of App Kernel SDK that is implemented.
3. The App Kernel Software is provided with a security guidance document that describes how the App Kernel Software is to be operated by an Attestation and Monitoring Service provider.
4. The App Kernel Software security guidance document defines an explicit App Kernel SDK boundary.
5. The App Kernel Software security guidance document provides details about how the App Kernel Software code and configuration settings can be updated securely.
6. The App Kernel Software security guidance document provides details about how any software-protected cryptography implementations impact the frequency of App Kernel Application updates.
7. The App Kernel Software security guidance document contains detailed guidance for secure integration that includes configuration flags, usage of APIs, and expected security mechanisms to be applied, as applicable.
8. The App Kernel Software security guidance document details how any secure channels that are able to be managed or configured by the App Kernel Application are secured.
9. The App Kernel Software security guidance document indicates which COTS Platforms (including platform versions such as OS, TEE, and SE) and external devices (such as PCI PTS POI devices or non-PTS Approved MSRs) are supported.
10. If the attestation needs an interaction from the App Kernel Application, the App Kernel Software security guidance document defines the scope, dependencies, and actors of an attestation policy that is used by the App Kernel Solution.
11. The App Kernel Software security guidance document provides details on the required key management processes and operations.
12. Where vendor verification is to be used for the integration of their isolating SDK(s) procedures for the validation of App Kernel Applications exist and are demonstrably in use.

3.8.2.3.2. Domain 2: App Kernel Integration

Module 2A: App Kernel Integration

• 2A.1 Secure App Kernel SDK Integration and Usage

Requirements

1. When an App Kernel SDK is used, the App Kernel SDK is part of a listed App Kernel Product.App KernelApp KernelApp Kernel
2. The App Kernel SDK is integrated with the COTS-based App Kernel Software and other aspects of the App Kernel Product in accordance with the App Kernel Software security guidance.App KernelApp KernelApp Kernel
3. The COTS-based App Kernel Software integrating the App Kernel SDK does not bypass, circumvent, reimplement, or modify any of the security or operational features provided by the App Kernel SDK. All card-based payment functions are provided by the integrated App Kernel SDK(s).App KernelApp KernelApp Kernel
4. The COTS-based App Kernel Software that is integrating the App Kernel SDK does not manage, process, or provide for the input of any sensitive assets, or the COTS-based App Kernel Software is assessed to the requirements of Domain 1.App KernelApp Kernel
5. Attestation functions provided by the App Kernel Software are securely and correctly integrated into the COTS-based App Kernel Software.App KernelApp Kernel
6. The App Kernel Application does not integrate more than two App Kernel SDKs.App KernelApp Kernel
7. The COTS-based App Kernel Software integrating the App Kernel SDK does not implement, or allow for, the decryption of encrypted sensitive assets output by the App Kernel SDK.App KernelApp Kernel
8. The App Kernel Application does not share assets between different App Kernel SDKs.App KernelApp Kernel
9. The App Kernel Application is assigned only the privileges required for its secure operation.App Kernel
10. COTS-based App Kernel Software which implement its own secure channels for connections to third-party payment hosts meet the requirements of Section .App KernelApp Kernel
11. The COTS-based App Kernel Software that integrates the App Kernel SDK is either unable to access any memory and storage locations where App Kernel assets may be processed or reside, or the requirements of Module 2B have been met.

Module 2B: App Kernel Security

• 2B.1 App Kernel Security

Requirements

1. All software in the App Kernel is developed and complies to quality criteria defined in Common.SECC.
2. The App Kernel data and code are protected against tampering (modification), including at runtime, to a pre-defined attack rating.
Protections must include controls to mitigate attempts to perform rollback on the App Kernel or COTS OS.

3.8.2.3.3. Domain 3: Attestation and Monitoring

Module 3A: App Kernel Security Guidance Compliance

• 3A.1 Deployment and Configuration of Back-end Systems

Requirements

1. When an App Kernel Software product is used, the App Kernel Software product is listed on the PCI SSC website.
2. Back-end systems are deployed and configured in accordance with the App Kernel Software security guidance.
3. The Attestation and Monitoring Service provider does not bypass, circumvent, reimplement, or modify any of the security or operational features provided by App Kernel Software.
4. The Attestation and Monitoring Service provider has processes in place to detect when their back-end systems require updates.

Module 3B: Attestation and Monitoring

• 3B.1 *Attestation and Monitoring Policy*

Requirements

1. A documented attestation policy exists and is demonstrably in use.
2. If the App Kernel Software supports offline transactions, the documented attestation policy contains an explicit offline operation mode.
3. If offline operation is implemented, the offline attestation policy is demonstrably in use.
4. Personnel involved in maintaining the operation of the A&M are appropriately skilled.

• 3B.2 *Monitoring*

Requirements

1. There is an overview of the App Kernel Solution being monitored.
2. A documented operational procedure for monitoring exists and is demonstrably in use.
3. The A&M results are made available to the payment processing back- end.

Module 3C: Operational Security

• 3C.1 *Operational Management*

Requirements

1. Where A&M systems are sufficiently isolated from any payment processing systems and Cardholder Data Environment the A&M environment complies with the relevant requirements defined in Appendix A: Back-end Environment Security Requirements
2. When the A&M service provider supports more than one App Kernel Solution, the assets of the different App Kernel Solution providers are segregated.

3.8.2.3.4. Domain 4: App Kernel Software Management

Module 4A: Software Management

• 4A.1 COTS Software Distribution and Updates

Requirements

1. Information about how software is provisioned securely to the supported COTS devices exists.
2. The App Kernel Application is installed and updated exclusively through defined COTS application distribution methods.
3. The interface to each of the implemented App Kernel Application distribution methods is protected.
4. The methods implemented to distribute the App Kernel Application ensure the authenticity of the App Kernel Application prior to initial execution.
5. The App Kernel Application, or the distribution methods used for the App Kernel Application, include methods to allow the merchant to validate the authenticity of the App Kernel Application.
6. The App Kernel Application vendor implements a distribution method that is able to provide secure and timely updates of the App Kernel SDK.

• 4A.2 Key Management Operations

Requirements

1. Procedures to generate, distribute, revoke, and renew keys and certificates follow the App Kernel Software security guidance and are demonstrably in use.
2. Secret or private cryptographic keys used for the security of the implementation in the back-end environments, which are not related to PIN security, are one of the following:
 - Protected through use of HSMs compliant to FIPS140-2/3 level 3, or PCI HSM requirements.
 - Protected through use of HSMs compliant to FIPS 140-2/3 level 2 and deployed in a Controlled Environment (as per the definition in ISO13491).
 - Unique per session and forward secret.
3. Work instructions to operate HSMs exist and are demonstrably in use for each type of HSM used.

4. If the back-end systems include the use of cloud-based HSM's, the cryptographic keys are managed by relevant App Kernel entity, and not accessible to the Cloud HSM provider.
5. Operational key management of secret and private cryptographic keys ensure the confidentiality of the keys throughout their lifecycle
6. Operational management of cryptographic keys ensure the integrity and authenticity of the keys throughout their lifecycle.
7. Management of secret and private cryptographic keys implement the principles of dual control and split knowledge.
8. Mechanisms are in place to identify expired, invalid, and/or revoked certificates, and to prevent continued processing using certificates that have expired or been revoked.

• 4A.3 COTS Baseline and Vulnerability Management

Requirements

1. A penetration test has been performed on the interfaces between the COTS-based App Kernel Software and back- end environments (e.g., A&M, payment processing and/or remote kernel) prior to the validation and listing of an App Kernel Solution or A&M service provider, and at least once per year thereafter.
2. A security-flaw-reporting program is implemented to encourage the finding and reporting of vulnerabilities by internal and external entities.
3. A COTS platform baseline exists.
4. A procedure for managing the COTS platform baseline exists and is demonstrably in use.
5. The baseline COTS OS is regularly and frequently reviewed for vulnerabilities.

• 4A.4 Security of Back-end Systems

Requirements

1. Environments that store, process, or transmit account data comply with the requirements of PCI DSS (including environments implementing remote kernels).
2. Environments performing PIN processing, or that manage PIN related cryptographic keys, comply with the requirements of PCI PIN.
3. Environments that manage account data related cryptographic keys, comply with the requirements of Section .

- **4A.4** *Security of Back-end Systems*

Requirements

4. The A&M environment complies with the requirements in Domain 3 of this standard.

3.8.2.3.5. *Domain 5: App Kernel Solution*

Module 5A: Third-Party Management

- **5A.1** *Merchant Identification and Communication*

Requirements

1. The process of onboarding new merchants is documented. At a minimum, the process must describe how merchant identification is performed.
2. The merchant-onboarding process includes the provisioning of a unique merchant identifier, and the provisioning process of this unique merchant identifier is documented.

- **5A.2** *Support for multiple Entities in the Solution*

Requirements

1. Documentation exists that describes how the operational processes are aligned between the different entities in the App Kernel Solution.
2. The App Kernel solution is supported by the Attestation and Monitoring systems implemented.

3.8.3. Security Requirements for the Capture of Biometrics by the POI

In view of the current market status, this version of Book 4 does not contain Security Requirements for the capture of Biometrics by the POI. However, [EMV SB 185] provides some implementation guidance. The aim is to include the topic in a future version of this book.

3.8.4. 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.
- If the Virtual POI supports multiple applications (for instance, supporting Card Based and non-Card Based Payment Transactions), it *shall* enforce the separation between applications. It *shall* not be possible that one application interferes with or tampers with another application.
- 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 Account Data, but controls how the Account Data is collected from the Customer.
- The acceptor website stores, processes or transmits Account Data.

3.8.5. Physical POI (for MOTO)

When a physical POI is configured and used to process MOTO transactions, the relevant Security Requirements specified in section 3.8.1 apply.

3.8.6. 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 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 S33: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 S34: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 S35: 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.

3.9. 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 Customer 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 24: SECURITY GUIDELINES FOR A CONSUMER DEVICE

3.10. Security Requirements for Automated Teller Machines ATMs

This section defines the minimum applicable security requirements for ATMs.

Req S36: The requirements defined in section 3.8.1.1 using the “PIN Entry” functionality of the Applicability Matrix provided in section 3.8.1.2. apply.

Req S37: The ATM shall support the authenticity of the EPP by cryptographic means. For authentication purposes the EPP shall have a unique identifier which shall be implemented by a secure initialisation process. This identifier shall not be modified or outputted without notice.

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.

Guidance for more detailed security requirements are given in

- [EMV B2] EMV, Integrated Circuit Card Specifications for Payment Systems, Book 2, Security and Key Management
- [EMV E] EMV, Contactless Specifications for Payment Systems, Book E
- [PCI ATM PIN] Transaction Security Point of Interaction Security Requirements (PCI PTS POI), Information Supplement: ATM Security Guidelines

3.11. 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.

3.11.1. 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 Payment Transactions. They contribute to the protection of Account Data confidentiality, authenticity and integrity; for example protection of real-time messages such as PIN translation between security zones for online PIN, to Customer and Account 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.

3.11.2. 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.

3.11.3. 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).

3.11.4. Security Zones

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

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

Examples of HSM Use

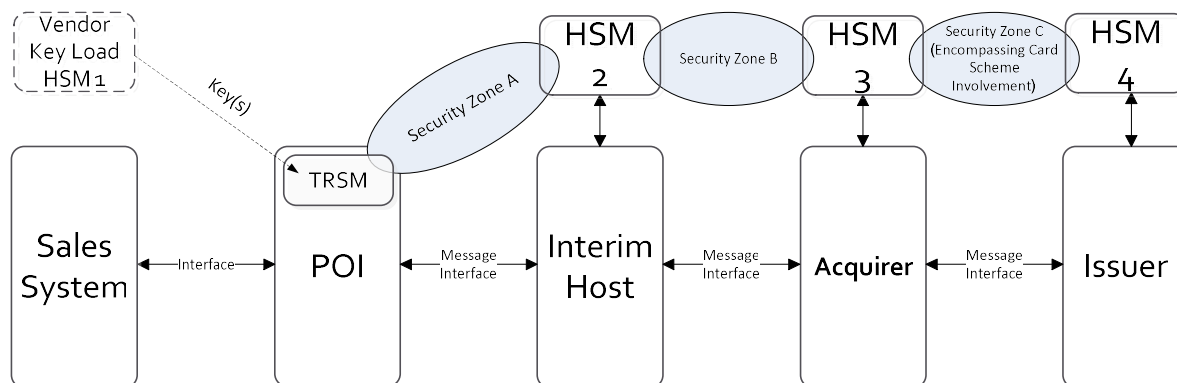


FIGURE 25: EXAMPLES OF HSM USE

3.11.5. 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.

3.11.6. 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.

3.11.7. 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.

3.11.8. 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.

3.11.9. 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.

3.11.10. 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.

3.11.11. 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.

3.11.12. 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.

3.11.13. 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.

3.11.14. 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.

3.11.15. 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.

3.11.16. 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.

3.11.17. 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.

3.11.18. 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.

3.12. Security Requirements for Communication Protocols

3.12.1. Security Requirements for POI to Acquirer Protocols

Authenticity and integrity of data and its confidentiality (as appropriate) in all payment messages are required to protect the financial system. The mechanism for this is to use cryptographic techniques²². 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. Payment Schemes may choose to accept the security provided by a POI to acquirer protocol that meets their specific risk requirements.

3.12.2. Security Requirements for Consumer Device to Virtual POI Protocols

Req S38: The protocol shall establish and maintain 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 S39: 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 S40: The protocol shall support messages to enable the authentication of both the consumer device and the virtual POI.

Req S41: The consumer device (e.g. through the browser) shall display an icon or similar graphical information to enable the Customer to recognise that a secure channel has been established with the virtual POI.

Req S42: During the payment stage, the protocol shall convey information to the Customer on the status of the transaction.

²² EPC342-08 Guidelines on algorithms usage and key management v7.0

3.12.3. Security Requirements for Instant Credit Transfer Protocols

Authenticity and integrity of data and its confidentiality (as appropriate) in all payment messages are required to protect the financial system. The mechanism for this is to use cryptographic techniques.

For Instant Credit Transfer Transactions the security requirements listed in section 3.11.2 "Security Requirements for Consumer Device to Virtual POI Protocols" apply.

Several security protocols are to be considered:

- Protocols to establish session layers
 - Mobile Device to PISP
 - PISP and ASPSP

Further information is provided in [RFC 8446] and in the Federal Office for Information Security (BSI) technical guideline [BSI TR-02102-2].

- Protocols to authenticate the PISP by the ASPSP (e.g. OAuth described in [RFC 6749])
 - Authentication of the PSP against the trustworthy ETSI Certificate [TS 119 495]
- Protocols to authenticate the Customer by the ASPSP
 - Embedded, decoupled, and redirected modes using for instance FIDO.

4. FIGURES AND TABLES

Figure 1: Overview of Card Authentication and Cardholder Verification Method	10
Figure 2: The MCP System Architecture	12
Table 3: The MCP System Architecture – Different approaches	13
Figure 4: The Mobile Application and Mobile Application Cloud Platform	15
Figure 5: Combination of authentication methods / CVMs for e- and m-commerce	21
Figure 6: architecture and components on a typical multi-application Chip Card	30
Table 7: Security Objectives	34
Table 8: EAL4 assurance criteria	35
Table 9: Contactless Cards Security Requirements	36
Figure 10: MCP Application residing within a secure element on a mobile device	37
Table 11: Security Requirements for Secure Elements and MCP applications	42
Table 12: Type of assurance augmentation	43
Figure 13: components for HCE-based Mobile Contactless Payments	43
Table 14: Security Objectives for MCP applications based on HCE	48
Figure 15: Typical examples of locations for storage and processing of (M)RP related data	50
Figure 16: Security Requirements for secure environments and (M)RP credentials	52
Figure 17: Security Requirements for secure environments and (M)RP / Authentication Applications	57
Figure 18: Type of assurance augmentation	58
Figure 19: Example of a TEE model	59
Figure 20: Security Requirements for a TEE and (M)RP related data	61
Table 21: Functionality Description	84
Table 22: Supported Functionalities	89
Figure 23: Example of COTS use	86
Figure 24: Security Guidelines for a Consumer Device	164
Figure 25: Examples of HSM Use	166