RULES FOR THE SECURE MANAGEMENT OF CB ACCEPTANCE SYSTEMS

REMPARTS REFERENCE DOCUMENT

COURTESY TRANSLATION
Please refer to the French version for certified audits

DPE-ESS-REF-2016-006-EN (version 2.0)
April 2019

INTÉGRATEUR D'INNOVATION

DOCUMENT WRITTEN BY:

COMPANY	NAME	ROLE	DATE
SCASSI	Aimeric Pieters	Security Engineer	June 2016
Galitt	Bruno Kovacs Paul Noël Jean-François Henry	Practice Manager Security Consultant Expert Consultant	May 2018
DPE/ESS	Emmanuel le Chevoir	ESS Security Expert	April 2019

DOCUMENT VALIDATED BY:

COMPANY	NAME	ROLE	DATE
PayCert	Didier Duville	Acceptance and Certification Expert	April 2019
DPE/ESS	Mathieu Robert	ESS Manager	April 2019

DOCUMENT HISTORY:

UPDATE	REVISION	DESCRIPTION OF THE CHANGES
June 2016	1.0	Initial version
January 2017	1.2.1	First applicable version of the reference document
April 2019	2.0	Extension of the scope of the reference document (Online PIN) Document restructuring: • Reorganisation and categorisation of requirements. • Presentation of the rules in two levels (main security principles for referencing and detailed requirements for certification). • Specification of eligibility rules for referencing and certification.

Contents

1 INTRODUCTION

1.1 Context and purposes

In response to the recommendations issued by Banque de France during the *Oversight Framework for Card Payment Schemes* mission, CB has carried out an inventory of the management procedures for CB Acceptance Systems and Electronic Payment Servers, covering the vendors and service providers to CB institutions.

Then, CB has implemented a process to reinforce the oversight of CB Acceptance Systems in the field, which aims in particular at:

- Identify and make all CB acceptance parties aware
- Strengthen security about acceptance products and businesses
- Improve the responsiveness of the CB system in the event of fraud

For this purpose, CB has defined a set of security rules covering the various activities in the lifecycle of CB Acceptance Systems and Electronic Payment Servers (e.g., delivery, installation, maintenance, etc.). This is the purpose of the hereby document, that forms the security requirements reference document, also called "REMPARTS[1]".

The purpose of this document is twofold:

1. Defining the main security principles to be respected by parties wishing to commit in the CB Referencing process.
2. Defining the security rules for CB certification of parties involved in the management of CB Acceptance Systems. These rules will be validated by authorised third party auditors and duly recognised by CB and its certification body.

Note: some stages, such as the making of equipment by the vendor, have been excluded from this reference document as they are already subject to explicit security constraints and are audited (e.g., during the CB approval of equipment).

[1] Renforcement Et Maîtrise du Parc d'Acceptation : Résilience, Transparence et Sécurité (*Reinforcing And Monitoring Payment Acceptance: Resilience, Transparency and Security*).

1.2 Referencing and CB certification

CB Referencing and Certification are two distinct procedures that can both be initiated on a dedicated portal[2] maintained by the Groupement des Cartes Bancaires. Details of the CB Referencing and Certification procedures are set out in the document called Referencing and Certification of CB Acceptance Professionals - General Framework [1]

Referencing

CB Referencing is a self-declaration procedure offered to CB Acceptance Professionals. The purposes of referencing aim to:

- Promote the main security principles defined by the Groupement des Cartes Bancaires and applicable to all Acceptance parties,
- Highlight professionals who comply with these security principles through a dedicated portal.

It is worth noting that only a part of the activities specified in the rest of this document is eligible for Referencing. Activities considered as sensitive [Appendix B4] can only be covered by the CB Certification procedure.

However, a transitional regime was implemented in 2015, opening up CB Referencing to all parties until the end of 2020, while they comply. Some sensitive activities may therefore be temporarily covered by CB Referencing until this date.

Certification

The CB Certification is a more formal procedure aiming at ensuring that CB Acceptance Professionals comply with the requirements specified in the rest of this document.
It relies on:

- An audit of the sites where electronic payment activities are performed,
- Certification of the results of this audit by the Groupement des Cartes Bancaires Certification Body.

The purpose of certification aims at:

- Providing strong security assurance, by guaranteeing that a certified professional complies with all the strict rules set out below,
- Highlighting these professionals, in particular with CB members and instructing parties likely to contract with these parties, on a dedicated portal,
- More generally, helping to reinforce the security of the management of the CB Acceptance network as a whole.

[2] https://labelisation.cartes-bancaires.com

1.3 Audience

This document is intended for all parties involved in the REMPARTS scheme:

- Firstly, to service providers working on CB Acceptance Systems and who must comply with the principles and rules set out in the rest of this document.
- To instructing parties likely to contract with these service providers (CB Acceptors, CB Acquirers, CB approved equipment vendors, CB institutions and their affiliated members…) and wishing to be aware of the applicable principles and rules.
- Finally, auditors and certifiers recognised by CB and involved in the CB Certification procedure.

1.4 Document structure

This document is organised as follows:

Chapter 1 Review of the context and presentation of the purpose of this new version of the document, description of the CB referencing and Certification procedures, designation of the recipients, description of its structure and reference elements.

Chapter 2 Description of the activities and application scope of this document reference.

Chapter 3 Definition of the security principles to be followed as part of referencing, organised by activity with a common core.

Chapter 4 Definition of security requirements for Certification, organised by activity with a common core.

Appendices Contact forms with CB, definition of security risks to be remedied and sensitive assets to be protected through the implementation of the hereby reference document, definition of security zones, identification of sensitive activities for which the certification is mandatory, and identification of updates applied to the previous version.

1.5 References, Acronyms, and Definitions

References

[1] CB – Referencing and Certification of CB Acceptance Professionals – General framework, reference DPE-ESS-NTE-2015-002, latest applicable version

[2] CB – Security requirements for Acceptance Systems,
reference DPE-ESS-REF-2018-17, latest applicable version

[3] CB – Security requirements for the implementation of "PIN Online" in the CB system, reference DPE-ESS-REF-2017-15, latest applicable version

[4] Payment Card Industry (PCI) – Data Security Standard (DSS), Requirements and Security Assessment Procedures, latest applicable version

[5] Payment Card Industry (PCI) - PIN Security Requirements, version 2.0 of December 2014 or later

Acronyms

BDK	Base Derivation Key
DMZ	Demilitarized Zone
EMV	EuroPay MasterCard Visa
DAB	Distributeur Automatique de Billet (*Automatic Teller Machine*)
DUKPT	Derived Unique Key Per Transaction
GAB	Guichet Automatique de Banque (*Automated Banking Machine*)
GDG	Gestionnaire de DAB/GAB (ATM/ABM Manager)
HSM	Hardware Security Module
ITP	Identifiant de Terminal de Paiement (*Identifier of Electronic Payment Termina*l)
KSN	Key Serial Number
PA	Point d’Acceptation (*Point of Acceptance*)
PCI	Payment Card Industry
POI	Point of Interaction
PSP	Payment Service Provider
PXE	Preboot eXecution Environment
REMPARTS	Renforcement Et Maîtrise du Parc d’Acceptation : Résilience, Transparence et Sécurité
SA	Serveur d’Acceptation (*Acceptance Server*)
SSH	Secure Shell
STCA	Secure Transactions Certificate Authority
TIK	Terminal Initiation Key
TLS	Transport Layer Security
TMS	Terminal Management System
TPE	Terminal de Paiement Électronique (*Electronic Payment Terminal*)
VPN	Virtual Private Network

Definitions

CB Acquirer

Any Groupement member Payment Service Provider that acquires, processes, and inserts into a system of exchanges with all international "CB" Issuers and Community information and regulation systems, data for transactions made with "CB" Bank Cards or "CB" Approved Cards at a point of acceptance for Acceptors with which it is bound by a “CB” acceptance agreement.

CB Acceptor

Any merchant, any service organisation, any self-employed professional and, generally, any private or public organisation or professional authorised to receive funds in payment by card, and which has signed a “CB” acceptance agreement with its Payment Service Provider.
It operates the Acceptance System.

Anti-passback

A type of access control that prevents any people from entering the same zone twice without first leaving it. Anti-passback prevents the lending of badges between employees. It involves implementing an access control system both at the entrance and exit. An anti-passback system is generally used with appropriate door equipment (access corridor, airlock, etc.).

Certification authority approved by CB

Any certification authority whose organisational and technical features are clearly published in a certification policy already analysed and validated by the Groupement des Cartes Bancaires. At the date of publication of this document, the authorised certification authorities are STCA[3] and the authorities of the main vendors. If any doubt, a professional is requested to contact CB to determine whether an authority is authorised or not.

Vendor

Party supplying hardware components or developing software installed on the acceptance system.
It manufactures, develops, and provides the acceptance systems in compliance with the MPE. As such, it manages the application manager for:

- Providing the acceptance system with the peripheral management and system functions.
- Updating the kernel software.

The vendor is the legal entity that signs the Approval Agreement.

Distributed Electronic Payment

Expression used to refer to an Acceptance System in which the acceptance function is distributed in a system, typically between a Point of Acceptance and an Acceptance Server. In the CB system, the term "Integrated Electronic Payment" is also used to refer to the same system.

[3] STCA: Secure Transactions Certification Authority, autority managed by PayCert http://www.secure-transactions-ca.eu/

PCI reactivation tool

Tools and procedures allowing an organisation, after being authenticated, to put or put back into service a CB Point of Acceptance that has not been initialized or whose "tamper responsive" protection devices were triggered by a sensitive repair operation.

Gateway

Forwarding system located between acceptance systems and an acquirer system; its purpose is to transport the various electronic payment flows. There can be one or more "forwarding systems" between an acceptance system and an acquirer system.

Gateway Provider

Organisation managing the electronic payment platforms transporting the CB transactions (authorisation requests, daily data captures) to the bank servers via an electronic payments' "gateway".

Point of Acceptance (PA)

Point of interaction with the Cardholder, making it possible to display the transaction amount, enter data for CB cards or CB-approved cards into the CB Acceptance System, or the confidential code by the Cardholder when it is required by Acceptance System.

Card holder

A physical person having a contract with an Issuer establishment for the use of a CB card or a CB-approved bank card. The Cardholder's CB card gives access to various services: domestic or international cash withdrawals, domestic or international payments.

Acceptance server (AS)

"Server" type element in an Acceptance System called distributed or integrated which is generally used in major companies. This server focuses the flows from several Points of Acceptance during payment transaction and handles in a centralised way a part of the operations which are required by these transactions.

Acceptance System

The Acceptance System is a device or a set of devices allowing electronic payment transactions to be carried out with "CB" bank cards or "CB" approved bank cards in compliance with the specifications required by the Groupement. It handles the CB interbank payment functions that require links with outside systems or parties. An Acceptance System can consist of a single unit performing all the expected payment functions (equipment which is commonly called an "autonomous electronic payment terminal," or autonomous EPT) or be a complex distributed system composed of an Acceptance Server (AS) and Points of Acceptance (PA).

Terminal Management System (TMS).

Group of servers for managing Points of Acceptance. Three functions are identified:

- Remote change to system settings (parameter downloading).
- Managing and monitoring all the PAs and their lifecycle.
- Remote software update (either system software or CB2A application software).

Sealed[4]

A security device enabling to detect any attempted attack likely to damage the physical integrity of the equipment on which it is placed, whether successful or not.

Secret

Any authentication element giving privileges on a system or an application.

[4] Definition from the ANSSI Technical Guide "for the implementation and use of security seals for information system equipment".

2 APPLICATION SCOPE

This chapter defines all the activities covered by this reference document, and for each activity the corresponding tasks and sensitive assets.

A CB Acceptance professional may implement one or more activities. The activities described in this document are composed of consistent tasks and usually related to the same party. However, the description of the activities may not be exhaustive and for some of them the attachment to a specific type of party may not always correspond to the ground reality.

These gaps can nevertheless be offset by the Certification procedure. The auditors, in agreement with CB and its certifier, will be able to adjust the applicable requirements for a given party, if need be.

ACTIVITY	TYPICAL TASKS RELATED TO THE ACTIVITY
Software development	Development of electronic payment applications capable of processing a transaction in accordance with the functional specifications recognised by CB[5]. Development of application for IT stock management (TMS). Development of applications for electronic payment gateways. Development of applications deployed on an electronic payment server (consolidation of transactions for data capture, applications specific to Electronic Payment Servers, development of applications implementing all or part of EMV level 2, etc.)
Integration	Integration of a hardware module (e.g., card reader, keypad for PIN entry, display...) within equipment used for other non-electronic payment transaction functions (e.g., kiosk, parking lot terminal). Integration of the Point of Acceptance into the logical environment of an Acceptor. Installation or update of initial software (operating system, application) in a CB Point of Acceptance. Generation or retrieving of the secrets required for authentication in secure exchanges (dual keys, Vendor's certificate, and server's certificate) and signature of the public keys by a Certification Authority approved by CB.

[5] Development is carried out through the using of the SDK (*Software Development Kit*) supplied by the Acceptance System Vendor. This SDK contains, among other things, the tools enabling the developer to electronically sign the software approved by CB.

ACTIVITY	TYPICAL TASKS RELATED TO THE ACTIVITY
Preparation / Installation	Receiving an unprepared CB Point of Acceptance. Installation of the necessary software in a CB Point of Acceptance (via TMS, Bluetooth, USB key, RS-232 serial port, etc.). Acquirer Remote configuration of a CB Acceptance System. Producing of merchant's domiciliation card (when required). Installation of the prepared CB Acceptance System at the Acceptor's premises. Remote updating of a CB Acceptance System. Generation or retrieving of the secrets required for authentication in secure exchanges (dual keys, Vendor's certificate, and server's certificate) and signature of the public keys by a Certification Authority approved by CB.
Maintenance	Level-1 maintenance: • Retrieving of a CB Point of Acceptance to be repaired. • Repair of a Point of Acceptance without opening the equipment (no reactivation required). • Return to preparation if necessary[6]. • Packing and shipping of a repaired CB Point of Acceptance. Level-2 maintenance: • Repair of a Point of Acceptance with opening of the equipment (reactivation required). • Checking the integrity of the disassembled Point of Acceptance. • Reactivation of a Point of Acceptance (using a PCI reactivation tool to restore the functions and secrets of a Point of Acceptance). Scrapping of a CB Point of Acceptance (removal from the stock due to the expiration of the PA's approval or inability to repair): • Disassembly of a CB Point of Acceptance to be destroyed. • Storage of sensitive components of a disassembled CB Point of Acceptance. • Scrapping of sensitive components of the disassembled PA.

[6] A maintainer can carry out the preparation activity itself but must then declare this activity and comply with the related principles and requirements.

ACTIVITY	TYPICAL TASKS RELATED TO THE ACTIVITY
Operation	Maintaining in operational condition of CB Acceptance System on behalf of an Acceptor. Management of a centralisation server for data capture (prior to transmission to the Acquirer). System remote configuration. Configuration and implementing communication protection in accordance with the requirements set out in the document reference [2]. Management of electronic payment gateways: • Network / protocol gateways. • Application gateways. TMS management (stock management, security status management, key management, etc.).
Storage / Logistics	Receiving CB Points of Acceptance. Storage of CB Points of Acceptance. Stock removal of CB Point of Acceptance. Packaging and preparation for dispatch of CB Points of Acceptance.
Distribution	Retrieving of CB Points of Acceptance. Bulk transport of CB Points of Acceptance. Disassembly of CB Points of Acceptance by a party in charge of the management of CB Acceptance Systems. *Note: the requirements for the distribution activity do not apply to the unit transport of Points of Acceptance*
Management of a remote keying centre (PIN Online)	Injection or renewal of the PIN encryption key (TIK) in remote Points of Acceptance (usually via a TMS), in accordance with the requirements of the PCI PIN Security standard [5].
Management of key injection centre (PIN Online)	Injection or renewal of the PIN encryption key (TIK) in the Points of Acceptance according to a customisation process in compliance with the requirements of the PCI PIN Security standard [5].
Management of a tran-encryption server (PIN Online)	Remote keying and maintaining in operational conditions a CB-approved HSM that performs the encrypted PIN trans-encryption, in accordance with the requirements of the PCI PIN Security standard [5].

Table 1: Detailed description of the activities covered by REMPARTS

3 SECURITY PRINCIPLES FOR REFERENCING

This chapter defines the main security principles to which a CB Acceptance System operator must adhere in order to be referenced by the Groupement des Cartes Bancaires.
The security principles for referencing are noted as PR_TC_x for the common core and as follows for each additional activity:

- PR_DEV_x for the software Development,
- PR_INT_x for Integration,
- PR_PREP_x for the Preparation/Installation,
- PR_MAINT_x for the Maintenance and scrapping,
- PR_EXPL_x for Operation,
- PR_STOCK_x for Storage/Logistics,
- PR_DIST_x for the Distribution.

For each category of principles, a reference is made to the chapter covering the corresponding security requirements. Therefore, relevant parties have a clear view of the accurate requirements they will need to comply with if they wish to go beyond Referencing and apply for Certification.

3.1 Common security principles

For its referencing, the organisation must first comply with the general security principles described below.

Organisations wishing to prepare for the Certification can refer to the corresponding requirements listed in Chapter Common security requirement to all activities)

PRINCIPLE	DESCRIPTION
PR_TC_1	The organisation has formalised a security policy identifying the areas of covered activities, organising the security of information, the subcontracting security, and listing sensitive assets and their security classification.
PR_TC_2	The organisation has a staff management system suited to the security requirements of electronic payment activities, including the recruitment, training, and follow-up of its employees.
PR_TC_3	The organisation protects its rooms and equipment by implementing physical access monitoring and management. It has defined appropriate security zones for sensitive activities (see Appendix C1).
PR_TC_4	The organisation protects its IT systems. It has a logical security policy combined with operational security measures (control of third-party maintenance, periodic control, secure backups...).
PR_TC_5	The organisation checks the electronic payment software of the Points of Acceptance on which it operates and ensures that there are approved and intact. It reports any suspected fraud or non-compliance to the Groupement des Cartes Bancaires.
PR_TC_6	The organisation has a security incident management procedure covering the stages of detection, reporting, investigation, processing, and remediation. This procedure enables it to prevent the recurrence of incidents.
PR_TC_7	The organisation has formalised and implemented a procedure for the expedition of the Points of Acceptance, so that these equipment are tracked at any time
PR_TC_8	The organisation ensures the continuity of its activities in order to guarantee an operational electronic payment service to its customers.
PR_TC_9	The organisation can prove its compliance with all the principles that apply to its activities and is committed to facilitating the audit process.

3.2 Development

In addition to the common security principles, an organisation with a Development activity must comply with the specific security principles described below.

Organisations wishing to prepare for the Certification can refer to the corresponding requirements listed in Chapter 4.2 (Security requirements for Development activities)

PRINCIPLE	DESCRIPTION
PR_DEV_1	The organisation must maintain a detailed inventory of the electronic payment applications it develops and dispenses.
PR_DEV_2	The organisation controls the security of the source code of its applications. It guarantees its integrity and authenticity, ensures that it has a complete history of modifications and ensures that it is only available to authorised persons. It has a secure backup and archiving process.
PR_DEV_3	The organisation has formalised and follows a secure development methodology and follows good practice associated with the development activity.
PR_DEV_4	The organisation electronically signs all the electronic payment software it publishes and ensures that its customers can verify its integrity and authenticity.
PR_DEV_5	The organisation has formalised and implemented secure management of the cryptographic secrets used to sign and the distribution of its software.

3.3 Integration

In addition to the common security principles, an organisation with an Integration activity must comply with the specific security principles described below.

Organisations wishing to prepare for the Certification can refer to the corresponding requirements listed in Chapter 4.3 (Security requirements for Integration activities)

PRINCIPLE	DESCRIPTION
PR_INT_1	The organisation ensures the organisational security of its activities. It has identified the parties involved in the retrieving and loading of electronic payment software and their roles and responsibilities as well. It keeps an up-to-date inventory of the approved versions of the software to be loaded.
PR_INT_2	The organisation controls the security of the integration procedure. It has implemented a rigorous management of the Point of Acceptance to be integrated, ensures the protection of the confidentiality and integrity of the certificates and TLS keys integrated in the Points of Acceptance and has appropriate security zones (see Appendix C1).

3.4 Preparation/Installation

In addition to the common security principles, an organisation with a Preparation/Installation activity must comply with the specific security principles described below.

Organisations wishing to prepare for the Certification can refer to the corresponding requirements listed in Chapter 4.4 (Security requirements for Preparation/Installation activities)

PRINCIPLE	DESCRIPTION
PR_PREP_1	The organisation has formalised, documented, and implemented a preparation procedure and an installation procedure to control the organisation and operations security.
PR_PREP_2	The organisation informs its clients of the end-of-market and end-of-life dates of the Points of Acceptance on which it operates.
PR_PREP_3	The organisation controls the security of the preparation. It has implemented a rigorous management of the Points of Acceptance to be prepared and has appropriate security zones (see Appendix C1).
PR_PREP_4	The organisation controls the Points of Acceptance after installation and ensures their physical integrity. It has implemented an appropriate incident management procedure and reports to the Groupement des Cartes Bancaires any suspected fraud or non-compliance following version checks (see Appendix AAppendix A:).

3.5 Maintenance

In addition to the common security principles, an organisation with a Maintenance activity must comply with the specific security principles described below.

> *Organisations wishing to prepare for the Certification can refer to the corresponding requirements listed in Chapter 4.5 (Security requirements for Maintenance activities)*

General principles

PRINCIPLE	DESCRIPTION
PR_MAINT_1	The organisation has formalised, documented, and implemented a repair procedure to control the organisation and security of maintenance operations. This procedure enables to identify the in-process Points of Acceptance and the repaired Points of Acceptance.
PR_MAINT_2	The organisation has formalised, documented, and implemented a procedure for remote updating of the Points of Acceptance undergoing maintenance. This procedure must anticipate that a data capture operation is triggered prior to any remote update.
PR_MAINT_3	The organisation has formalised, documented, and implemented a procedure for the scrapping of Points of Acceptance. This procedure details the disassembly modalities and destruction of the Points of Acceptance and provides for the systematic notification of the Vendor.
PR_MAINT_4	The organisation controls the security of its maintenance and scrapping activities. It has implemented a rigorous management of the Points of Acceptance to be repaired or destroyed and has appropriate security zones (see Appendix C1).
PR_MAINT_5	The organisation controls the Points of Acceptance during maintenance operations and ensures their physical integrity. It has implemented an appropriate incident management procedure and reports any suspected fraud to the Groupement des Cartes Bancaires (see Appendix A).

Principles applicable to level 2 maintenance activities

A level 2 (or higher) intervention involves opening the Point of Acceptance and therefore requires the reactivation of PCI security. As such, this activity is much more sensitive than level 1 maintenance and requires special handling by the organisation.

> *Note: Level 2 maintenance activities may be subject to CB Referencing during the transitional phase defined in 2015. This phase will end in December 2020. After this date, these activities will no longer be eligible for CB Referencing and will have to be subject to CB Certification.*

PRINCIPLE	DESCRIPTION
PR_MAINT_6	The organisation must take strict organisational measures to control the operators authorised to perform during a level 2 maintenance.
PR_MAINT_7	The organisation ensures that the PCI reactivation of repaired Points of Acceptance is under control. It has implemented a secure management of the reactivation tools and related secrets and keeps a detailed log of these operations.

3.6 Operation

In addition to the common security principles, an organisation with an Operation activity must comply with the specific security principles described below.

Organisations wishing to prepare for the Certification can refer to the corresponding requirements listed in Chapter 4.6 (Security requirements for Operation activities)

PRINCIPLE	DESCRIPTION
PR_EXPL_1	The organisation ensures the organisational security of its activities. It maintains an inventory enabling it to identify the hardware and software involved in its electronic payment activity. It has formalised and implemented operating procedures covering data capture and remote configuration.
PR_EXPL_2	The organisation, if it operates data capture/remote configuration servers, ensure that it uses TLS certificates enabling the Points of Acceptance to authenticate these servers. These certificates must have been issued by a Certification Authority approved by CB, and must be protected in terms of confidentiality and integrity.
PR_EXPL_3	The organisation ensures the operational security of its activities. it has appropriate security zones (see Appendix C1) and protects communications with the acquisition servers in accordance with the CB security requirements for Acceptance Systems [2].

3.7 Storage/Logistics

In addition to the common security principles, an organisation with a Storage/Logistics activity must comply with the specific security principles described below.

> *Organisations wishing to prepare for the Certification can refer to the corresponding requirements listed in Chapter 4.7 (Security requirements for Storage/Logistics activities)*

PRINCIPLE	DESCRIPTION
PR_STOCK_1	The organisation ensures the organisational security of its storage activities of Points of Acceptance and logistics. It maintains an inventory of the Points of Acceptance and has formalised procedures for entry into stock and removal from stock.
PR_STOCK_2	The organisation ensures the operational security of its activities. It has appropriate security zones (see Appendix C1) and has formalised an incident management procedure for packaging seals.

3.8 Distribution

In addition to the common security principles, an organisation with a Distribution activity must comply with the specific security principles described below.

Organisations wishing to prepare for the Certification can refer to the corresponding requirements listed in Chapter 4.8 (Security requirements for Distribution activities)

PRINCIPLE	DESCRIPTION
PR_DIST_1	The organisation ensures the organisational security of its transport activities of Points of Acceptance. It has formalised the distribution process, from packaging to delivery to the customer.
PR_DIST_2	The organisation ensures the operational security of its activities. It implements measures to protect packaging and seals, and systematically provides shipping notes and receiving reports[7]. It has formalised incident management and notifies the Groupement des Cartes Bancaires without delay in the event of the proven disappearance of a Point of Acceptance.

[7] Only bulk transports are concerned. The transport of a single Point of Acceptance, e.g., during an exchange, is not concerned.

4 REQUIREMENT FOR CERTIFICATION

General information

The security requirements below must ensure that the security risks considered are covered. It particularly refers to the risks of mass compromise (see Appendix B1).

In order to detect a mass compromise, the involvement of all parties in the Acceptance Systems lifecycle is necessary. This particularly consists of:

- Ensure end-to-end traceability of management actions.
- Control inventories, stocks, and follow-up.
- Implement procedures for monitoring compliance with security rules.
- Implement procedures for detecting physical and software integrity breaches.

All of these points can be found in each of the activities covered by the certification reference document.

Preparation of Certification audits

For each applicable requirement, the organisation must have documents or proofs (security device, report, official report, paper record, equipment configuration, IT trace...) showing that they are covered. The auditor responsible for assessing the organisation's compliance with regard to this requirements reference document must be able to consult these elements.

Note: Generally, an organisation that already has security certifications for its environment and its business processes (such as, for example, a PCI-DSS certification [4]) could submit the related certificates so that the results can be reused, if it shows, for example by consulting the corresponding Report Of Compliance (ROC), that the relevant scope is the same and that the requirements covered are of the same nature.

Terminology

- The term "organisation" means the legal entity subject to the requirements for the declared activities.
- The term "equipment rooms" means the rooms hosting the network and server infrastructure.
- Unless otherwise specified, the requirements applying to "IT servers", "electronic payment servers", "IT workstations", "software" and "information system components" only concern the scope specific to the management of CB Acceptance Systems and Electronic Payment Servers.

Details of the requirements

- The requirements for Storage are applicable in all stages of the Acceptance System lifecycle.
- The requirements for transport and shipment are defined in the Distribution activity and are applicable in all stages of the Acceptance System lifecycle.
- Wherever possible, and in order to make easier convergence with other security compliance approaches, the requirements are organised in categories identified in the structured list in Appendix A of ISO 27001 dealing with "Information Security Management".

4.1 Security requirements common to all activities

4.1.1 Security policy

REQUIREMENT	DESCRIPTION
EXI_TC_1	Information security strategy The organisation must initiate an information security strategy supported by its management and communicated to employees. This security strategy must define clear objectives and organisation and be aligned with the overall business strategy.
EXI_TC_2	Risk analysis A risk assessment must be carried out on the security perimeters concerning hardware, workstations, and servers, as well as on the network and telecoms equipment involved in the management of CB Acceptance Systems and Electronic Payment Servers. This document must in particular consider internal and external malicious intent, as well as accidental threats.
EXI_TC_3	Implementation of security policy A security policy must be implemented and must: • Describe the implemented organisation to manage security, in particular the groups, roles and responsibilities of the staff involved in the security of CB Acceptance Systems and Electronic payment Servers during their lifecycle, including the protection of equipment rooms, IT equipment (servers, workstations) and networks. • Describe how the risks previously identified by the organisation are addressed. This risk treatment plan must make it possible to verify that the policy defined is consistent with the risks identified.

4.1.2 Human resources security

These requirements relate to the management of staff involved in the management of CB Acceptance Systems and Electronic payment Servers.

REQUIREMENT	DESCRIPTION
EXI_TC_4	Special monitoring in the recruitment process. The recruitment of operators in charge of sensitive activities (see Appendix B4) in the CB Acceptance Systems life chain and Electronic Payment Servers must be subject to special monitoring. An excerpt from police record (B3) or its equivalent abroad must be requested in order to assess the ability of the recruits to occupy the offered job. The Excerpts from police record must not be kept.
EXI_TC_5	Security charter A security charter, or equivalent corporate document (e.g., a general information notice), must be signed by the staff involved in the management of CB Acceptance Systems and Electronic Payment Servers. This charter must summarise the security requirements of the hereby reference document that staff must follow and comply with. It must also make the parties aware of their responsibilities with regard to the sensitivity of electronic payment activities.
EXI_TC_6	Staff awareness and training A process of awareness-raising and training for staff involved in the management of CB Acceptance Systems and Electronic Payment Servers must be formalised and implemented. Awareness-raising and training sessions must be regular and suited to the type of activity carried out. They must take place at least once a year. The minutes formalising the presence of the staff concerned at these sessions must be signed by the various parties and kept by the organisation.

4.1.3 Assets management

REQUIREMENT	DESCRIPTION
EXI_TC_7	Protection of the organisation's sensitive assets The organisation must have identified and inventoried all its assets, and designated a responsible person for each one, as well as the rules for its use. At least, the assets described as "sensitive assets" referenced in Appendix B3 must be considered.
EXI_TC_8	Inventory of hardware and software platforms The various hardware platforms used (IT and telecommunications) as part of the management of CB Acceptance Systems and Electronic Payment Servers must be identified and inventoried. The inventory of the hardware platforms used must include the configurations deployed (brands and models) and the software used
EXI_TC_9	Information classification policy The organisation must have an information classification policy that takes into account the value, sensitivity and criticality of the relevant assets, as well as the applicable regulations. The appropriate level of classification must be applied to information relating to the management of CB Acceptance Systems and Electronic Payment Servers.
EXI_TC_10	Rules for the use of information and their media The information classification policy must specify, for each level, the rules for using the information and their media. These rules must regulate the distribution, storage and destruction of information and their media. The means for implementing these rules must be identified. Media containing information classified as sensitive must: • Be stored in a secure environment (locked cabinet, dedicated room, etc.). • Be destroyed or erased in a secure manner when no longer used.
EXI_TC_11	Removable media management A strict control procedure must be implemented for removable media (CD/DVD, USB key, etc.) used on workstations and servers involved in the management of CB Acceptance Systems and Electronic Payment Servers.

4.1.4 Access control

4.1.4.1 Management of physical access

REQUIREMENT	DESCRIPTION
EXI_TC_12	Building access control The physical perimeters protecting the buildings must be access-controlled, regulated, and under video-surveillance.
EXI_TC_13	Access to secure zones by the organisation's staff Access to the various security zones must be restricted to authorised staff only, according to the procedures specific to each zone (see Appendix C)
EXI_TC_14	Access to secure zone by third parties Visitors access to security zone must be strictly controlled: • A book mentioning the identity, time and date of arrival and departure of visitors must be kept and retained. • A badge must be issued to each visitor, giving access only to those zones necessary for the purpose of the visit. • Visitors must be accompanied at all times by a duly authorised representative of the organisation.
EXI_TC_15	Procedures for reviewing and updating physical access rights Procedures for reviewing and updating physical access rights to security zones must be implemented and applied. The parties are identified, and reviews must be tracked. Allocation of access rights: • is done as and when required. • is approved by a manager. • complies with the principle of the segregation of duties. • complies with the need-to-know principle. The traceability of rights allocations (requests and validations) must be ensured. Authorisations must be reviewed periodically: • Account review audits are quarterly (checking that accounts have been removed correctly). • Needs audits (updating rights) are half-yearly.
EXI_TC_16	Incident management when unauthorised access is detected If unauthorised access (attempted access, physical intrusion) to a site/location is detected, an incident management procedure must be implemented as defined in § 4.1.12.

REQUIREMENT	DESCRIPTION
EXI_TC_17	Control of physical security installations Regular controls on the proper operation of the security installations (access control unit, access badge management PC) must be carried out and tracked. These controls must be carried out at least once a year.

4.1.4.2 Logical access management

REQUIREMENT	DESCRIPTION
EXI_TC_18	Identification and authentication of staff Any person involved in the management of CB Acceptance Systems and Electronic payment Servers must be identified by name and authenticated in a secure manner (at least using a strong password) when accessing workstations or IT servers. The management of authentication factors must be done according to the best practice. In particular, passwords must be encrypted or stored as non-reversible hashing.
EXI_TC_19	Strong authentication when remote access Any remote access to the information system (via VPN, modem access, etc.), e.g., in the case of on-call or remote maintenance operations, must be strongly authenticated, based on at least two distinct factors (e.g., using a certificate or electronic key and an authentication server).
EXI_TC_20	Procedures for reviewing and updating logical access rights Procedures for reviewing and updating logical access rights to workstations or IT servers involved in the management of CB Acceptance Systems and Electronic Payment Servers must be implemented and applied, particularly when a position is changed or when a staff member leave the organisation.

4.1.5 Security zones

The security zones used as part of this reference document (green 🟩, yellow 🟨, orange 🟧 and red 🟥 zones) are defined in Appendix C1.

REQUIREMENT	DESCRIPTION
EXI_TC_21	Division of the site into security zones The organisation must have overall plans of the various sites involved in the management of CB Acceptance Systems and Electronic Payment Servers and their division into security zones (see Appendix C1). The organisation must ensure that the defined security zones are consistent with the activities carried out therein.
EXI_TC_22	Compliance with security zone constraints The organisation must implement appropriate physical access control and surveillance suited to each zone. The constraints associated with each type of zone are defined in Appendix C1.
EXI_TC_23	Location of equipment room hosting IT servers The equipment rooms hosting the IT servers used to manage the CB Acceptance Systems or which have an electronic payment function must be located in the orange zone 🟧.
EXI_TC_24	Location of physical security management installations The equipment room hosting the security installations (access control centre, access badge management PC) must be located in an orange zone 🟧. The administration tools for these installations are subject to the same constraints.

4.1.6 Security related to IT operation

REQUIREMENT	DESCRIPTION
EXI_TC_25	Remote management of servers and electronic payment equipment A special procedure for the remote management (teleadministration during any support sessions) of the IT servers and network equipment involved in the management of CB Acceptance Systems and Electronic Payment Servers must be implemented if the need has been identified by the organisation. This must: • Describe the roles and responsibilities of the relevant staff, the conditions for action and their traceability. • Identify and inventory the devices and software used to provide protection for this teleadministration (authentication type, protocols, and network, etc).
EXI_TC_26	Periodic review of network equipment configurations A formal process for periodic review of the configuration of network equipment (routers, switches, firewalls, etc.) involved in the management of CB Acceptance Systems and Electronic Payment Servers must be implemented. The traces of the reviews must be kept.
EXI_TC_27	Securing IT workstations related to the operation The fixed operating stations and the mobile workstations having access, through the local networks or remotely via VPN access (in the case of a in-call, for example), to the IT servers involved in the management of CB Acceptance Systems and Electronic Payment Servers must be secure: • Activated, up-to-date antivirus software, configured to carry out analyses of accesses and complete periodic scans that cannot be deactivated by the operator. • Activated firewall software that cannot be deactivated by the operator, which rules must be adjusted to the uses. • The hard disk must have surface encryption and sequestration measures for the keys utilised. • Regular user accounts used on workstations must not have privileges. • The use of software not authorised by the organisation must be prohibited. • A quarterly audit of access rights for these workstations must be carried out. • A secure Operating System (password-protected access, unauthorised start-up from a removable medium) must be used by organisations whose activity of managing CB Acceptance Systems or Electronic Payment Servers is combined with other unrelated electronic payment activities.

REQUIREMENT	DESCRIPTION
EXI_TC_28	Hardening of the operating systems of the involved servers The IT servers involved in the management of CB Acceptance Systems and Electronic Payment Servers must operate with a "hardened" operating system, i.e., consisting exclusively of only the software and hardware elements required for its operation. Hardening an operating system consists at least of: • Removing the unused modules (executables, software libraries, drivers ...) and the unnecessary services (protocols, TCP/IP services, system services, etc). • Removing the unused user accounts and changing the default passwords. • Updating the operating system with the latest security patches, once a month for the most critical ones, and quarterly for the others. • Deactivating the means of remotely booting operating systems (e.g., Ethernet PXE remote boot). • Complying with the hardening rules proposed by the suppliers of commercial operating system or free software. The measures implemented to harden the systems must be documented.
EXI_TC_29	Integrity control of system files and sensitive data Integrity control systems for system files and data must be implemented and executed regularly on the servers involved in the management of CB Acceptance Systems and Electronic Payment Servers. These systems must maintain a detailed log. When an integrity defect is detected, an incident management procedure in compliance with the requirements set out in EXI_TC_53 must be followed.
EXI_TC_30	Software updates A process for regularly updating the operating systems and software installed on portable workstations, IT servers and network equipment involved in the management of CB Acceptance Systems and Electronic Payment Servers must be implemented. The latter must check that all relevant security patches have been applied and that new ones are applied within one month of their release for the most critical ones and within two months for the others.

REQUIREMENT	DESCRIPTION
EXI_TC_31	Maintenance of IT systems All maintenance operations on workstations and IT servers, as well as on network and telecom equipment involved in the management of CB Acceptance Systems and Electronic Payment Servers must be carried out by authorised member of staff. All maintenance operations must be traced.
EXI_TC_32	Deleting data before maintenance A maintenance service launching procedure must be implemented. This must include the secure deleting of sensitive data or removal of storage devices before any equipment is removed from the organisation's premises for maintenance purpose.
EXI_TC_33	Scrapping of IT equipment A procedure for the scrapping of workstations, IT servers, removable media and backup and archive media involved in the management of CB Acceptance Systems and Electronic Payment Servers must be implemented. This procedure must anticipate for the secure erasure or destruction of data storage media.

4.1.7 Backup security

REQUIREMENT	DESCRIPTION
EXI_TC_34	Backup policy A backup policy must be implemented (planning, storage location, application, retention) for the servers involved in the management of the CB Acceptance Systems and the Electronic Payment Servers.
EXI_TC_35	Security level of saved data Backed-up data must have the same level of security as the original data.
EXI_TC_36	Inventory of IT backup media An inventory of the IT media involved in the backup must be carried out and reviewed regularly.

4.1.8 Logging and Monitoring

REQUIREMENT	DESCRIPTION
EXI_TC_37	Activation of the audit logs of the servers and network equipment involved The audit logs of IT servers and network equipment (routers, switches, firewalls, etc.) involved in the management of CB Acceptance Systems and Electronic Payment Servers must be activated.
EXI_TC_38	Analysis of audit logs servers and network equipment The audit logs of an IT server and network equipment protecting it must be analysed at least once a day, so as to identify as early as possible any suspicious or unauthorised action. The analyses can be automated with specialist solutions for analysing audit logs.
EXI_TC_39	Traceability of actions Actions carried out in the IT tools used to manage CB Points of Acceptance or Electronic Payment Servers must be logged. The logs must contain at least the following information: • Date and time of the action • Identity of the user • Type of action • Origin of the action • Data / resources involved • Result of the action (success or failure) Besides, the logging devices of the IT servers and network equipment involved in the management of CB Acceptance Systems and Electronic Payment Servers must trace user access, particularly those with administration privileges.

4.1.9 Communication security

REQUIREMENT	DESCRIPTION
EXI_TC_40	Network mapping A detailed network map of the IS dedicated to the management of CB Acceptance Systems and Electronic Payment Servers must be maintained. It must specify the network interfaces used with external parties (international gateways, business information systems, extranet websites).

REQUIREMENT	DESCRIPTION
EXI_TC_41	Identification of network and business flows The network and business flows necessary for the operation of the servers used as part of the activities covered by the hereby reference document must be clearly identified. It is recommended that a network flow matrix (technical view) and a business flow diagram (synthetic view) be formalised and maintained.
EXI_TC_42	Partitioning of the information system The business components of the information system involved in the management of Acceptance Points and Electronic Payment Servers must be physically and/or logically partitioned from the other organisation networks. If they are to be accessible from a public network, they must be placed in a demilitarised zone (DMZ). Internal local networks must not be accessible directly from public networks.
EXI_TC_43	Protection of exposed interfaces on public networks Interfaces exposed to public networks (Internet, etc.) must be protected by firewalls. These firewalls must be configured to allow only the incoming network flows required by business applications.
EXI_TC_44	Detection/Network intrusion prevention Detection and/or network intrusion prevention devices must be implemented on the public interfaces of the networks involved in the management of the CB Acceptance Systems and Electronic Payment Servers.

4.1.10 Permanent control

REQUIREMENT	DESCRIPTION
EXI_TC_45	Security surveillance A security surveillance process covering the operating systems and software installed on operating stations, laptops, IT servers and network equipment involved in the management of CB Acceptance Systems and Electronic Payment Servers must be implemented and specifically focus on new vulnerabilities and the related security patches.

REQUIREMENT	DESCRIPTION
EXI_TC_46	Internal and external penetration test campaigns Intrusion test campaigns must be carried out regularly on the networks and applications involved in the management of CB Acceptance Systems and Electronic Payment Systems. These tests must enable to determine the organisation's exposure to internal attacks (attack on the organisation's network) and external attacks (attack exploiting public interfaces). These campaigns must result in the production of reports and any related action plans, which will improve the risk analysis maintained by the organisation.
EXI_TC_47	Periodic and permanent control The management processes of CB Points of Acceptance and Electronic Payment Servers must be subject to periodic and permanent controls, as follows: • A permanent control of the compliance, security and validation of the performed operations is carried out by an employee of the organisation with an operational role. The frequency of this permanent control must be adapted to the organisation's activity and the sensitivity of the controlled operations. Permanent control points must be carried out at least once a month. • A periodic review of compliance with procedures and the effectiveness and appropriateness of the permanent control systems is performed by an employee of the organisation who does not have an operational role. The frequency of this control may be quarterly, semi-annually, or annually, depending on the organisation's activity and the sensitivity of the controlled operations. These controls must follow a clear reference framework that is maintained over time and be the subject of reports attesting to the results observed.
EXI_TC_48	Control of the CB approval status of Acceptance Systems A systematic control of the CB approval status of the Acceptance Systems on which the organisation is involved must be carried out. Depending on the status of the Acceptance System, appropriate measures must be taken (see Appendix B2). In particular: • The organisation must make its customers aware of the various deadlines related to the approval of their Acceptance Systems • The organisation must warn the Groupement des Cartes Bancaires as soon as an item of equipment has reached its marketing end-of-date.

4.1.11 Subcontracting management

REQUIREMENT	DESCRIPTION
EXI_TC_49	Subcontractor list The organisation must declare to its clients the list of subcontractors to which it delegates part of its activities and specify the nature of this delegation. This declaration, where necessary, must be included in the organisation's contracts.
EXI_TC_50	Subcontracting legal framework All subcontracting must be legally framed, at least, by a service agreement and a confidentiality agreement. The legal framework of all subcontracting must specify the security requirements and responsibilities transmitted to the subcontractor. An audit clause must also be included in the legal framework agreed between the parties.
EXI_TC_51	Subcontracting audit Audits must be carried out regularly to ensure that the subcontractor has actually implemented the security measures necessary to cover the agreement's security requirements. The audit can be carried out by the organisation's internal control mechanisms or by a third party authorised by the latter.
EXI_TC_52	List of "second level" subcontractors Every so-called "first-level" subcontractor must declare its own list of companies to which it subcontracts a part of its service provision and specify the nature of this delegation. These so-called "second-level" subcontractors must be audited by the first-level subcontractor.

4.1.12 Security incident management

REQUIREMENT	DESCRIPTION
EXI_TC_53	Implementation of a security incident management procedure A security incident management procedure for the management of CB Acceptance Systems and Electronic Payment Servers must be implemented. It must provide for: • Identification of the parties involved in managing incidents. • Management of alerts. • A procedure to find the incident's causes and origins. • A sampling-based control. • A procedure for forwarding information to GIE CB, especially for suspected fraud, according to the procedure described in Appendix A1. • Archival of incidents.

REQUIREMENT	DESCRIPTION
EXI_TC_54	Documentation of the activities carried out for each client In order to facilitate incident response and the information of parties in the event of a compromise of the organisation, a list of the different activities carried out for each client must be kept up to date.

4.1.13 Shipping Points of Acceptance

REQUIREMENT	DESCRIPTION
EXI_TC_55	Shipping conditions (seal and inventory) Before a set of Points of Acceptance is shipped, the organisation must: • Affix a seal onto the Points of Acceptance packages. • Provide a printed and electronic inventory of the Points of Acceptance intended for the recipient(s). This inventory must include the serial numbers of the CB Points of Acceptance.

4.1.14 Business Continuity Management

REQUIREMENT	DESCRIPTION
EXI_TC_56	Guarantee of business continuity Measures must be utilised to ensure continuity of the activities related to the management of CB Acceptance Systems and Electronic Payment Servers. It is recommended that these measures be an integral part of a Business Continuity Plan.

4.2 Development

4.2.1 Assets management

REQUIREMENT	DESCRIPTION
EXI_DEV_1	<u>List of developed electronic payment applications</u> The organisation must keep an up-to-date list of the applications that it develops and that are dedicated to CB Acceptance Systems and Electronic Payment Servers. This list must contain at least: • A unique user ID for each software • The version numbers of each maintained and supported software • A state-of-the-art cryptographic fingerprint to check the integrity of each version of maintained and supported software

4.2.2 Source code security

REQUIREMENT	DESCRIPTION
EXI_DEV_2	<u>Software version management</u> The organisation must have a version management system that ensures that all changes to the code are traceable, that the code has integrity and that access to the source code of applications by developers is authenticated.
EXI_DEV_3	<u>Access to the source code of the software</u> Access to the source code of the software for a CB Acceptance System or an Electronic Payment Server must be restricted to only those contractors who need to know this information. The source code of software programs intended to be embedded in a CB Acceptance System or in an Electronic Payment Server must be deposited on servers hosted at least in an orange zone 🟧. This applies equally to the physical server and to the virtualisation server executing the corresponding virtual machine.
EXI_DEV_4	<u>Backup and archiving of source codes</u> A management procedure for the backups and the archiving of the source code of software programs for CB Acceptance Systems and Electronic Payment Servers must be implemented and applied. These backups must be kept at least in orange zones 🟧.

4.2.3 Development security

REQUIREMENT	DESCRIPTION
EXI_DEV_5	<u>Software development in a secure zone</u> The development of software intended to be embedded in a CB Acceptance System or in an Electronic Payment Server must be performed within the organisation premises: • At least in a yellow zone 🟨 for organisations whose activity is mainly devoted to developing software for CB Acceptance Systems or Electronic Payment Software. • At least in an orange zone 🟧 for the other organisations.
EXI_DEV_6	<u>Security of development environments</u> Development environments must be separated from the rest of the organisation's network. Production, pre-production, acceptance, and test environments must be separate and protected from each other. The production environment must not be accessible from a developer's workstation.
EXI_DEV_7	<u>Secure development</u> The organisation must define and implement a formal process for the secure development of acceptance software. This process must allow: • Avoiding development errors leading to vulnerabilities in applications, • Ensuring the training and maintenance of developers' expertise in the field of secure development, • Identify potential security vulnerabilities from the creation throughout the software lifecycle, relying on a risk analysis methodology and threat modelling
EXI_DEV_8	<u>Functional and secure acceptance</u> The functional (functional tests on the implementation of the specification recognised by CB) and security acceptance of software intended to be embedded in a CB Acceptance System must be carried out by the organisation on the development site at least in a yellow zone 🟨. If the development is carried out in a yellow zone 🟨 (case of an activity mainly dedicated to the development of electronic payment software), the zones can be combined. In this scenario, the technical environments must be separated (logically or physically).

REQUIREMENT	DESCRIPTION
EXI_DEV_9	Separation of tasks The organisation in charge of development must comply with the principle of the separation of tasks. That means that the same contractors do not perform the development, acceptance, and operational support activities (when this service is provided by the organisation in question, "support" means any activity assisting with installation and with incident support).

4.2.4 Signature and software control

REQUIREMENT	DESCRIPTION
EXI_DEV_10	Electronic signature of software The organisation must define and implement a process for electronically signing of its acceptance software, including in particular a description of the tools needed to sign the embedded software. The electronic signature of software must be performed by the organisation on the development site in a suitable zone: • At least in a yellow zone 🟨 for those organisations whose activity is mainly devoted to developing software for CB Acceptance Systems or Electronic Payment Software. • At least in an orange zone 🟧 for the other organisations. The security level of the signature must comply with the best practice.
EXI_DEV_11	Storage of tools and electronic signature keys The tools for the electronic signature of software intended to be embedded in a CB Acceptance System or in a Electronic Payment Server must be stored at least in an orange zone 🟧. The cryptographic secrets necessary for this signature must be kept in the red zone 🟥.
EXI_DEV_12	Control of the software in operation The organisation must provide its customers with the documentation and means to enable them to check the software supplied. Specifically, the organisation's customers must be able to validate the signature of each version supplied to them.

4.2.5 Protection of cryptographic secrets

REQUIREMENT	DESCRIPTION
EXI_DEV_13	Management of cryptographic secrets A process for managing cryptographic secrets (as defined in Appendix B3) must be implemented and provide for: • Management of access to secrets: ○ Identification of authorised staff, ○ Traceability of access ○ Annual review of access rights • Compliance with the principles of mutual control and distributed knowledge • A process for verifying the integrity of secrets • A process for renewing secrets (every two years) • Secret archiving management
EXI_DEV_14	Archiving of cryptographic secrets The archiving of cryptographic secrets must comply with the following rules: • It must be hosted in an internal storage space owned by the organisation. • It must be accessible according to the rules set out in the access management procedure. • The archived data must be encrypted. • The minimum retention period of the archive must be 6 months.

4.3 Integration

4.3.1 Assets management

REQUIREMENT	DESCRIPTION
EXI_INT_1	Inventory of CB Acceptance Points A precise inventory of the CB Points of Acceptance undergoing integration must be kept up to date. This must specify the terminal's serial number, the terminal type and its CB approval status and details of installed software versions. For each device, it must specify its status (undergoing integration, in stock, shipped, etc). For detailed software versions, a level of detail similar to that provided in the "*approval files*" or "ID CB " sheets is expected (software components, checksums). The list of approved hardware, corresponding ITPs and end-of-life dates is maintained by the Groupement des Cartes Bancaires and published on its website

4.3.2 Procedures and responsibilities

REQUIREMENT	DESCRIPTION
EXI_INT_2	Secure loading of software in a Point of Acceptance Firmware, bootloaders, and payment applications to be loaded into a CB Point of Acceptance during its integration must be retrieved and deployed in a secure manner, ensuring their integrity and authenticity: • The integrator must ensure that the software versions deployed are approved by CB, in particular by checking the valuation of the ITP. • The procedure for carrying out this verification must be formalised (parties, means, roles and responsibilities). If a software integrity or authenticity defect is detected, an incident management procedure complying with the requirements set out above (EXI_TC_53) must be followed.
EXI_INT_3	Secrets retrieving process (signing, reactivation) In the integration phase of a CB Acceptance System, a process for retrieving the secrets required for signature validation and PCI reactivation must be implemented and must include: • An integrity verification procedure (parties, resources). • An incident management procedure in the event of integrity defects (parties, resources) complying with the aforementioned requirements (EXI_TC_53)

4.3.3 Security zones

REQUIREMENT	DESCRIPTION
EXI_INT_4	Storage zone for electronic payment software Electronic payment software must be stored on an IT medium or on a server hosted in an orange zone 🟧.
EXI_INT_5	Loading zone for electronic payment software The organisation must load the system software (operating system and EMV modules) and/or electronic payment software (CB approved applications) needed in CB Acceptance System from a hosted system at least in an orange zone 🟧.
EXI_INT_6	Storage zones of Points of Acceptance CB Points of Acceptance must be stored in dedicated rooms located in the yellow zone 🟨. Points of Acceptance awaiting integration and those already integrated must be stored in separate rooms.

4.3.4 Cryptographic measures (TLS certificate security)

REQUIREMENT	DESCRIPTION
EXI_INT_7	Loading of Certification authority Root Certificates Before any use is made of a Point of Acceptance, a root certificate from the certification authority is loaded by the integrator in a personalisation phase of the Acceptance System. Several certification authority root certificates can be installed in a single machine. The certificates may be obtained from the corresponding certification authorities. If necessary, the root certificates can be renewed during a return for maintenance. For traceability purposes, the list of public keys installed must be available for browsing.
EXI_INT_8	Security of CB Point of Acceptance authentication keys If a mutual authentication mechanism of the CB Points of Acceptance with the acceptance system is used, the private key of the customer certificate of the Points of Acceptance is installed by the integrator. Only persons authorised by the integration organisation must be able to handle this private key. This must remain confidential, in particular with regard to the acceptor, the cardholders and any person not authorised by the integrator to work on the Acceptance System. They cannot be exported from the Acceptance System, nor be consulted.

REQUIREMENT	DESCRIPTION
EXI_INT_9	Certificate of the vendor's certification authority The certificate of the vendor's certification authority is obtained from the latter. The public keys are supplied by a certificate complying with CB requirements for the Acceptance Systems security [2]

4.4 Preparation/Installation

4.4.1 Assets management

REQUIREMENT	DESCRIPTION
EXI_PREP_1	Inventory of CB Points of Acceptance undergoing preparation An accurate inventory of the CB Points of Acceptance undergoing preparation must be kept up to date. This must specify the terminal's serial number, the terminal type and its CB approval status and details of installed software versions. For each device, it must specify its status (undergoing preparation, in stock, shipped, etc). For detailed software versions, a level of detail similar to that provided in the "approval files" or "ID CB " sheets is expected (software components, checksums). The list of approved hardware, corresponding ITPs and end-of-life dates is maintained by the Groupement des Cartes Bancaires and published on its website.

4.4.2 Procedures and responsibilities

REQUIREMENT	DESCRIPTION
EXI_PREP_2	Retrieving and secure loading of software in a Point of Acceptance During the preparation of CB Point of acceptance, all the software components (firmware, system software and payment applications etc) must be retrieved and deployed in a secure manner, ensuring their integrity and authenticity: • The preparator must ensure that the software versions deployed are approved by CB, in particular by checking the valuation of the ITP. • The procedure for carrying out this verification must be formalised (parties, means, roles and responsibilities). When a software integrity or authenticity defect is detected, an incident management procedure complying with the requirements set out above (EXI_TC_53) must be followed.
EXI_PREP_3	Procedure for installing Points of Acceptance A procedure for installing CB Points of Acceptance must be formalised, identifying the involved parties and the resources for checking their identity. It must also describe the means of assistance made available to Acceptors (on-site installation, telephone support, etc.).

REQUIREMENT	DESCRIPTION
EXI_PREP_4	Information on the end-of-life date of Points of Acceptance The organisation preparing a CB Point of Acceptance must specify to its client (generally the Acceptor) the end-of-life date of the said Point of Acceptance. It is recommended that this date be included in the PA installation procedure, and that a reference be added to the "acceptance approvals" section on the GIE CB website (the end-of-life dates are specified for each approved item of equipment).

4.4.3 Security zones

REQUIREMENT	DESCRIPTION
EXI_PREP_5	Security zone for the preparation For the organisations whose activity of managing CB Acceptance Systems is combined with other activities unrelated with electronic payment, the preparation of Points of Acceptance must be carried out in at least an orange zone 🟧. For the organisations whose main activity is managing CB Acceptance Systems is the main activity, the preparation of Points of Acceptance must be carried out in at least a yellow zone 🟨.
EXI_PREP_6	Storage zones for the Points of Acceptance CB Points of Acceptance must be stored in dedicated rooms located in the yellow zone 🟨. Points of Acceptance awaiting preparation and those already prepared must be stored in separate rooms.
EXI_PREP_7	Storage zone for the activation tools Activation tools must be stored in a dedicated room or safe in the red zone 🟥.

4.4.4 Cryptographic measures

REQUIREMENT	DESCRIPTION
EXI_PREP_8	Loading of Certification authority root certificates Before any use is made of a Point of Acceptance, a root certificate from the certification authority is loaded by the preparator in a personalisation phase of the Acceptance System. Several certification authority root certificates can be installed in a single machine. The certificates may be obtained from the corresponding certification authorities. If necessary, the root certificates can be renewed during a return for maintenance. For traceability purposes, the list of public keys installed must be available for browsing.

4.4.5 Controld during installation

REQUIREMENT	DESCRIPTION
EXI_PREP_9	Control of the physical integrity of Points of Acceptance Procedures to control the physical integrity of CB Points of Acceptance must be implemented and applied throughout the hardware installation chain (commissioning, initialisation, deployment).
EXI_PREP_10	Management of physical integrity incidents during installation In a physical integrity defect is detected during the installation procedure of CB Point of Acceptance, an incident management procedure complying with the requirements set out above (EXI_TC_53) must be followed.

4.5 Maintenance and scrapping

4.5.1 Assets management

REQUIREMENT	DESCRIPTION
EXI_MAINT_1	Inventory of CB Acceptance Points undergoing maintenance An accurate inventory of the CB Points of Acceptance undergoing maintenance must be kept up to date. This must specify the terminal's serial number, the terminal type and its CB approval status and details of installed software versions and the acceptor's references (company, address, phone number). The inventory of software versions must have a level of detail similar to that provided in the "*approval files*" or "ID CB " sheets (software components, checksums). The list of approved hardware, corresponding ITPs and end-of-life dates is maintained by the Groupement des Cartes Bancaires and published on its website.
EXI_MAINT_2	Retention of information on destroyed Points of Acceptance The organisation must keep (for at least a rolling 12-month period), on the destruction site, the serial number of a destroyed CB Point of Acceptance, and the customer involved (company, address, contact details).

4.5.2 Procedures and responsibilities

REQUIREMENT	DESCRIPTION
EXI_MAINT_3	Reparation of a Point of Acceptance A repair procedure for a CB Points of Acceptance or an Electronic Payment Server must be implemented. This must: • Identify the parties (external or internal) involved in the process and their responsibilities. • List the resources used to carry out this maintenance operation. • Verify that each electronic payment maintenance operation on a CB Point of Acceptance or on an Electronic Payment Server is tracked, by identifying at least the maintainer, the date and the type of maintenance operation carried out. • Identify whether the logging of maintenance operations is carried out by an automatic or manual process.

REQUIREMENT	DESCRIPTION
EXI_MAINT_4	Traceability of maintenance operations The traces of all electronic payment maintenance operations on a CB Point of Acceptance or an electronic payment server must be available for consultation afterwards.
EXI_MAINT_5	Identification of assets by telephone support. Before any phone support action, the maintainer must ask a merchant for the CB Point of Acceptance's serial number or ID of the relevant electronic payment server.
EXI_MAINT_6	Secure retrieval of electronic payment software All software components likely to be loaded by the maintainer in a CB Point of Acceptance (firmware, system software, payment applications, etc.) must be retrieved from the vendor, distributor, or developer in a secure manner, guaranteeing their integrity and authenticity: • The organisation must identify the resources used (download from a server, retrieval from a physical medium, etc.) for the retrieval of the software versions to be loaded and ensure that these means guarantee the authenticity and integrity of the software. • The organisation must ensure that the retrieved software versions are indeed approved by CB, in particular by checking the ITP valuation and recalculating the checksums. • The procedure followed to carry out these checks must be formalised (parties, means, roles and responsibilities). If a software integrity or authenticity defect is detected, an incident management procedure complying with the requirements set out above (EXI_TC_53) must be followed.

REQUIREMENT	DESCRIPTION
EXI_MAINT_7	Control of the software version of the Points of Acceptance During maintenance operations on a CB Point of Acceptance, a procedure for checking the version numbers of the installed software must be followed to ensure their integrity and authenticity: • The maintainer must ensure that the software versions deployed are approved by CB, in particular by checking the ITP valuation. • The maintainer must ensure that no software regression has occurred since the last maintenance of the Point of Acceptance. • The procedure followed to perform these verifications must be formalised (parties, means, roles and responsibilities). If a software integrity or authenticity defect or if a regression software is detected, an incident management procedure complying with the requirements set out above (EXI_TC_53) must be followed.
EXI_MAINT_8	Procedure for remote updating of a CB Point of Acceptance A procedure for remote updating of a CB Point of Acceptance must be formalised. It must identify all the parties and resources required to carry out a remote update. In particular, it must provide for the case of a remote update during operation following a data capture or remote configuration operation of the CB Point of Acceptance.

4.5.3 Human ressources security

REQUIREMENT	DESCRIPTION
EXI_MAINT_9	Personal undertaking for the reactivation of a Point of Acceptance The organisation must have a personal confidentiality undertaking signed by all operators responsible for reactivating the security of a CB Point of Acceptance.

4.5.4 Security zone

REQUIREMENT	DESCRIPTION
EXI_MAINT_10	Zone for support activities Maintenance-related support activities (telephone support) must be carried out in the green zone 🟩.

REQUIREMENT	DESCRIPTION
EXI_MAINT_11	Zone for the storage of Points of Acceptance to be repaired Points of Acceptance awaiting repair must be stored at least in the green zone 🟩.
EXI_MAINT_12	Zone for the storage of repaired Points of Acceptance Repaired Points of Acceptance that have been reactivated must be stored in the yellow zone 🟨.
EXI_MAINT_13	Hosting zone for repair monitoring tools The CB Point of Acceptance repair monitoring tool must be installed on a hosted server (the physical server or the virtualisation server running the corresponding virtual machine) in at least an orange zone 🟧.
EXI_MAINT_14	Zone of PCI reactivation For organisations whose CB Acceptance System management activity is combined with other activities, on-site reactivation of the security of a CB Point of Acceptance must be carried out in the orange zone 🟧. For organisations whose main activity is the management of CB Acceptance Systems, on-site reactivation may be carried out in the yellow zone 🟨.
EXI_MAINT_15	Hosting and storage zone for PCI reactivation tools The tools used for the Reactivation of a CB Point of Acceptance are stored in the red zone 🟥.
EXI_MAINT_16	Zone for disassembly and destruction activities of CB Points of Acceptance If the organisation ensures itself the destruction of the scrapped Point of Acceptance, it must carry out the disassembly and destruction in the yellow zone 🟨.
EXI_MAINT_17	Storage zone for the components of a Point of Acceptance after destruction Storage in the destruction site of non-sensitive components of a scrapped CB Point of Acceptance must be carried out in a green zone 🟩. The storage of sensitive components must be carried out in an orange zone 🟧.

4.5.5 Controls during maintenance

REQUIREMENT	DESCRIPTION
EXI_MAINT_18	Control of the physical integrity of Points of Acceptance before repairing The physical integrity of CB Points of Acceptance must be verified before repairing. In case of doubt about the integrity of the equipment or if a physical compromise is detected, an incident management procedure complying with the requirements set out above (EXI_TC_53) must be followed.

4.5.6 Control of the PCI reactivation

REQUIREMENT	DESCRIPTION
EXI_MAINT_19	Traceability of reactivation operations The organisation must keep an up to date log book (or IT log) of all reactivations carried out, containing the reactivation date and time, the name or identifier of two operators present, and the serial number of the CB Point of Acceptance reactivated.
EXI_MAINT_20	Secret management related to reactivation tools A process for managing secrets (authentication data, cryptographic elements, etc.) related to reactivation tools must be implemented and provide for: • Management of access to the secrets. • Compliance with the principle of mutual monitoring and distributed knowledge. • A secrets renewal process. • Management of secrets archival (storage, access). • A procedure for checking the integrity of secrets.
EXI_MAINT_21	Protection of reactivation tools The tools used for the reactivation of a CB Point of Acceptance must be adequately protected: • Parties with access to the tools must be identified. • Access to or use of the reactivation tools must be subject to double control. A single person must not be able to initiate a reactivation. • Any removal from stock of reactivation tools must be traced. The tools are placed under the responsibility of a named and duly authorised operator (see § 4.1.2). • Reactivation tools must be returned to the secure zone (EXI_MAINT_15) after each use, or at the end of the day at the latest.

REQUIREMENT	DESCRIPTION
EXI_MAINT_22	Compliance with good practice related to reactivation tools The organisation must follow the recommendations and comply with the good security practices (operating mode, security measures to be implemented) described in the documentation of the CB Points of Acceptance reactivation tools provided by the vendor.
EXI_MAINT_23	Incident management in case of compromise of reactivation tools In case of physical or logical compromise of the tools used for the reactivation of a CB Point of Acceptance, an incident management procedure complying with the requirements set out above (EXI_TC_53) must be followed.

4.5.7 Scrapping

REQUIREMENT	DESCRIPTION
EXI_MAINT_24	Formalisation of the scrapping process A process for the scrapping of a CB Acceptance System must be formalised. This must: • Identify the parties (external or internal) involved in the process and their responsibilities. • List the means used to carry out the scrapping operations. • Check that all scrapping operations are traced, identifying at least the maintainer, the date and the nature of the scrapping operation performed. • Identify whether the logging of scrapping operations is carried out by an automatic or manual process. • Check that the traces of all scrapping operations can be consulted afterwards (see EXI_MAINT_2).
EXI_MAINT_25	Notification to the vendor of the Points of Acceptance scrapping If a CB Acceptance System cannot be repaired, the maintainer must notify the vendor of the scrapping of the equipment. The equipment to be destroyed must then be sealed and delivered according to the requirements of the distribution activities.

REQUIREMENT	DESCRIPTION
EXI_MAINT_26	Destruction procedure of Points of Acceptance If the organisation carries out itself the destruction of the Points of Acceptance, it must formalise a procedure for disassembling the CB Points of Acceptance to be destroyed. This procedure must enable to identify the components of the Points of Acceptance considered as sensitive and must guarantee that sensitive data (cryptographic keys, authentication data) are securely deleted prior to the destruction of the Point of Acceptance.
EXI_MAINT_27	Removal from stock of sensitive components stored for destruction The organisation must ensure that the removal from stock of sensitive components from a CB Point of Acceptance is only allowed for the purpose of destruction (no use or resale for spare parts is allowed).
EXI_MAINT_28	Destruction of labels with Point of Acceptance serial numbers The organisation must ensure that all labels showing the serial number of a CB Point of Acceptance are destroyed during its disassembly.
EXI_MAINT_29	Destruction certificate of Points of Acceptance The organisation must provide its customers with a certificate of destruction for each destroyed CB Point of Acceptance. This certificate must specify the serial number of the Point of Acceptance.

4.5.8 Relationships with suppliers

REQUIREMENT	DESCRIPTION
EXI_MAINT_30	Contract agreement with electronic payment software providers Contracts with suppliers who have developed the electronic payment software or distributed the CB Points of Acceptance maintained by the organisation must provide for: • The methods for maintaining in operational condition of electronic payment software, • The provision of documentation and resources allowing to check the authenticity and integrity of software retrieved and deployed in the Points of Acceptance.

4.6 Operation

4.6.1 Assets management

REQUIREMENT	DESCRIPTION
EXI_EXPL_1	Inventory of CB Points of Acceptance An inventory of the CB Points of Acceptance undergoing operation must be kept up to date. This must specify the terminal's serial number, the terminal type and its CB approval status and details of installed software versions and references of the acceptor (company, address, phone details). The inventory of software versions must have a level of detail similar to that provided in the "*approval files*" or "ID CB " sheets (software components, checksums). The list of approved hardware, corresponding ITPs and end-of-life dates is maintained by the Groupement des Cartes Bancaires and published on its website
EXI_EXPL_2	Inventory of electronic payment servers Each organisation involved in the management of electronic payment servers must be able to specify, for each customer (in the contractual meaning of the term), servers it manages (nominal, first or second backup).
EXI_EXPL_3	Formalised data capture/remote configuration process A process for data capture/remote configuration or management of data capture files (CB2A) of a CB Acceptance System must be formalised. The parties are identified and resources to carry out the data capture and remote configuration are provided for.

4.6.2 Security zone

REQUIREMENT	DESCRIPTION
EXI_EXPL_4	Security zone for data capture servers Data capture servers must be located in a room located in the orange zone 🟧.
EXI_EXPL_5	Security zone for Electronic Payment Servers The Electronic Payment Servers must be located in a room in the red zone 🟥.

4.6.3 Cryptographic measures

REQUIREMENT	DESCRIPTION
EXI_EXPL_6	Protection of servers' private keys Private keys associated with server TLS certificates must be protected for confidentiality and integrity. At the very least, strict permissions must be applied to the key files. Whenever possible, it is recommended that the private key must be made non-exportable.
EXI_EXPL_7	Renewal of CB Point of Acceptance private keys When a mutual authentication mechanism of CB Points of Acceptance with a server is operated by the organisation in charge of the operation, a procedure for the renewal of the private keys of CB Points of Acceptance must be implemented. Only persons authorised by the organisation in charge of operations must be able to handle these private keys. They must remain confidential, particularly with regard to the Acceptor and any person not authorised by the operator to work on the Acceptance System.

4.6.4 Organisational security

REQUIREMENT	DESCRIPTION
EXI_EXPL_8	Control of the software integrity and authenticity A procedure for checking the version number and integrity of the software of a CB Acceptance System or an electronic payment server must be implemented: • The operator must ensure that the versions of the software used are approved by CB, in particular by checking the valuation of the ITP. • The procedure followed to carry out this verification must be formalised (parties, means, roles and responsibilities). In the event of a proven compromise of one of the components of the Acceptance System, or where a software integrity or authenticity defect is detected, an incident management procedure complying with the requirements set out above (EXI_TC_53) must be followed.

4.6.5 Relationship with the suppliers

REQUIREMENT	DESCRIPTION
EXI_EXPL_9	Contract with the software developer Contracts with organisations developing software must provide for: • A service for maintaining software in operational conditions. • The provision of documentation and means to carry out software integrity checks.

4.6.6 Compliance with CB security requirements

REQUIREMENT	DESCRIPTION
EXI_EXPL_10	Compliance with CB security requirements for Acceptance Systems As a third-party electronic payment provider, the organisation in charge of the operation must comply with the CB security requirements for the security of Acceptance Systems [2]. These requirements include IT server security, communication security and TLS certificate management.

4.7 Storage/Logistic

4.7.1 Assets management

REQUIREMENT	DESCRIPTION
EXI_STOCK_1	Inventory of stored Points of Acceptance An inventory of stored CB Points of Acceptance must be kept up to date. It must include at least the following information: the number, type, and serial number of the CB stored Points of Acceptance.

4.7.2 Procedures and responsibilities

REQUIREMENT	DESCRIPTION
EXI_STOCK_2	Receiving procedure of Points of Acceptance A receiving procedure for the Points of Acceptance must be formalised. It must at least handle the following items: • A verification of the Acceptance System's CB approval status must be carried out; depending on the Acceptance System's status, suitable measures must be applied (see Appendix B2 Verification of the CB approval status). • The physical integrity of Points of Acceptance must be verified. This consists of verifying the integrity of the seal, or of the packaging if there is no seal. • A Points of Acceptance acknowledgement of receipt must be sent to the shipper by the recipient if the Distributor does not track delivery. In addition, the parties involved in the process of receiving Points of Acceptance must be clearly identified and comply with the related procedure.

REQUIREMENT	DESCRIPTION
EXI_STOCK_3	Stock removal procedure The procedure for removal a CB Point of Acceptance from stock must be formalised and specify the following elements: • A CB Points of Acceptance must not be left unmonitored during removal from stock. During the phase of transit between storage and the destination (e.g., preparation room), the Point of Acceptance must remain under the control of a logistics provider. • Depositing and retrieving CB Points of Acceptance on the storage zones must be carried out by different people. For instance: ○ The logistics providers deposit the non-prepared CB Points of Acceptance in the dedicated storage zones. ○ The preparers take the non-prepared CB Points of Acceptance from the dedicated storage zones. In addition, the parties involved in the procedure for removal Points of Acceptance from stock must be clearly identified and comply with the related procedure.

4.7.3 Security zones

REQUIREMENT	DESCRIPTION
EXI_STOCK_4	Security zone for management tools and stock identification The management tools and stock identification of CB Points of Acceptance must be installed on a server hosted in an orange zone 🟧.
EXI_STOCK_5	Security zone for the storage of Points of Acceptance For all organisations: • Storage of Points of Acceptance must be carried out in the yellow zone 🟨. • Points of Acceptance must be separated by status (unprepared, prepared, scrapped). For organisations whose CB Acceptance Systems management activity is combined with other activities unrelated to electronic payment, the storage zones of the Points of Acceptance must be different from those dedicated to the organisation's other activities.

4.7.4 Security incident management

REQUIREMENT	DESCRIPTION
EXI_STOCK_6	Management of incidents related to the physical integrity of packaging An incident management procedure must be defined and followed in the event of a suspicion of a deliberate attack on the physical integrity of the seals or packaging of the Points of Acceptance upon receipt. This procedure must comply with the requirements set out above (EXI_TC_53). It must also formalise the reporting of alerts with the shipper.

4.8 Distribution

4.8.1 Procedures and responsibilities

REQUIREMENT	DESCRIPTION
EXI_DIST_1	Transport process for CB Points of Acceptance A transport process for CB Points of Acceptance must be formalised from the retrieval of the PA through to the delivery to the recipient. This must specify: • The physical protection measures implemented. • The means implemented to ensure the detection of a non-authorised opening of the packaging. • The parties involved in the transport process. • The delivery conditions for the merchant's domiciliation card.

4.8.2 Operational security

REQUIREMENT	DESCRIPTION
EXI_DIST_2	Integrity of the seals and packaging During the transport, the integrity of CB Point of Acceptance must be secured. Checks of the integrity of the seals or packaging must be carried out at each stage of the transport.
EXI_DIST_3	Information to be mentioned on shipping notes The shipping notes must comprehensively mention the list of serial numbers of the CB Points of Acceptance transported. The list must be provided by the shipper in compliance with security requirements set out in EXI_TC_55
EXI_DIST_4	Delivery traceability Each stage of the delivery process must be tracked and be the subject of a report (collection, verifications, and delivery), in order to make it possible to detect the disappearance of an Acceptance System.

4.8.3 Security incident management

REQUIREMENT	DESCRIPTION
EXI_DIST_5	Management of incidents in case of disappearance of Points of Acceptance An incident management procedure must be defined and followed in case one or more Points of Acceptance disappear during transport. This procedure must comply with the requirements set out above (EXI_TC_53). It must also formalise the reporting of alerts to the shipper and the recipient.

4.9 Activities related to Online PIN

The Online PIN activities mentioned in Chapter 2 are as follows:

- Management of a remote keying centre (Online PIN)
- Management of a key injection centre (Online PIN)
- Management of a trans-encryption server (Online PIN)

If either of these activities is carried out, then the following requirement must be met:

REQUIREMENT	DESCRIPTION
EXI_PIN_1	Compliance of Online PIN management The management of an Online PIN activity by the Acceptance System must comply with the international requirements defined in the PCI PIN Security standard [5]. For an understanding of the general framework on the implementation of PIN Online in the CB system, please do refer to the dedicated CB reference document [3].

APPENDIX A: FORWARDING OF INFORMATION TO THE GROUPEMENT DES CARTES BANCAIRES

Two types of notifications are specified in this document's requirements: the notification of a **suspected fraud**, and the notification of an **unauthorised operation** order in the CB system (end of deployment date, end of life date). The related notification forms are given below.

A1. Procedure concerning suspected fraud

When the professional has to carry out operations on all or part of an acceptance systems, if he or she detects an element that could generate a fraud (Point of Acceptance modified abnormally, theft of a pallet of points of acceptance, software not validated) and considers that this is not an isolated action that could be an unintentional operator error, he or she must send an e-mail to labelisation@cartes-bancaires.com using the following format:

Notice of suspected fraud	
Observation date	
Identification of the notifying professional	
Organisation's corporate name	
Address	
Reference / Certification No	
Technical information about the Acceptance System concerned	
Vendor	
Model	
ITP	
Software version	
Detailed observations	

This notification only covers fraud relating to payment means (hardware or software modifications to an acceptance system, intrusion/malware on an acceptance system, theft of the software signature secret, large-scale theft of acceptance systems).
It does not cover commercial fraud (improper invoicing, mis-selling, ...).

A2. Procedure concerning non-compliance arising from end-of-life checks

When the professional has to install a CB Acceptance System whose approval status is "end of sales/deployment" or "end of life" (other than a standard exchange in the event of a breakdown), or for any maintenance operation carried out on a CB Acceptance System whose approval status is "end of life", he or she must send an e-mail to labelisation@cartes-bancaires.com using the following format:

Notification of operation on a CB Acceptance System past its end-of-life	
Operation date	
Identification of the notifying professional	
Organisation's corporate name	
Address	
Reference / Certification No	
Technical information about the Acceptance System concerned	
Vendor	
Model	
ITP	
Software version	
Type of operation carried out	
Commercial information	
Customer name	
Customer contact data	
Point of sale name	
Point of sale address	

APPENDIX B: CONSTRAINTS

B1. Security risks to be covered

The following table summarises the threat scenarios that have been considered by the Groupement des Cartes Bancaires (GCB), coverage of which is provided by the security requirements.

Physical threats

PHY_MOD-01 Adding booby-trapped hardware (skimming device) on a CB Acceptance System, without removing it (e.g., adding a device to capture magnetic stripe/cardholder data)

PHY_SUB-01 Replacing a CB Point of Acceptance by another that is booby-trapped or obsolete/vulnerable

PHY_PIE-01 Booby-trapping a CB Acceptance System by modifying its hardware components (adding a device to capture magnetic stripe/cardholder data or deactivate the security PCI)

PHY_PIE-02 Reactivating, in an unauthorised way, the security PCI of a previously booby-trapped CB Point of Acceptance using the PCI reactivation cards/tools supplied by the vendor

PHY_PIE-03 Stealing the PCI reactivation cards/tools supplied by the vendor, to be able to reactivate the security PCI of a previously booby-trapped CB Point of Acceptance

PHY_PIE-04 Gaining access to CB Acceptance System components (motherboards, complete terminals) intended to be scrapped or modified, to be able to retrieve actual parameter setting elements making it possible to make official terminals work again or to test ways of bypassing the security PCI

Logical threats

LOG_MOD-01 Modifying the settings of a CB Acceptance System to cause data capture on a hacked server

LOG_MOD-02 Modifying the settings of a CB Acceptance System to cause an update on a hacked TMS server loading obsolete/vulnerable software

LOG_SUB-01 Replacing one of the software programs intended to be installed in a CB Acceptance System by another that is booby-trapped or obsolete/vulnerable (stored locally or in a TMS)

LOG_SUB-02 Replacing in a CB Point of Acceptance (via a USB key, RS-232 serial port, etc) an installed software program by another that is booby-trapped or obsolete/vulnerable

LOG_VLN-01 Remotely exploiting a security vulnerability in a software program installed in a CB Point of Acceptance (e.g., via IP or GPRS)

LOG_PIE-01 Booby-trapping the source code of a software program intended to be installed in a CB Acceptance System (e.g., adding a function to capture magnetic stripe/cardholder data or deactivate the security PCI)

LOG_PIE-02 Stealing the software signature cards/tools supplied by the vendor, to be able to sign the software programs intended to be installed in a CB Acceptance System

B2. Verification of the CB approval status

The document "*Referencing and Certification of CB Acceptance Professionals - General Framework*" [1] describes each stage of the lifecycle of an Acceptance System, as well as the general obligations therein. This chapter specifies the rules for operations at each stage of the lifecycle.

Stages in the lifecycle of an Acceptance System

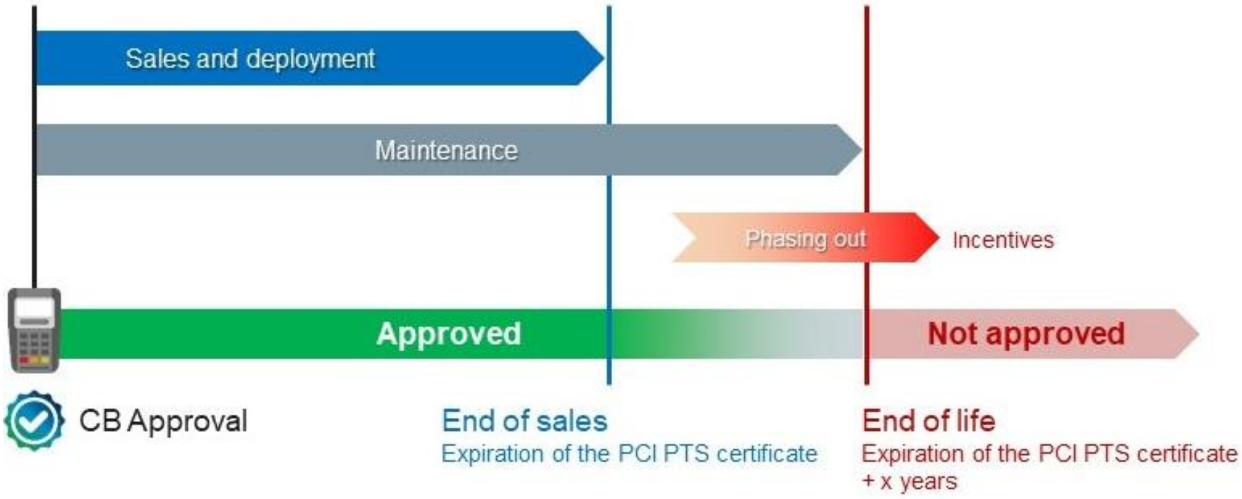


Figure 1 – Approval status of CB Acceptance System

Status between "*End of sales/deployment*" and "*End of life*"

When a Point of Acceptance can no longer be marketable (expiration of PCI PTS certificate). No new agreement can be signed by the Vendor, one of its Distributors/Retailers or an Integrator. It can no longer be deployed as well.
However, as long as a Point of Acceptance has not reached the end-of-life date of its approval, it can be:

- Maintained/repaired as-is or replaced by an identical model.
- Updated to a software version that has a current approval.
- Scrapped

During this phase, phased recall operations must be encouraged by all the parties.

"*End of life*" Status

Any CB Point of Acceptance at the approval end of life can no longer be maintained and must be phased out and scrapped. CB has specified incentive measures (see document [1]) to avoid the maintenance of Acceptance System versions that are obsolete from a security point of view.

Responsibilities

STATUS	PARTIES
End of sales	Vendors, Distributors / Retailers, Integrators
Between end of deployment and end of life	Vendors, Integrators, Preparers, Distributors/Retailers, Acceptors, Acquirers, Maintainers
End of life	All the parties are concerned by this verification.

Obligations for the Acceptance Professional

The acceptance professional's permanent verification measures (see § 4.1.10) must include provisions for verifying that the CB Acceptance Systems managed, their configuration and their embedded software comply with the CB approval.
In particular, any installation of a CB Acceptance System whose status is "end of sales/deployment" must be notified to the requester of the service and to CB using the form defined in Appendix A2 (other than a standard exchange in the event of a breakdown).
This also applies for any maintenance operation carried out on a CB Acceptance System whose CB approval status is "end of life". This CB Acceptance System must then be replaced as quickly as possible by a CB Acceptance System whose approval is current.

B3. Sensitive assets

Cryptographic secrets

The security of an Acceptance System relies on several cryptographic secrets. These secrets are used by the functions protecting sensitive data, such as identification and authentication data, certificates, card data and the various software embedded in its components.

Cryptographic secrets are mostly keys or double keys, used for:

- Signing of embedded software, and therefore securely identifying electronic payment software and their version,
- Mutually authenticate the Acceptance Systems,
- Enable PCI reactivation of a Point of Acceptance,
- Implement PIN Online encryption.

Embedded electronic payment software

There are different types of software embedded in an acceptance system. We can particularly distinguish:

- Firmware, in particular that embedded in security modules (PED, EPP, HSM),
- Bootloaders,
- System software (OS, EMV module, etc.),
- French electronic payment software (CB approved applications).

Electronic payment software for servers

Electronic payment software deployed on servers used in the management and operation of an acceptance system is subject to the requirements of this reference document. At least, the following software is considered to be a sensitive asset to be protected:

- Software for electronic payment servers (distributed electronic payment, m-acceptance, etc.)
- Software for remote updating of the Acceptance Systems
- In stock management software
- Software for data capture and remote configuration
- DUKPT management and TIK renewal software
- PIN trans-encryption software.

PCI reactivation tools

PCI reactivation implements a security mechanism that allows the acceptance system to return to service under PCI compliance conditions. This reactivation can only be performed during a Level 2 maintenance operation.

The mechanism is defined by the Acceptance System Vendor and relies on a software or hardware device, referred to in this document as the "PCI reactivation tool".

The PCI reactivation tool must be protected in terms of availability, confidentiality, and integrity under the responsibility of the party that the vendor has supplied.

PIN encryption keys

The keys used for PIN encryption or trans-encryption ensure the confidentiality and integrity of the PIN when it is transported from the Point of Acceptance to the Issuer, which validates its value prior to authorise or not the payment transaction.

These keys must therefore be adequately protected at all times during their lifecycle, whether they are loaded into a Point of Acceptance or into an HSM in the acceptance chain.

B4. Sensitive activities

By their very nature, sensitive activities are not eligible for referencing. Organisations carrying out these activities must therefore undergo REMPARTS certification.

These activities are listed in the table 2.

Note: Any party who holds operational PCI reactivation tools, even if they are not used as part of their declared activities, is subject to the certification process.

ACTIVITY	SENSITIVE OPERATIONS
Maintenance	Level-2 maintenance: • Repair of a Point of Acceptance with opening of the equipment (reactivation required). • Checking the integrity of the disassembled Point of Acceptance. • Reactivation of a Point of Acceptance (using a PCI reactivation card or PCI reactivation tool to restore the functions and secrets of a Point of Acceptance).
Management of a remote keying centre (Online PIN)	Injection or renewal of the PIN encryption key (TIK) in remote Points of Acceptance (usually via a TMS), in accordance with the requirements of the PCI PIN Security standard [5].
Management of key injection centre (Online PIN)	Injection or renewal of the PIN encryption key (TIK) in the Points of Acceptance according to a customisation process in compliance with the requirements of the PCI PIN Security standard [5].
Management of a tran-encryption server (Online PIN)	Remote keying and maintaining in operational conditions a CB-approved HSM that performs the encrypted PIN trans-encryption, in accordance with the requirements of the PCI PIN Security standard [5].

Table 2 – Identification of sensitive activities with mandatory certification

APPENDIX C: SECURITY ZONE CONFIGURATIONS

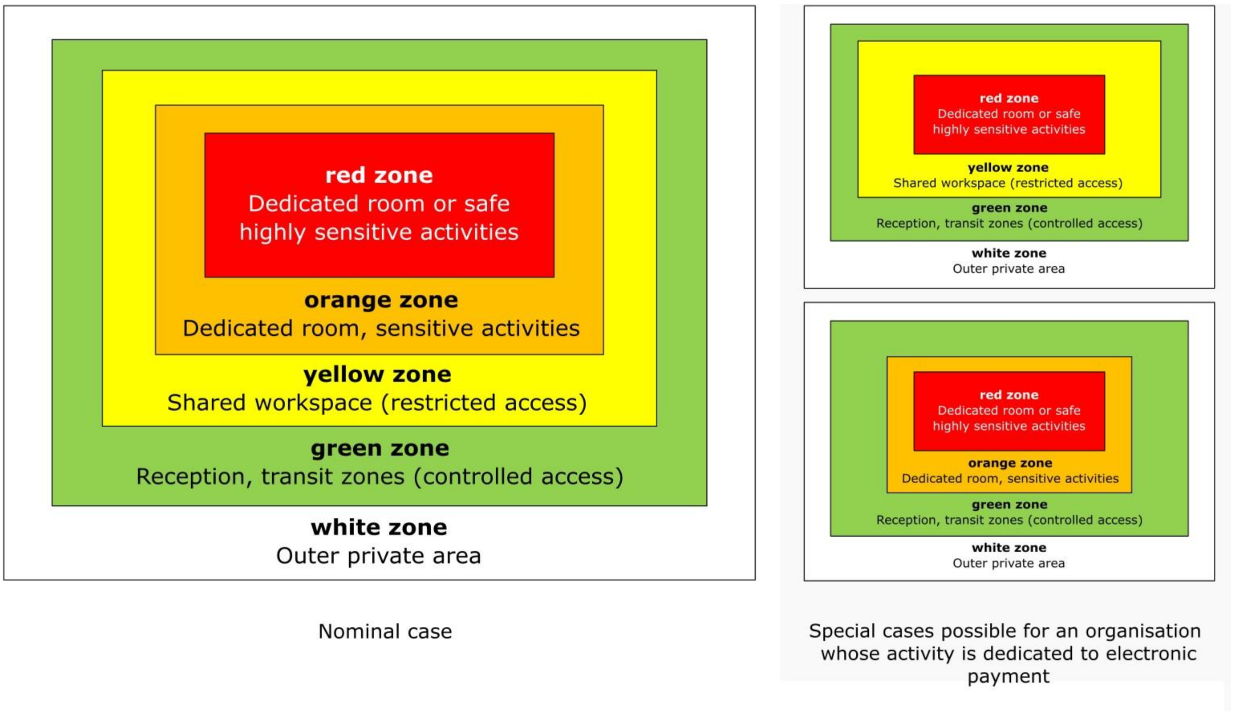
C1. Definition of security zone

This paragraph describes the different types of activity zones defined by the Groupement des Cartes Bancaires CB for the certification reference document.

The activities and related security requirements are specified in the chapter on requirements (see chapter 4).

It should be noted that a distinction is made between organisations whose main activity is the management of CB Acceptance Systems or Electronic Payment Servers and those for whom this is only part of their activity.

Figure 2 shows the different security zones that are defined in this chapter. Examples of possible layout configurations are shown in Appendix C2.


red zone
Dedicated room or safe
highly sensitive activities
orange zone
Dedicated room, sensitive activities
yellow zone
Shared workspace (restricted access)
green zone
Reception, transit zones (controlled access)
white zone
Outer private area
red zone
Dedicated room or safe
highly sensitive activities
yellow zone
Shared workspace (restricted access)
green zone
Reception, transit zones (controlled access)
white zone
Outer private area
red zone
Dedicated room or safe
highly sensitive activities
orange zone
Dedicated room, sensitive activities
green zone
Reception, transit zones (controlled access)
white zone
Outer private area

Nominal case

Special cases possible for an organisation whose activity is dedicated to electronic payment

Figure 2 – Layout of security zones

Green zone

- Access is controlled.
- The emergency exits and delivery docks must be under video-surveillance 24/7/365.
- The emergency exits must have an alarm system operating 24/7/365.
- When not in use, the delivery docks must be closed, locked, and have an alarm system operating.

Yellow zone

- The access doors from the green zone 🟩 to a yellow zone 🟨 must have restricted access controlled by badge at the entrance, active 24/7/365. Restricted means that the list of people authorised to access the yellow zone 🟨 is more limited than the green zone's 🟩.
- Easily accessible windows (ground floor, patio...) in the yellow zone 🟨 must be equipped with an intrusion detection device.

Orange zone

- For the organisations whose activity of managing CB Acceptance Systems is combined with other activities, access to an orange zone 🟧 must only be possible after going through a yellow zone 🟨.
- For the organisations whose activity of managing CB Acceptance Systems is the main activity, access to an orange zone 🟧 must only be possible after going through a green zone 🟩.
- Access doors to an orange zone 🟧 must have restricted access control on entry and exit, active 24/7 ("*anti-passback*" system). Restricted means that the list of persons authorised to access the orange zone 🟧 is more limited than that of the access zone (green zone 🟩 or yellow zone 🟨).
- The corridor and access doors to offices of the orange zone 🟧 must be under video-surveillance 24/7/365

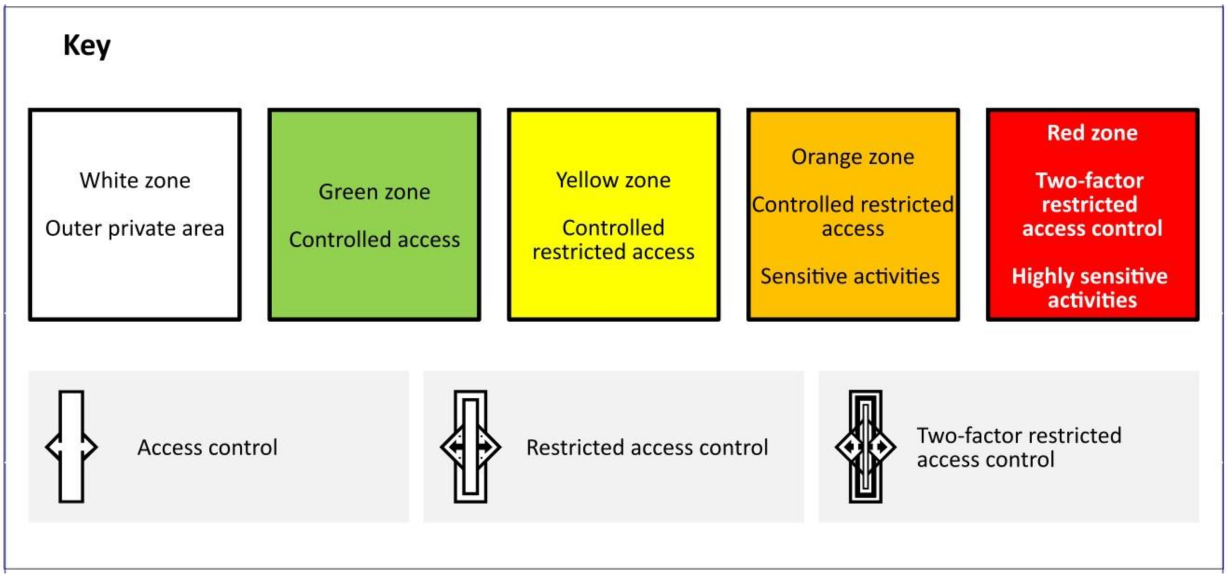
Red zone

- For the organisations whose activity of managing CB Acceptance Systems is combined with other activities, access to a red zone 🟥 must only be possible after going through an orange zone 🟧.
- For the organisations whose activity of managing CB Acceptance Systems is the main activity, access to a red zone 🟥 must only be possible, at least, after going through a yellow zone 🟨.
- A red zone 🟥 may be a safe:
  - The latter must resist break-in attempts.
  - It must consist of a steel door unit, a leaf made of several thicknesses of steel plates, and locks reinforced with at least 3 side attachment points to resist break-in attempts.
- If the red zone 🟥 is a room,
  - Access doors must be equipped with a two-factor restricted access control system on entry and exit, active 24/7 ("*anti-passback*" system). Access doors must also be reinforced to limit the risk of intrusion. It means that the list of authorised persons to access the red zone 🟥 is more limited than that of the orange zone 🟧.
  - There must be no less than two people in this zone.
  - Access doors to this zone must be equipped with a 24/7 opening delay device with an audible alarm triggering device.
  - The access doors to this zone must be secure and an alarm must be triggered in the event of attempted break-ins.
  - The walls, floors and ceilings surrounding the offices and corridors in this zone must be reinforced (resistant materials such as blocks, bricks or walls/tiles made of concrete or steel) or equipped with devices making it possible to detect drilling 24/7/365 (e.g., vibration sensors, acoustic sensors).
  - The offices and corridors in this zone must not have windows that can be accessed easily from outside (ground floor, patio ...).
  - The offices and corridors in this zone must not have direct access to the outside of the building (emergency exits, light shafts ...).
  - The offices and corridors in this zone must have a system for detecting physical intrusions active 24/7/365 (e.g., presence of a guard, space sensors, detection of movements by video-surveillance, infrared barriers, glass breakage sensors, acoustic sensors)
  - The emergency exits of this zone must correspond to the access doors for this zone and must have a secure emergency opening device making it possible to deactivate the two-factor access control in order to evacuate the zone.

C2. Mapping and examples

The following diagrams give examples of possible security zone configurations for the activities described in the hereby reference document.

Note: All contexts are not shown.


Key
White zone
Outer private area
Green zone
Controlled access
Yellow zone
Controlled restricted access
Orange zone
Controlled restricted access
Sensitive activities
Red zone
Two-factor restricted access control
Highly sensitive activities
Access control
Restricted access control
Two-factor restricted access control

Cases where electronic payment activities are combined with other activities

This paragraph gives layout examples of physical zones for organisations whose activities are not solely related to the Electronic Payment.

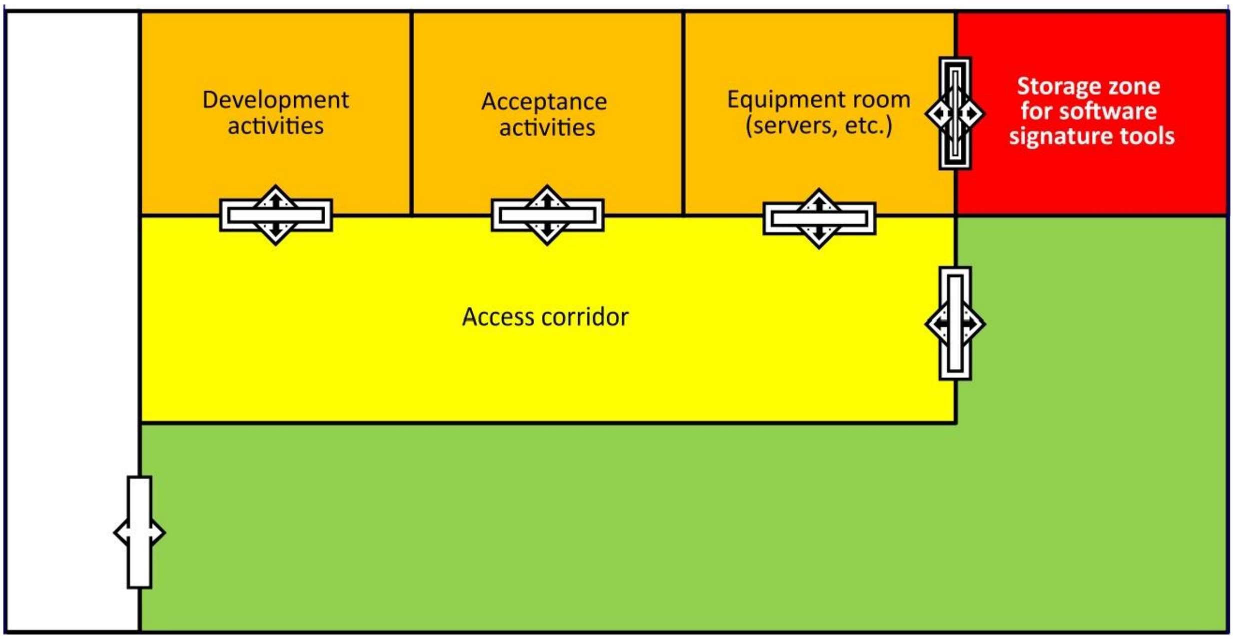

Development activities
Acceptance activities
Equipment room (servers, etc.)
Storage zone for software signature tools
Access corridor

Figure 3 – Layout example for a Developer (combined activity)

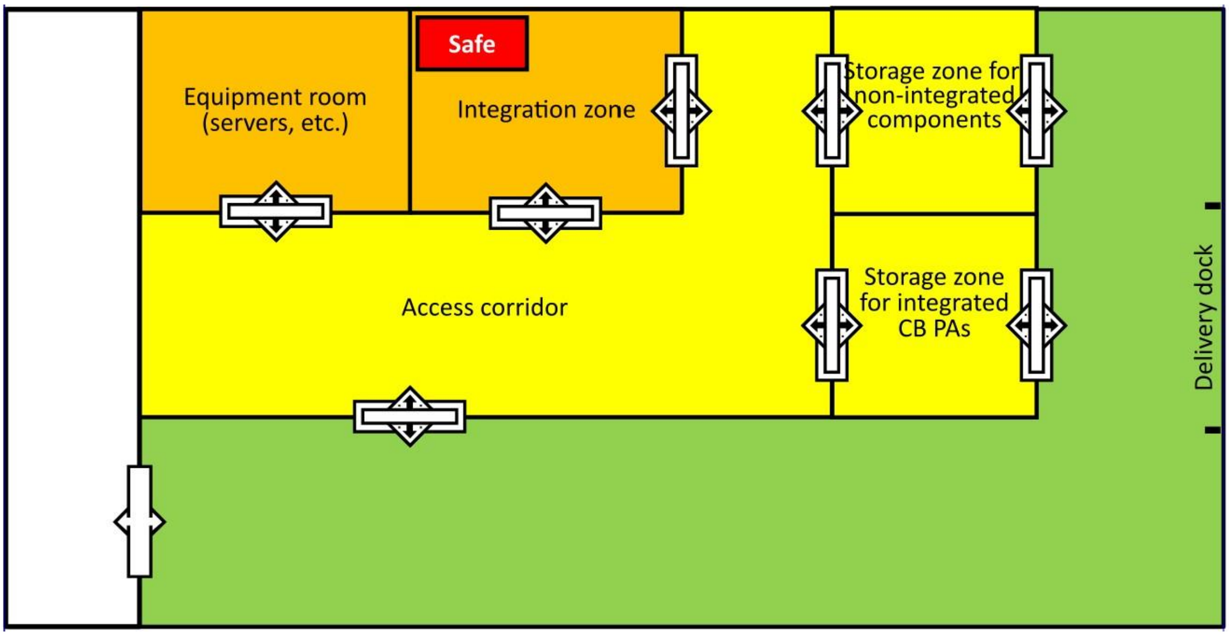

Safe
Equipment room (servers, etc.)
Integration zone
Storage zone for non-integrated components
Storage zone for integrated CB PAs
Access corridor
Delivery dock

Figure 4 – Layout example for an Integrator

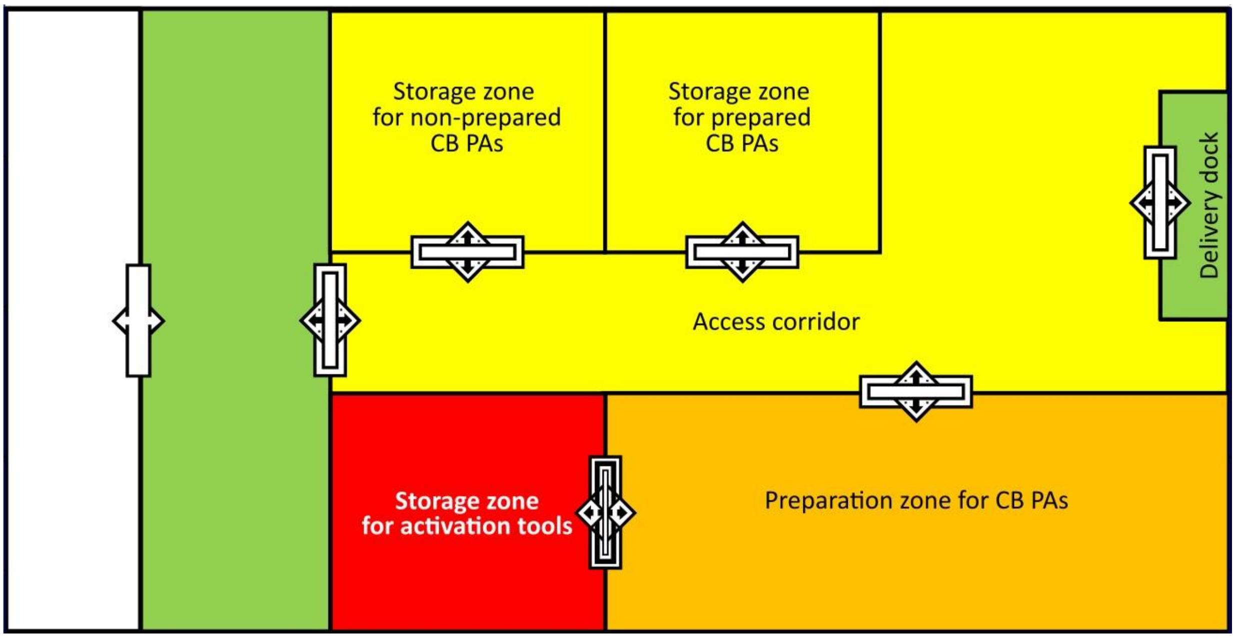


Figure 5 – Layout example 1 for a Preparer

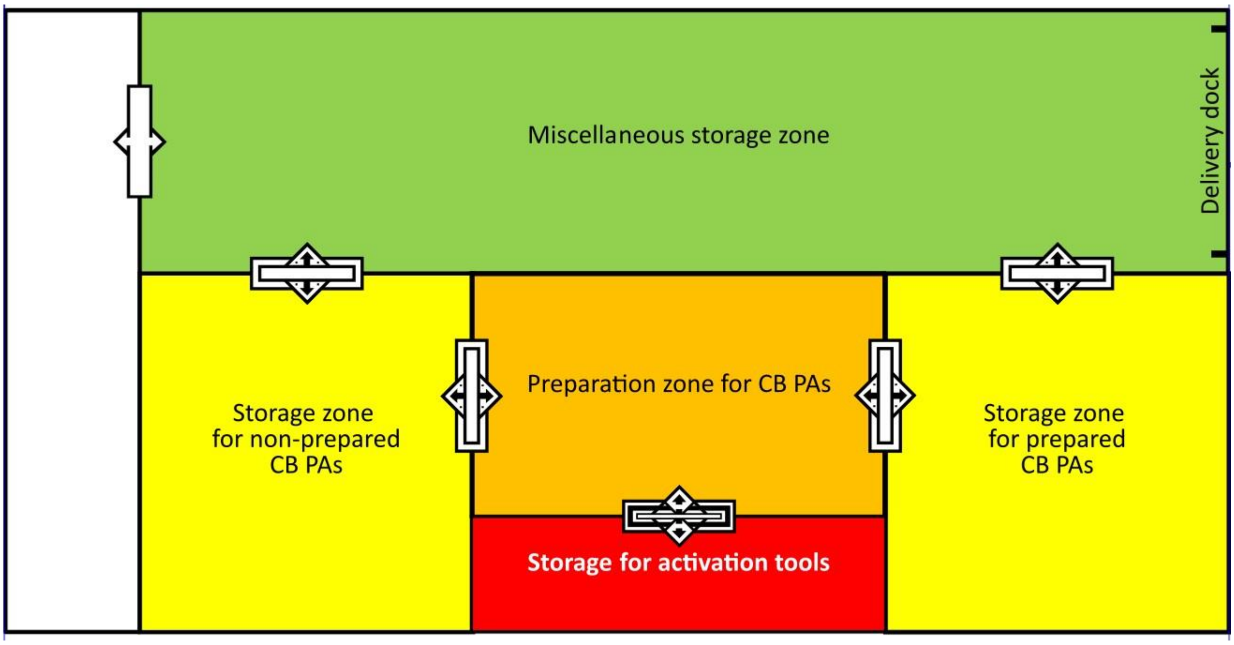

Miscellaneous storage zone
Delivery dock
Storage zone
for non-prepared
CB PAs
Preparation zone for CB PAs
Storage zone
for prepared
CB PAs
Storage for activation tools

Figure 6 – Layout example 2 for a Preparer

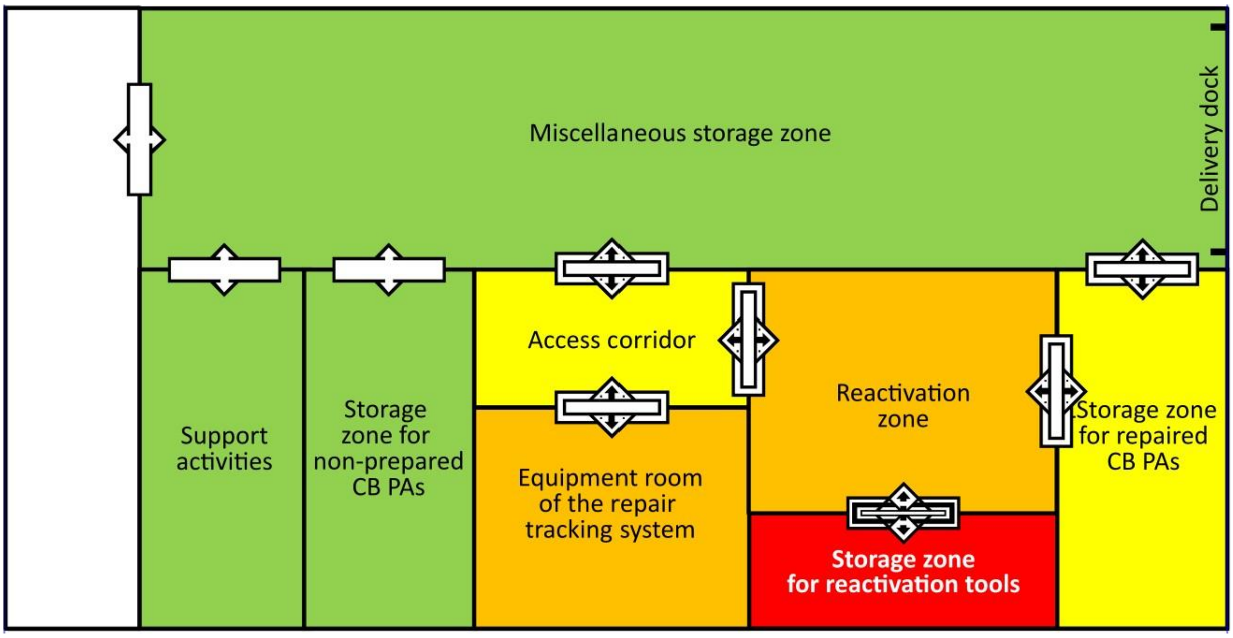

Miscellaneous storage zone
Delivery dock
Support activities
Storage zone for non-prepared CB PAs
Access corridor
Equipment room of the repair tracking system
Reactivation zone
Storage zone for reactivation tools
Storage zone for repaired CB PAs

Figure 7 – Layout example for the CB PA Maintenance

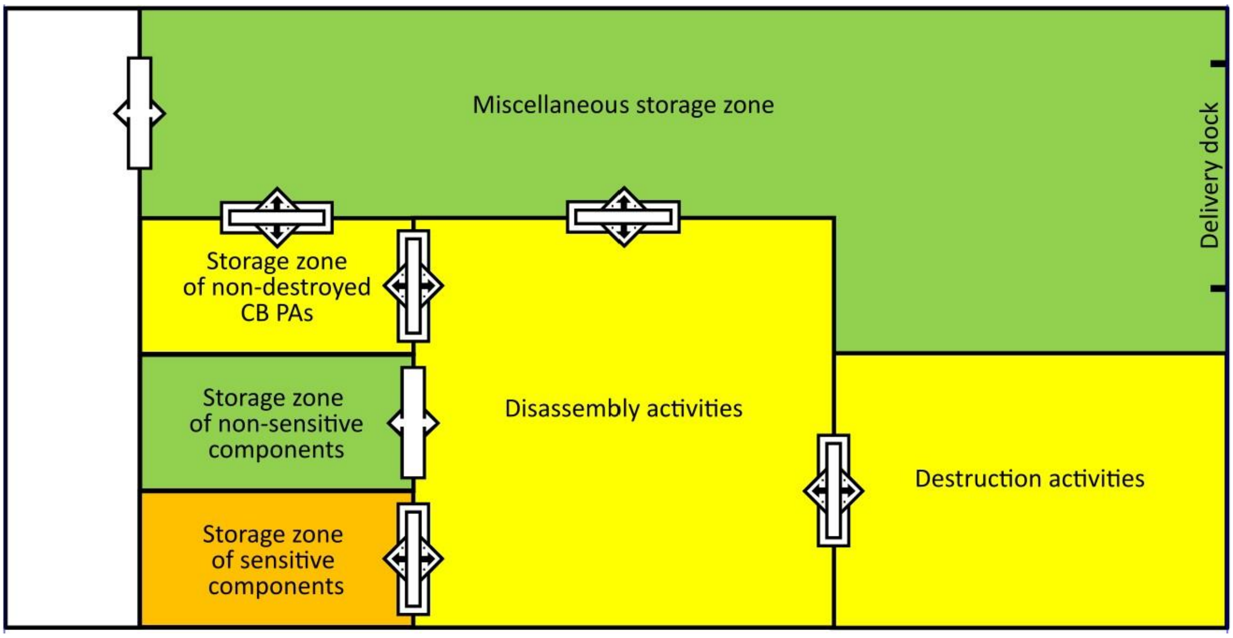

Miscellaneous storage zone
Delivery dock
Storage zone of non-destroyed CB PAs
Storage zone of non-sensitive components
Storage zone of sensitive components
Disassembly activities
Destruction activities

Figure 8 – Layout example for the CB PA Scrapping

Cases where the activity is dedicated to electronic payment

This paragraph gives layout examples of physical zones for organisations whose activities are solely dedicated to electronic payment.

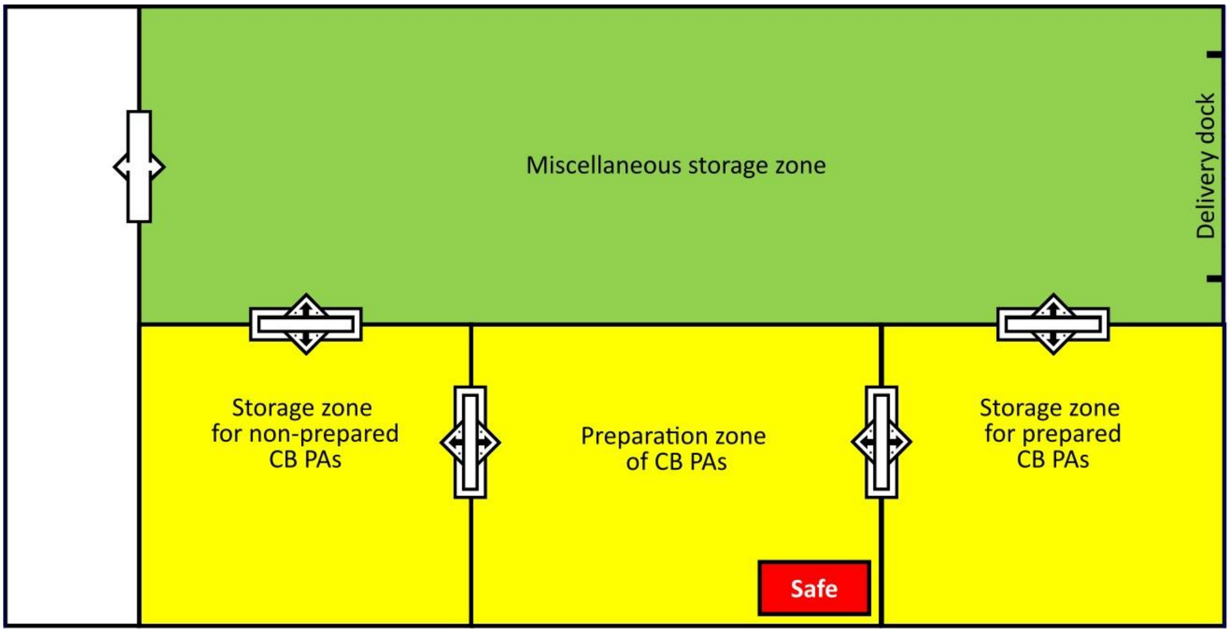

Miscellaneous storage zone
Delivery dock
Storage zone for non-prepared CB PAs
Preparation zone of CB PAs
Storage zone for prepared CB PAs
Safe

Figure 9 – Layout example for a Preparer (dedicated activity)

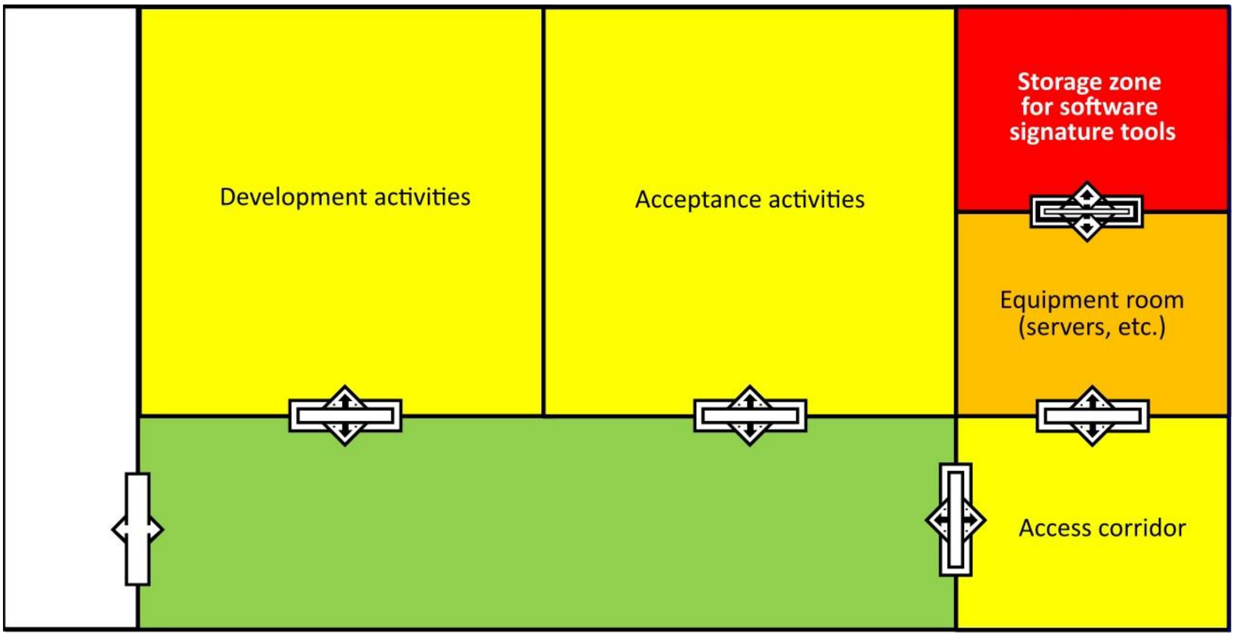

Development activities
Acceptance activities
Storage zone for software signature tools
Equipment room (servers, etc.)
Access corridor

Figure 10 – Layout example for a Developer (dedicated activity)

END OF THE DOCUMENT