RÈGLES POUR LA GESTION SÉCURISÉE DES SYSTÈMES D'ACCEPTATION CB

RÉFÉRENTIEL REMPARTS

DPE-ESS-REF-2016-006 (version 2.0)
Avril 2019

INTÉGRATEUR D'INNOVATION

DOCUMENT PRÉPARÉ PAR :

SERVICE	NOM	FONCTION	DATE
SCASSI	Aimeric Pieters	Ingénieur Sécurité	Juin 2016
Galitt	Bruno Kovacs Paul Noël Jean-François Henry	Practice Manager Consultant sécurité Consultant expert	Mai 2018
DPE/ESS	Emmanuel le Chevoir	Expert Sécurité ESS	Avril 2019

DOCUMENT VALIDÉ PAR :

SERVICE	NOM	FONCTION	DATE
PayCert	Didier Duville	Expert Acceptation et Certification	Avril 2019
DPE/ESS	Mathieu Robert	Responsable ESS	Avril 2019

HISTORIQUE DES MODIFICATIONS

DATE	RÉVISION	DESCRIPTION DES MODIFICATIONS
Juin 2016	1.0	Version initiale
Janvier 2017	1.2.1	Première version applicable du référentiel
Avril 2019	2.0	Extension du périmètre du référentiel (PIN online) Restructuration du document : • Réorganisation et catégorisation des exigences. • Présentation des règles en deux niveaux (grands principes de sécurité pour le référencement et corps d'exigences détaillées pour la labélisation). • Précision des règles d'éligibilité pour le référencement et la labélisation.

Table des matières

1 INTRODUCTION

1.1 Contexte et objectifs

En réponse aux recommandations émises par la Banque de France lors de la mission *Oversight Framework for Card Payment Schemes*, CB a réalisé un état des lieux des processus de gestion des Systèmes d'Acceptation CB et des Serveurs Monétiques, tant chez les constructeurs que chez les prestataires de services des établissements CB.

CB a ensuite mis en place un processus de renforcement de la surveillance des Systèmes d'Acceptation CB sur le terrain, qui vise notamment à :

- Identifier et responsabiliser l'ensemble des acteurs de l'acceptation CB
- Renforcer la sécurité autour des produits et métiers de l'acceptation
- Améliorer la réactivité du système CB en cas de fraude

Pour ce faire, CB a défini un ensemble de règles de sécurité dont le périmètre couvre les différentes activités entrant dans le cycle de vie des Systèmes d'Acceptation CB et des Serveurs Monétiques (ex : livraison, installation, maintenance, …). C'est l'objet du présent document, qui constitue le référentiel d'exigences sécuritaires dit « REMPARTS[1] ».

L'objectif de ce document est double :

1. Définir les grands principes de sécurité à respecter par les acteurs souhaitant s'engager dans le processus de Référencement CB.
2. Définir les règles sécuritaires pour la Labélisation CB des acteurs intervenant dans la gestion des Systèmes d'Acceptation CB. Ces règles seront validées par les auditeurs tiers habilités et reconnus par CB et son organisme de certification.

Note : certaines étapes, comme la fabrication du matériel par le constructeur, ont été exclues de ce référentiel car elles sont déjà soumises à des contraintes de sécurité explicites, et auditées par ailleurs (par exemple lors de l'agrément CB des équipements).

[1] Renforcement Et Maîtrise du Parc d'Acceptation : Résilience, Transparence et Sécurité.

1.2 Référencement et Labélisation CB

Le Référencement et la Labélisation CB sont deux démarches distinctes qui peuvent toutes deux être initiées sur un portail dédié[2] maintenu par le Groupement des Cartes Bancaires. Le détail des procédures de Référencement et de Labélisation CB est précisé dans le document Référencement et Labélisation des professionnels de l'Acceptation CB - Cadre général [1].

Référencement

Le Référencement CB est une démarche d'auto-déclaration proposée aux Professionnels de l'Acceptation CB. Le Référencement a pour objectifs de :

- Diffuser les grands principes de sécurité définis par le Groupement des Cartes Bancaires, et applicables à l'ensemble des acteurs de l'Acceptation,
- Mettre en avant les professionnels respectant ces principes de sécurité à travers un portail dédié.

Il est important de noter que seule une partie des activités décrites dans la suite de ce document est éligible au Référencement. Les activités qualifiées de sensibles [Annexe B4] ne peuvent être couvertes que par la démarche de Labélisation CB.

Toutefois, un régime transitoire a été mis en place en 2015, ouvrant le Référencement CB à l'ensemble des acteurs jusqu'à fin 2020, le temps qu'ils se mettent en conformité. Certaines activités sensibles peuvent donc temporairement être couvertes par un Référencement CB jusqu'à cette date.

Labélisation

La Labélisation CB est une démarche plus formelle permettant de s'assurer de la conformité des Professionnels de l'Acceptation CB aux exigences précisées dans la suite de ce document. Elle s'appuie sur :

- Un audit des sites sur lesquels les activités monétiques sont assurées,
- Une certification des résultats de cet audit par l'Organisme de Certification du Groupement des Cartes Bancaires.

La Labélisation a pour objectifs :

- D'apporter une assurance sécuritaire forte, en garantissant qu'un professionnel labélisé respecte l'ensemble des règles strictes énoncées par la suite,
- De mettre en avant ces professionnels, notamment auprès des membres CB et des donneurs d'ordre susceptibles de contractualiser avec ces acteurs, sur un portail dédié,
- De manière plus générale, de contribuer à renforcer la sécurité de la gestion du parc d'Acceptation CB dans son ensemble.

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

1.3 Audience

Ce document est destiné à l'ensemble des acteurs concernés par le dispositif REMPARTS :

- En premier lieu, aux prestataires de service intervenant sur les Systèmes d'Acceptation CB et devant se conformer aux principes et règles énoncés dans la suite de ce document ;
- Aux donneurs d'ordre susceptibles de faire appel à ces prestataires de service (Accepteurs CB, Acquéreurs CB, fabricants d'équipements agréés CB, établissements CB et leurs membres rattachés…) et souhaitant prendre connaissance des principes et règles applicables ;
- Enfin, aux auditeurs et certificateurs reconnus par CB et intervenant dans le processus de Labélisation.

1.4 Structure du document

Ce document est structuré de la manière suivante :

Chapitre 1	Rappel du contexte et présentation de l'objectif de cette nouvelle version du document, description des processus de Référencement et de Labélisation CB, désignation des destinataires, description de sa structure et des éléments de références.
Chapitre 2	Description des activités et du périmètre d'application du présent référentiel.
Chapitre 3	Définition des principes de sécurité à respecter pour le Référencement, organisés par activité avec un tronc commun.
Chapitre 4	Définition des exigences de sécurité pour la Labélisation, organisées par activité avec un tronc commun.
Annexes	Formulaires de contact avec CB, définition des risques sécuritaires à remédier et biens sensibles à protéger via la mise en œuvre du référentiel, définition des zones de sécurité, identification des activités sensibles à labélisation obligatoire et recensement des mises à jour appliquées à la précédente version.

1.5 Références, acronymes et définitions

Références

[1] CB – Référencement et Labélisation des Professionnels de l'Acceptation CB – Cadre Général, référence DPE-ESS-NTE-2015-002, dernière version applicable

[2] CB – Exigences sécuritaires applicables aux Systèmes d'Acceptation, référence DPE-ESS-REF-2018-17, dernière version applicable

[3] CB – Exigences sécuritaires pour la mise en œuvre du « PIN Online » dans le système CB, référence DPE-ESS-REF-2017-15, dernière version applicable

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

[5] Payment Card Industry (PCI) - PIN Security Requirements, version 2.0 de décembre 2014 ou ultérieure

Acronymes

BDK	Base Derivation Key
DMZ	Demilitarized Zone
EMV	EuroPay MasterCard Visa
DAB	Distributeur Automatique de Billets
DUKPT	Derived Unique Key Per Transaction
GAB	Guichet Automatique de Banque
GDG	Gestionnaire de DAB/GAB
HSM	Hardware Security Module
ITP	Identifiant de Terminal de Paiement
KSN	Key Serial Number
PA	Point d'Acceptation
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
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
VPN	Virtual Private Network

Définitions

Acquéreur CB

Tout Prestataire de Service de Paiement membre du Groupement qui acquiert, traite et introduit, dans un système d'échanges avec l'ensemble des Émetteurs « CB », internationaux et des systèmes d'information et de régulation communautaires, les données des transactions par Cartes Bancaires « CB » ou cartes agréées « CB » chez les Accepteurs avec lesquels il est lié par un contrat d'acceptation « CB ».

Accepteur CB

Tout commerçant, tout organisme de services, toute profession libérale et, d'une manière générale, tout professionnel ou organisme privé ou public habilité à recevoir des fonds en paiement par carte, ayant signé un contrat d'acceptation « CB » avec son Prestataire de Service de Paiement.
Il assure l'exploitation du Système d'Acceptation.

Anti-passback

Type de contrôle d'accès permettant d'éviter à une personne d'entrer deux fois dans une même zone sans en être sortie au préalable. L'anti-passback permet d'éviter le prêt de badge entre employés. Il suppose de mettre en place un contrôle d'accès en entrée et un en sortie. Un système anti-passback est généralement utilisé en conjonction avec un matériel de porte approprié (couloir d'accès, sas…).

Autorité de certification autorisée par CB

Toute autorité de certification dont les caractéristiques organisationnelles et techniques sont clairement publiées au travers d'une politique de certification qui a été analysée et validée par le Groupement des Cartes Bancaires. A la date de publication de ce document, les autorités de certification autorisées sont STCA[3] et les autorités des principaux constructeurs. En cas de doute, un professionnel est invité à se rapprocher de CB pour déterminer si une autorité est autorisée ou non.

Constructeur

Acteur assurant la fourniture des composantes matérielles et le développement des logiciels présents sur le système d'acceptation.
Il construit, développe et met à disposition les systèmes d'acceptation conformes au MPE.
Dans ce cadre, il gère le gestionnaire d'application pour :

- Fournir au système d'acceptation les fonctions du système et de gestion des périphériques,
- Mettre à jour le logiciel du noyau.

Le constructeur est la personne morale signataire de la Convention d'Agrément.

[3] STCA : Secure Transactions Certification Authority, autorité gérée par PayCert
http://www.secure-transactions-ca.eu/

Monétique Répartie

Expression utilisée pour désigner un Système d'Acceptation où la fonction d'acceptation de paiement est distribuée dans un système, typiquement entre un Point d'acceptation et un Serveur d'acceptation. Dans le système CB, on parle aussi de « Monétique Intégrée » pour désigner le même système.

Outil de réactivation PCI

Outils et procédures permettant à un organisme de mettre ou remettre en service, après s'être authentifié, un Point d'Acceptation CB non initialisé ou ayant déclenché ses protections « tamper responsive » suite à une opération de réparation sensible, par exemple.

Passerelle

Système transmetteur situé entre des systèmes d'acceptation et un système acquéreur et qui a pour objet de transporter les différents flux monétiques. Il peut exister un ou plusieurs « systèmes transmetteurs » entre un système d'acceptation et un système acquéreur.

Passerelliste

Organisme gérant les plateformes monétiques acheminant les transactions CB (demandes d'autorisation, télécollectes journalières) vers les serveurs bancaires via une « passerelle » monétique.

Point d'Acceptation (PA)

Point d'interaction avec le Porteur, permettant l'affichage du montant de la transaction, l'entrée des données de cartes CB ou agréées CB sur le Système d'acceptation CB, ainsi que la saisie du code confidentiel par le porteur lorsque demandé par le Système d'Acceptation.

Porteur

Personne physique, ayant souscrit un contrat d'utilisation d'une carte bancaire CB ou agréée CB auprès d'un établissement émetteur. La carte CB permet d'accéder aux différents services : retraits nationaux ou internationaux, paiements nationaux ou internationaux.

Serveur d'acceptation (SA)

Élément de type serveur d'un Système d'acceptation dit réparti ou intégré, généralement utilisé dans l'environnement des grandes enseignes. Ce serveur concentre les flux de différents Points d'Acceptation lors des transactions de paiement tout en réalisant de manière centralisée une partie des opérations requises par ces transactions.

Système d'Acceptation

Le Système d'Acceptation est un équipement ou un ensemble d'équipements permettant de réaliser des transactions de paiement électronique par carte bancaire "CB" ou agréée "CB", conformément aux spécifications requises par le Groupement. Il gère des fonctions interbancaires de paiement CB qui requièrent des relations avec des systèmes et acteurs externes. Un Système d'acceptation peut se réduire à un simple boîtier rendant toutes les fonctions de paiement attendues (équipement qu'on appelle communément Terminal de paiement électronique autonome ou TPE autonome), ou être un système complexe réparti comprenant un Serveur d'acceptation (SA) et des Points d'Acceptation (PA).

Terminal Management System (TMS)

Ensemble de serveurs permettant la gestion des Points d'Acceptation. On distingue trois fonctions :

- Téléparamétrage système ;
- Gestion et monitoring du parc de PA et de leur cycle de vie ;
- Mises à jour à distance des logiciels (au sens système et au sens applicatif CB2A).

Scellé[4]

Dispositif capable de mettre en évidence une tentative d'atteinte à l'intégrité physique de l'équipement sur lequel il est placé, que cette tentative ait réussi ou non.

Secret

Tout élément d'authentification donnant des privilèges sur un système ou une application.

[4] Définition issue du Guide Technique de l'ANSSI « pour la réalisation et l'utilisation de scellés de sécurité pour les équipements des systèmes d'information ».

2 PÉRIMÈTRE D'APPLICATION

Ce chapitre définit l'ensemble des activités couvertes par le présent référentiel, et pour chaque activité les tâches et biens sensibles correspondants.

Un professionnel de l'Acceptation CB peut mettre en œuvre une ou plusieurs activités. Les activités décrites dans le présent document sont constituées de tâches cohérentes et habituellement rattachées à un même acteur. Cependant, il se peut que la description des activités ne soit pas exhaustive et que pour certaines d'entre-elles le rattachement à une typologie d'acteur précise ne corresponde pas toujours à la réalité du terrain.

Ces écarts peuvent néanmoins être compensés par le processus de Labélisation. Les auditeurs, en accord avec CB et son certificateur, pourront ajuster les exigences applicables pour un acteur donné, le cas échéant.

ACTIVITÉ	TÂCHES TYPIQUES LIÉES À L'ACTIVITÉ
Développement logiciel	Développement d'applications monétiques capables de traiter une transaction conforme aux spécifications fonctionnelles reconnues par CB[5]. Développement d'applications de gestion de parc (TMS). Développement d'applications pour passerelles monétiques. Développement d'applications déployées sur un serveur monétique (consolidation de transactions pour la télécollecte, applications spécifiques aux Serveurs Monétiques, développement d'applications implémentant tout ou partie du level 2 EMV, etc.)
Intégration	Intégration d'un module matériel (ex : lecteur carte, clavier pour la saisie du code confidentiel, afficheur, …) au sein d'un équipement servant à d'autres fonctions non monétiques (ex : kiosque, borne de parking). Intégration du Point d'Acceptation dans l'environnement logique d'un Accepteur. Installation ou mise à jour des logiciels initiaux (système d'exploitation, application) dans un Point d'Acceptation CB Génération ou récupération des secrets nécessaires à l'authentification dans les échanges sécurisés (bi-clés, certificat Constructeur et certificat serveur) et signature des clés publiques par une Autorité de certification autorisée par CB.

[5] Le développement se fait en utilisant un SDK (*Software Development Kit*) fourni par le Constructeur du Système d'Acceptation. Ce SDK contient, entre autres, les outils permettant au développeur de signer électroniquement les logiciels agréés par CB.

ACTIVITÉ	TÂCHES TYPIQUES LIÉES À L'ACTIVITÉ
Préparation / Installation	Réception d'un Point d'Acceptation CB non préparé. Installation des logiciels nécessaires dans un Point d'Acceptation CB (via TMS, Bluetooth, clé USB, port série RS-232, etc.). Téléparamétrage Acquéreur d'un Système d'Acceptation CB. Fabrication de la carte de domiciliation du commerçant (selon les besoins). Installation chez l'Accepteur du Système d'Acceptation CB préparé. Télémise à jour d'un Système d'Acceptation CB. Génération ou récupération des secrets nécessaires à l'authentification dans les échanges sécurisés (bi-clés, certificat Constructeur et certificat serveur) et signature des clés publiques par une Autorité de certification autorisée par CB.
Maintenance	Maintenance de niveau 1 : • Récupération d'un Point d'Acceptation CB à réparer ; • Réparation d'un Point d'Acceptation sans ouverture de l'équipement (pas de réactivation nécessaire) ; • Retour en préparation si nécessaire[6] ; • Emballage et expédition d'un Point d'Acceptation CB réparé. Maintenance de niveau 2 : • Réparation d'un Point d'Acceptation avec ouverture de l'équipement (réactivation nécessaire) ; • Contrôle de l'intégrité du Point d'Acceptation démonté ; • Réactivation d'un Point d'Acceptation (utilisation d'un outil de réactivation PCI pour restaurer les fonctions et secrets d'un Point d'Acceptation). Mise au rebut d'un Point d'Acceptation CB (retrait du parc suite à la fin de vie de l'agrément du PA ou impossibilité de réparer) : • Démontage d'un Point d'Acceptation CB à détruire ; • Stockage des composants sensibles d'un Point d'Acceptation CB démonté. • Mise au rebut des composants sensibles du PA démonté.

[6] Un mainteneur peut assurer lui-même l'activité de préparation, mais il doit alors déclarer cette activité et se conformer aux principes et exigences associés.

ACTIVITÉ	TÂCHES TYPIQUES LIÉES À L'ACTIVITÉ
Exploitation	Maintien en conditions opérationnelles d'un Système d'Acceptation CB pour le compte d'un Accepteur. Gestion d'un serveur de centralisation de la télécollecte (avant transmission à l'Acquéreur). Téléparamétrage système. Paramétrage et mise en œuvre de la protection des communications selon les exigences formulées dans le référentiel [2] Gestion des passerelles monétiques : • Passerelles réseaux / protocolaires. • Passerelles applicatives. Gestion d'un TMS (gestion de parc, gestion de l'état sécuritaire, gestion de clés, etc.).
Stockage / Logistique	Réception de Points d'Acceptation CB. Stockage de Points d'Acceptation CB. Retrait du stock de Points d'Acceptation CB. Emballage et préparation pour expédition de Points d'Acceptation CB.
Distribution	Récupération de Points d'Acceptation CB. Transport en masse de Points d'Acceptation CB. Dépose de Points d'Acceptation CB chez un acteur intervenant dans la gestion des Systèmes d'Acceptation CB. *Note : les exigences portant sur l'activité de distribution ne concernent pas le transport unitaire de Points d'Acceptation.*
Gestion d'un centre de mise à la clé à distance (PIN Online)	Injection ou renouvellement de la clé de chiffrement du PIN (TIK) dans les Points d'Acceptation à distance (généralement via un TMS), conformément aux exigences du standard sécuritaire PCI PIN Security [5].
Gestion d'un centre d'injection de clé (PIN Online)	Injection ou renouvellement de la clé de chiffrement du PIN (TIK) dans les Points d'Acceptation selon un processus de personnalisation conformément aux exigences du standard sécuritaire PCI PIN Security [5].
Gestion d'un serveur de transchiffrement (PIN Online)	Mise à la clé et maintien en conditions opérationnelles d'un HSM agréé CB effectuant le transchiffrement du PIN chiffré, conformément aux exigences du standard sécuritaire PCI PIN Security [5].

Tableau 1 : Description détaillée des activités couvertes par REMPARTS

3 PRINCIPES DE SÉCURITÉ POUR LE RÉFÉRENCEMENT

Ce chapitre définit les grands principes de sécurité auxquels un intervenant sur les Systèmes d'Acceptation CB doit adhérer afin de pouvoir être référencé par le Groupement des Cartes Bancaires.
Les principes sécuritaires pour référencement sont notés PR_TC_x pour le tronc commun et comme suit pour chaque activité supplémentaire :

- PR_DEV_x pour le Développement logiciel,
- PR_INT_x pour l'Intégration,
- PR_PREP_x pour la Préparation/Installation,
- PR_MAINT_x pour la Maintenance et la mise au rebut,
- PR_EXPL_x pour l'Exploitation,
- PR_STOCK_x pour le Stockage/Logistique,
- PR_DIST_x pour la Distribution.

Pour chaque catégorie de principes, une référence est faite au chapitre couvrant les exigences de sécurité correspondantes. Les intervenants concernés ont ainsi une vision claire des exigences précises auxquelles ils devront se conformer s'ils souhaitent aller au-delà du Référencement et se présenter à la Labélisation.

3.1 Principes sécuritaires communs

Pour son référencement, l'organisme doit en premier lieu respecter les principes de sécurité généraux décrits ci-après.

Les organismes souhaitant se préparer à la Labélisation peuvent se référer aux exigences correspondantes, listées au chapitre 4.1 (Exigences sécuritaires communes à toutes les activités)

PRINCIPE	DESCRIPTION
PR_TC_1	L'organisme a formalisé une politique de sécurité identifiant les domaines d'activités couverts, organisant la sécurité de l'information, la sécurité de la sous-traitance, et inventoriant les biens sensibles et leur classification sécuritaire.
PR_TC_2	L'organisme dispose d'une gestion du personnel adaptée aux exigences de sécurité requises par les activités monétiques, et couvrant notamment le recrutement, la formation et le suivi de ses employés.
PR_TC_3	L'organisme protège ses locaux et ses équipements et en mettant en œuvre une surveillance et une gestion des accès physiques. Il a défini des zones de sécurité appropriées pour les activités sensibles (cf. Annexe C1).
PR_TC_4	L'organisme protège ses systèmes informatiques. Il dispose d'une politique de sécurité logique couplée à des mesures opérationnelles de sécurité (contrôle de la tierce maintenance, contrôle périodique, sécurisation des sauvegardes…).
PR_TC_5	L'organisme contrôle les logiciels monétiques des Points d'Acceptation sur lesquels il intervient et s'assure qu'ils sont agréés et intègres. Il signale au Groupement des Cartes Bancaires toute suspicion de fraude ou non-conformité.
PR_TC_6	L'organisme dispose d'un processus de gestion des incidents de sécurité couvrant les étapes de détection, remontée d'informations, investigation, traitement et remédiation. Ce processus lui permet de prévenir la récurrence des incidents.
PR_TC_7	L'organisme a formalisé et mis en œuvre une procédure d'expédition des Points d'Acceptation, de façon à ne jamais perdre la trace de ces équipements.
PR_TC_8	L'organisme s'assure de la continuité de ses activités afin de garantir un service monétique opérationnel à ses clients.
PR_TC_9	L'organisme est en mesure de prouver sa conformité à l'ensemble des principes qui s'appliquent à ses activités et s'engage à faciliter les démarches d'audits.

3.2 Développement

En plus des principes sécuritaires communs, un organisme ayant une activité de développement doit respecter les principes de sécurité spécifiques décrits ci-après.

Les organismes souhaitant se préparer à la Labélisation peuvent se référer aux exigences correspondantes, listées au chapitre 4.2 (Exigences sécuritaires pour les activités de Développement)

PRINCIPE	DESCRIPTION
PR_DEV_1	L'organisme maintient un inventaire détaillé des applications dédiées à la monétique qu'il développe et distribue.
PR_DEV_2	L'organisme maîtrise la sécurité du code source de ses applications. Il se porte garant de son intégrité et de son authenticité, s'assure qu'il dispose de l'historique complet des modifications et fait en sorte qu'il ne soit accessible qu'aux seules personnes habilitées. Il dispose d'un processus de sauvegarde et d'archivage sécurisé.
PR_DEV_3	L'organisme a formalisé et suit une méthodologie de développement sécurisé et suit les bonnes pratiques associées à l'activité de développement.
PR_DEV_4	L'organisme signe électroniquement l'ensemble des logiciels monétiques qu'il publie et s'assure que ses clients puissent en vérifier l'intégrité et l'authenticité.
PR_DEV_5	L'organisme a formalisé et mis en œuvre une gestion sécurisée des secrets cryptographiques utilisés pour la signature et la diffusion de ses logiciels.

3.3 Intégration

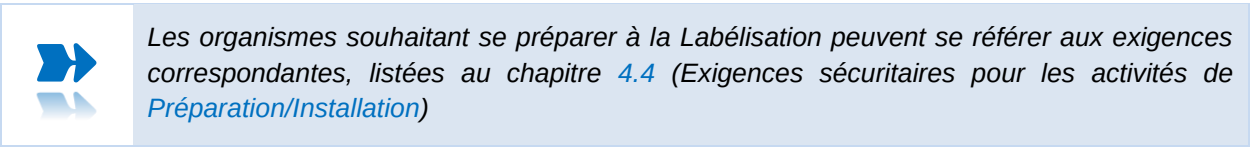
En plus des principes sécuritaires communs, un organisme ayant une activité d'intégration doit respecter les principes de sécurité spécifiques décrits ci-après.

Les organismes souhaitant se préparer à la Labélisation peuvent se référer aux exigences correspondantes, listées au chapitre 4.3 (Exigences sécuritaires pour les activités d'Intégration)

PRINCIPE	DESCRIPTION
PR_INT_1	L'organisme assure la sécurité organisationnelle de ses activités. Il a identifié les acteurs impliqués dans la récupération et le chargement des logiciels monétiques, ainsi que leur rôle et leurs responsabilités. Il tient un inventaire à jour des versions agréées des logiciels à charger.
PR_INT_2	L'organisme maitrise la sécurité du processus d'intégration. Il a mis en place une gestion rigoureuse des points d'Acceptation à intégrer, assure la protection de la confidentialité et de l'intégrité des certificats et clés TLS intégrés dans les Points d'Acceptation et dispose de zones de sécurité appropriées (cf. Annexe C1).

3.4 Préparation/Installation

En plus des principes sécuritaires communs, un organisme ayant une activité de Préparation/Installation doit respecter les principes de sécurité spécifiques décrits ci-après.



Les organismes souhaitant se préparer à la Labélisation peuvent se référer aux exigences correspondantes, listées au chapitre 4.4 (Exigences sécuritaires pour les activités de Préparation/Installation)

PRINCIPE	DESCRIPTION
PR_PREP_1	L'organisme a formalisé, documenté et mis en place une procédure de préparation et une procédure d'installation afin de maîtriser l'organisation et la sécurité des opérations.
PR_PREP_2	L'organisme communique à ses clients les dates de fin de commercialisation et de fin de vie des Points d'Acceptation sur lesquels il intervient.
PR_PREP_3	L'organisme maitrise la sécurité de la préparation. Il a mis en place une gestion rigoureuse des Points d'Acceptation à préparer et dispose de zones de sécurité appropriées (cf. Annexe C1).
PR_PREP_4	L'organisme contrôle les Points d'Acceptation après installation et s'assure de leur intégrité physique. Il a mis en place une procédure de gestion des incidents adaptée et signale au Groupement des Cartes Bancaires toute suspicion de fraude ou non-conformité suite aux contrôles de version (cf. Annexe A : Remontée d'informations au Groupement des Cartes Bancaires).

3.5 Maintenance

En plus des principes sécuritaires communs, un organisme ayant une activité de maintenance doit respecter les principes de sécurité spécifiques décrits ci-après.

Les organismes souhaitant se préparer à la Labélisation peuvent se référer aux exigences correspondantes, listées au chapitre 4.5 (Exigences sécuritaires pour les activités de Maintenance et mise au rebut)

Principes généraux

PRINCIPE	DESCRIPTION
PR_MAINT_1	L'organisme a formalisé, documenté et mis en place une procédure de réparation afin de maîtriser l'organisation et la sécurité des opérations de maintenance. Cette procédure permet d'identifier les Points d'Acceptation en cours de traitement et les Points d'Acceptation réparés.
PR_MAINT_2	L'organisme a formalisé, documenté et mis en place une procédure de télé-mise à jour des Points d'Acceptation traités en maintenance. Cette procédure doit prévoir qu'une opération de télécollecte est déclenchée préalablement à toute télé-mise à jour.
PR_MAINT_3	L'organisme a formalisé, documenté et mis en place une procédure de mise au rebut des Points d'Acceptation. Cette procédure précise les modalités de démontage et de destruction des Points d'Acceptation, et prévoit la notification systématique du Constructeur.
PR_MAINT_4	L'organisme maitrise la sécurité de ses activités de maintenance et de mise au rebut. Il a mis en place une gestion rigoureuse des Points d'Acceptation à réparer ou à détruire, et dispose de zones de sécurité appropriées (cf. Annexe C1).
PR_MAINT_5	L'organisme contrôle les Points d'Acceptation lors des opérations de maintenance et s'assure de leur intégrité physique. Il a mis en place une procédure de gestion des incidents adaptée et signale au Groupement des Cartes Bancaires toute suspicion de fraude (cf. Annexe A : Remontée d'informations au Groupement des Cartes Bancaires).

Principes applicables aux activités de maintenance de niveau 2

Une intervention de niveau 2 (ou supérieur) suppose l'ouverture du Point d'Acceptation et requiert par conséquent la réactivation de la sécurité PCI. À ce titre, cette activité est beaucoup plus sensible que la maintenance de premier niveau et nécessite des traitements particuliers de la part de l'organisme.

Note : les activités de maintenance de niveau 2 peuvent faire l'objet d'un Référencement CB pendant la phase transitoire définie en 2015. Cette phase prendra fin en décembre 2020. Passée cette date, ces activités ne seront plus éligibles au Référencement CB et devront faire l'objet d'une Labélisation CB.

PRINCIPE	DESCRIPTION
PR_MAINT_6	L'organisme doit prendre des mesures organisationnelles strictes pour contrôler les opérateurs habilités à intervenir en maintenance de niveau 2.
PR_MAINT_7	L'organisme s'assure de la maitrise de la réactivation PCI des Points d'Acceptation réparés. Il a mis en place une gestion sécurisée des outils de réactivation et des secrets associés et tient à jour un journal détaillé de ces opérations.

3.6 Exploitation

En plus des principes sécuritaires communs, un organisme ayant une activité d'exploitation doit respecter les principes de sécurité spécifiques décrits ci-après.

Les organismes souhaitant se préparer à la Labélisation peuvent se référer aux exigences correspondantes, listées au chapitre 4.6 (Exigences sécuritaires pour les activités d'Exploitation)

PRINCIPE	DESCRIPTION
PR_EXPL_1	L'organisme assure la sécurité organisationnelle de ses activités. Il maintient un inventaire lui permettant d'identifier les équipements matériels et les logiciels impliqués dans son activité monétique. Il a formalisé et mis en œuvre des procédures d'exploitation, couvrant la télécollecte et le téléparamétrage.
PR_EXPL_2	L'organisme, s'il opère des serveurs de télécollecte/téléparamétrage, s'assure qu'il utilise des certificats TLS permettant aux Points d'Acceptation d'authentifier ces serveurs. Ces certificats doivent avoir été émis par une Autorité de certification autorisée par CB, et doivent être protégés en confidentialité et en intégrité.
PR_EXPL_3	L'organisme assure la sécurité opérationnelle de ses activités. Il dispose de zones de sécurité appropriées (cf. Annexe C1) et protège les communications avec les serveurs d'acquisition conformément aux exigences sécuritaires CB applicables aux Systèmes d'Acceptation [2]

3.7 Stockage/Logistique

En plus des principes sécuritaires communs, un organisme ayant une activité de Stockage/Logistique doit respecter les principes de sécurité spécifiques décrits ci-après.

Les organismes souhaitant se préparer à la Labélisation peuvent se référer aux exigences correspondantes, listées au chapitre 4.7 (Exigences sécuritaires pour les activités de Stockage/Logistique)

PRINCIPE	DESCRIPTION
PR_STOCK_1	L'organisme assure la sécurité organisationnelle de ses activités de stockage des Points d'Acceptation et de logistique. Il maintient un inventaire des Points d'Acceptation et a formalisé les procédures de réception et de retrait.
PR_STOCK_2	L'organisme assure la sécurité opérationnelle de ses activités. Il dispose de zones de sécurité appropriées (cf. Annexe C1) et a formalisé une procédure de gestion des incidents portant sur les scellés des emballages.

3.8 Distribution

En plus des principes sécuritaires communs, un organisme ayant une activité de Distribution doit respecter les principes de sécurité spécifiques ci-après.

Les organismes souhaitant se préparer à la Labélisation peuvent se référer aux exigences correspondantes, listées au chapitre 4.8 (Exigences sécuritaires pour les activités de Distribution)

PRINCIPE	DESCRIPTION
PR_DIST_1	L'organisme assure la sécurité organisationnelle de ses activités de transport de Points d'Acceptation. Il a formalisé le processus de distribution, depuis l'emballage jusqu'à la livraison au client.
PR_DIST_2	L'organisme assure la sécurité opérationnelle de ses activités. Il met en place des mesures de protection des emballages et de scellés, et fournit systématiquement des bordereaux d'expédition et des PV de réception[7]. Il a formalisé une gestion des incidents, et notifie sans délai le Groupement des Cartes Bancaires en cas de disparition avérée d'un Point d'Acceptation.

[7] Ne sont concernés que les transports de masse. Le transport d'un Point d'Acceptation seul, par exemple lors d'un échange, n'est pas concerné.

4 EXIGENCES POUR LA LABÉLISATION

Généralités

Les exigences de sécurité ci-dessous doivent permettre d'assurer la couverture des risques sécuritaires considérés. Cela concerne notamment les risques de compromission de masse (cf. annexe B1).

Pour détecter une compromission de masse, une implication de l'ensemble des acteurs intervenant dans le cycle de vie des Systèmes d'Acceptation est nécessaire. Cela consiste notamment à :

- Assurer une traçabilité de bout en bout des actions de gestion ;
- Maîtriser les inventaires, les stocks et le suivi ;
- Mettre en place des procédures de contrôle du respect des règles de sécurité ;
- Mettre en place des procédures de détection d'atteinte à l'intégrité physique et logicielle.

L'ensemble de ces points se retrouvent dans chacune des activités couvertes par le référentiel de labélisation.

Préparation des audits de Labélisation

Pour chaque exigence applicable, l'organisme doit disposer de documentation ou de preuves (dispositif de sécurité, compte-rendu, PV, registre papier, configuration d'équipement, trace informatique…) démontrant la couverture de celle-ci. Ces éléments devront être consultables par l'auditeur chargé d'évaluer la conformité de l'organisme par rapport au présent référentiel d'exigences.

Note : d'une manière générale, un organisme qui disposerait déjà de certifications sécuritaires sur son environnement et ses processus métiers (comme par exemple une certification PCI-DSS [4]) pourra faire valoir les certificats associés afin que les résultats soient réutilisés, s'il démontre, par exemple par la consultation du Report On Compliance (ROC) correspondant, que le périmètre concerné est le même et que les exigences couvertes sont de même nature.

Terminologie

- Le terme « organisme » désigne l'entité juridique soumise aux exigences pour les activités déclarées.
- Le terme « locaux techniques » désigne les salles hébergeant les infrastructures réseaux et serveurs.
- Sauf précision contraire, les exigences s'appliquant aux « serveurs informatiques », « serveurs monétiques », « postes informatiques », « logiciels » et « composants du système d'information » ne concernent que le périmètre spécifique à la gestion des Systèmes d'Acceptation CB et des Serveurs Monétiques.

Précisions sur les exigences

- Les exigences encadrant le Stockage sont applicables dans toutes les étapes du cycle de vie du Système d'Acceptation ;
- Les exigences encadrant le transport et l'expédition sont définies dans l'activité de Distribution et sont applicables dans toutes les étapes du cycle de vie du Système d'Acceptation ;
- Dans la mesure du possible, et afin de faciliter la convergence avec d'autres démarches de conformité sécuritaire, les exigences sont organisées par catégories recensées dans la liste structurée de l'annexe A de la norme ISO 27001 traitant du « Management de la sécurité de l'information ».

4.1 Exigences sécuritaires communes à toutes les activités

4.1.1 Politique de sécurité

EXIGENCE	DESCRIPTION
EXI_TC_1	Stratégie de sécurité de l'information L'organisme doit engager une stratégie de sécurité de l'information soutenue par sa direction et communiquée aux employés. Cette stratégie de sécurité doit définir des objectifs et une organisation clairs et être alignée avec la stratégie globale de l'entreprise.
EXI_TC_2	Analyse des risques Une appréciation des risques doit être effectuée sur les périmètres de sécurité concernant les matériels, postes de travail et serveurs, ainsi que sur les équipements réseau et télécom impliqués dans la gestion des Systèmes d'Acceptation CB et des Serveurs Monétiques. Ce document doit notamment prendre en compte la malveillance interne et externe, ainsi que les menaces accidentelles.
EXI_TC_3	Mise en œuvre d'une politique de sécurité Une politique de sécurité doit être implémentée et doit : • Décrire l'organisation mise en place pour gérer la sécurité, en particulier les groupes, les rôles et les responsabilités des personnels impliqués dans la sécurité des Systèmes d'Acceptation CB et des Serveurs Monétiques durant leur cycle de vie, notamment pour la protection des locaux techniques, des équipements informatiques (serveurs, postes de travail) et des réseaux. • Décrire la façon dont les risques précédemment identifiés par l'organisme sont traités. Ce plan de traitement des risques doit permettre de vérifier que la politique définie est cohérente avec les risques identifiés.

4.1.2 Sécurité des ressources humaines

Ces exigences portent sur la gestion du personnel impliqué dans la gestion des Systèmes d'Acceptation CB et des Serveurs Monétiques.

EXIGENCE	DESCRIPTION
EXI_TC_4	Surveillance particulière dans le processus de recrutement. Le recrutement des opérateurs responsables des activités sensibles (cf. Annexe B4) sur la chaine de vie des Systèmes d'Acceptation CB et des Serveurs Monétiques doit faire l'objet d'une surveillance particulière. Un extrait de casier judiciaire (B3) ou son équivalent à l'étranger doit être demandé afin d'apprécier la capacité des recrues à occuper l'emploi proposé. Les extraits de casier judiciaire ne doivent pas être conservés.
EXI_TC_5	Charte de sécurité Une charte de sécurité, ou document d'entreprise équivalent (par exemple une notice générale d'information), doit être signée par le personnel impliqué dans la gestion des Systèmes d'Acceptation CB et des Serveurs Monétiques. Cette charte doit reprendre de manière synthétique les exigences de sécurité du présent référentiel que le personnel doit suivre et respecter. Elle doit également responsabiliser l'intervenant vis-à-vis de la sensibilité des activités monétiques.
EXI_TC_6	Sensibilisation et formation du personnel Un processus de sensibilisation et de formation du personnel impliqué dans la gestion des Systèmes d'Acceptation CB et des Serveurs Monétiques doit être formalisé et appliqué. Les séances de sensibilisation et les formations doivent être régulières et adaptées au type d'activité pratiquée. Elles doivent avoir lieu au moins annuellement. Un procès-verbal formalisant la présence du personnel concerné à ces séances doit être signé par les différentes parties prenantes et conservé par l'organisme.

4.1.3 Gestion des actifs

EXIGENCE	DESCRIPTION
EXI_TC_7	Protection des biens sensibles de l'organisme L'organisme doit avoir identifié et inventorié tous ses actifs, et désigné pour chacun un responsable ainsi que les règles d'utilisation. Au minimum, les actifs décrits comme des « biens sensibles » référencés par l'annexe B3 doivent être considérés.

EXIGENCE	DESCRIPTION
EXI_TC_8	Inventaire des plateformes matérielles et logicielles Les différentes plateformes matérielles utilisées (informatiques et télécommunications) dans le cadre de la gestion des Systèmes d'Acceptation CB et des Serveurs Monétiques doivent être identifiées et inventoriées. L'inventaire des plateformes matérielles utilisées doit inclure les configurations déployées (marques et modèles) et les logiciels utilisés
EXI_TC_9	Politique de classification des informations L'organisme doit disposer d'une politique de classification des informations prenant en compte la valeur, la sensibilité et la criticité des actifs concernés, ainsi que la réglementation applicable. Le niveau de classification approprié doit être appliqué pour les informations relatives à la gestion des Systèmes d'Acceptation CB et des Serveurs Monétiques.
EXI_TC_10	Règles d'usage des informations et de leurs supports La politique de classification des informations doit prévoir, pour chaque niveau, des règles d'usage des informations et de leurs supports. Ces règles doivent encadrer la diffusion, le stockage et la destruction des informations et de leurs supports. Les moyens de mise en œuvre de ces règles doivent être identifiés. Les supports contenant des informations classées comme sensibles doivent : • Être stockés dans un local sécurisé (armoire sous clé, local dédié, etc.) ; • Être détruits ou effacés de façon sécurisée lorsqu'ils ne sont plus utilisés.
EXI_TC_11	Gestion des supports amovibles Une procédure de contrôle strict des supports amovibles (CD/DVD, clé USB, etc.) utilisés sur les postes de travail et serveurs impliqués dans la gestion des Systèmes d'Acceptation CB et des Serveurs Monétiques doit être mise en œuvre.

4.1.4 Contrôle d'accès

4.1.4.1 Gestion des accès physiques

EXIGENCE	DESCRIPTION
EXI_TC_12	Contrôle d'accès aux bâtiments Les périmètres physiques protégeant les bâtiments doivent être sous accès contrôlés, réglementés et vidéo surveillés.

EXIGENCE	DESCRIPTION
EXI_TC_13	Accès aux zones sécurisées par le personnel de l'organisme L'accès aux différentes zones de sécurité doit être restreint au seul personnel habilité, selon les modalités propres à chaque zone (cf. Annexe C : Configurations des zones de sécurité)
EXI_TC_14	Accès aux zones sécurisées par des tiers L'accès des personnes étrangères à l'organisme aux zones de sécurité doit être strictement contrôlé : • Un registre conservant l'identité, l'heure et la date d'arrivée et de départ des visiteurs doit être tenu et conservé dans le temps. • Un badge doit être émis pour chaque visiteur, ne donnant accès qu'aux zones nécessaires pour l'objet de la visite. • Les visiteurs doivent être accompagnés à tout moment par un représentant de l'organisme dûment habilité.
EXI_TC_15	Procédures de revue et de mise à jour des droits d'accès physiques Des procédures de revue et de mise à jour des droits d'accès physiques aux zones de sécurité doivent être implémentées et appliquées. Les acteurs sont identifiés et les revues doivent être tracées. L'attribution des droits d'accès : • Se fait au fil de l'eau ; • Est validée par un responsable ; • Respecte le principe de séparation des tâches ; • Respecte le principe du besoin d'en connaître. La traçabilité des attributions de droits (demandes et validations) doit être assurée. Les habilitations doivent être revues périodiquement : • Les contrôles de revue des habilitations sont trimestriels (contrôle de la bonne suppression des droits) ; • Les contrôles de besoins (mise à jour des droits) sont semestriels.
EXI_TC_16	Gestion des incidents en cas de détection d'accès non autorisé En cas de détection d'un accès non autorisé (tentative d'accès, intrusion physique) dans un site/local, une procédure de gestion des incidents doit être implémentée comme défini au § 4.1.12.
EXI_TC_17	Contrôle des installations de sécurité physique Des contrôles réguliers du bon fonctionnement des installations de sécurité (centrale de contrôle d'accès, PC de gestion des badges d'accès), doivent être réalisés et tracés. Ces contrôles doivent être réalisés au minium annuellement.

4.1.4.2 Gestion des accès logiques

EXIGENCE	DESCRIPTION
EXI_TC_18	Identification et authentification du personnel Toute personne impliquée dans la gestion des Systèmes d'Acceptation CB et des Serveurs Monétiques doit être identifiée de manière nominative et authentifiée de façon sûre (au minimum à l'aide d'un mot de passe suffisamment complexe) lorsqu'elle accède à des postes de travail ou des serveurs informatiques. La gestion des facteurs d'authentification doit se faire dans les règles de l'art. En particulier, les mots de passe doivent être chiffrés ou stockés sous la forme de condensats non réversibles.
EXI_TC_19	Authentification forte en cas d'accès à distance Tout accès à distance au système d'information (par le biais de VPN, d'accès modem, etc.), par exemple dans le cas d'astreinte ou d'opérations de télémaintenance doit être authentifié de manière forte, sur la base d'au moins deux facteurs distincts (par exemple à l'aide d'un certificat ou d'une clé électronique et d'un serveur d'authentification).
EXI_TC_20	Procédures de revue et mise à jour des droits d'accès logiques Des procédures de revue et de mise à jour des droits d'accès logiques aux postes de travail ou aux serveurs informatiques impliqués dans la gestion des Systèmes d'Acceptation CB et des Serveurs Monétiques doivent être implémentées et appliquées, notamment lors d'un changement de poste ou du départ d'un personnel de l'organisme.

4.1.5 Zones de sécurité

Les zones de sécurité utilisées dans le cadre de ce référentiel (zones vertes, jaunes, oranges et rouges) sont définies en annexe C1.

EXIGENCE	DESCRIPTION
EXI_TC_21	Découpage du site en zones de sécurité L'organisme doit disposer des plans de masse des différents sites intervenant dans le cadre de la gestion des Systèmes d'Acceptation CB et des Serveurs Monétiques et leur découpage en zones de sécurité (cf. annexe C1). L'organisme doit s'assurer que les zones de sécurité définies sont cohérentes avec les activités qui y sont menées.

EXIGENCE	DESCRIPTION
EXI_TC_22	Respect des contraintes liées aux zones de sécurité L'organisme doit mettre en place les dispositifs de contrôle d'accès physique et de surveillance adaptés pour chaque zone. Les contraintes associées à chaque type de zone sont définies en annexe C1.
EXI_TC_23	Localisation des locaux techniques hébergeant des serveurs informatiques Les locaux techniques hébergeant les serveurs informatiques intervenant dans le cadre de la gestion des Systèmes d'Acceptation CB ou ayant une fonction monétique doivent être situés en zone orange .
EXI_TC_24	Localisation des installations de gestion de la sécurité physique Les locaux techniques hébergeant les installations de sécurité (centrale de contrôle d'accès, PC de gestion des badges d'accès) doivent être en zone orange . Les outils d'administration de ces installations sont soumis aux mêmes contraintes.

4.1.6 Sécurité liée à l'exploitation informatique

EXIGENCE	DESCRIPTION
EXI_TC_25	Gestion à distance des serveurs et équipements monétiques Une procédure particulière pour la gestion distante (télé administration lors d'éventuelles astreintes) des serveurs informatiques et des équipements réseaux impliqués dans la gestion des Systèmes d'Acceptation CB et des Serveurs Monétiques doit être implémentée si le besoin a été identifié par l'organisme. Celle-ci doit : • Décrire les rôles et les responsabilités des personnels concernés, ainsi que les conditions d'intervention et leur traçabilité ; • Identifier et répertorier les dispositifs et logiciels utilisés pour assurer la protection de cette télé administration (type d'authentification, protocoles réseaux, etc).
EXI_TC_26	Revue périodique des configurations des équipements réseaux Un processus formel pour la revue périodique des configurations des équipements réseaux (routeurs, commutateurs, pare-feu, etc.) impliqués dans la gestion des Systèmes d'Acceptations CB et des Serveurs Monétiques doit être implémenté. Les traces des revues doivent être conservées.
EXI_TC_27	Sécurisation des postes informatiques liés à l'exploitation Les postes d'exploitation fixes et les postes de travail nomades ayant accès, par les réseaux locaux ou à distance via des accès VPN (dans le cas d'astreintes par exemple), aux serveurs informatiques impliqués dans la gestion des Systèmes d'acceptation CB et des Serveurs Monétiques doivent être sécurisés : • Logiciel anti-virus activé et à jour, configuré pour réaliser des analyses sur accès et des scans périodiques complets, et non désactivable par l'exploitant ; • Logiciel pare-feu, activé et non désactivable par l'exploitant, dont les règles doivent être adaptées aux usages ; • Le disque dur doit avoir un chiffrement de surface et des mesures de séquestre des clés mises en œuvre ; • Les comptes des utilisateurs courants des postes de travail ne doivent pas être à privilèges ; • L'installation de logiciels non autorisés par l'organisme doit être interdite ; • Un contrôle trimestriel des droits d'accès à ces postes de travail doit être effectué ; • Un Système d'Exploitation sécurisé (accès par mot de passe, démarrage sur un support amovible interdit) doit être utilisé pour les organismes dont l'activité de gestion des Systèmes d'Acceptation CB est mutualisée avec d'autres activités non liées à la monétique.

EXIGENCE	DESCRIPTION
EXI_TC_28	Durcissement des systèmes d'exploitation des serveurs impliqués Les serveurs informatiques impliqués dans la gestion des Systèmes d'Acceptation CB et des Serveurs Monétiques doivent fonctionner avec un système d'exploitation « durci », c'est-à-dire composé exclusivement des seuls éléments logiciels et matériels nécessaires à son fonctionnement. Le durcissement d'un système d'exploitation consiste au minimum à : • Supprimer les modules inutilisés (exécutables, bibliothèques logicielles, pilotes…) et les services inutiles (protocoles, services TCP/IP, services systèmes, etc.) ; • Supprimer les comptes utilisateurs inutilisés et changer les mots de passe par défaut ; • Mettre à jour le système d'exploitation avec les derniers patches de sécurité selon une fréquence mensuelle pour les plus critiques et trimestrielle pour les autres ; • Désactiver les moyens de démarrage à distance des systèmes d'exploitation (exemple : télé démarrage Ethernet PXE) ; • Respecter les règles de durcissement proposées par les fournisseurs de systèmes d'exploitation commerciaux ou logiciels libres. Les mesures mises en œuvre pour le durcissement des systèmes doivent être documentées.
EXI_TC_29	Contrôle d'intégrité des fichiers systèmes et des données sensibles Des dispositifs de contrôle d'intégrité des fichiers systèmes et des données doivent être mis en place et exécutés régulièrement sur les serveurs impliqués dans la gestion des Systèmes d'Acceptation CB et des Serveurs Monétiques. Ces dispositifs doivent être journalisés. Lorsqu'un défaut d'intégrité est détecté, une procédure de gestion des incidents conforme aux exigences formulées dans EXI_TC_53 doit être suivie.
EXI_TC_30	Mises à jour logicielles Un processus de mise à jour régulière des systèmes d'exploitation et des logiciels installés sur les postes de travail portables, les serveurs informatiques et équipements réseau impliqués dans la gestion des Systèmes d'Acceptation CB et des Serveurs Monétiques doit être implémenté. Celui-ci doit vérifier que tous les patchs de sécurité pertinents ont été appliqués et que les nouveaux sont appliqués dans le mois qui suit leur publication pour les plus critiques et dans les deux mois pour les autres.

EXIGENCE	DESCRIPTION
EXI_TC_31	Maintenance des systèmes informatiques Toute opération de maintenance sur les postes de travail et les serveurs informatiques, ainsi que sur les équipements réseau et télécom impliqués dans la gestion des Systèmes d'Acceptation CB et des Serveurs Monétiques doit être réalisée par du personnel autorisé. Toutes les opérations de maintenance doivent être tracées.
EXI_TC_32	Suppression des données avant maintenance Une procédure de déclenchement de service de maintenance doit être implémentée. Celle-ci doit prévoir l'effacement sécurisé des données sensibles ou le retrait des dispositifs de stockage avant toute sortie d'un matériel hors des locaux de l'organisme pour cause de maintenance.
EXI_TC_33	Mise au rebut du matériel informatique Une procédure de mise au rebut des postes de travail, des serveurs informatiques, des supports amovibles et des médias de sauvegarde et d'archivage impliqués dans la gestion des Systèmes d'Acceptation CB et des Serveurs Monétiques doit être implémentée. Cette procédure doit prévoir l'effacement sécurisé ou la destruction des supports de stockage de données.

4.1.7 Sécurité des sauvegardes

EXIGENCE	DESCRIPTION
EXI_TC_34	Politique de sauvegarde Une politique de sauvegarde doit être implémentée (planification, lieu de stockage, application, rétention) pour les serveurs impliqués dans la gestion des Systèmes d'Acceptation CB et des Serveurs Monétiques.
EXI_TC_35	Niveau de sécurité des données sauvegardées Les données sauvegardées doivent bénéficier du même niveau de sécurité que les données d'origine.
EXI_TC_36	Inventaire des supports informatiques de sauvegarde Un inventaire des supports informatiques impliqués dans la sauvegarde doit être réalisé et revu régulièrement.

4.1.8 Journalisation et Surveillance

EXIGENCE	DESCRIPTION
EXI_TC_37	Activation des journaux d'audit des serveurs et équipements réseaux impliqués Les journaux d'audit des serveurs informatiques et des équipements réseau (routeurs, commutateurs, pare-feu, etc.) impliqués dans la gestion des Systèmes d'Acceptation CB et des Serveurs Monétiques doivent être activés.
EXI_TC_38	Analyse des journaux d'audit des serveurs et des équipements réseaux Les journaux d'audit des serveurs informatiques et des équipements réseaux les protégeant doivent être analysés au moins une fois par jour, pour pouvoir identifier au plus tôt toute action suspecte ou non autorisée. Les analyses peuvent être automatisées avec des solutions spécialisées dans l'analyse des journaux d'audit.
EXI_TC_39	Traçabilité des actions Les actions réalisées dans les outils informatiques utilisés pour la gestion des Points d'Acceptation CB ou des Serveurs Monétiques doivent être journalisées. Les journaux doivent au minimum contenir les informations suivantes : • Date et heure de l'action • Identité de l'utilisateur • Type d'action • Origine de l'action • Données / ressources concernées • Résultat de l'action (succès ou échec) De plus, les dispositifs de journalisation des serveurs informatiques et des équipements réseau impliqués dans la gestion des Systèmes d'Acceptation CB et des Serveurs Monétiques doivent tracer les accès utilisateurs, notamment ceux avec des privilèges d'administration.

4.1.9 Sécurité des communications

EXIGENCE	DESCRIPTION
EXI_TC_40	Cartographie du réseau Une cartographie réseau détaillée du SI dédié aux activités de gestion des Systèmes d'Acceptation CB et Serveurs Monétiques doit être maintenue. Elle doit spécifier les interfaces réseaux utilisées avec les acteurs externes (passerelles internationales, systèmes d'information métier, extranets).

EXIGENCE	DESCRIPTION
EXI_TC_41	Identification des flux réseaux et métiers Les flux réseaux et métiers nécessaires au fonctionnement des serveurs utilisés dans les activités couvertes par le présent référentiel doivent être clairement identifiés. Il est recommandé de formaliser et maintenir une matrice des flux réseaux (vision technique), ainsi qu'un diagramme des flux métiers (vision synthétique).
EXI_TC_42	Cloisonnement du système d'information Les composants métiers du système d'information participant à la gestion de Points d'Acceptation et des Serveurs Monétiques doivent être physiquement et/ou logiquement cloisonnés des autres réseaux de l'organisme. S'ils doivent être accessibles depuis un réseau public, ils doivent être placés dans une zone démilitarisée (DMZ). Les réseaux locaux internes ne doivent pas être accessibles directement depuis les réseaux publics.
EXI_TC_43	Protection des interfaces exposées sur des réseaux publics Les interfaces exposées sur des réseaux publics (Internet, etc.) doivent être protégées par des pare-feu. Ces pare-feu doivent être paramétrés pour n'autoriser que les flux réseau entrants nécessaires aux applications métiers.
EXI_TC_44	Détection/prévention d'intrusion réseau Des dispositifs de détection et/ou de prévention d'intrusion réseau doivent être mis en place sur les interfaces publiques des réseaux impliqués dans la gestion des Systèmes d'Acceptation CB et des Serveurs Monétiques.

4.1.10 Contrôle permanent

EXIGENCE	DESCRIPTION
EXI_TC_45	Veille sécuritaire Un processus de veille sécuritaire concernant les systèmes d'exploitation et logiciels installés sur les postes d'exploitation, les PC portables, les serveurs informatiques et équipements réseau impliqués dans la gestion des Systèmes d'Acceptation CB et des Serveurs Monétiques doit être implémenté et porter notamment sur les nouvelles vulnérabilités et les patchs de sécurité associés.

EXIGENCE	DESCRIPTION
EXI_TC_46	Campagnes de tests d'intrusion internes et externes Des campagnes de tests d'intrusion doivent être régulièrement réalisées sur les réseaux et applicatifs impliqués dans la gestion des Systèmes d'Acceptation CB et des Serveurs Monétiques. Ces tests doivent permettre de déterminer l'exposition de l'organisme aux attaques internes (attaquant sur le réseau de l'organisme) et externes (attaquant exploitant les interfaces publiques). Ces campagnes doivent donner lieu à la production de rapports et d'éventuels plans d'actions associés, qui viendront enrichir l'analyse des risques maintenue par l'organisme.
EXI_TC_47	Contrôle périodique et contrôle permanent Les processus de gestion des Points d'Acceptation CB et des Serveurs Monétiques doivent faire l'objet de contrôles, périodiques et permanents, selon les modalités suivantes : • Un contrôle permanent de la conformité, de la sécurité et de la validation des opérations réalisées est effectué par un employé de l'organisme ayant un rôle opérationnel. La fréquence de ce contrôle permanent doit être adaptée en fonction de l'activité de l'organisme et de la sensibilité des opérations contrôlées. Les points de contrôle permanent doivent être au strict minimum réalisés mensuellement. • Un contrôle périodique du respect des procédures, de l'efficacité et du caractère approprié des dispositifs de contrôle permanent est réalisé par un employé de l'organisme n'ayant pas un rôle opérationnel. La fréquence de ce contrôle peut être trimestrielle, semestrielle ou annuelle, en fonction de l'activité de l'organisme et de la sensibilité des opérations contrôlées. Ces contrôles devront suivre un référentiel clair et maintenu dans le temps, et faire l'objet de compte-rendu attestant des résultats observés.
EXI_TC_48	Contrôle du statut de l'agrément CB des Systèmes d'Acceptation Un contrôle systématique du statut de l'agrément CB des Systèmes d'Acceptation sur lesquels l'organisme est amené à intervenir doit être effectué. En fonction du statut du Système d'Acceptation, les mesures adéquates doivent être prises (voir l'annexe B2). En particulier : • L'organisme doit sensibiliser ses clients en leur communiquant les différentes échéances liées à l'agrément de leurs Systèmes d'Acceptation • L'organisme doit alerter le Groupement des Cartes Bancaires dès qu'un matériel a atteint sa date de fin de commercialisation.

4.1.11 Gestion de la sous-traitance

EXIGENCE	DESCRIPTION
EXI_TC_49	Liste des sous-traitants L'organisme doit déclarer à ses clients la liste des sous-traitants auxquels il délègue une partie de ses activités et préciser la nature de cette délégation. Cette déclaration, lorsqu'elle est nécessaire, doit être intégrée dans les contrats de l'organisme.
EXI_TC_50	Cadre juridique de la sous-traitance Chaque sous-traitance doit être encadrée juridiquement, au minimum par une convention de service et un accord de confidentialité. Le cadre juridique de chaque sous-traitance doit spécifier les responsabilités et exigences de sécurité transmises au sous-traitant. Une clause d'audit doit également être incluse dans le cadre juridique convenu entre les parties.
EXI_TC_51	Audit de la sous-traitance Des audits doivent être régulièrement menés pour s'assurer que le sous-traitant a effectivement implémenté les mesures de sécurité nécessaires à la couverture des exigences de sécurité du contrat. Les audits peuvent être réalisés par les équipes en charge du contrôle interne de l'organisme ou par un tiers mandaté par ce dernier.
EXI_TC_52	Liste des sous-traitants de « second niveau » Chaque sous-traitant dit de « premier niveau » doit déclarer sa propre liste des entreprises auxquelles il sous-traite une partie de ses activités et préciser la nature de cette délégation. Ces sous-traitants dits de « second niveau » doivent être audités par le sous-traitant de premier niveau.

4.1.12 Gestions des incidents de sécurité

EXIGENCE	DESCRIPTION
EXI_TC_53	Mise en œuvre d'une procédure de gestion d'incident de sécurité Une procédure de gestion d'incident de sécurité dans le cadre de la gestion des Systèmes d'Acceptation CB et des Serveurs Monétiques doit être implémentée. Elle doit prévoir : • Une identification des acteurs intervenant dans la gestion des incidents ; • Une gestion des alertes ; • Une procédure de recherche des causes et des origines de l'incident ; • Un contrôle par échantillonnage ; • Une procédure de remontée d'information auprès du GIE CB, notamment en cas de suspicion de fraude, selon la procédure décrite en annexe A1 ; • Un archivage des incidents.
EXI_TC_54	Documentation des activités effectuées pour chaque client Afin de faciliter la réponse à incident et l'information des parties prenantes en cas de compromission de l'organisme, la liste des différentes activités réalisées pour chaque client doit être tenue à jour.

4.1.13 Expédition de Points d'Acceptation

EXIGENCE	DESCRIPTION
EXI_TC_55	Conditions d'expédition (scellé et inventaire) Avant toute expédition d'un ensemble de Point d'Acceptation, l'organisme doit : • Apposer un scellé sur les emballages des Points d'Acceptation ; • Fournir un inventaire électronique et papier des Points d'Acceptation à destination de chaque destinataire. Cet inventaire doit préciser les numéros de série des Points d'Acceptation CB.

4.1.14 Gestion de la Continuité d'Activité

EXIGENCE	DESCRIPTION
EXI_TC_56	Garantie de continuité des activités Des mesures doivent être mises en œuvre pour garantir une continuité des activités liées à la gestion des Systèmes d'Acceptation CB et des serveurs monétiques. Il est recommandé que ces mesures fassent partie intégrante d'un Plan de Continuité d'Activité.

4.2 Développement

4.2.1 Gestion des actifs

EXIGENCE	DESCRIPTION
EXI_DEV_1	Liste des applications monétiques développées L'organisme doit tenir à jour la liste des applications qu'il développe et qui sont dédiées aux Systèmes d'Acceptation CB et au Serveurs Monétiques. Cette liste doit contenir au minimum : • Un identifiant unique pour chaque logiciel • Les numéros de version de chaque logiciel maintenu et supporté • Une empreinte cryptographique à l'état de l'art permettant de vérifier l'intégrité de chaque version de logiciel maintenu et supporté

4.2.2 Sécurité des codes sources

EXIGENCE	DESCRIPTION
EXI_DEV_2	Gestion de versions logicielles L'organisme doit disposer d'un système de gestion des versions garantissant que l'ensemble des modifications apportées au code sont traçables, que le code est intègre et que l'accès au code source des applications par les développeurs est authentifié.
EXI_DEV_3	Accès au code source du logiciel L'accès au code source du logiciel d'un Système d'Acceptation CB ou d'un Serveur Monétique doit être réservé aux seuls contractants ayant le besoin d'en connaître. Le dépôt des codes sources des logiciels destinés à être embarqués dans un Système d'Acceptation CB ou dans un Serveur Monétique doit être réalisé sur des serveurs hébergés au minimum dans une zone orange. Cela concerne aussi bien le serveur physique que le serveur de virtualisation exécutant la machine virtuelle correspondante.
EXI_DEV_4	Sauvegarde et archivage des codes sources. Une procédure de gestion des sauvegardes et de l'archivage des codes sources des logiciels de Systèmes d'Acceptation CB et des Serveurs Monétiques doit être implémentée et appliquée. Ces sauvegardes doivent être conservées au minimum dans des zones orange.

4.2.3 Sécurité du développement

EXIGENCE	DESCRIPTION
EXI_DEV_5	Développement des logiciels en zone sécurisée Le développement des logiciels destinés à être embarqués dans un Système d'Acceptation CB ou dans un Serveur Monétique doit être réalisé au sein des locaux de l'organisme : • Au minimum en zone jaune, pour les organismes dont l'activité est principalement dédiée au développement des logiciels des Systèmes d'Acceptation CB ou des Logiciels Monétiques. • Au minimum en zone orange pour les autres organismes.
EXI_DEV_6	Sécurité des environnements de développement Les environnements de développement doivent être séparés du reste du réseau de l'organisme. Les environnements de production, de pré-production, de recette et de test doivent être distincts et protégés les uns des autres. L'environnement de production ne doit pas être accessible depuis un poste de développeur.
EXI_DEV_7	Développement sécurisé L'organisme doit définir et mettre en œuvre un processus formel pour le développement sécurisé des logiciels d'acceptation. Ce processus doit permettre : • D'éviter les erreurs de développement conduisant à des vulnérabilités dans les applications, • D'assurer la formation et le maintien des compétences des développeurs dans le domaine du développement sécurisé, • D'identifier les failles potentielles de sécurité dès la conception et tout au long du cycle de vie des logiciels, en s'appuyant sur une méthodologie d'analyse de risques et sur la modélisation des menaces.
EXI_DEV_8	Recette fonctionnelle et sécuritaire La recette fonctionnelle (tests fonctionnels sur l'implémentation de la spécification reconnue par CB) et sécuritaire des logiciels destinés à être embarqués dans un Système d'Acceptation CB doit être réalisée par l'organisme sur le site de développement, dans une zone jaune au minimum. Si le développement est réalisé en zone jaune (cas d'une activité principalement dédiée au développement de logiciels monétiques), les zones peuvent être mutualisées. Dans ce cas de figure, les environnements techniques doivent toutefois être séparés (logiquement ou physiquement).

EXIGENCE	DESCRIPTION
EXI_DEV_9	Séparation des tâches L'organisme en charge du développement doit respecter le principe de séparation des tâches. C'est-à-dire que ce ne sont pas les mêmes contractants qui développent, réalisent la recette et les activités de support d'exploitation (lorsque ce service est fourni par l'organisme en question, est entendu par support toute activité d'aide à l'installation et au support sur incidents).

4.2.4 Signature et contrôle des logiciels

EXIGENCE	DESCRIPTION
EXI_DEV_10	Signature électronique des logiciels L'organisme doit définir et mettre en œuvre un processus de signature électronique de ses logiciels d'acceptation, incluant en particulier une description des outils nécessaires pour signer les logiciels embarqués. La signature électronique des logiciels doit être réalisée par l'organisme sur le site de développement dans une zone adaptée : • Au minimum en zone jaune, pour les organismes dont l'activité est principalement dédiée au développement des logiciels des Systèmes d'Acceptation CB ou des Logiciels Monétiques. • Au minimum en zone orange pour les autres organismes. Le niveau de sécurité de la signature doit être conforme à l'état de l'art.
EXI_DEV_11	Stockage des outils et clés de signature électronique Les outils de signature électronique des logiciels destinés à être embarqués dans un Point d'Acceptation CB et dans un serveur monétique doivent être stockés au minimum en zone orange. Les secrets cryptographiques nécessaires à cette signature doivent être conservés en zone rouge.
EXI_DEV_12	Contrôle des logiciels en exploitation L'organisme doit fournir à ses clients la documentation et les moyens leur permettant d'effectuer un contrôle des logiciels fournis. En particulier, les clients de l'organisme doivent être en mesure de valider la signature de chaque version qui leur est fournie.

4.2.5 Protection des secrets cryptographiques

EXIGENCE	DESCRIPTION

EXI_DEV_13	Gestion des secrets cryptographiques
	
	Un processus de gestion des secrets cryptographiques (tels que définis en annexe B3) doit être implémenté et prévoir :
	• Une gestion des accès aux secrets :
	  ○ Identification du personnel habilité,
	  ○ Traçabilité des accès
	  ○ Revue annuelle des droits d'accès
	• Le respect des principes de contrôle mutuel et de connaissance répartie
	• Un processus de vérification de l'intégrité des secrets
	• Un processus de renouvellement des secrets (tous les deux ans)
	• Une gestion de l'archivage des secrets

EXI_DEV_14	Archivage des secrets cryptographiques L'archivage des secrets cryptographiques doit respecter les règles suivantes : • Il doit être hébergé sur un espace de stockage interne à l'organisme et propriété de celui-ci. • Il doit être accessible selon les règles prévues par la procédure de gestion des accès. • Les données archivées doivent être chiffrées. • La durée de rétention minimale des archives doit être de 6 mois.

4.3 Intégration

4.3.1 Gestion des actifs

EXIGENCE	DESCRIPTION
EXI_INT_1	Inventaire des Points d'Acceptation CB Un inventaire des Points d'Acceptation CB en cours d'intégration doit être tenu à jour. Celui-ci doit spécifier le numéro de série du terminal, le type de terminal, le statut de son agrément CB, et le détail des versions des logiciels installés. Il doit préciser pour chaque appareil son statut (en cours d'intégration, en stock, expédié, etc.). Pour les versions logicielles détaillées, un niveau de détail similaire à ce qui est fourni dans les « *approval files* » ou les fiches « ID CB » est attendu (composants logiciels, checksums). La liste des matériels agréés, des ITP correspondants et des dates de fin de vie est tenue à jour par le Groupement des Cartes Bancaires et publiée sur son site.

4.3.2 Procédures et responsabilités

EXIGENCE	DESCRIPTION
EXI_INT_2	Chargement sécurisé des logiciels dans un Point d'Acceptation Les micro-logiciels (*Firmware*), les chargeurs d'amorçage (*bootloader*) et les applications de paiement à charger dans un Point d'Acceptation CB lors de son intégration doivent être récupérés et déployés de manière sécurisée, en garantissant leur intégrité et leur authenticité : • L'intégrateur doit s'assurer que les versions des logiciels déployés sont bien agréées par CB, en vérifiant en particulier la valorisation de l'ITP. • La procédure suivie pour effectuer cette vérification doit être formalisée (acteurs, moyens, rôles et responsabilités). Lorsqu'un défaut d'intégrité ou d'authenticité des logiciels est détecté, une procédure de gestion des incidents conforme aux exigences formulées précédemment (EXI_TC_53) doit être suivie.

EXIGENCE	DESCRIPTION
EXI_INT_3	Processus de récupération des secrets (signature, réactivation) Lors de la phase d'intégration d'un Système d'Acceptation CB, un processus de récupération des secrets nécessaires à la validation de signature et à la réactivation PCI doit être implémenté et prévoir : • Une procédure de contrôle de l'intégrité (acteurs, moyens) ; • Une procédure de gestion des incidents en cas de défaut d'intégrité (acteurs, moyens) conforme aux exigences formulées précédemment (EXI_TC_53).

4.3.3 Zones de sécurité

EXIGENCE	DESCRIPTION
EXI_INT_4	Zone de stockage des logiciels monétiques Les logiciels monétiques doivent être stockés sur un support informatique ou sur un serveur hébergé en zone orange .
EXI_INT_5	Zone de chargement des logiciels monétiques L'organisme doit réaliser le chargement des logiciels systèmes (système d'exploitation et modules EMV) et/ou des logiciels monétiques (applications agréées CB) nécessaires dans un Système d'Acceptation CB depuis un système hébergé au minimum dans une zone orange .
EXI_INT_6	Zones de stockage des Points d'Acceptation Les Points d'Acceptation CB doivent être stockés dans des salles dédiées localisées en zone jaune . Les Points d'Acceptation en attente d'intégration et les Points d'Acceptation déjà intégrés doivent être stockés dans des salles distinctes.

4.3.4 Mesures cryptographiques (sécurité des certificats TLS)

EXIGENCE	DESCRIPTION
EXI_INT_7	Chargement des certificats racines d'Autorité de Certification Avant toute utilisation d'un Point d'Acceptation, un certificat racine d'autorité de certification est chargé par l'intégrateur dans une phase de personnalisation du Système d'Acceptation. Plusieurs certificats racines d'autorités de certification peuvent être installés dans une seule machine. Les certificats pourront être obtenus auprès des autorités de certification correspondantes. Si nécessaire, le renouvellement des certificats racines peut se faire lors d'un retour en maintenance. Dans un but de traçabilité, la liste des clés publiques installées doit être consultable.
EXI_INT_8	Sécurité des clés d'authentification des Points d'Acceptation CB Lorsqu'un mécanisme d'authentification mutuelle des Points d'Acceptation CB avec le système d'acceptation est utilisé, la clé privée du certificat client des Points d'Acceptation est installée par l'intégrateur. Seules les personnes habilitées par l'organisme en charge de l'intégration doivent être en mesure de manipuler cette clé privée. Elle doit rester confidentielle, notamment vis-à-vis de l'accepteur, des porteurs et de toute personne non habilitée par l'intégrateur à intervenir sur le Système d'Acceptation. Elle ne doit pas pouvoir être exportée ou consultée sur le Système d'Acceptation.
EXI_INT_9	Certificat de l'autorité de certification du constructeur Le certificat de l'autorité de certification du constructeur est obtenu auprès de celui-ci. Les clés publiques sont fournies par le biais d'un certificat conforme aux exigences CB pour la sécurité des Systèmes d'Acceptation [2].

4.4 Préparation/Installation

4.4.1 Gestion des actifs

EXIGENCE	DESCRIPTION
EXI_PREP_1	Inventaire des Points d'Acceptation en cours de préparation Un inventaire précis des Points d'Acceptation CB en cours de préparation doit être tenu à jour. Celui-ci doit spécifier le numéro de série du terminal, le type de terminal, le statut de son agrément CB et le détail des versions des logiciels installés. Il doit préciser pour chaque appareil son statut (en cours de préparation en stock, expédié, etc.) Pour les versions logicielles détaillées, un niveau de détail similaire à ce qui est fourni dans les « *approval files* » ou les fiches « ID CB » est attendu (composants logiciels, checksums). La liste des matériels agréés, des ITP correspondants et des dates de fin de vie est tenue à jour par le Groupement des Cartes Bancaires et publiée sur son site.

4.4.2 Procédures et responsabilités

EXIGENCE	DESCRIPTION
EXI_PREP_2	Récupération et chargement sécurisé des logiciels dans un Point d'Acceptation Lors de la préparation d'un Point d'Acceptation CB, tous les composants logiciels (firmware, logiciels système, applications de paiement, etc.) doivent être récupérés et déployés de manière sécurisée, en garantissant leur intégrité et leur authenticité : • Le préparateur doit s'assurer que les versions des logiciels déployés sont bien agréées par CB, en vérifiant en particulier la valorisation de l'ITP • La procédure suivie pour effectuer cette vérification doit être formalisée (acteurs, moyens, rôles et responsabilités) Lorsqu'un défaut d'intégrité ou d'authenticité des logiciels est détecté, une procédure de gestion des incidents conforme aux exigences formulées précédemment (EXI_TC_53) doit être suivie.
EXI_PREP_3	Procédure d'installation des Points d'Acceptation Une procédure d'installation des Points d'Acceptation CB doit être formalisée, identifiant les acteurs impliqués et les moyens de contrôle de leur identité. Elle doit également décrire les moyens d'assistance mis à disposition des Accepteurs (installation sur site, support téléphonique, etc.).

EXIGENCE	DESCRIPTION
EXI_PREP_4	Information sur la date de fin de vie des Points d'Acceptation L'organisme réalisant la préparation d'un Point d'Acceptation CB doit préciser à son client (en général l'Accepteur) la date de fin de vie dudit Point d'Acceptation. Il est recommandé d'insérer cette date dans la procédure d'installation du PA, et d'y ajouter une référence à la section « agréments acceptation » sur le site du GIE CB (les dates de fin de vie sont précisées pour chaque matériel agréé).

4.4.3 Zones de sécurité

EXIGENCE	DESCRIPTION
EXI_PREP_5	Zone de sécurité pour la préparation Pour les organismes dont l'activité de gestion des Systèmes d'Acceptation CB est mutualisée avec d'autres activités non liées à la monétique, la préparation des Points d'Acceptation doit être effectuée en zone orange, au minimum. Pour les organismes dont la gestion de Systèmes d'Acceptation CB est la principale activité, la Préparation des Points d'Acceptation doit être effectuée en zone jaune au minimum.
EXI_PREP_6	Zones de stockage des Points d'Acceptation Les Points d'Acceptation CB doivent être stockés dans des salles dédiées localisées en zone jaune. Les Points d'Acceptation en attente de préparation et les Points d'Acceptation déjà préparés doivent être stockés dans des salles distinctes.
EXI_PREP_7	Zone de stockage des outils d'activation Les outils d'activation doivent être stockés dans une salle dédiée ou un coffre-fort, en zone rouge.

4.4.4 Mesures cryptographiques

EXIGENCE	DESCRIPTION
EXI_PREP_8	Chargement des certificats racines d'Autorité de Certification Avant toute utilisation d'un Point d'Acceptation, un certificat racine d'autorité de certification est chargé par le préparateur dans une phase de personnalisation du Système d'Acceptation. Plusieurs certificats racines d'autorités de certification peuvent être installés dans une seule machine. Les certificats pourront être obtenus auprès des autorités de certification correspondantes. Si nécessaire, le renouvellement des certificats racines peut se faire lors d'un retour en maintenance. Dans un but de traçabilité, la liste des clés publiques installées doit être consultable.

4.4.5 Contrôles en installation

EXIGENCE	DESCRIPTION
EXI_PREP_9	Contrôle de l'intégrité physique des Points d'Acceptation Des procédures de contrôle de l'intégrité physique des Points d'Acceptation CB doivent être implémentées et appliquées sur l'ensemble de la chaîne d'installation du matériel (mise en service, initialisation, déploiement).
EXI_PREP_10	Gestion des incidents de défaut d'intégrité physique à l'installation En cas de défaut d'intégrité physique constaté lors de la procédure d'installation d'un Point d'acceptation CB, une procédure de gestion des incidents conforme aux exigences formulées précédemment (EXI_TC_53) doit être suivie.

4.5 Maintenance et mise au rebut

4.5.1 Gestion des actifs

EXIGENCE	DESCRIPTION
EXI_MAINT_1	Inventaire des Points d'Acceptation en cours de maintenance Un inventaire des Points d'Acceptation CB en cours de maintenance doit être tenu à jour. Celui-ci doit spécifier le numéro de série du terminal, le type de terminal, le statut de son agrément CB, le détail des versions des logiciels installés et les références de l'accepteur (société, adresse, téléphone). L'inventaire des versions des logiciels doit avoir un niveau de détail similaire à ce qui est fourni dans les « *approval files* » ou les fiches « ID CB » (composants logiciels, checksums). La liste des matériels agréés, des ITP correspondants et des dates de fin de vie est tenue à jour par le Groupement des Cartes Bancaires et publiée sur son site.
EXI_MAINT_2	Conservation des informations sur les Points d'Acceptation détruits L'organisme doit conserver (sur au moins 12 mois glissants), sur le site de destruction, le numéro de série d'un Point d'Acceptation CB détruit, ainsi que le client concerné (société, adresse, coordonnées).

4.5.2 Procédures et responsabilités

EXIGENCE	DESCRIPTION
EXI_MAINT_3	Réparation d'un Point d'Acceptation Un processus de réparation des Points d'Acceptation CB et des serveurs monétiques doit être implémenté. Celui-ci doit : • Identifier les acteurs (externes ou internes) intervenant dans le processus et leurs responsabilités, • Lister les moyens utilisés pour réaliser cette opération de maintenance, • Vérifier que toute opération de maintenance monétique sur un Point d'Acceptation CB ou d'un serveur monétique est tracée, en identifiant au minimum le mainteneur, la date et la nature de l'opération de maintenance effectuée, • Identifier si la journalisation des opérations de maintenance est effectuée de façon automatique ou manuelle.
EXI_MAINT_4	Traçabilité des opérations de maintenance Les traces de toutes les opérations de maintenance monétique sur un Point d'Acceptation CB ou un serveur monétique doivent être consultables a posteriori.

EXIGENCE	DESCRIPTION
EXI_MAINT_5	Identification des actifs par le support téléphonique Avant toute action de support téléphonique, le mainteneur doit demander au commerçant le numéro de série du Point d'Acceptation CB ou l'identifiant du serveur monétique concerné.
EXI_MAINT_6	Récupération sécurisée des logiciels monétiques Tous les composants logiciels susceptibles d'être chargés par le mainteneur dans un Point d'Acceptation CB (firmware, logiciels système, applications de paiement, etc.) doivent être récupérés auprès du constructeur, du distributeur ou du développeur de manière sécurisée, en garantissant leur intégrité et leur authenticité : • L'organisme doit identifier les moyens utilisés (téléchargement depuis un serveur, récupération depuis un support physique, etc.) pour la récupération des versions des logiciels à charger, et s'assurer que ces moyens garantissent l'authenticité et l'intégrité des logiciels. • L'organisme doit s'assurer que les versions des logiciels récupérées sont bien agréées par CB, en vérifiant en particulier la valorisation de l'ITP et en recalculant les sommes de contrôles. • La procédure suivie pour effectuer ces vérifications doit être formalisée (acteurs, moyens, rôles et responsabilités). Lorsqu'un défaut d'intégrité ou d'authenticité des logiciels est détecté, une procédure de gestion des incidents conforme aux exigences formulées précédemment (EXI_TC_53) doit être suivie.
EXI_MAINT_7	Contrôle de la version des logiciels des Point d'Acceptation Lors des opérations de maintenance sur un Point d'Acceptation CB, une procédure de contrôle des numéros de version des logiciels installés doit être suivie afin de s'assurer de leur intégrité et leur authenticité : • Le mainteneur doit s'assurer que les versions des logiciels déployés sont bien agréées par CB, en vérifiant en particulier la valorisation de l'ITP. • Le mainteneur doit s'assurer qu'aucune régression logicielle n'a eu lieu depuis la dernière maintenance du Point d'Acceptation. • La procédure suivie pour effectuer ces vérifications doit être formalisée (acteurs, moyens, rôles et responsabilités). Lorsqu'un défaut d'intégrité ou d'authenticité des logiciels est détecté ou si une régression logicielle est constatée, une procédure de gestion des incidents conforme aux exigences formulées précédemment (EXI_TC_53) doit être suivie.

EXIGENCE	DESCRIPTION
EXI_MAINT_8	Procédure de télé mise à jour d'un Point d'Acceptation CB Une procédure de télé mise à jour d'un Point d'Acceptation CB doit être formalisée. Elle doit identifier l'ensemble des acteurs et des moyens permettant de réaliser une télé mise à jour. Elle doit notamment prévoir le cas d'une télé mise à jour en cours d'exploitation faisant suite à une opération de télécollecte ou de télé paramétrage du Point d'Acceptation CB.

4.5.3 Sécurité des ressources humaines

EXIGENCE	DESCRIPTION
EXI_MAINT_9	Engagement personnel pour la réactivation d'un Point d'Acceptation L'organisme doit faire signer un engagement personnel de confidentialité par tous les opérateurs responsables de la réactivation de la sécurité d'un Point d'Acceptation CB.

4.5.4 Zones de sécurité

EXIGENCE	DESCRIPTION
EXI_MAINT_10	Zone pour les activités de support Les activités de support liées à la maintenance (support téléphonique) doivent être effectuées en zone verte .
EXI_MAINT_11	Zone pour le stockage des Points d'Acceptation à réparer Les Points d'Acceptation en attente de réparation doivent être stockés au minimum en zone verte .
EXI_MAINT_12	Zone pour le stockage des Points d'Acceptation réparés Les Points d'Acceptation réparés et ayant été réactivés doivent être stockés en zone jaune .
EXI_MAINT_13	Zone d'hébergement des outils de suivi des réparations L'outil de suivi des réparations des Points d'Acceptation CB doit être installé sur un serveur hébergé (le serveur physique ou le serveur de virtualisation exécutant la machine virtuelle correspondante) au minimum dans une zone orange .

EXIGENCE	DESCRIPTION
EXI_MAINT_14	Zone de réactivation PCI Pour les organismes dont l'activité de gestion des Systèmes d'Acceptation CB est mutualisée avec d'autres activités, la réactivation sur site de la sécurité d'un Point d'Acceptation CB doit être réalisée en zone orange. Pour les organismes dont l'activité de gestion des Systèmes d'Acceptation CB est la principale activité, la réactivation sur site peut être réalisée en zone jaune.
EXI_MAINT_15	Zone d'hébergement et stockage des outils de réactivation PCI Les outils utilisés pour la Réactivation d'un Point d'Acceptation CB sont stockés en zone rouge.
EXI_MAINT_16	Zone pour les activités de démontage et destruction des Points d'Acceptation CB L'organisme, s'il assure lui-même la destruction des Points d'Acceptation mis au rebut, doit effectuer le démontage et la destruction en zone jaune.
EXI_MAINT_17	Zone de stockage des composants d'un Point d'Acceptation après destruction Le stockage sur le site de destruction des composants non sensibles d'un Point d'Acceptation CB mis au rebut doit être effectué en zone verte. Le stockage des composants sensibles doit être effectué en zone orange.

4.5.5 Contrôles en maintenance

EXIGENCE	DESCRIPTION
EXI_MAINT_18	Contrôle de l'intégrité physique des Points d'Acceptation avant réparation L'intégrité physique des Points d'Acceptation CB doit être vérifiée avant leur réparation. En cas de doute sur l'intégrité du matériel ou lorsqu'une compromission physique est détectée, une procédure de gestion des incidents conforme aux exigences formulées précédemment (EXI_TC_53) doit être suivie.

4.5.6 Contrôle de la réactivation PCI

EXIGENCE	DESCRIPTION
EXI_MAINT_19	Traçabilité des opérations de réactivation L'organisme doit tenir à jour une main courante (ou un journal informatique) de toutes les réactivations réalisées, contenant la date et l'heure de la réactivation, le nom ou l'identifiant des deux opérateurs présents et le numéro de série du Point d'Acceptation CB réactivé.
EXI_MAINT_20	Gestion des secrets liés aux outils de réactivation Un processus de gestion des secrets (données d'authentifications, éléments cryptographiques, etc.) liés aux outils de réactivation doit être implémenté et prévoir : • Une gestion des accès aux secrets, • Un respect du principe de contrôle mutuel et de connaissance répartie, • Un processus de renouvellement des secrets, • Une gestion de l'archivage des secrets (stockage, accès), • Une procédure de contrôle de l'intégrité des secrets.
EXI_MAINT_21	Protection des outils de réactivation Les outils utilisés pour la réactivation d'un Point d'Acceptation CB doivent être protégés de manière adéquate : • Les acteurs ayant accès aux outils doivent être identifiés. • L'accès ou l'utilisation des outils de réactivation doit être soumis à un double contrôle. Une personne seule ne doit pas pouvoir initier une réactivation. • Toute sortie des outils de réactivation doit être tracée. Les outils sont placés sous la responsabilité d'un opérateur désigné nominativement et dûment habilité (voir § 4.1.2). • Les outils de réactivation doivent être remis en zone sécurisée (EXI_MAINT_15) après chaque utilisation, ou au plus tard en fin de journée.
EXI_MAINT_22	Respect des bonnes pratiques liées aux outils de réactivation L'organisme doit suivre les préconisations et respecter les bonnes pratiques sécuritaires (mode opératoire, mesures de sécurité à mettre en place) décrites dans la documentation des outils de réactivation des Point d'Acceptation CB fournie par le constructeur.

EXIGENCE	DESCRIPTION
EXI_MAINT_23	Gestion d'incident en cas de compromission des outils de réactivation En cas de compromission physique ou logique des outils utilisés pour la réactivation d'un Point d'Acceptation CB, une procédure de gestion des incidents conforme aux exigences formulées précédemment (EXI_TC_53) doit être suivie.

4.5.7 Mise au rebut

EXIGENCE	DESCRIPTION
EXI_MAINT_24	Formalisation du processus de mise au rebut Un processus de mise au rebut d'un Système d'Acceptation CB doit être formalisé. Celui-ci doit : • Identifier les acteurs (externes ou internes) intervenant dans le processus et leurs responsabilités ; • Lister les moyens utilisés pour réaliser les opérations de mise au rebut ; • Vérifier que toute opération de mise au rebut est tracée, en identifiant au minimum le mainteneur, la date et la nature de l'opération de mise au rebut effectuée ; • Identifier si la journalisation des opérations de mise au rebut est effectuée par un processus automatique ou manuel ; • Vérifier que les traces de toutes opérations de mise au rebut sont consultables à posteriori (cf. EXI_MAINT_2).
EXI_MAINT_25	Notification au constructeur de la mise au rebut des Points d'Acceptation En cas d'impossibilité de réparation d'un Système d'Acceptation CB, le mainteneur doit notifier le constructeur de la mise au rebut du matériel. Le matériel à détruire doit alors être mis sous scellé et livré selon les exigences propres aux activités de distribution.
EXI_MAINT_26	Procédure de destruction des Points d'Acceptation S'il réalise lui-même la destruction des Points d'Acceptation, l'organisme doit formaliser une procédure de démontage des Points d'Acceptation CB à détruire. Cette procédure doit permettre d'identifier les composants des Points d'Acceptation considérés comme sensibles et doit garantir que les données sensibles (clés cryptographiques, données d'authentification) sont effacées de façon sûre préalablement à la destruction du Point d'Acceptation.

EXIGENCE	DESCRIPTION
EXI_MAINT_27	Sortie des composants sensibles stockés pour destruction L'organisme doit garantir que la sortie du stock des composants sensibles d'un Point d'Acceptation CB n'est autorisée que pour procéder à leur destruction (aucun usage ou revente à des fins de pièces détachées n'est autorisé).
EXI_MAINT_28	Destruction des étiquettes avec les numéros de série du Point d'Acceptation L'organisme doit garantir que toutes les étiquettes mentionnant le numéro de série d'un Point d'Acceptation CB sont détruites lors de son démontage.
EXI_MAINT_29	Certificat de destruction des Points d'Acceptation L'organisme doit fournir à ses clients un certificat de destruction pour chaque Point d'Acceptation CB détruit. Ce certificat doit préciser le numéro de série du Point d'Acceptation.

4.5.8 Relations avec les fournisseurs

EXIGENCE	DESCRIPTION
EXI_MAINT_30	Contractualisation avec les fournisseurs de logiciels monétiques Les contrats avec les fournisseurs ayant développé les logiciels monétiques ou ayant distribué les Points d'Acceptation CB maintenus par l'organisme doivent prévoir : • Les modalités de maintien en condition opérationnelle des logiciels monétiques, • La mise à disposition de la documentation et des moyens permettant d'effectuer le contrôle de l'authenticité et de l'intégrité des logiciels récupérés et déployés sur les Points d'Acceptation.

4.6 Exploitation

4.6.1 Gestion des actifs

EXIGENCE	DESCRIPTION
EXI_EXPL_1	Inventaire des Points d'Acceptation CB Un inventaire des Points d'Acceptation CB en cours d'exploitation doit être tenu à jour. Celui-ci doit spécifier le numéro de série du terminal, le type de terminal, le statut de son agrément CB, le détail des versions des logiciels installés et les références de l'accepteur (société, adresse, téléphone). L'inventaire des versions des logiciels doit avoir un niveau de détail similaire à ce qui est fourni dans les « *approval files* » ou les fiches « ID CB » (composants logiciels, checksums). La liste des matériels agréés, des ITP correspondants et des dates de fin de vie est tenue à jour par le Groupement des Cartes Bancaires et publiée sur son site.
EXI_EXPL_2	Inventaire des serveurs monétiques Chaque organisme intervenant dans la gestion de serveurs monétiques doit être en mesure de préciser, pour chaque client (au sens contractuel du terme), les serveurs qu'il gère pour lui (nominal, premier ou deuxième secours).
EXI_EXPL_3	Processus de télécollecte/téléparamétrage formalisé Un processus de télécollecte/téléparamétrage ou de gestion des fichiers de télécollecte (CB2A) d'un Système d'Acceptation CB doit être formalisé. Les acteurs sont identifiés et les moyens pour réaliser la télécollecte et le téléparamétrage sont prévus.

4.6.2 Zones de sécurité

EXIGENCE	DESCRIPTION
EXI_EXPL_4	Zone de sécurité pour les serveurs de télécollecte Les serveurs de télécollecte doivent être localisés dans une salle située en zone orange.
EXI_EXPL_5	Zone de sécurité pour les Serveurs Monétiques Les Serveurs Monétiques doivent être localisés dans une salle située en zone rouge.

4.6.3 Mesures cryptographiques

EXIGENCE	DESCRIPTION
EXI_EXPL_6	Protection des clés privées des serveurs Les clés privées associées aux certificats TLS des serveurs doivent être protégées en confidentialité et en intégrité. Au minimum, des permissions strictes doivent être appliquées sur les fichiers de clés. Lorsque cela est possible, il est recommandé que la clé privée ne soit pas exportable.
EXI_EXPL_7	Renouvellement des clés privées des Points d'Acceptation CB Lorsqu'un mécanisme d'authentification mutuelle des Points d'Acceptation CB avec un serveur est opéré par l'organisme en charge de l'exploitation, une procédure de renouvellement des clés privées des Points d'Acceptation CB doit être implémentée. Seules les personnes habilitées par l'organisme en charge de l'exploitation doivent être en mesure de manipuler ces clés privées. Elles doivent rester confidentielles, notamment vis-à-vis de l'Accepteur et de toute personne non habilitée par l'exploitant à intervenir sur le Système d'Acceptation.

4.6.4 Sécurité organisationnelle

EXIGENCE	DESCRIPTION
EXI_EXPL_8	Contrôle de l'intégrité et de l'authenticité des logiciels Une procédure de contrôle du numéro de version et de l'intégrité des logiciels d'un Système d'Acceptation CB ou d'un serveur monétique doit être implémentée : • L'exploitant doit s'assurer que les versions des logiciels utilisés sont bien agréées par CB, en vérifiant en particulier la valorisation de l'ITP. • La procédure suivie pour effectuer cette vérification doit être formalisée (acteurs, moyens, rôles et responsabilités). En cas de compromission avérée de l'un des composants du Système d'Acceptation, ou lorsqu'un défaut d'intégrité ou d'authenticité des logiciels est détecté, une procédure de gestion des incidents conforme aux exigences formulées précédemment (EXI_TC_53) doit être suivie.

4.6.5 Relations avec les fournisseurs

EXIGENCE	DESCRIPTION
EXI_EXPL_9	Contrat avec le développeur des logiciels Les contrats avec les organismes ayant développé les logiciels doivent prévoir : • Un service de maintien en conditions opérationnelles des logiciels ; • La mise à disposition de la documentation et des moyens permettant d'effectuer le contrôle de l'intégrité des logiciels.

4.6.6 Conformité aux exigences sécuritaires CB

EXIGENCE	DESCRIPTION
EXI_EXPL_10	Respect des exigences de sécurité CB applicables aux Systèmes d'Acceptation En tant que prestataire monétique tiers, l'organisme en charge de l'exploitation doit respecter les exigences de sécurité CB pour la sécurité des Systèmes d'Acceptation [2]. Ces exigences portent notamment sur la sécurité des serveurs informatiques, la sécurité des communications et la gestion des certificats TLS.

4.7 Stockage/Logistique

4.7.1 Gestion des actifs

EXIGENCE	DESCRIPTION
EXI_STOCK_1	Inventaire des Points d'Acceptation stockés Un inventaire des Points d'Acceptation CB stockés doit être tenu à jour. Il doit contenir au minimum les informations suivantes : le nombre, le type et le numéro de série des Points d'Acceptation CB stockés.

4.7.2 Procédures et responsabilités

EXIGENCE	DESCRIPTION
EXI_STOCK_2	Procédure de réception des Points d'Acceptation Une procédure de réception des Points d'Acceptation doit être formalisée. Elle doit au minimum traiter les points suivants : • Un contrôle sur le statut d'agrément CB des Systèmes d'Acceptation doit être effectué. Suivant le statut des Systèmes d'Acceptation, les mesures adéquates doivent être appliquées (voir l'annexe B2 Contrôle du statut d'agrément CB). • Un contrôle de l'intégrité physique des Points d'Acceptation doit être réalisé. Cela consiste à vérifier l'intégrité du scellé, ou de l'emballage en cas d'absence de scellé. • Un Procès-Verbal de bonne réception des Points d'Acceptation doit être renvoyé à l'expéditeur par le destinataire si le Distributeur ne procède pas à une traçabilité de la livraison. Par ailleurs, les acteurs intervenant dans le processus de réception des Points d'Acceptation doivent être clairement identifiés et respecter la procédure associée.

EXIGENCE	DESCRIPTION

EXI_STOCK_3	Procédure de retrait du stock
	
	Une procédure de retrait d'un Point d'Acceptation CB du stock doit être formalisée. Elle doit spécifier les éléments suivants :
	• Un Point d'Acceptation CB ne doit jamais être laissé sans surveillance lors du retrait du stock. Dans la phase de transit entre le stock et la destination (par exemple : la salle de préparation), le Point d'Acceptation doit rester sous le contrôle d'un logisticien ;
	• La dépose et la récupération des Points d'Acceptation CB dans les zones de stockage doivent être effectuées par des personnes différentes. Par exemple :
	  ○ Les logisticiens déposent les Points d'Acceptation CB non préparés dans les zones de stockages dédiées ;
	  ○ Les préparateurs prennent les Points d'Acceptation CB non préparés dans les zones de stockages dédiées.
	Par ailleurs, les acteurs intervenant dans le processus de retrait des Points d'Acceptation du stock doivent être clairement identifiés et respecter la procédure associée.

4.7.3 Zones de sécurité

EXIGENCE	DESCRIPTION
EXI_STOCK_4	Zone de sécurité pour les outils de gestion et d'identification du stock Les outils de gestion et d'identification du stock des Points d'Acceptation CB doivent être installés sur un serveur hébergé dans une zone orange.
EXI_STOCK_5	Zone de sécurité pour le stockage des Points d'Acceptation Pour l'ensemble des organismes : • Le stockage des Points d'Acceptation doit être effectué en zone jaune. • Les Points d'Acceptation doivent être séparés par statut (non préparés, préparés, mis au rebut). Pour les organismes dont l'activité de gestion des Systèmes d'Acceptation CB est mutualisée avec d'autres activités non liées à la monétique, les zones de stockage des Points d'Acceptation doivent être différentes de celles dédiées aux autres activités de l'organisme.

4.7.4 Gestion des incidents de sécurité

EXIGENCE	DESCRIPTION
EXI_STOCK_6	Gestion des incidents liés à l'intégrité physique des emballages Une procédure de gestion d'incident doit être définie et suivie en cas de suspicion d'atteinte délibérée à l'intégrité physique des scellés ou des emballages des Points d'Acceptation à leur réception. Cette procédure doit être conforme aux exigences formulées précédemment (EXI_TC_53). Elle doit en outre formaliser la remontée d'alerte auprès de l'expéditeur.

4.8 Distribution

4.8.1 Procédures et responsabilités

EXIGENCE	DESCRIPTION
EXI_DIST_1	Processus de transport des Points d'Acceptation CB Un processus de transport des Points d'Acceptation CB doit être formalisé depuis la récupération du PA jusqu'à la livraison au destinataire. Celui-ci doit préciser : • Les mesures de protection physique mises en œuvre ; • Les moyens mis en œuvre pour garantir la détection d'une ouverture non autorisée de l'emballage ; • Les acteurs intervenant dans le processus de transport ; • Les conditions de livraison des cartes de domiciliation des commerçants.

4.8.2 Sécurité opérationnelle

EXIGENCE	DESCRIPTION
EXI_DIST_2	Intégrité des scellés et des emballages L'intégrité des Points d'Acceptation CB doit être assurée lors de leur transport. Des contrôles des scellés ou des emballages doivent être effectués à chaque étape du transport.
EXI_DIST_3	Informations à faire figurer sur les bordereaux de livraison Les bordereaux de livraison doivent contenir la liste complète des numéros de série des Points d'Acceptation CB transportés. Cette liste est fournie par l'expéditeur, conformément aux exigences sécuritaires définies en EXI_TC_55 .
EXI_DIST_4	Traçabilité de la livraison Chaque étape du processus de livraison doit être tracée et faire l'objet d'un PV (remise, contrôles et livraison), afin de permettre notamment la détection d'une disparition d'un Système d'Acceptation.

4.8.3 Gestion des incidents de sécurité

EXIGENCE	DESCRIPTION
EXI_DIST_5	Gestion des incidents en cas de disparition de Points d'Acceptation Une procédure de gestion d'incident doit être définie et suivie en cas de disparition d'un ou plusieurs Points d'Acceptation pendant leur transport. Cette procédure doit être conforme aux exigences formulées précédemment (EXI_TC_53). Elle doit en outre formaliser la remontée d'alerte auprès de l'expéditeur et du destinataire.

4.9 Activités liées au PIN Online

Les activités liées au PIN Online présentées au chapitre 2 sont les suivantes :

- Gestion d'un centre de mise à la clé à distance (PIN Online)
- Gestion d'un centre d'injection de clés (PIN Online)
- Gestion d'un serveur de transchiffrement (PIN Online)

Dans le cas où l'une ou l'autre de ces activités est exercée, alors l'exigence suivante doit être respectée :

EXIGENCE	DESCRIPTION
EXI_PIN_1	Conformité de la gestion du PIN Online La gestion d'une activité liée au PIN Online par le Système d'Acceptation doit respecter les exigences internationales définies dans le standard PCI PIN Security [5]. Pour une compréhension du cadre général sur la mise en œuvre du PIN Online dans le système CB, le lecteur pourra se référer au référentiel CB dédié [3].

ANNEXE A : REMONTÉE D'INFORMATIONS AU GROUPEMENT DES CARTES BANCAIRES

Deux types de notifications sont prévus dans les exigences du présent document : la notification pour **suspicion de fraude** et la notification pour commande **d'opération non autorisée** dans le système CB (date de fin de déploiement, date de fin de vie). Les modèles de notification associés sont donnés ci-dessous.

A1. Procédure concernant la suspicion de fraude

Lorsque le professionnel est amené à réaliser des opérations sur tout ou partie d'un système d'acceptation, et qu'il détecte un élément de nature à générer de la fraude (Point d'acceptation modifié anormalement, vol d'une palette de points d'acceptation, logiciel non valide), et qu'il estime qu'il ne s'agit pas d'un fait isolé pouvant relever d'une erreur involontaire de manipulation, il doit envoyer un courriel à l'adresse « labelisation@cartes-bancaires.com » selon le format suivant :

Notification pour suspicion de fraude	
Date d'observation	
Identification du professionnel signalant	
Raison social organisme	
Adresse	
Référence / Labélisation n°	
Information technique sur le Système d'acceptation visé	
Constructeur	
Modèle	
ITP	
Version logicielle	
Observations détaillées	

Cette notification ne vise que la fraude aux moyens de paiement (modification matérielle ou logicielle d'un système d'acceptation, intrusion/malware sur un système d'acceptation, vol de secret de signature de logiciel, vol en masse de systèmes d'acceptation).
Elle ne vise pas la fraude commerciale (facturation abusive, vente abusive, …).

A2. Procédure concernant les non-conformités issues des contrôles de fin de vie

Lorsque le professionnel est amené à installer un Système d'acceptation CB dont le statut de l'agrément est à « fin de commercialisation/déploiement » ou « fin de vie » (sauf échange standard en cas de panne), ou pour toute opération de maintenance apportée sur un Système d'acceptation CB dont le statut de l'agrément CB est à « fin de vie », il doit envoyer un courriel à l'adresse « labelisation@cartes-bancaires.com » selon le format suivant :

Notification d'opération sur un Système d'Acceptation CB en fin de vie	
Date d'intervention	
Identification du professionnel signalant	
Raison social organisme	
Adresse	
Référence / Labélisation n°	
Information technique sur le Système d'acceptation visé	
Constructeur	
Modèle	
ITP	
Version logicielle	
Type d'opération effectuée	
Information commerciale	
Nom du client	
Donnée de contact du client	
Nom du point de vente	
Adresse du point de vente	

ANNEXE B : CONTRAINTES

B1. Risques sécuritaires à couvrir

Le tableau ci-dessous synthétise les scénarii de menace qui ont été considérés par le Groupement des Cartes Bancaires (GCB) et dont les exigences sécuritaires assurent la couverture.

Menaces physiques

PHY_MOD-01	Ajouter un piège matériel sur un Système d'Acceptation CB, sans le démonter (ajout d'un dispositif de capture piste magnétique/données porteur, par exemple)
PHY_SUB-01	Substituer un Point d'Acceptation CB par un autre piégé ou obsolète/vulnérable
PHY_PIE-01	Piéger un Système d'Acceptation CB en modifiant ses composants matériels (ajout d'un dispositif de capture piste magnétique/données porteur ou désactivation de la sécurité PCI, par exemple)
PHY_PIE-02	Réactiver de manière non autorisée, à l'aide des cartes/outils de réactivation PCI fournis par le fabricant, la sécurité PCI d'un Point d'Acceptation CB préalablement piégé
PHY_PIE-03	Voler les cartes/outils de réactivation PCI fournis par le fabricant, pour pouvoir réactiver la sécurité PCI d'un Point d'Acceptation CB préalablement piégé
PHY_PIE-04	Accéder à des composants de Systèmes d'Acceptation CB (cartes mères, terminaux entiers) destinés à être réformés, pour pouvoir récupérer des éléments de paramétrage réels permettant de refaire fonctionner des terminaux officiels ou de tester des moyens de contournement de la sécurité PCI

Menaces logiques

LOG_MOD-01	Modifier le paramétrage d'un Système d'Acceptation CB pour provoquer une télécollecte sur un serveur pirate
LOG_MOD-02	Modifier le paramétrage d'un Système d'Acceptation CB pour provoquer une mise à jour sur un serveur TMS pirate chargeant un logiciel obsolète/vulnérable
LOG_SUB-01	Substituer un des logiciels destinés à être installés dans un Système d'Acceptation CB par un autre piégé ou obsolète/vulnérable (stocké localement ou dans un TMS)
LOG_SUB-02	Substituer dans un Point d'Acceptation CB (via une clé USB, le port série RS-232, etc.) un logiciel installé par un autre piégé ou obsolète/vulnérable
LOG_VLN-01	Exploiter à distance une faille de sécurité d'un logiciel installé dans un Système d'Acceptation CB (par exemple via IP ou GPRS)
LOG_PIE-01	Piéger les codes sources d'un des logiciels destinés à être installés dans un Système d'Acceptation CB (ajout d'une fonction de capture piste magnétique/données porteur ou désactivation de la sécurité PCI, par exemple)
LOG_PIE-02	Voler les cartes/outils de signature logicielle fournis par le fabricant, pour pouvoir signer les logiciels destinés à être installés dans un Système d'Acceptation CB

B2. Contrôle du statut d'agrément CB

Le document « *Référencement et Labélisation des professionnels de l'Acceptation CB - Cadre général* » [1] décrit chaque étape du cycle de vie d'un Système d'Acceptation, ainsi que les obligations générales qui y sont associées. Ce chapitre précise les règles pour les opérations sur chaque étape du cycle de vie.

Étapes du cycle de vie d'un système d'acceptation

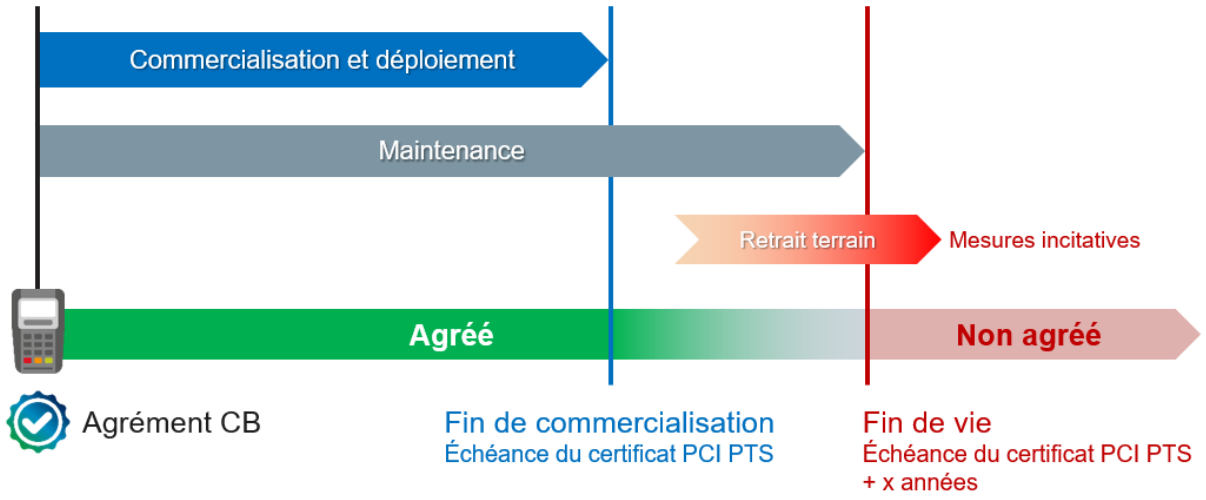


Figure 1 – Statut d'agrément d'un Système d'Acceptation CB

Statut entre « Fin de commercialisation / déploiement » et « Fin de vie »

Lorsqu'un Point d'Acceptation atteint l'échéance de fin de commercialisation (certificat PCI PTS échu), il n'est plus commercialisable. Aucun nouveau contrat ne peut être signé par le constructeur, l'un de ses Distributeur/Revendeurs ou bien un Intégrateur. De même, le Point d'Acceptation ne peut plus être déployé.
Toutefois, tant qu'un Point d'Acceptation n'a pas atteint la date de fin de vie de son agrément, il peut être :

- Maintenu/réparé en l'état ou remplacé par un modèle identique ;
- Mis à jour dans une version logicielle ayant un agrément à jour ;
- Mis au rebut.

Durant cette phase, les opérations de retrait progressif doivent être encouragées par l'ensemble des acteurs.

Statut « Fin de vie »

Tout Point d'Acceptation CB ayant atteint la date de fin de vie de son agrément ne peut plus être maintenu et doit être retiré du terrain et mis au rebut. CB a prévu des mesures incitatives (cf. document [1]) afin d'éviter le maintien sur le terrain de versions de Points d'Acceptation obsolètes d'un point de vue sécuritaire.

Responsabilités

STATUT	ACTEURS
Fin de commercialisation	Constructeurs, Distributeurs / Revendeurs, Intégrateur
Entre fin de déploiement et fin de vie	Constructeurs, Intégrateurs, Préparateurs, Distributeurs / Revendeurs, Accepteurs, Acquéreurs, Mainteneurs
Fin de vie	Tous les acteurs sont concernés par ce contrôle.

Obligations pour les Professionnels de l'Acceptation

Le dispositif de contrôle permanent du professionnel de l'acceptation (cf. § 4.1.10) doit inclure des dispositions relatives à la vérification de la conformité des Systèmes d'Acceptation CB gérés, de leur configuration et de leurs logiciels embarqués vis-à-vis de l'agrément CB.
En particulier, toute installation d'un Système d'Acceptation CB dont le statut de l'agrément est « fin de commercialisation/déploiement » doit être signalée au demandeur de la prestation ainsi qu'au Groupement des Cartes Bancaires CB via le formulaire défini en annexe A2 (sauf échange standard en cas de panne).
De même, pour toute opération de maintenance apportée sur un Système d'Acceptation CB dont le statut de l'agrément CB est « fin de vie ». Ce Système d'Acceptation CB doit alors au plus vite être remplacé par un Système d'Acceptation CB à jour vis-à-vis de son agrément.

B3. Biens sensibles

Secrets cryptographiques

La sécurité d'un Système d'Acceptation s'appuie sur un certain nombre de secrets cryptographiques. Ces secrets sont utilisés par les fonctions de protection des données sensibles, telles que les données d'identification et d'authentification, les certificats, les données carte ainsi que les différents logiciels embarqués dans ses composants.

Les secrets cryptographiques sont la plupart du temps des clés ou des bi-clés, utilisées pour :

- Signer les logiciels embarqués, et ainsi identifier de manière sûre les logiciels monétiques et leur version,
- Authentifier mutuellement les Systèmes d'Acceptation,
- Permettre la réactivation PCI d'un Point d'Acceptation,
- Mettre en œuvre le chiffrement du PIN Online.

Logiciels monétiques embarqués

Les logiciels monétiques embarqués dans un système d'acceptation sont de différentes natures. On peut notamment distinguer :

- Les micrologiciels (*Firmware*), en particulier ceux embarqués dans les modules de sécurité (PED, EPP, HSM),
- Les chargeurs d'amorçage (*bootloader*),
- Les logiciels système (OS, module EMV…),
- Les logiciels monétiques français (applications agréées CB).

Logiciels monétiques serveurs

Les logiciels monétiques déployés sur les serveurs utilisés dans la gestion et l'exploitation d'un système d'acceptation sont concernés par les exigences du présent référentiel. Au minimum, les logiciels suivants sont considérés comme des biens sensibles à protéger :

- Les logiciels des serveurs monétiques (monétique répartie, m-acceptation, etc.)
- Les logiciels de télé-mise à jour système des Systèmes d'Acceptation
- Les logiciels de gestion de parc
- Les logiciels permettant d'assurer la télécollecte et le téléparamétrage
- Les logiciels de gestion DUKPT et de renouvellement des TIK
- Les logiciels de transchiffrement du PIN.

Outils de réactivation PCI

La réactivation PCI met en œuvre un mécanisme sécuritaire autorisant la remise en service du système d'acceptation dans les conditions de conformité PCI. Cette réactivation ne peut être effectuée que lors d'une opération de maintenance de niveau 2.

Le mécanisme est défini par le Constructeur du Système d'Acceptation et s'appuie sur un dispositif logiciel ou matériel, désigné dans le présent document par le terme « outil de réactivation PCI ».

L'outil de réactivation PCI doit être protégé en disponibilité, en confidentialité et en intégrité sous la responsabilité de l'intervenant que le constructeur a approvisionné.

Clés de chiffrement du PIN

Les clés utilisées pour le chiffrement ou le transchiffrement du PIN permettent d'assurer la confidentialité et l'intégrité du PIN lors de son transport depuis le Point d'Acceptation jusqu'à l'Émetteur, qui en valide la valeur avant d'autoriser ou non l'opération de paiement.

Ces clés doivent donc être protégées de façon adéquate à tout moment de leur cycle de vie, qu'elles soient chargées dans un Point d'Acceptation ou dans un HSM de la chaine d'acceptation.

B4. Activités sensibles

De par leur nature, les activités sensibles ne sont pas éligibles au référencement. Les organismes exerçant ces activités doivent donc se soumettre à une labélisation REMPARTS.

Ces activités sont recensées dans le Tableau 2.

Note : tout acteur qui détient des outils de réactivation PCI opérationnels, même s'ils ne sont pas utilisés dans le cadre des activités déclarées, est soumis au processus de labélisation.

ACTIVITÉ	OPÉRATIONS SENSIBLES
Maintenance	Maintenance de niveau 2 : • Réparation d'un Point d'Acceptation avec ouverture de l'équipement (réactivation nécessaire) • Contrôle de l'intégrité du Point d'Acceptation démonté ; • Réactivation d'un Point d'Acceptation (utilisation d'une carte d'activation PCI ou d'un outil de réactivation PCI pour restaurer les fonctions et secrets d'un Point d'Acceptation).
Gestion d'un centre de mise à la clé à distance (PIN Online)	Injection ou renouvellement de la clé de chiffrement du PIN (TIK) dans les Points d'Acceptation à distance (généralement via un TMS), conformément aux exigences du standard sécuritaire PCI PIN Security [5].
Gestion d'un centre d'injection de clé (PIN Online)	Injection ou renouvellement de la clé de chiffrement du PIN (TIK) dans les Points d'Acceptation selon un processus de personnalisation conformément aux exigences du standard sécuritaire PCI PIN Security [5].
Gestion d'un serveur de transchiffrement (PIN Online)	Mise à la clé et maintien en conditions opérationnelles d'un HSM agréé CB effectuant le transchiffrement du PIN chiffré, conformément aux exigences du standard sécuritaire PCI PIN Security [5].

Tableau 2 – Identification des activités sensibles à labélisation obligatoire

ANNEXE C : CONFIGURATIONS DES ZONES DE SÉCURITÉ

C1. Définition des zones de sécurité

Le présent paragraphe décrit les différents types de zones d'activités définis par le Groupement des Cartes Bancaires CB pour le référentiel de labélisation.

Les activités et exigences de sécurité associées sont précisées dans le chapitre sur les exigences (voir chapitre 4).

À noter que l'on distingue les organismes dont l'activité principale est la gestion des Systèmes d'Acceptation CB ou des Serveurs Monétiques de ceux dont ce n'est qu'un élément d'ensemble.

La Figure 2 présente les différentes zones de sécurité qui sont définies dans ce chapitre. Des exemples de configuration possibles sont présentés en annexe C2.

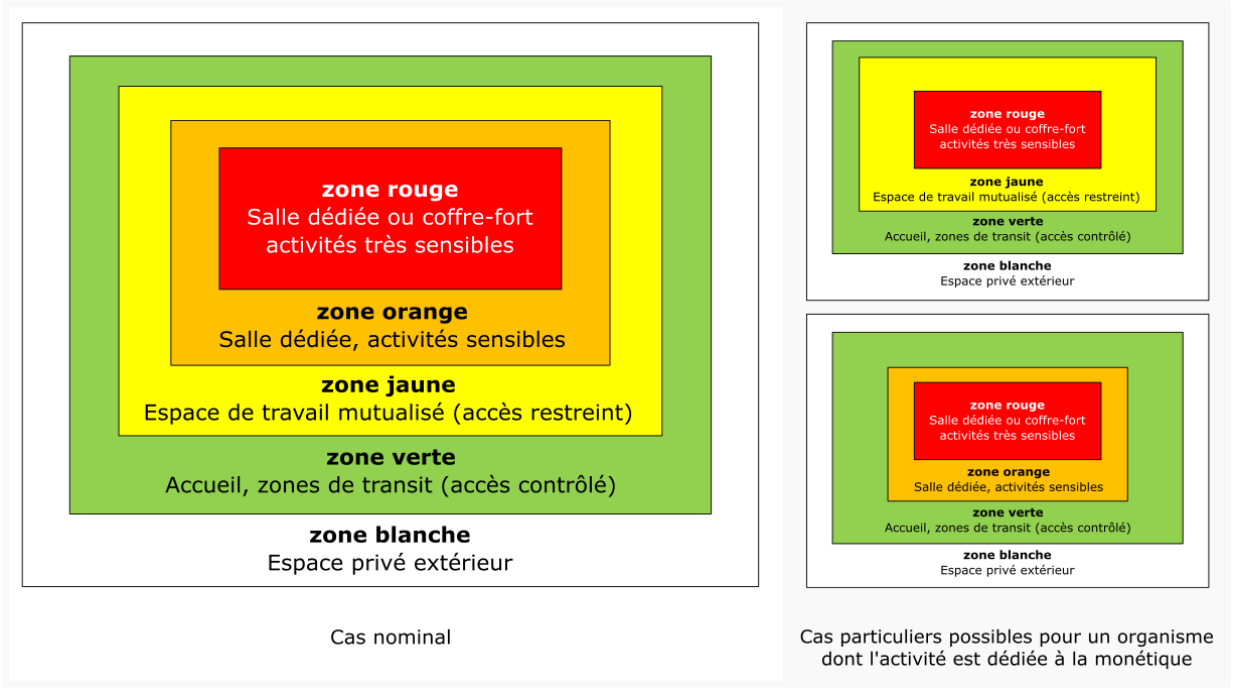


Figure 2 – Imbrication des zones de sécurité

Zone verte

- Les accès sont contrôlés ;
- Les issues de secours et les quais de livraison doivent être vidéo surveillés en 24/7 ;
- Les issues de secours doivent être sous alarme 24/7 ;
- Les quais de livraison doivent être fermés, verrouillés et sous alarme en cas de non utilisation.

Zone jaune

- Les portes d'accès à une zone jaune depuis la zone verte doivent disposer d'un contrôle d'accès restreint par badge à l'entrée, actif 24h/24 et 7j/7. Par restreint, il est entendu que la liste de personnes autorisées à accéder à la zone jaune est plus limitée que celle de la zone verte.
- Les fenêtres facilement accessibles (rez-de-chaussée, terrasse…) de la zone jaune doivent être équipées d'un dispositif de détection d'intrusion.

Zone orange

- Pour les organismes dont l'activité de gestion des Systèmes d'Acceptation CB est mutualisée avec d'autres activités, l'accès à une zone orange ne doit être possible qu'après un passage dans une zone jaune minimum.
- Pour les organismes dont l'activité de gestion des Systèmes d'Acceptation CB est la principale activité, l'accès à une zone orange ne doit être possible, au minimum, qu'après un passage dans une zone verte.
- Les portes d'accès à une zone orange doivent disposer d'un contrôle d'accès restreint à l'entrée et à la sortie, actif 24h/24 et 7j/7 (système « *anti-passback* »). Par restreint, il est entendu que la liste de personnes autorisées à accéder à la zone orange est plus limitée que celle de la zone d'accès (zone verte ou zone jaune).
- Les couloirs et les accès aux bureaux de la zone orange doivent être vidéo surveillés 24h/24 et 7j/7.

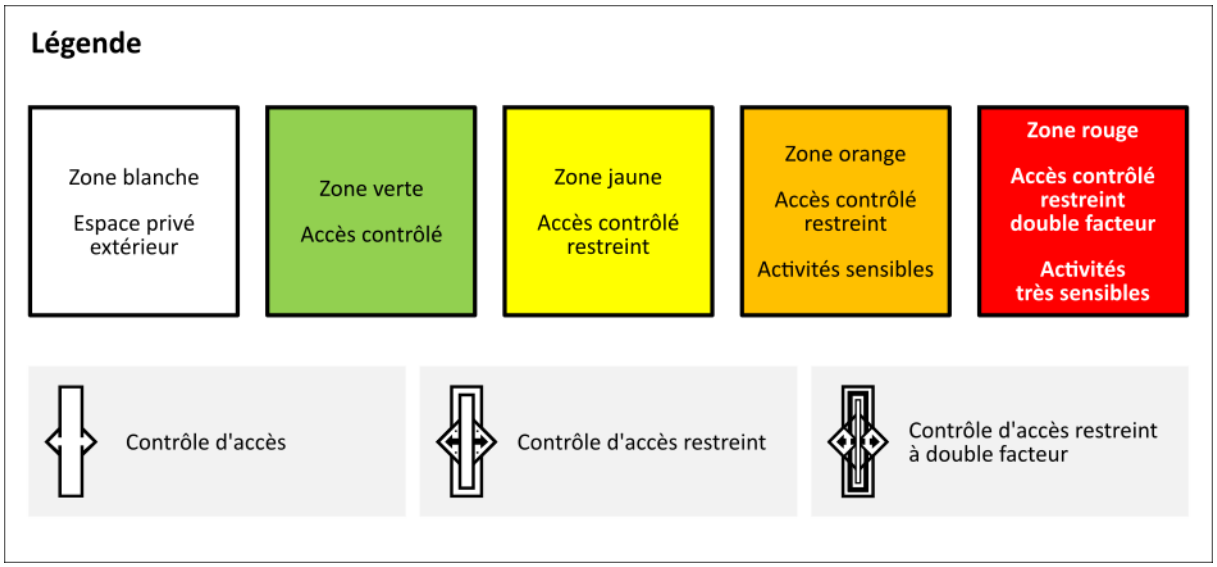
Zone rouge

- Pour les organismes dont l'activité de gestion des Systèmes d'Acceptation CB est mutualisée avec d'autres activités, l'accès à une zone rouge ne doit être possible qu'après un passage dans une zone orange.
- Pour les organismes dont l'activité de gestion des Systèmes d'Acceptation CB est la principale activité, l'accès à une zone rouge ne doit être possible, au minimum, qu'après un passage dans une zone jaune.
- Une zone rouge peut être un coffre-fort :
  - Ce dernier doit résister aux tentatives d'effraction.
  - Il doit être constitué d'un bloc porte en acier, d'un vantail de plusieurs épaisseurs de tôle d'acier et de serrures renforcées au minimum avec 3 points latéraux d'ancrage pour résister aux tentatives d'effraction.
- Si la zone rouge est une salle,
  - Les portes d'accès doivent disposer d'un contrôle d'accès restreint à double facteur à l'entrée et à la sortie, actif 24h/24 et 7j/7 (système « *anti-passback* »). Les portes doivent également être renforcées pour limiter les risques d'intrusion. Par restreint, il est entendu que la liste des personnes autorisées à accéder à la zone rouge est plus limitée que celle de la zone orange.
  - Il ne peut y avoir moins de deux personnes dans cette zone.
  - Les portes d'accès à cette zone doivent être équipées d'un dispositif de temporisation d'ouverture 24h/24 et 7j/7, avec déclenchement d'alarme sonore.
  - Les portes d'accès à cette zone doivent être sécurisées et une alerte doit être déclenchée en cas de tentative d'effraction.
  - Les murs, sols et plafonds entourant les bureaux et couloirs de cette zone doivent être renforcés (matériaux résistants comme les parpaings, les briques ou les murs/dalles en béton ou en acier) ou équipés de dispositifs permettant de détecter les perçages 24h/24 et 7j/7 (capteurs de vibration, capteurs acoustiques, par exemple).
  - Les bureaux et couloirs de cette zone ne doivent pas comporter de fenêtres facilement accessibles depuis l'extérieur (rez-de-chaussée, terrasse…).
  - Les bureaux et couloirs de cette zone ne doivent pas comporter un accès direct à l'extérieur du bâtiment (issues de secours, puits de lumière…).
  - Les bureaux et couloirs de cette zone doivent être équipés d'un dispositif de détection des intrusions physiques 24h/24 et 7j/7 (présence d'un gardien, capteurs volumétriques, détection de mouvements par vidéosurveillance, barrières infrarouges, capteurs de bris de glace, capteurs acoustiques, par exemple).
  - Les issues de secours de cette zone doivent correspondre aux portes d'accès à cette zone et doivent être équipées d'un dispositif sécurisé d'ouverture d'urgence permettant de désactiver le contrôle d'accès en double contrôle, pour pouvoir évacuer la zone.

C2. Schématisation et exemples

Les schémas suivants donnent des exemples de configurations de zones de sécurité possibles pour les activités décrites dans le présent référentiel.

NB : Tous les contextes ne sont pas représentés.



Cas où les activités monétiques sont mutualisées avec d'autres activités

Ce paragraphe donne des exemples d'organisation des zones physiques pour les organismes dont les activités ne sont pas uniquement monétiques.

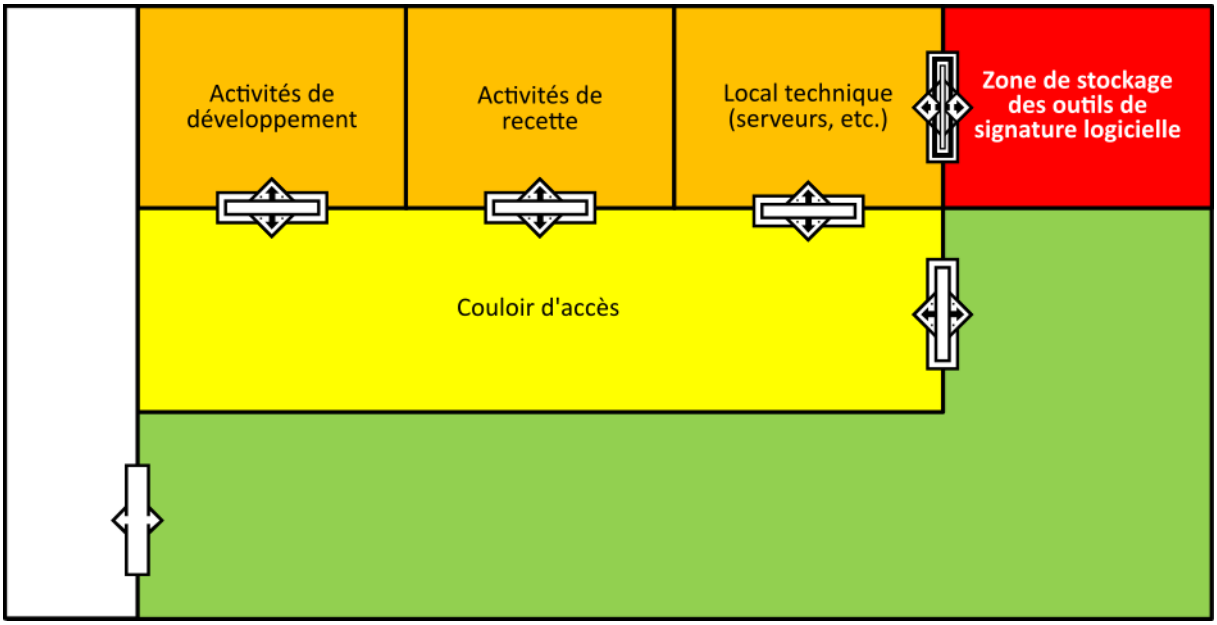


Figure 3 – Exemple de configuration pour un Développeur (activité mutualisée)

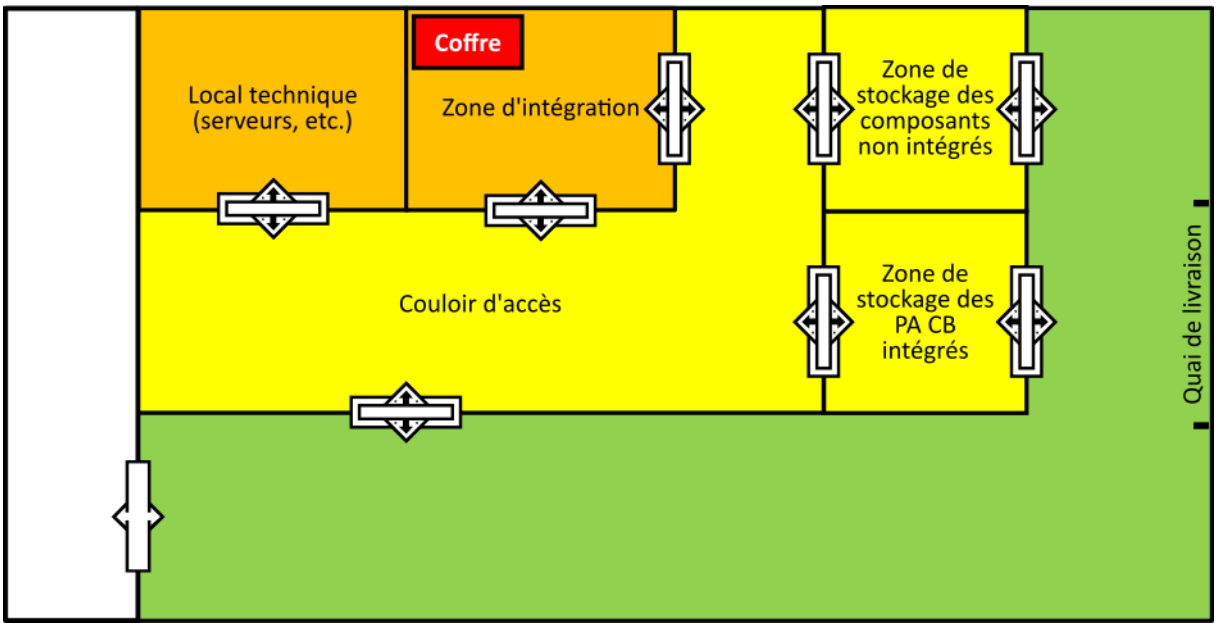


Figure 4 – Exemple de configuration pour un Intégrateur

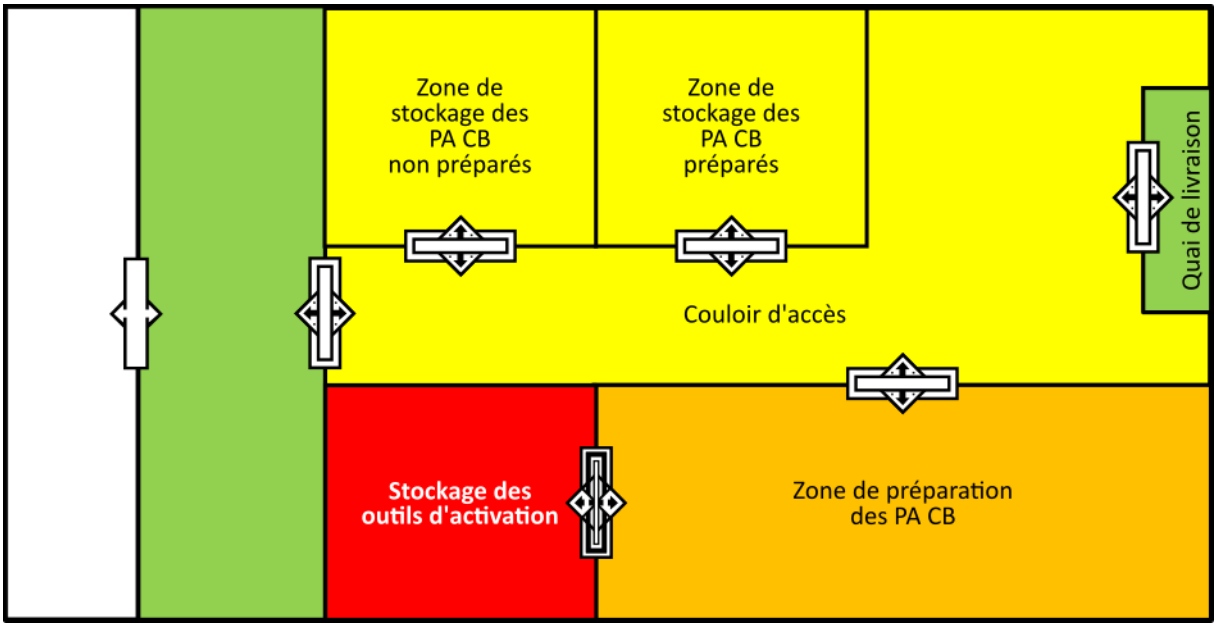


Figure 5 – Exemple 1 de configuration pour un Préparateur

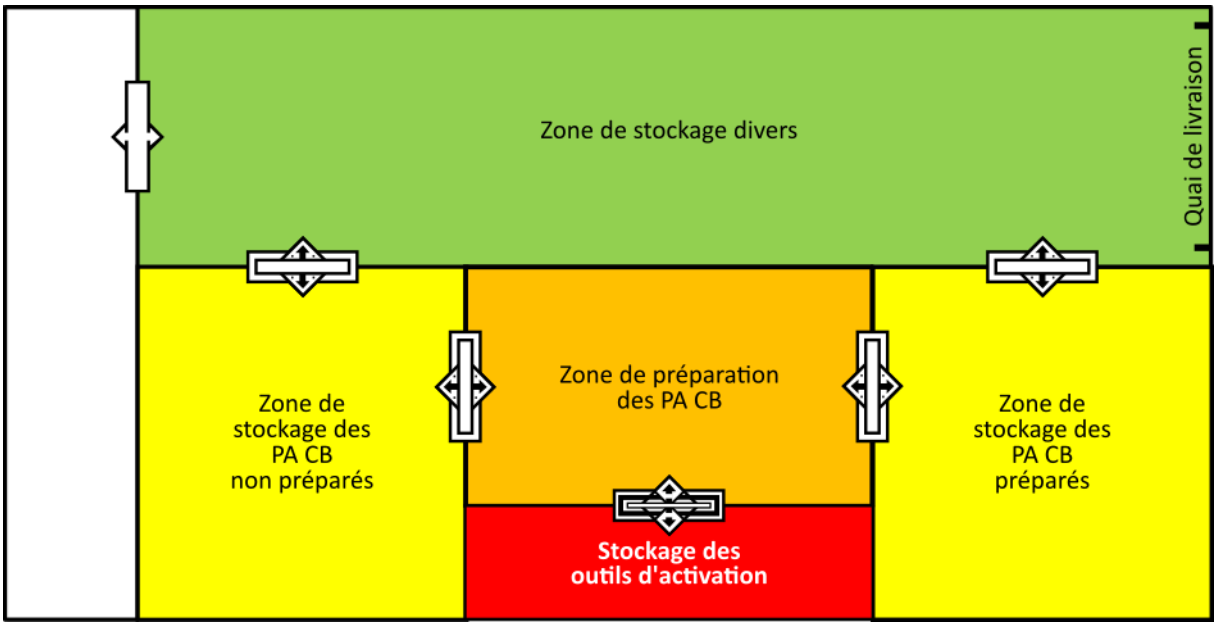


Figure 6 – Exemple 2 de configuration pour un Préparateur

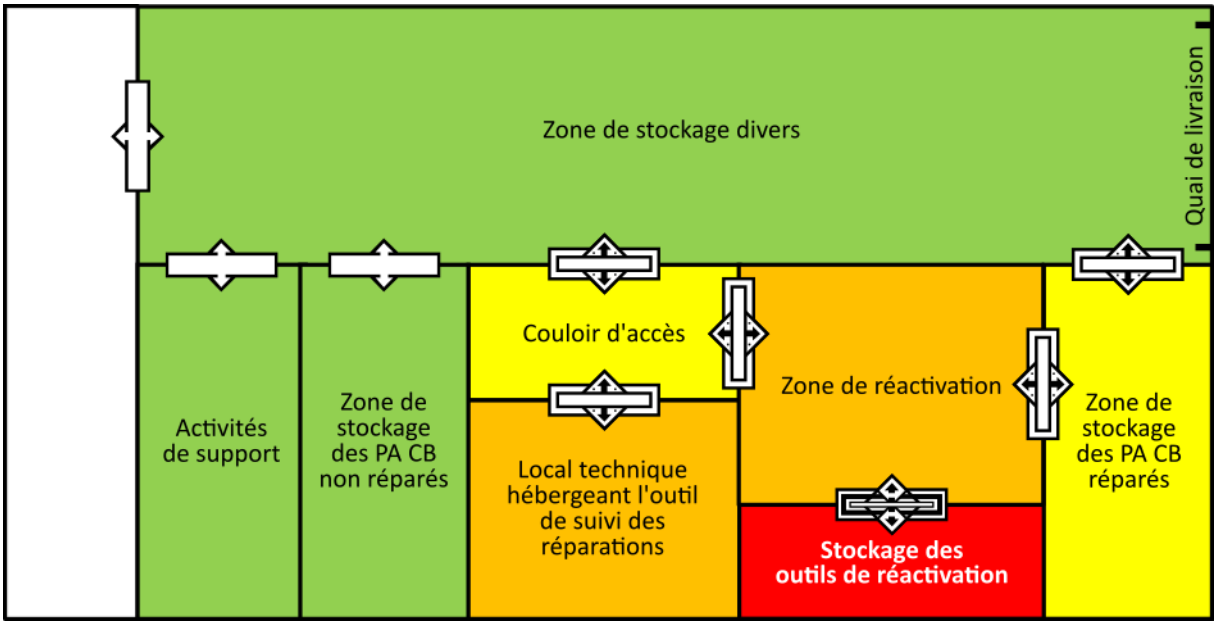


Figure 7 – Exemple de configuration pour la Maintenance de PA CB

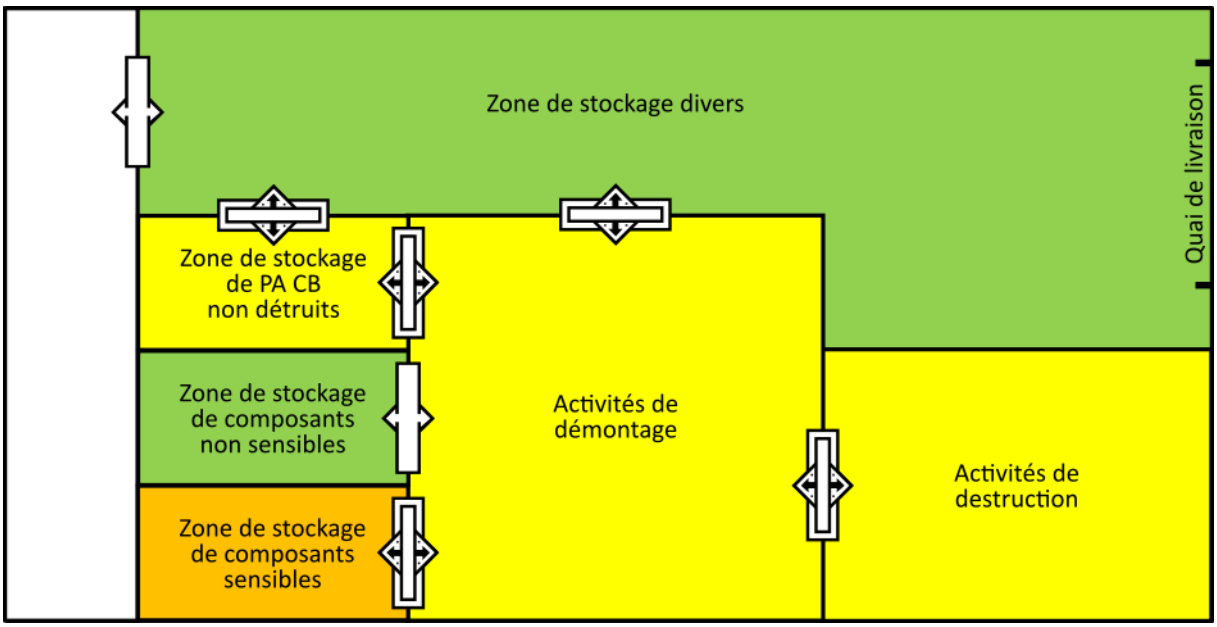


Figure 8 – Exemple de configuration pour la Mise au rebut de PA CB

Cas où l'activité est dédiée à la monétique

Ce paragraphe donne des exemples d'organisation des zones physiques pour les organismes dont les activités sont uniquement dédiées à la monétique.

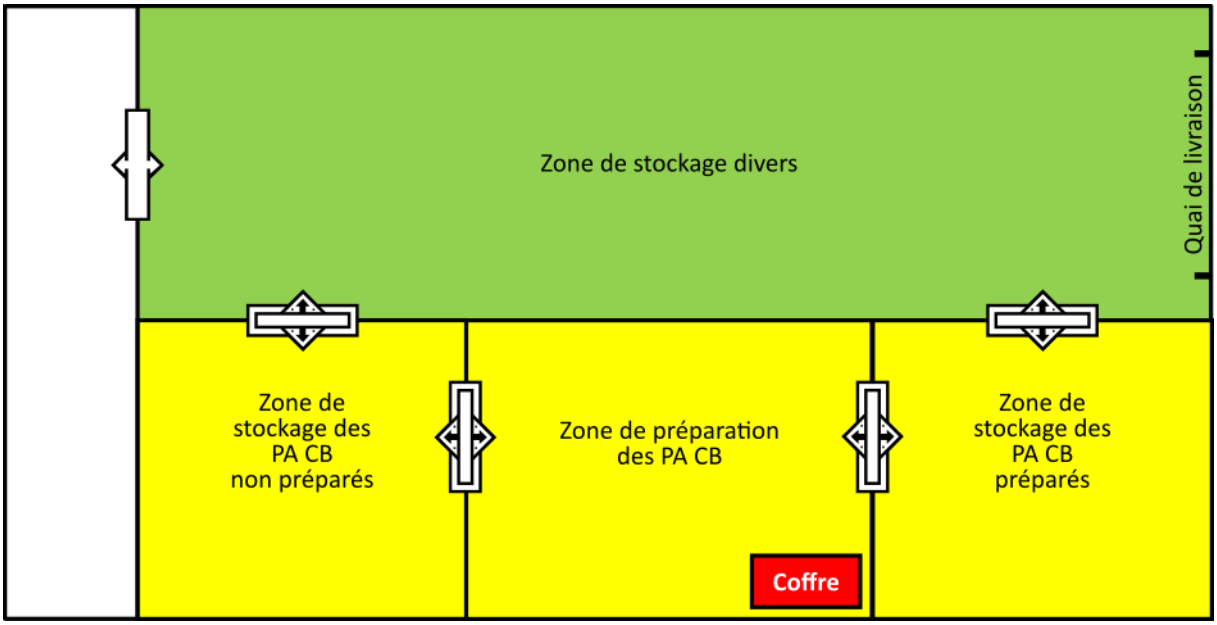


Figure 9 – Exemple de configuration pour un Préparateur (activité dédiée)

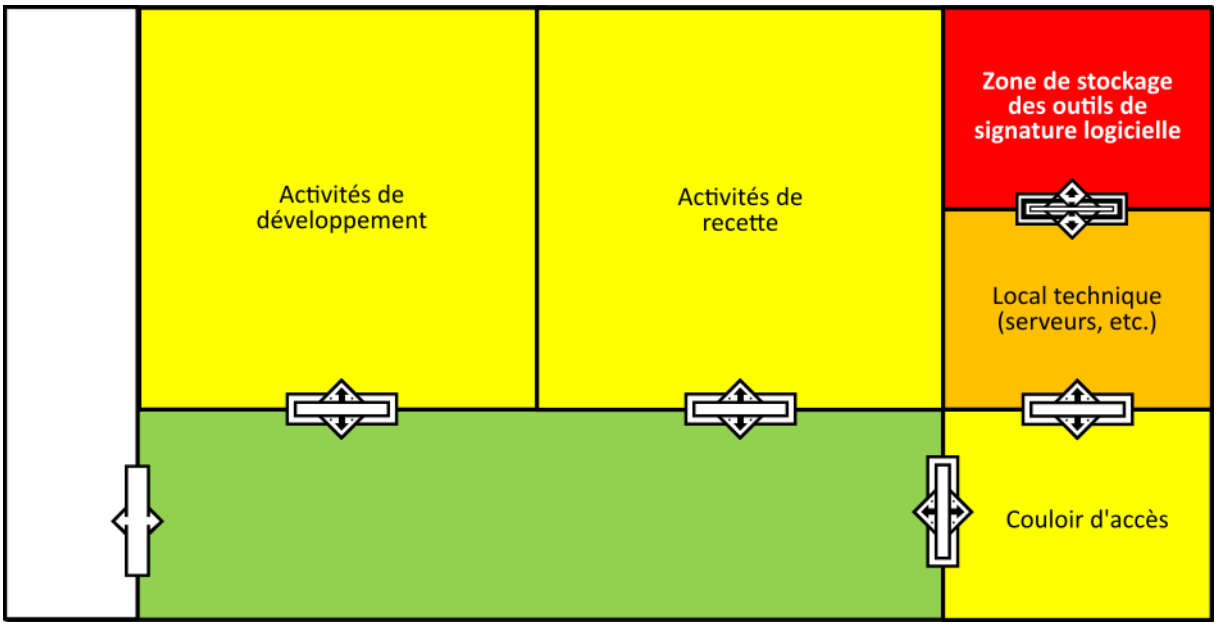


Figure 10 – Exemple de configuration pour un Développeur (activité dédiée)

FIN DU DOCUMENT