Questions Fréquentes

Demandes de clarifications et interprétations du référentiel REMPARTS

Version 202403-01 (mars 2024)

1 Introduction

Cette note a pour objectif de référencer les différentes questions adressées à CB à propos du référentiel REMPARTS (référence DPE-ESS-REF-2016-006) et du programme associé, ainsi que les réponses apportées par CB.

Elle peut être utilisée par les sociétés inscrites dans le programme REMPARTS et par les auditeurs habilités pour lever les éventuelles ambiguïtés associées à certaines exigences du référentiel, et permet d'affiner la compréhension générale des exigences et d'éviter des interprétations divergentes.

Ce document peut être amené à évoluer régulièrement, selon que de nouvelles questions sont posées ou non.

Il est cependant important de noter que ce document n'est pas normatif. Le référentiel REMPARTS reste le document de référence pour tout audit de Labélisation REMPARTS certifié. Par ailleurs, toute mise à jour du référentiel REMPARTS ultérieure à la date de dernière mise à jour de cette note est susceptible d'en invalider le contenu.

2 Questions / Réponses

Question 1. Dispositifs de détection d'intrusion sur les fenêtres en zone orange

L'annexe C1 du référentiel REMPARTS impose la présence de dispositifs de détection d'intrusion sur les fenêtres facilement accessible dans les zones jaunes uniquement. Aucune exigence de ce type n'est précisée pour les zones orange : cela signifie-t-il qu'il n'est pas nécessaire d'en installer en zone orange ?

Réponse : Il s'agit d'une omission du référentiel. L'objectif de la progressivité du zonage est de faire en sorte que la sécurité d'une zone orange soit supérieure à celle apportée par une zone jaune. Une zone orange hérite donc au minimum du besoin de sécurité de la zone jaune ; par conséquent, les fenêtres présentes dans une zone orange doivent également disposer d'un dispositif anti-intrusion.

Question 2. Dispositifs de détection d'intrusion sur les fenêtres

L'annexe C1 du référentiel REMPARTS impose la présence de dispositifs de détection d'intrusion sur les fenêtres facilement accessible dans les zones jaunes. L'installation sur toutes les fenêtres d'un dispositif de détection d'intrusion peut présenter plusieurs inconvénients (inutile lorsque la fenêtre est cassée ou en cas d'intrusion par le mur adjacent, coûts importants de mise en œuvre au regard du gain en sécurité apporté, délais initiaux de câblage élevés si le nombre de fenêtres est conséquent, problématique esthétique, etc.)

Est-il acceptable et suffisant pour répondre aux exigences de remplacer ces dispositifs de détection d'intrusion par des détecteurs volumétriques couvrant toute la zone concernée ?

Réponse : Cette proposition est acceptable, à condition que les détecteurs volumétriques couvrent effectivement l'intégralité de la zone concernée et que les alertes remontées par ces détecteurs soient prises en compte 24h/24 et 7j/7. Le bon fonctionnement de ces détecteurs doit par ailleurs être vérifié régulièrement, conformément à l'exigence de tronc commun EXI_TC_17.

Enfin, il est impératif de s'assurer que les fenêtres équipant les zones sensibles ne facilitent pas une intrusion dans les locaux et qu'elles ne sont pas considérées comme des issues de secours. Au minimum, et en plus des dispositifs de détection mentionnés précédemment, elles devraient être équipées de compas empêchant leur ouverture complète.

Question 3. Précisions sur le contrôle d'accès à double facteur en zone rouge

Dans les contraintes applicables aux zones rouge précisées dans l'annexe C1 du référentiel REMPARTS, qu'entendez-vous par « contrôle d'accès à double facteur » ? Cela nécessite-t-il l'installation de deux lecteurs de badges indépendants, conditionnant l'ouverture au passage de 2 badges distincts ?

Réponse : Par double facteur, on entend « deux modalités distinctes d'authentification d'une même personne ». Par exemple, en utilisant un code et un badge, ou en couplant l'utilisation d'un badge et une authentification biométrique.

Question 4. Processus de dérogation aux exigences REMPARTS

Nous pensons que certaines exigences applicables à l'une de nos activités ne peuvent pas s'appliquer à notre contexte, et nous souhaiterions nous en dispenser. Existe-t-il un processus officiel de dérogation à certaines exigences REMPARTS ?

Réponse : De manière générale, il n'est pas possible de déroger aux exigences REMPARTS. Toutefois, il existe certaines situations exceptionnelles où il est envisageable de répondre à une exigence d'une manière qui pourrait entrainer une non-conformité lors d'un audit certifié. Dans ce type de situation, une demande de dérogation dûment argumentée doit être adressée à CB préalablement à l'audit. Si la demande est validée, l'accord sera transmis par CB aux auditeurs et au certificateur.

Question 5. Création de sas pour éviter un saut de zone (multi activité)

Du fait de notre multi activité, l'annexe C1 du référentiel n'autorise pas un saut de zone verte vers orange ; nous devons donc créer une zone jaune entre notre zone verte et notre zone orange. Nous n'avons cependant aucune activité à mener dans cette zone jaune, il s'agirait uniquement d'un sas avec 2 portes, l'une donnant sur la zone verte, l'autre sur la zone orange.

Nous pensons que l'intérêt d'un tel sas est très limité, et cela nous pose de réelles contraintes d'occupation de l'espace. Est-il possible de déroger à la règle ? Si oui, pourriez-vous nous préciser dans quelles conditions ?

Réponse : Cette situation fait partie des cas où une dérogation peut être envisagée, en fonction du contexte dans lequel elle est demandée. Il est toutefois important de noter qu'un tel saut ne peut être systématique. Pour que la demande puisse être considérée, des contre-mesures additionnelles doivent être déployées en zone verte :

- La porte d'accès à la zone orange doit être vidéosurveillée depuis la zone verte,
- La partie de la zone verte concernée ne doit pas disposer de fenêtres facilement accessibles. Dans le cas contraire, les exigences de la zone jaune portant sur ces fenêtres doivent s'appliquer.

Question 6. Signalement de perte de points d'acceptation.

Il arrive que certains accepteurs ne renvoient pas le matériel d'acceptation à la suite d'une opération de montée en gamme ou à la signature d'un nouveau contrat. Devons-nous déclarer à CB les matériels qui ne nous ont pas été retournés par les accepteurs, sachant que ce matériel peut potentiellement nous être retourné par la suite ?

Lorsque le matériel d'acceptation a été facturé à l'accepteur, faut-il également vous déclarer ces points d'acceptation ?

Réponse : Les remontées à faire à CB sont celles qui concernent des suspicions de fraude (EXI_TC_53). Ces alertes peuvent être liées à la perte ou au vol de matériel, ou à la détection d'un incident. Le cas ici décrit ne correspond pas à une fraude potentielle ; il ne fait donc pas l'objet d'une remontée systématique à CB.

Il est toutefois important que ces matériels apparaissent dans l'inventaire, avec le statut approprié. Cela permettra, en cas de fraude détectée sur ces matériels, de remonter à la dernière source connue et de réagir en conséquence.

Question 7. Portée des audits de contrôle annuels

Pourriez-vous préciser le périmètre des audits de contrôle annuels ? Les sociétés labélisées doivent-elles contacter une société d'audit habilitée ? Ces sociétés connaissent-elles la procédure à suivre ? Quels sont les points qui doivent être audités ?

Réponse : Comme CB s'y est engagé en octobre 2021, une note clarifiant les modalités de réalisation des audits de contrôle annuels et la liste des contrôles attendus a été publiée. Cette note répond à l'ensemble des questions posées et peut être transmise à tous les acteurs impliqués dans le processus. Les sociétés d'audits habilitées ont bien entendu connaissance de cette note, et sont d'ores et déjà en mesure de vous accompagner dans la réalisation de ces audits.

Question 8. Conditions de livraison des cartes de domiciliation

Les cartes de domiciliation doivent-elles être envoyées séparément des terminaux de paiement ?

Réponse : C'est une bonne pratique de sécurité que de livrer la carte séparément du terminal. Cela permet ainsi de limiter, par exemple, les risques de fraude à la facture crédit en cas d'interception du colis. Cependant, le référentiel REMPARTS n'impose pas cette livraison en deux temps.

Il est en revanche demandé de formaliser tout le processus de transport, incluant notamment les conditions de livraison des cartes de domiciliation des commerçants (EXI_DIST_1).

Question 9. Contraintes portant sur les équipes de développement

L'exigence EXI_DEV_9 précise que « ce ne sont pas les mêmes contractants qui développent, réalisent la recette et les activités de support d'exploitation ». Doit-on comprendre la phrase comme indiquant qu'il doit y avoir 1 équipe A pour le développement, 1 équipe B pour la recette et 1 équipe C pour le support d'exploitation, ces 3 équipes étant totalement disjointes ?

Réponse : L'exigence EXI_DEV_9 du référentiel a pour objectif d'insister sur la séparation des rôles plus que des personnes. Une équipe de 2 développeurs ne peut pas se couper en 3, mais une procédure doit permettre de faire en sorte qu'en toute situation (personne malade, situation exceptionnelle, départ de l'entreprise), les rôles puissent être réaffectés sans qu'une seule et même personne ne soit en charge de tous les sujets, et ce pour éviter les points de défaillance uniques.

Question 10. Modalités de mise au rebut des terminaux

Les TPE mis au rebut doivent-ils être percés au niveau de leur carte mère avant d'être mis dans l'octabin ?

Réponse : Non, ce type d'opération n'est pas nécessaire. Tous les terminaux agréés ont été évalués par PCI (certification PCI PTS), qui pose comme contrainte que toutes les données sensibles soient effacées dès qu'il est ouvert. Il ne devrait donc pas rester de secrets dans la mémoire présente sur la carte mère des terminaux mis au rebut. Cela suppose en revanche que ces terminaux soient correctement désactivés avant d'être mis au rebut, comme le précise notamment l'exigence EXI_MAINT_26 du référentiel.

Question 11. Version anglaise du référentiel REMPARTS

Existe-t-il une traduction du référentiel en anglais ?

Réponse : Oui, la version 2.0 du référentiel REMPARTS a été traduite en anglais en août 2021. Elle est disponible sur le portail REMPARTS, dans la section « document utiles » (Rules for the Secure Management of CB Acceptance Systems - REMPARTS Reference Document).

Question 12. Responsabilité des acteurs labélisés vis-à-vis de l'agrément CB

Pourriez-vous préciser ce qui est attendu des acteurs labélisés vis-à-vis des vérifications de l'agrément du matériel d'acceptation ? Est-il possible de déléguer tout ou partie de ces actions aux clients ?

Réponse : L'exigence EXI_TC_48 précise qu'un contrôle systématique du statut de l'agrément CB des systèmes d'acceptation sur lesquels la société labélisée intervient doit être réalisé. Les exigences supplémentaires liées à l'intégration (EXI_INT_1), la préparation (EXI_PREP_1, EXI_PREP_4), la maintenance (EXI_MAINT_1), l'exploitation (EXI_EXPL_1), le stockage (EXI_STOCK_2) demandent aux sociétés labélisées de tenir à jour un inventaire des systèmes d'acceptation contenant la version logicielle actuellement installée sur le matériel et le statut de l'agrément de chacun des systèmes d'acceptation. Enfin, l'annexe B2 précise les obligations pour les sociétés labélisées :

> *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.*

Les sociétés labélisées ont donc la responsabilité de :

- Préparer tout nouveau système d'acceptation avec la dernière version agréée du logiciel d'acceptation.
- Vérifier la version déployée sur les systèmes d'acceptation revenant en maintenance, et proposer à leurs clients de mettre à jour ces systèmes d'acceptation avec la dernière version agréée du logiciel d'acceptation, en particulier lorsque la version installée a fait l'objet d'un événement terrain et d'un correctif.
- Informer leurs clients des échéances liées aux systèmes d'acceptation, et attirer leur attention sur la nécessité d'utiliser des versions agréées et à jour.
- Informer CB de toute opération réalisée sur des systèmes non-agréés.

Dans le cas ou le client d'une société labélisée exigerait de la société labélisée qu'elle contrevienne aux règles REMPARTS (déploiement d'un applicatif non agréé ou d'un terminal ayant atteint sa fin de commercialisation), la société labélisée doit en informer CB sans délai.

Il est à noter que les remontées d'informations à CB ne peuvent pas être déléguées à un tiers.

Question 13. Définition d'un Serveur Monétique

Pourriez-vous préciser la notion de « Serveur Monétique » ? Qu'entendez-vous par celle-ci ?

Réponse : Cette définition a en effet été oubliée dans la section dédiée du référentiel (chapitre 1.5). Voici la définition d'un Serveur Monétique qui sera ajoutée à la prochaine itération du document :

> *Un serveur monétique est un serveur ayant une fonction associée à un traitement monétique. Il peut s'agir d'un serveur d'acceptation (concentration des flux en provenance de terminaux de paiement ou de DAB/GAB pour le retrait, consolidation des transactions pour télécollecte, pilotage des transactions EMV), d'un TMS, d'une passerelle monétique, ou tout autre serveur traitant ou manipulant les données de paiement/retrait.*

Question 14. Mise au rebut des cartes SIM

Faut-il appliquer à l'identique la procédure de destruction des points d'acceptations (TPE) pour les cartes SIM équipant les terminaux ? Notamment, est-il nécessaire d'archiver les numéros de série et d'émettre un certificat de destruction spécifique ?

Réponse : Les cartes SIM des terminaux autonomes ne font pas partie des biens sensibles répertoriés dans REMPARTS. Il est bien entendu possible pour une société labélisée de les considérer comme telles, mais cela n'est pas imposé par le référentiel. Par conséquent, et sauf directive contraire préconisée par le constructeur ou l'opérateur fournissant les SIM, il n'est pas nécessaire d'archiver les numéros de série des SIM détruites, ni d'émettre un certificat de destruction.

Question 15. Fréquence des tests d'intrusion

L'exigence EXI_TC_46 demande à ce que des campagnes de tests d'intrusion soient régulièrement réalisées sur les réseaux et applicatifs impliqués dans la gestion des Systèmes d'Acceptation CB et des Serveurs Monétiques. Pourriez-vous préciser ce qui est entendu par « régulièrement » ? Tous les 6 mois ? Tous les ans ? Tous les 3 ans ?

Réponse : La formulation est effectivement peu précise et mériterait d'être mieux qualifiée. Selon la taille des acteurs et de leur périmètre informatique, cette fréquence elle est généralement fixée à une période d'entre 12 à 18 mois entre deux tests. Cette exigence sera reformulée pour être plus explicite dans la prochaine itération.

Question 16. Conditions d'expédition pour les petits volumes

L'exigence EXI_TC_55 demande de fournir un inventaire électronique et papier, précisant les numéros de série des points d'acceptation, pour chaque destinataire. La fourniture du bon de livraison est-elle obligatoire pour les petits commerçants si le numéro de série est précisé sur le bon du transporteur ?

D'autre part, l'envoi des numéros de série par mail pour les petits commerçants est-il nécessaire ? Ils sont par ailleurs informés qu'ils vont recevoir un terminal, suite à une panne ou à un achat, et disposent d'une date de livraison.

Réponse : Le contexte évoqué correspond à une distribution unitaire, pour laquelle les règles REMPARTS n'ont pas été conçues. Dans ce cas précis, l'exigence EXI_TC_55 peut donc effectivement être assouplie, dès lors que le besoin de traçabilité du matériel est garanti et que le commerçant ou l'expéditeur peut s'assurer que le matériel qui a été envoyé est bien identique à celui qui a été réceptionné.

Cependant, la règle doit être suivie strictement dès lors que le volume de points d'acceptation distribué est supérieur à 5 terminaux à destination de la même entité (et ce quel que soit le nombre de colis).

Question 17. Durée de conservation des données du registre visiteur

L'exigence EXI_TC_14 demande de maintenir un registre contenant l'identité, l'heure et la date d'arrivée et de départ des visiteurs. Pouvez-vous préciser la durée de conservation des données personnelles du registre ?

Réponse : Les respect des exigences REMPARTS doit se faire dans le respect du cadre législatif applicable. La durée de conservation de ce registre doit être définie par le responsable de traitement, auquel CB ne peut pas se substituer en fixant une durée arbitraire.

Toutefois, et à titre purement indicatif, la CNIL a publié un cas pratique très proche dans lequel elle a proposé une durée de conservation de 3 mois pour les données du registre visiteur.

Question 18. Stockage de terminaux non fonctionnels

Certains terminaux, notamment les matériels appartenant à certaines gammes utilisées en monétique répartie, ne peuvent pas être utilisés pour accepter des paiements sans avoir été préalablement initialisés via un outil dédié de gestion de parc après une authentification explicite. Le gestionnaire de parc peut procéder à l'initialisation à distance – après l'installation du matériel sur site. Pour de tels terminaux, les contraintes de stockage en zone jaune peuvent-elles être assouplies ? Le risque en cas de vol de matériel nous semble en effet réduit par rapport à un terminal autonome pré-initialisé.

Réponse : La version actuelle du référentiel est un peu ambigüe, puisqu'elle impose une zone jaune pour le stockage de tous les Points d'Acceptation (EXI_STOCK_5), mais autorise une zone verte pour les Points d'Acceptation à réparer (EXI_MAINT_11).

Dans le cas où un terminal non-activé ne peut pas être utilisé pour effectuer un paiement, la sensibilité de ce matériel est a priori comparable à celle d'un point d'acceptation à réparer. Leur stockage dans une salle en zone verte peut donc être envisagé.

Plusieurs conditions doivent toutefois être réunies pour que ce stockage soit acceptable :

- L'activation des terminaux doit suivre une procédure stricte permettant de tracer, d'identifier et d'authentifier la personne ou l'entité demandant l'activation, ainsi que le commerçant pour le compte duquel cette activation est effectuée.
- Tous les accès à l'espace de stockage doivent être contrôlés.
- L'inventaire des terminaux entreposés dans cette salle doit être tenu à jour, conformément à l'exigence EXI_STOCK_1, afin de garantir la traçabilité des opérations et de permettre de détecter toute perte ou tout vol.

Note rédigée par : Emmanuel le Chevoir
Date de publication : 20 mars 2024
Référence de la note : DPE-ESS-NTE-2022-003
Révision : 202403-01
Classification : C1 - Diffusion publique