

Cryptage point à point PCI (CP2P) 3.1 – Guide d'emploi (GEC)

Canada - Version 1.0

Avril 2025

1. Renseignements de la solution CP2P et coordonnées du fournisseur

1.1 Renseignements de la solution CP2P	
Nom de la solution :	<i>CP2P Global Payments</i>
Numéro de référence de la solution sur le site web PCI SSC :	2022.00056.003

1.2 Coordonnées du fournisseur de solution	
Nom de l'entreprise :	<i>Global Payments Canada GP</i>
Adresse de l'entreprise :	<i>3381 Steeles Avenue East Suite 200 Toronto, ON M2H 3S7</i>
URL de l'entreprise :	<i>globalpayments.com/fr-ca</i>
Ressource :	<i>Service à la clientèle de Global Payments</i>
Numéro de téléphone :	<i>1 888 682-3309</i>

CP2P et PCI DSS

Les marchands qui utilisent cette solution CP2P peuvent être tenus de valider leur conformité PCI DSS et doivent connaître les exigences PCI DSS applicables. Les marchands doivent contacter leur acquéreur ou les marques de paiement afin de déterminer leurs exigences de validation PCI DSS.

2. Vérifier que les dispositifs n'ont pas été trafiqués et confirmer l'identité du personnel tiers

2.1 Instructions pour s'assurer que les dispositifs proviennent d'un expéditeur de confiance
<p>Les entreprises Global Payment prennent toutes les mesures nécessaires pour s'assurer que les dispositifs ne sont pas trafiqués avant leur expédition.</p> <p>Cependant, pour vérifier que les dispositifs ne sont pas falsifiés durant le transport, vous devez suivre les étapes ci-dessous.</p> <p>D'abord, vous devez confirmer que la livraison s'est faite à partir de notre établissement d'injection de clé (KIF) validé CP2P PCI ou de notre centre de déploiement, dont l'adresse est la suivante :</p> <p>Global Payment Canada GP 151 Carlingview Drive, Unit 16 Etobicoke, M9W 5S4</p> <p>Les employés de Global Payments ont la responsabilité d'installer les dispositifs de remplacement. Vérifiez auprès d'eux qu'ils ont le modèle approprié.</p> <p>Pour confirmer que les dispositifs ont été expédiés par une source autorisée, vous pouvez comparer les données d'expédition du fournisseur avec les renseignements ci-dessus. Si vous recevez des dispositifs d'un autre fournisseur, vous devez contacter le Service à la clientèle (voir section 1.2) pour confirmation. Nous tâchons de communiquer toute mise à jour de notre liste de KIF.</p>

2.2 Instructions pour confirmer que les dispositifs et les cartons d'expédition n'ont pas été trafiqués, et assurer la sécurité des communications avec le fournisseur de solution.

Inspection lors de la réception : Tous les dispositifs de ce programme sont expédiés dans des emballages à témoin d'intégrité par des partenaires de distribution autorisés. Ce type d'emballage peut être, par exemple, du ruban adhésif inviolable (sur une boîte ou un sac contenant le dispositif CP2P).

Inspectez l'emballage et les dispositifs pour voir s'ils n'ont pas été altérés. Si vous croyez qu'un sac inviolable a été ouvert en cours d'expédition, suivez toutes les instructions de la section 6.2 pour intervenir dans ce cas. Les dispositifs qui semblent avoir été trafiqués ne doivent pas être retirés du sac inviolable, sauf avis contraire du Service à la clientèle de Global. Avant d'activer un dispositif, les marchands doivent suivre les instructions d'inspection ci-dessous en vue de s'assurer qu'il est intact.

Des sceaux inviolables sont placés sur les vis et les joints des dispositifs, et permettent de déterminer s'il y a eu falsification, comme dans les fichiers ci-dessous :



Sécurisez les dispositifs en votre possession, y compris ceux qui sont :

- en attente de déploiement
- en cours de réparation ou ne sont pas utilisés
- en attente d'un transfert d'un établissement à l'autre

2.3 Instructions pour confirmer le besoin commercial et l'identité des employés de soutien ou de réparation tiers, avant de leur donner l'accès aux dispositifs

L'accès aux dispositifs par du personnel de réparation/d'entretien tiers doit être surveillé. Cette surveillance permet d'éviter tout accès non autorisé qui pourrait entraîner la falsification, le vol ou la substitution d'un dispositif. Pour assurer un contrôle adéquat de l'accès, dotez-vous d'une politique qui comporte ce qui suit :

- La date et l'heure de l'entretien ou de la réparation du dispositif doivent être fixées au préalable, et la tâche doit être effectuée par des employés tiers identifiés. Les visites impromptues de réparation/d'entretien doivent être validées. Si aucune validation n'est possible, l'accès doit être refusé.
- Avant de donner l'accès à un dispositif, l'identité et l'autorisation d'accès de l'employé tiers doivent être confirmées.
- L'accès d'un employé tiers doit être inscrit dans un registre et comprendre le nom de l'employé et son entreprise, ainsi que l'heure et le but de l'accès. Ces données doivent être conservées au moins un an.
- Le personnel tiers doit être escorté et observé en tout temps.
- Un employé tiers ne peut retirer ou remplacer un dispositif sans autorisation. Si une autorisation est donnée, les nouveaux dispositifs doivent être dûment inspectés et répertoriés.

3 – Dispositifs et applications/logiciels approuvés, et inventaire du marchand

3.1 Renseignements sur les dispositifs

Le tableau ci-dessous contient les renseignements relatifs aux dispositifs approuvés PCI pour la solution CP2P.

Notez que tous les renseignements des dispositifs se trouvent à l'adresse suivante :

https://www.pcisecuritystandards.org/approved_companies_providers/approved_pin_transaction_security.php

Consultez également la section 9.2 : « Instructions pour confirmer les versions du matériel, des micrologiciels et des applications des dispositifs ».

Code d'approbation PCI PTS	Fournisseur	Nom et numéro du modèle	Version de matériel	Versions de micrologiciel
4-30400	Verifone Inc	T650P	H561-07-aa-ONx-xx-A 1 (a=0-9; A à F)	Android: 2.0C.x SP Core DLL: T650-A-D-1A.x.x SP Core: T650-A-P-2A.x.x SP Core: T650-A-P-3A.x.x SP Core: T650p-A-P-1A.x.x SP Driver: T650P-A-S-1A.x.x SP Driver: T650p-A-S-1A.x.x SRED 1.0.0.xxx Android: 1A.x.x SRED 1.x.x.xxx
4-30392	Verifone Inc	T650C	H560-07-aa-ONx-xxx-A 1 (a=0-9; A à F)	Android: 2.0C.x SP Core DLL: T650-A-D-1A.x.x SP Core: T650-A-P-2A.x.x SP Core: T650-A-P-3A.x.x SP Core: T650C-A-P-1A.x.x SP Driver: T650C-A-S-1A.x.x SP Driver: T650C-A-S-1A.x.x SRED 1.0.0.xxx Android: 1A.x.x SRED 1.x.x.xxx
4-80062	Verifone Inc	P630	H565-0007-xxxx-xx-xx x-A1	VOS3: 01.xx.xx, VOS3: 02.xx.xx, Vault: APFW_01.01.xx.xx, Vault: APFW_01.02.xx.xx, Vault: SPBL_01.01.xx.xx, Vault: SPBL_01.02.xx.xx, Vault: SPFW_01.01.xx.xx, Vault: SPFW_01.02.xx.xx, Vault: SPFW_01.04.xx.xx,Android: 3.00D.xx,Android: 3.01D.xx,VOS3: 01.xx.xx: 31 déc 2025,Android: 3.01D.xx: 31 déc 2025,Vault: SPFW_01.04.xx.xx: 31 déc 2025,VOS3: 02.xx.xx: 31 déc 2025,Android: 3.00D.xx: 31 déc 2024,Vault: SPBL_01.01.xx.xx: 31 déc 2024,Vault: SPFW_01.01.xx.xx: 31 déc 2024,Vault: APFW_01.01.xx.xx: 31 déc 2024,Vault: SPBL_01.02.xx.xx: 31 déc 2024,Vault: SPFW_01.02.xx.xx: 31 déc 2024,Vault: APFW_01.02.xx.xx: 31 déc 2024

3.2 Renseignements sur les logiciels/applications

Ci-dessous se trouvent les renseignements relatifs aux logiciels et applications (applications CP2P et logiciels CP2P autres que de paiement) des dispositifs utilisés pour la solution CP2P.

Toutes les applications ayant accès à des données de compte en clair doivent être vérifiées en vertu du Domaine 2 et sont comprises dans la liste des solutions CP2P. Ces applications peuvent être ajoutées à la liste CP2P PCI d'applications validées, à la discrétion du distributeur ou du fournisseur de solution.

Fournisseur, nom et version de l'application	Fournisseur de dispositifs	Nom et numéro du modèle	Versions de matériel et de micrologiciels	L'application figure-t-elle dans la liste PCI? (O/N)	L'application a-t-elle accès aux données de compte en clair? (O/N)
Global Payments Direct Inc Unified Payment Application (UPA) V 02.*.*.* (2023-00056.007) Verifone Secure Data Interface (VFISDI):1.6X (2022-00154.108)	Verifone Inc	T650P	HW #: H561-07-aa-ONx-xxx-A1 (a=0-9; A to F) FW #: Android: 2.0C.x SP Core DLL: T650-A-D-1A.x.x SP Core: T650-A-P-2A.x.x SP Core: T650-A-P-3A.x.x SP Core: T650p-A-P-1A.x.x SP Driver: T650P-A-S-1A.x.x SP Driver: T650p-A-S-1A.x.x SRED 1.0.0.xxx Android: 1A.x.x SRED 1.x.x.xxx	O	O
Global Payments Direct Inc Unified Payment Application (UPA) V 02.*.*.* (2023-00056.007) Verifone Secure Data Interface (VFISDI):1.6X (2022-00154.108)	Verifone Inc	T650C	HW #: H560-07-aa-ONx-xxx-A1 (a=0-9; A to F) FW #: Android: 2.0C.x SP Core DLL: T650-A-D-1A.x.x SP Core: T650-A-P-2A.x.x SP Core: T650-A-P-3A.x.x SP Core: T650c-A-P-1A.x.x SP Driver: T650C-A-S-1A.x.x SP Driver: T650c-A-S-1A.x.x SRED 1.0.0.xxx Android: 1A.x.x SRED 1.x.x.xxx	O	O
Global Payments Direct Inc Unified Payment Application (UPA) V 02.*.*.* (2023-00056.007) Verifone Secure Data Interface (VFISDI):1.6X (2022-00154.108)	Verifone Inc	P630	HW #: H565-0007-xxxx-xxx-xxx-A1 FW #: VOS3: 01.xx.xx, VOS3: 02.xx.xx, Vault: APFW_01.01.xx.xx, Vault: APFW_01.02.xx.xx, Vault: SPBL_01.01.xx.xx, Vault: SPBL_01.02.xx.xx, Vault: SPFW_01.01.xx.xx, Vault: SPFW_01.02.xx.xx, Vault: SPFW_01.04.xx.xx,Android: 3.00D.xx,Android: 3.01D.xxVOS3: 01.xx.xx: 31 déc 2025,Android: 3.01D.xx: 31 déc 2025,Vault: SPFW_01.04.xx.xx: 31 déc 2025,VOS3: 02.xx.xx: 31 déc 2025,Android: 3.00D.xx: 31 déc 2024,Vault: SPBL_01.01.xx.xx: 31 déc 2024,Vault: SPFW_01.01.xx.xx: 31 déc 2024,Vault: APFW_01.01.xx.xx: 31 déc 2024,Vault: SPBL_01.02.xx.xx: 31 déc 2024,Vault: SPFW_01.02.xx.xx: 31 déc 2024,Vault: APFW_01.02.xx.xx: 31 déc 2024	O	O

3.3 Inventaire et vérification des dispositifs

Tous les dispositifs doivent être répertoriés par le biais d'un inventaire et d'une vérification, notamment de leur statut (déployé, en attente de déploiement, en cours de réparation/non utilisé ou en transit).

L'inventaire doit être effectué au moins une fois par année, selon les directives du PCI.

Cependant, comme meilleure pratique, nous recommandons de le faire chaque mois ou plus fréquemment, en fonction de la configuration du dispositif et du volume de transactions.

3.3 Inventaire et vérification des dispositifs

- Tous les dispositifs doivent être répertoriés par le biais d'un inventaire et d'une vérification, notamment de leur statut (déployé, en attente de déploiement, en cours de réparation/non utilisé ou en transit).
- L'inventaire doit être effectué au moins une fois par année, selon les directives du PCI.
- Cependant, comme meilleure pratique, nous recommandons de le faire chaque mois ou plus fréquemment, en fonction de la configuration du dispositif et du volume de transactions.
- Tout écart d'inventaire, y compris les dispositifs manquants ou substitués, doit être signalé à Global Payments aux coordonnées indiquées à la section 1.2 ci-dessus.
- L'exemple de tableau d'inventaire ci-dessous est fourni à titre indicatif seulement. L'inventaire doit être consigné et conservé dans un document externe.

Les marchands qui utilisent la solution CP2P de Global Payments doivent maintenir à jour un document d'inventaire des dispositifs, selon les instructions suivantes :

1. Avant la mise en œuvre, choisissez le type de document ou de système électronique qui convient à la consignation des informations énoncées dans l'exemple ci-dessous pour tous les dispositifs CP2P.
 - Ce peut être une feuille de calcul, un document de traitement de texte ou un autre fichier électronique. Vous pouvez également utiliser un système de gestion des stocks pour faire le suivi de vos dispositifs, mais ce n'est pas requis. Tout système qui vous permet de relever des données exactes sur vos dispositifs et de mettre à jour ces données respecte cette exigence.
 - Bien que les données d'inventaire doivent comprendre le fournisseur, le nom et le numéro du modèle, l'emplacement, le statut et le numéro de série ou un autre identifiant unique, vous pouvez consigner d'autres renseignements sur le dispositif, comme les résultats de l'inspection (voir la section 6.1), le numéro de magasin, l'état du dispositif, la version du micrologiciel, la version du matériel, l'état des connecteurs et les personnes ou les postes autorisés à utiliser le dispositif (« personnel autorisé »).
 - Le « numéro de série ou autre identifiant unique » peut être le numéro de série inscrit sur l'étiquette située au bas du dispositif ou un autre identifiant unique. L'identifiant unique doit permettre de reconnaître formellement le dispositif et être infalsifiable, comme une balise RFID. Dans la plupart des cas, le numéro de série du fabricant est le meilleur choix.
2. Avant la mise en œuvre, lors du changement de statut ou d'emplacement de dispositifs, et au moins chaque année par la suite, comparez tous les dispositifs à votre liste d'inventaire, en prenant note des divergences.
 - Ce processus peut être jumelé avec le processus d'inspection énoncé à la section 6.1, ou être effectué séparément.
 - S'il y a une divergence (dispositif manquant ou substitué), vous devez immédiatement contacter le Service à la clientèle aux coordonnées indiquées à la section 1.2.
 - Il est recommandé, mais pas obligatoire, d'employer le document d'inventaire lors de l'inspection (voir la section 6.1), pour aider à la détection d'une substitution ou d'un retrait non autorisé de dispositif.
3. Conservez un exemplaire de votre inventaire, chaque année, pour rester au fait de l'état de vos dispositifs. Cet exemplaire peut également servir dans le cadre de votre évaluation annuelle.

Exemple de tableau d'inventaire

Fournisseur	Nom et numéro du modèle	Emplacement du dispositif	Statut du dispositif	Numéro de série ou autre identifiant unique	Date de l'inventaire

4. Instructions d'installation de dispositif

Ne pas utiliser de dispositifs de capture de données non approuvés.

La solution CP2P ne peut être utilisée qu'avec certains dispositifs approuvés PCI. Seuls les dispositifs énoncés au tableau 2.1 ci-dessus sont autorisés pour la capture de données de détenteurs de carte.

Si un dispositif approuvé PCI est connecté à un mécanisme de capture de données qui n'est pas approuvé PCI (p. ex., un lecteur approuvé PCI connecté à un clavier qui n'est pas approuvé PCI) :

- l'utilisation d'un tel mécanisme pour recueillir les données de cartes de paiement PCI peut entraîner la hausse des exigences PCI DSS applicables au marchand.

Ne pas modifier ou tenter de modifier la configuration ou les réglages d'un dispositif.

Toute modification ou tentative de modification de la configuration ou des réglages d'un dispositif invalide entièrement la solution CP2P approuvée PCI.

Parmi les exemples, on compte :

- Tentative d'activation d'interfaces ou de mécanismes de capture de données ayant été désactivés sur le dispositif de la solution CP2P
- Tentative de modification des réglages de sécurité ou des contrôles d'authentification
- Ouverture physique du dispositif
- Tentative d'installation d'applications sur le dispositif

4.1 Instructions d'installation et de connexion

Pour obtenir les instructions d'installation ou de connexion de vos dispositifs, allez à <https://soutien.globalpay.com/> ou contactez votre fournisseur PDV.

Remarque : *Seuls les dispositifs approuvés PCI énoncés dans ce guide peuvent être utilisés avec la solution CP2P pour la capture de données.*

4.2 Directives de sélection d'un emplacement approprié pour les dispositifs

Vous devez choisir un endroit approprié pour l'installation ou l'entreposage des dispositifs afin d'assurer leur protection :

- Lors de l'installation, placez le dispositif de sorte que le public ait facilement accès à l'écran, au clavier NIP et aux interfaces permettant d'effectuer la transaction. Si possible, évitez que le public ait accès au bas ou à la partie arrière du dispositif.
- Placez les dispositifs à un endroit où il est facile pour le personnel autorisé de les surveiller. Cela permet également d'effectuer des inspections régulières (voir la section 6.1).
- L'emplacement des dispositifs doit être suffisamment éclairé pour en faciliter l'utilisation et prévenir le vol ou une manipulation non autorisée.
- Le clavier NIP doit être placé de sorte qu'une surveillance vidéo ou une observation visuelle non autorisée soit impossible. L'utilisation d'un écran d'intimité pour la saisie de NIP est recommandée pour que seul le client puisse voir le code entré.
- Seuls les employés ayant besoin des dispositifs dans le cadre de leur travail devraient être autorisés à y accéder.

4.3 Directives de sécurisation physique des dispositifs déployés pour prévenir les substitutions ou les retraits non autorisés

Les moyens utilisés pour prévenir les substitutions ou les retraits non autorisés varient selon que le dispositif est solidement fixé ou est supervisé par l'opérateur. Les dispositifs supervisés peuvent être fixés ou non. Ceux qui ne le sont pas doivent être sécurisés.

- Si fixé, le dispositif doit être installé en accord avec les instructions d'installation du fabricant.
 - Lorsque le fabricant ne fournit pas d'instructions d'installation, les marchands doivent utiliser du matériel de fixation permettant aux clients d'accéder aux interfaces de paiement par carte et de saisie de NIP, sans modifier le boîtier du dispositif, exercer une tension sur les joints ou retirer des vis.
 - Le dispositif doit être fixé de sorte qu'il ne peut pas être retiré ou substitué facilement et rapidement par des personnes non autorisées.
- Si un marchand choisit de ne pas fixer le dispositif (utilisation mobile ou au comptoir avec supervision) ou d'employer un support non permanent (Velcro, socle, support à relâchement rapide), le dispositif doit être supervisé de façon constante, en prenant des mesures additionnelles pour éviter un retrait ou une substitution. Parmi ces précautions, on compte :
 - Donner l'accès uniquement au personnel autorisé. Remarque : cette exigence n'empêche pas le marchand de tendre le dispositif aux clients pour qu'ils puissent insérer ou glisser leur carte, ou saisir leur NIP. Cependant, le personnel autorisé doit surveiller l'utilisation du dispositif pour prévenir un retrait ou une substitution.
 - Lorsqu'il n'est pas utilisé, le dispositif doit rester solidement fixé (voir ci-dessus) ou être conservé en lieu sûr et demeurer accessible seulement au personnel autorisé.

5- Transport de dispositifs

5.1 Instructions de sécurisation des dispositifs en vue de leur transport

Il arrive parfois qu'un marchand doive expédier des dispositifs, que ce soit d'un établissement à l'autre ou vers une entreprise de réparation autorisée. Dans ce cas, le marchand a la responsabilité de sécuriser les dispositifs en vue de leur transport et de prendre les précautions suivantes :

- Il doit faire affaire avec une entreprise fiable, comme un service de livraison privé, la poste ou un expéditeur public (FedEx, UPS, DHL, p. ex.).
- L'entreprise de livraison doit fournir au marchand des données de suivi uniques et le statut de l'expédition.
- Le destinataire doit recevoir un avis de livraison et les données de suivi.

Sécurisez les dispositifs en votre possession, y compris ceux qui sont :

- en attente de déploiement
- en cours de réparation ou ne sont pas utilisés
- en attente d'un transfert d'un établissement à l'autre

5.2 Instructions pour s'assurer que les dispositifs sont expédiés uniquement aux établissements de confiance

L'expédition et la réception des dispositifs ne doivent se faire que par le biais des distributeurs et centres de réparation autorisés de Global Payments. Global Payments fait affaire avec les centres de déploiement suivants pour la distribution et la réparation des dispositifs.

- Avant l'expédition des dispositifs, vous devez vous assurer qu'ils seront livrés à l'un des établissements de confiance suivants :
- À la réception des dispositifs, vous devez vérifier qu'ils proviennent uniquement de l'un des établissements de confiance suivants.

Vous trouverez la liste des centres de déploiement fiables à la section 2.1.

Si vous recevez un dispositif d'un établissement ne figurant pas dans la liste ci-dessus, contactez le Service à la clientèle (voir les coordonnées à la section 1.2) pour vérifier son authenticité, et prévoir son remplacement, s'il y a lieu. Le dispositif ne doit pas être utilisé, sauf si vous avez eu confirmation, de la part d'une source autorisée, qu'il est authentique.

À leur réception, les dispositifs doivent être inspectés selon les instructions de la section 6.1.

6- Inspection des dispositifs

6.1 Instructions d'inspection des dispositifs pour prévenir le clonage, et instructions de signalement d'activité suspecte

Vous trouverez des directives additionnelles sur l'inspection des terminaux dans le document intitulé *Skimming Prevention : Best Practices for Merchants*, accessible à www.pcisecuritystandards.org.

- **But :** L'inspection a pour but de détecter la substitution, le retrait non autorisé ou la falsification d'un dispositif, ou toute autre activité suspecte. L'inspection sert également à s'assurer que les identifiants d'inventaire concordent avec le dispositif et que le dispositif est demeuré intact. Indicateurs de falsification : sceau de sécurité enlevé ou brisé, dispositif endommagé ou présence de connexions additionnelles et inhabituelles. En cas de divergence durant l'inventaire (dispositif manquant ou substitué) ou d'apparence d'activité suspecte (dispositif trafiqué), suivez les directives de la section 6.2 immédiatement.
- **Fréquence :** Selon le PCI, les inspections doivent être faites périodiquement (au moins une fois par année). Pour limiter les risques, Global Payments recommande plutôt de procéder à des inspections mensuelles, au minimum. En cas de haut volume de transactions et selon l'emplacement des dispositifs, les inspections doivent être plus fréquentes (chaque semaine ou chaque jour).
- **Instructions d'inspection :** Le guide du PCI contenant toutes les meilleures pratiques en matière d'inspection, *Skimming Prevention : Best Practices for Merchants*, se trouve dans la bibliothèque des documents du site web pcisecuritystandards.org. Les conseils ci-dessous sont fournis par Global Payments pour l'inspection de base des dispositifs CP2P utilisés avec la solution CP2P de Global Payments :
 - **Sceaux de sécurité inviolables :**
 - Consultez les photos de l'annexe A pour savoir où se trouvent les sceaux de chaque modèle, et reconnaître les signes de manipulation.
 - Durant l'inspection, vérifiez la présence et l'intégrité des sceaux.

- L'emplacement des sceaux peut varier d'un dispositif ou d'un fabricant à l'autre. Cependant, les sceaux sont généralement installés sur les joints ou les vis. Les sceaux servent à prévenir l'accès fortuit à des zones sensibles du dispositif, et à repérer les signes de falsification (sceaux retirés, brisés ou modifiés).

o Vis et joints :

- Consultez les photos de l'annexe A pour voir l'emplacement et l'aspect des vis et des joints en fonction du modèle, et reconnaître les signes de retrait de vis ou de modification de joints.
- Vérifiez que toutes les vis sont en place et que la zone entourant chaque vis ne présente pas de signes de tentative d'ouverture (raclage, grattage).
- Examinez les joints pour vous assurer qu'ils n'ont pas été soulevés ou forcés. Sur les joints, tous les sceaux doivent être en place, sans bris ou déchirure.

o Inspection visuelle du dispositif :

- Dans les photos de l'annexe A, voyez l'aspect normal des fentes de glissement et d'insertion de carte du lecteur, du clavier et du boîtier de chaque modèle. Voyez également à quoi ressemble l'ajout d'un appareil de clonage, la superposition d'une couche sur le clavier NIP, la modification d'un boîtier ou la substitution d'un dispositif.
- Inspectez les fentes de glissement et d'insertion de carte du lecteur. Voyez s'il y a des traces de manipulation, y compris des câbles additionnels, des trous ou du matériel inhabituel inséré dans les fentes.
- Inspectez le clavier NIP. Voyez s'il y a des traces de manipulation, y compris des câbles additionnels, des trous ou une couche recouvrant l'écran ou le clavier.
- Inspectez le boîtier externe. Voyez s'il y a des bris, du raclage, des trous ou d'autres altérations indiquant qu'il a été forcé, modifié, recouvert d'une couche additionnelle ou doté d'un appareil de clonage. Vérifiez que l'équipement correspond au design du fabricant (couleur, forme et taille).

o Connexions :

- Durant l'inspection, assurez-vous qu'il n'y a pas de câbles, fils ou cordons additionnels reliés au terminal, car cela pourrait signifier qu'un appareil de clonage a été inséré dans votre dispositif.

o Matériel de fixation :

- Consultez la section 4.3 sur la manière de sécuriser les dispositifs déployés.
- Si le dispositif est fixé de façon permanente, inspectez le matériel de fixation pour vous assurer que le dispositif est bien sécurisé et qu'il ne peut pas être retiré.
- Si le dispositif n'est pas fixé, assurez-vous qu'il est conservé en lieu sûr lorsqu'il ne sert pas, et que seul le personnel autorisé y a accès.

- **Supervision :**

- Les dispositifs doivent être surveillés par le personnel, selon les directives de la section 4.3.
- Les dispositifs autonomes doivent être solidement fixés et supervisés pour éviter toute falsification ou substitution. Parmi les contrôles acceptables, on compte la surveillance vidéo ou l'activation d'un système qui alerte le personnel par voie électronique en cas de tentative de retrait de dispositif. Le bon fonctionnement et la calibration des contrôles doivent également être vérifiés.

- **Mise à jour d'inventaire :** Si un changement de statut est détecté durant l'inspection, l'inventaire doit être mis à jour. Voyez les instructions de maintien de l'inventaire à la section 3.3.
- **Formation :** Tous les employés chargés d'inspecter les dispositifs doivent connaître les directives ci-dessus et avoir le présent guide à leur disposition. Il est également possible de fournir (à titre de matériel de formation) des instructions ou procédures propres à un marchand, du moment que celles-ci respectent les lignes directrices ci-dessus. Cela permet de s'assurer que tous les processus du marchand sont compris dans la procédure d'inspection.

6.2 Instructions d'intervention en cas de falsification de dispositif

Si durant l'inspection, l'inventaire, l'entreposage ou l'utilisation normale d'un dispositif, il y a détection de falsification, vous devez aviser le Service à la clientèle et cesser le déploiement ou l'utilisation de ce dispositif. En contactant le Service à la clientèle, vous devez confirmer le fabricant, le modèle et le numéro de série du dispositif. Les coordonnées du Service à la clientèle se trouvent à la section 1.2.

Aucun dispositif trafiqué ne doit être déployé ou rester connecté pour le traitement des transactions. Vous devez cesser de l'utiliser immédiatement.

Vous devez mettre à jour la liste d'inventaire en indiquant que le dispositif a été retourné en raison de la détection d'une anomalie lors de l'inspection.

7. Problèmes de cryptage

7.1 Instructions d'intervention en cas d'échec de cryptage du dispositif

Tout problème de cryptage, de clé ou de fonction cryptographique doit être réglé immédiatement. Vous devez cesser de traiter les transactions en cas d'échec de cryptage.

Pour régler ce problème :

1. Cessez immédiatement d'utiliser le dispositif et notez le message d'erreur ou les détails servant à démontrer qu'il y a eu échec de cryptage.
2. Contactez le Service à la clientèle aux coordonnées indiquées à la section 1.2.
3. Le Service à la clientèle réglera le problème.
4. Si le problème peut être résolu de sorte que les fonctions de cryptage normales sont entièrement restaurées, le Service à la clientèle peut vous autoriser à continuer d'utiliser le dispositif.
5. Si une réparation du dispositif est nécessaire, le Service à la clientèle générera une étiquette de retour, qui vous sera envoyée pour faciliter l'expédition.
6. Si le problème n'est pas entièrement réglé, vous ne pourrez pas réactiver le dispositif. Si vous ne désirez pas continuer d'utiliser la solution CP2P, suivez les instructions de renonciation à la section 9.1.

8. Dépannage

8.1 Instructions de dépannage

1. Si un dispositif ne peut authentifier ou traiter une transaction, et communique un code d'erreur, contactez le Service à la clientèle aux coordonnées indiquées à la section 1.2.
2. Si le Service à la clientèle n'est pas en mesure de régler le problème, une demande de remplacement de dispositif peut être faite. Le Service à la clientèle créera une étiquette qu'il vous enverra afin que vous puissiez retourner le dispositif à un établissement de déploiement approuvé, par le biais d'une entreprise de livraison de confiance. Le Service à la clientèle demandera qu'un nouveau dispositif vous soit envoyé. À la réception, vous devrez respecter les contrôles d'inventaire décrits plus haut.

9. Renseignements supplémentaires

9.1 Renseignements supplémentaires sur la solution CP2P

Instructions de demande formelle d'interruption du cryptage CP2P des données de compte auprès du fournisseur de solution CP2P

Étant donné les implications des normes PCI DSS, si vous ne désirez plus participer au programme CP2P PCI (en raison d'un échec de cryptage ou d'une autre contrainte commerciale), vous devez contacter le Service à la clientèle.

De plus, vous devez remplir un formulaire de renonciation fourni par Global Payments, où vous indiquez que vous comprenez les enjeux de sécurité et de conformité se rattachant à votre renonciation : contrôles PCI DSS additionnels, inadmissibilité au questionnaire d'autoévaluation annuel (SAQ) CP2P, notification devant être envoyée aux banques acquéreuses et incidence sur la validation de conformité PCI DSS. Vous avez la responsabilité de respecter toutes les exigences applicables et vous devez transmettre ce formulaire rempli au Service à la clientèle (les options d'envoi de ce formulaire sont fournies lors de la communication avec le Service à la clientèle).

Global Payments collaborera avec vous pour la rétrogradation du terminal, ou la création d'une étiquette qui vous sera envoyée afin que vous puissiez retourner le dispositif à un établissement de déploiement approuvé, par le biais d'une entreprise de livraison de confiance.

9.2 Instructions pour confirmer les versions du matériel, des micrologiciels et des applications des dispositifs

Étant donné que les instructions pour confirmer les versions du matériel, des micrologiciels et des applications des dispositifs varient d'un dispositif à l'autre, veuillez consulter votre fabricant ou votre revendeur à ce sujet.

Annexe A – Photos de dispositifs

Les illustrations suivantes doivent être utilisées lors de l'inspection d'un dispositif pour confirmer son apparence physique. Voir la section 5.1.



T650P



Devant



Derrière



Côté gauche



Côté droit

P630



Devant



Derrière



Côté gauche



Côté droit