

Solution de chiffrement point à point (P2PE) de SCTD

Manuel d'instructions

Le présent document s'adresse aux commerçants qui utilisent la solution de chiffrement point à point pour la norme PCI de la TD. Il vise à vous aider à mieux comprendre la solution et à protéger votre entreprise de la fraude.

Pour les appareils :

- Verifone MX 915 & MX 925



1. Information sur la solution P2PE et coordonnées du fournisseur de solutions

1.1 Information sur la solution P2PE

Nom de la solution : Solution de chiffrement point à point (P2PE) de SCTD

Numéro de référence de la solution selon le site Web du Conseil des normes de sécurité de l'industrie des cartes de paiement : 2020-01281.001

1.2 Coordonnées du fournisseur de solutions

Nom de l'entreprise : Solutions aux commerçants TD

Adresse de l'entreprise : 77 King Street West, 15th Floor, Toronto (Ontario) M5K 1A2

URL de l'entreprise[https : www.td.com/ca/fr/entreprises/solutions-aux-commerçants/](https://www.td.com/ca/fr/entreprises/solutions-aux-commerçants/)

Nom de la personne-ressource : Service d'assistance de Solutions aux commerçants TD

Numéro de téléphone de la personne-ressource: 1-800-363-1163 / ATS 1-888-670-6651

Adresse courriel de la personne-ressource : Sans objet

P2PE et PCI DSS

Les commerçants qui utilisent la présente solution de chiffrement point à point (P2PE) peuvent se voir demander de valider la conformité à la norme de sécurité de l'industrie des cartes de paiement (PCI DSS) et doivent connaître les exigences PCI DSS les concernant. Ils doivent communiquer avec leur acquéreur ou avec leurs marques de paiement pour définir les exigences de validation propres à leurs normes PCI DSS.

2. Terminaux de paiement interactifs approuvés, applications/logiciel et stocks du commerçant

2.1 Caractéristiques du terminal de paiement interactif

L'information ci-après énumère les caractéristiques des terminaux de paiement interactifs approuvés par l'industrie des cartes de paiement en prévision de leur utilisation dans le cadre de la solution P2PE.

Veillez noter que toute l'information relative aux terminaux de paiement interactifs peut être vérifiée en visitant ce site : <https://fr.pcisecuritystandards.org/minisite/env2>

Fournisseur du terminal de paiement interactif : Verifone Inc.

Nom et numéro du modèle du terminal de paiement interactif : MX 915

No de version du matériel : P177-409-01-R (MX 915)

No(s) de version du micrologiciel : Vault : 13.x.x, AppM : 7.x.x; SRED : 4.x.x, OP : 7.x.x

No(s) d'approbation PCI PTS : 4-10177

Fournisseur du terminal de paiement interactif : Verifone Inc.

Nom et numéro du modèle du terminal de paiement interactif : MX 925

No(s) de version du matériel : P177-50x-xx-xxx (MX 925)

No(s) de version du micrologiciel : Vault : 13.x.x, AppM : 7.x.x, SRED : 4.x.x.110, OP : 7.x.x

No(s) d'approbation PCI PTS : 4-10177

2.2 Caractéristiques du logiciel/de l'application du terminal de paiement interactif

L'information ci-après énumère les caractéristiques de tout le logiciel/de toutes les applications (tant les applications P2PE que le logiciel de non-paiement P2PE) applicables aux terminaux de paiement interactifs utilisés dans le cadre de la présente solution P2PE.

Veillez noter que toutes les applications ayant accès aux données de compte en texte clair doivent être revues en fonction du Domaine 2 et sont incluses dans la liste de la solution P2PE. Ces applications peuvent également être incluses sur une base optionnelle dans la liste P2PE de l'industrie des cartes de paiement, qui énumère les applications P2PE validées, à la discrétion du fournisseur ou du fournisseur de solutions.

| Fournisseur, nom et no de version de l'application | Fournisseur du terminal de paiement interactif | Nom(s) et numéro du modèle du terminal de paiement interactif : | No de version du matériel et du micrologiciel du terminal de paiement interactif | L'application figure-t-elle dans la liste de l'industrie des cartes de paiement? (O/N) | L'application a-t-elle accès aux données de compte en texte clair? (O/N) |
|---|---|--|---|---|---|
| Verifone, Formagent / XPI 5300 | VeriFone | MX 925 | P177-50x-xx-xxx Vault: 13.x.x, AppM: 7.x.x, SRED: 4.x.x.1105300, OP: 7.x.x | Y | Y |
| | Verifone | MX 915 | P132-409-01-R Vault: 13.x.x, AppM: 7.x.x, SRED: 4.x.x.110, OP: 7.x.x | | |

2.3 Inventaire et surveillance des terminaux de paiement interactifs

- Tous les terminaux de paiement interactifs doivent faire l'objet d'un contrôle des stocks et de procédures de surveillance dûment documentés, notamment en ce qui a trait à l'état du terminal (en service, en attente de la mise en service, en réparation ou non utilisé, ou encore, en transit).
- Cet inventaire doit être effectué au moins chaque année.
- Toute fluctuation de l'inventaire, incluant les terminaux de paiement interactifs manquants ou remplacés, doit être signalée à Solutions aux commerçants de la TD, au moyen des coordonnées fournies à la section 1.2 plus haut.
- Le modèle de tableau des stocks ci-dessous est fourni à titre indicatif uniquement. L'inventaire actuel doit être saisi et mis à jour par le commerçant dans un document externe.

Pour demeurer conforme, vous devez inspecter vos terminaux à la livraison/à l'installation et tenir un inventaire de vos claviers NIP actuels.

L'information ci-après doit être consignée après l'installation de votre clavier NIP :

- fabricant du terminal (coin supérieur gauche sur le devant du terminal – dans le cas présent, Verifone);
- marque et modèle du terminal (sur l'étiquette apposée au dos du terminal);
- numéro de série du terminal (sur l'étiquette apposée au dos du terminal [voir l'image à droite]);
- emplacement et état du terminal (stockage, lieu de la mise en service, en transit, en attente de réparation ou retourné);
- date de l'inspection de l'emplacement (la dernière date à laquelle l'emplacement du terminal a été confirmé);
- date de la dernière inspection (la dernière fois que le terminal a été inspecté aux fins de recherche de signes d'altération);
- nom de la fonction ou du membre du personnel ayant procédé à l'inspection;
- date de la dernière mise à jour de l'inventaire.



Pendant votre processus d'inspection, vous devez déterminer quels sont les terminaux qui ont été remplacés. Si vous deviez trouver un signe d'un tel remplacement, votre commerce pourrait avoir été compromis. Pour déterminer si un terminal a été remplacé, vous devez comparer l'information figurant sur l'appareil comme tel avec l'information d'inventaire que vous avez colligée au préalable.

Votre inspection doit également vous permettre de surveiller toute indication d'altération de vos terminaux. Par exemple :

- Sceaux manquants, endommagés ou altérés
- Mauvaises clés
- Vis manquantes
- Grilles de clavier incorrectes
- Câbles externes
- Trous dans le terminal
- Étiquettes, peinture ou recouvrements qui pourraient camoufler des altérations
- Tout élément inhabituel ou déplacé
- L'insertion d'un dispositif d'« écrémage » à même le lecteur de bande magnétique du terminal. Ces dispositifs d'écrémage, qui sont en fait de faux lecteurs de cartes, sont utilisés par du personnel non autorisé dans le but de tenter de saisir les données avant même que le clavier NIP puisse lire la carte. Ils sont insérés dans le lecteur de bande magnétique du terminal ou plaqués directement contre ce dernier.

REMARQUE : Nous vous recommandons d'assurer la formation d'un des utilisateurs de vos claviers NIP pour qu'il puisse en faire l'inspection quotidienne aux fins de recherche de signes d'altération.

Si vous croyez qu'un terminal a été compromis, que votre inventaire indique un terminal manquant ou qu'un terminal a été remplacé, vous devez immédiatement le signaler au service d'assistance de Solutions aux commerçants TD au 1-800-363-1163.

Pour assurer la tenue de votre inventaire, vous devez faire le suivi de l'emplacement de votre terminal et désigner une personne qui sera chargée de maintenir l'inventaire et d'inspecter les terminaux.

L'inventaire des terminaux doit être effectué :

- au moins une fois par année, pour confirmer qu'il a été répertorié et qu'il a été correctement exécuté;
- quand un terminal entre ou sort du service, ou qu'il passe d'un lieu à un autre;
- pour confirmer que tous les terminaux identifiés sont actuellement en votre possession et qu'il n'en manque pas.

Le lieu de stockage doit comprendre les éléments suivants :

- Les terminaux qui ne sont pas en service doivent être stockés dans une pièce ou un contenant verrouillé, comme un classeur ou un tiroir.

- Le lieu de stockage doit pouvoir répondre aux critères d'accès restreint au personnel autorisé, en étant notamment équipé des caractéristiques suivantes :
- porte ou contenant nécessitant un accès par clé, à laquelle des membres désignés du personnel ont accès;
- porte ou contenant nécessitant la connaissance du code de la serrure et que les membres désignés du personnel connaissent.
- L'accès au lieu de stockage doit être consigné. Il peut s'agir d'une tâche manuelle (registre manuscrit) ou automatique (système de carte d'identité).
- L'accès à la pièce de stockage doit faire l'objet d'une surveillance par caméra ou par observation.
- N'ÉCHANGEZ PAS les terminaux entre les établissements ou emplacements sans d'abord en aviser le service d'assistance de Solutions aux commerçants TD au 1-800-363-1163.

Modèle de tableau des stocks

| Fournisseur du terminal | Nom(s) et numéro du modèle du terminal | Emplacement du terminal | Statut du terminal | Numéro de série ou autre identificateur unique |
|-------------------------|--|-------------------------|--------------------|--|
| | | | | |

3. Directives d'installation du terminal de paiement interactif

Ne branchez pas d'appareils de saisie de données de titulaire de carte non approuvés.

La solution P2PE inclut des terminaux de paiement interactifs précis, approuvés par l'industrie des cartes de paiement. Seuls les terminaux figurant au tableau 2.1 plus haut sont autorisés aux fins de la saisie de données de titulaire de carte.

Si votre terminal de paiement interactif approuvé par l'industrie des cartes de paiement est branché à un mécanisme de saisie de données non approuvé par cette industrie (p. ex. un lecteur de carte sécurisé approuvé par l'industrie des cartes de paiement a été branché à un clavier qui n'est pas approuvé par cette industrie) :

- L'utilisation de tels mécanismes pour recueillir les données de paiement par carte PCI pourrait signifier qu'il y aurait plus de normes PCI DSS auxquelles vous êtes désormais assujetti.
- Seuls les mécanismes de saisie P2PE approuvés figurant sur la liste de solutions P2PE validées de l'industrie des cartes de paiement ainsi que dans le manuel d'instruction des terminaux P2PE peuvent être utilisés.

Ne changez pas ou ne tentez pas de changer les configurations ou les paramètres du terminal.

Le fait de changer ou de tenter de changer les configurations ou les paramètres du terminal rendra complètement invalide la solution P2PE approuvée par l'industrie des cartes de paiement. Voici une liste non exhaustive d'exemples de changement de configuration ou de paramètres :

- tenter d'activer des interfaces ou des mécanismes de saisie de données du terminal qui avaient été désactivés sur le terminal de paiement interactif de la solution P2PE;
- tenter d'altérer les configurations de sécurité ou les contrôles de vérification de l'identité;
- ouvrir physiquement le terminal;
- tenter d'installer des applications sur le terminal.

3.1 Installation et instructions de connexion

Les techniciens de Solutions aux commerçants TD se chargeront de l'installation, de la démonstration et de la formation à votre établissement.

MX 915

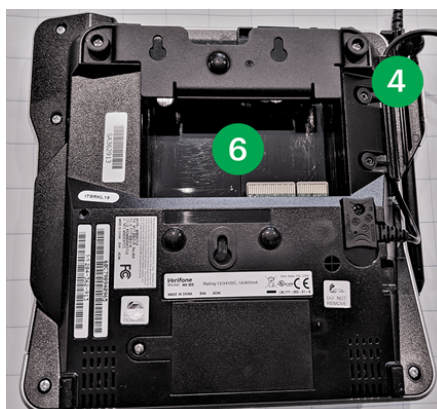
1. Lecteur de carte à puce
2. Lecteur de bande magnétique
3. Lecteur de carte sans contact
Passez la carte devant l'écran tactile.
4. Stylet
5. Clavier
6. Câbles de données reliés à la caisse
Veuillez noter qu'il peut y avoir plus d'un câble, selon le type de connexion de la solution.

Sur l'image de droite, on utilise une connexion USB ainsi qu'un troisième câble pour l'alimentation.



Connexions par câble sur l'appareil :

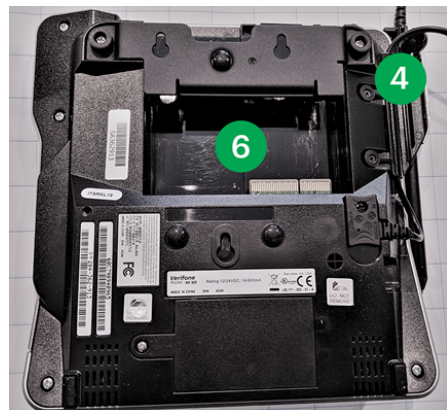
- Câble USB relié à la caisse électronique
- COM2
- Ethernet
- Audio
- Alimentation



MX 925

1. Lecteur de carte à puce
2. Lecteur de bande magnétique
3. Lecteur de carte sans contact
Passez la carte devant l'écran tactile.
4. Stylet
5. Clavier
6. Câbles de données reliés à la caisse
Veillez noter qu'il peut y avoir plus d'un câble, selon le type de connexion de la solution.

Sur l'image de droite, on utilise une connexion USB ainsi qu'un troisième câble pour l'alimentation.



Connexions par câble sur l'appareil :

- Câble USB relié à la caisse électronique
- COM2
- Ethernet
- Audio
- Alimentation

Remarque : Seuls les terminaux de paiement interactifs approuvés par l'industrie des cartes de paiement et indiqués dans le manuel d'instruction des terminaux P2PE peuvent être utilisés avec la solution P2PE aux fins de saisie de données de compte.

Procédez à la sécurisation physique des terminaux de paiement interactifs en votre possession, y compris les terminaux :

- en attente de mise en service;
- en réparation ou autrement non utilisés;
- en attente d'un transit entre deux emplacements.

3.2 Conseils pour la sélection d'endroits appropriés pour la mise en service de terminaux

Au moment de déterminer où vous installerez votre clavier NIP, vous devez prendre les éléments suivants en considération pour déterminer l'endroit idéal.

Les claviers NIP NE DOIVENT PAS être installés :

- à la lumière directe du soleil;
- à moins de 60 cm (2 pi) d'appareils qui sont une source excessive de fluctuations de tension ou de bruits électriques, ou qui diffusent de la chaleur;
- à moins de 2 m (6,5 pi) des portes antivols;
- à moins de 45 cm (1,5 pi) de surfaces de désactivation;
- à l'extérieur, lorsqu'ils sont conçus en prévision d'une utilisation à l'intérieur seulement;
- dans des zones les exposant à une chaleur excessive, à la poussière, à la graisse et à l'humidité;
- près d'une source d'eau.

Les claviers NIP doivent être installés :

- sous un bon éclairage, bien à la vue du personnel autorisé, en vue de dissuader toute tentative de compromission;
- dans des zones pourvues d'une ventilation adéquate et à l'abri des dommages physiques;
- de façon à restreindre l'accès physique aux terminaux pour que seules les parties normalement utilisées par une personne, comme le clavier NIP et le lecteur de carte, soient accessibles;
- de façon à restreindre l'accès à toute partie du terminal qui n'est pas nécessaire aux fins d'utilisation par le public, comme les câbles, les câbles d'alimentation et les panneaux d'accès;
- de façon à rendre difficile, pour un tiers, d'épier la saisie du NIP;
- de façon à rendre la saisie du NIP sur le clavier inaccessible aux caméras de surveillance de l'établissement.

Nous vous recommandons fortement de prendre des photos de votre clavier NIP (avant et arrière) une fois ce dernier installé. Ensuite, utilisez ces photos comme référence lorsque vous inspectez le clavier NIP.

3.3 Conseils en vue de sécuriser les terminaux installés pour en prévenir le retrait ou la substitution sans autorisation

Nous vous recommandons fortement d'envisager l'installation de stations verrouillées pour prévenir tout retrait non autorisé des terminaux.

Le clavier NIP doit :

- être installé sur le comptoir; et
- les câbles doivent être solidement fixés, de façon à ne pas se débrancher par le simple fait de retourner le clavier NIP.

Si les terminaux ne peuvent pas être sécurisés physiquement (comme les terminaux sans fil et les terminaux mobiles), vous devez :

- sécuriser les terminaux en les rangeant dans une pièce verrouillée quand ils ne sont pas utilisés;

- consigner l'entrée et la sortie des terminaux, au besoin;
- assigner la responsabilité du terminal utilisé à une personne désignée;
- garder vos terminaux à l'œil en tout temps.

Vous devez sécuriser physiquement les terminaux lorsqu'ils ne sont pas en service ou en cours d'utilisation. Cette consigne prévaut dans les cas suivants :

- terminaux envoyés à la réparation ou en maintenance alors qu'ils sont en la possession du commerçant;
- terminaux en attente de leur mise en service ou de leur transport entre deux emplacements.

Vous devez prévenir tout accès physique non autorisé aux terminaux ayant besoin de réparation ou de maintenance s'ils sont en votre possession, en :

- vérifiant l'identité et l'autorisation du personnel chargé des réparations avant de donner l'accès;
- escortant et en surveillant le personnel autorisé en tout temps.

4. Terminal de paiement interactif en transit

4. Directives pour sécuriser les terminaux de paiement interactifs en vue de leur transit et pendant celui-ci

Un clavier NIP ne doit jamais transiter d'un établissement du commerçant à un autre sans l'assistance d'un technicien de Solutions aux commerçants TD.

Vous devez appeler le service d'assistance de Solutions aux commerçants TD au 1-800-363-1163 pour lancer :

- une demande de désinstallation qui nécessitera la visite d'un technicien pour ramasser l'équipement;
- un bordereau d'envoi d'UPS et un endroit où laisser la boîte pour l'expédition par messagerie.

Si vous avez des questions, veuillez communiquer avec le service d'assistance de Solutions aux commerçants TD au 1-800-363-1163.

4.2 Directives pour s'assurer que les terminaux de paiement interactifs ne proviennent que d'emplacements de confiance, et qu'ils sont expédiés à de tels endroits

Un technicien de Solutions aux commerçants TD se rendra à votre établissement avec le clavier NIP en prévision de son installation.

Assurez-vous de vérifier son identité pour confirmer qu'il est bel et bien le technicien qu'il prétend être.

Si vous avez des questions, veuillez communiquer avec le service d'assistance de Solutions aux commerçants TD au 1-800-363-1163.

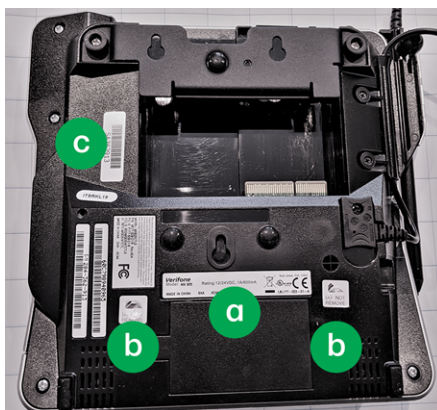
5. Surveillance de l'altération et prévention de l'écrémage d'un terminal de paiement interactif

5.1 Directives pour procéder à l'inspection physique et prévenir l'écrémage des terminaux de paiement interactifs, y compris les directives et les coordonnées pour signaler toute activité suspecte

Vous pouvez trouver d'autres conseils pour la prévention de l'écrémage des terminaux de paiement interactifs dans le document intitulé *Skimming Prevention: Best Practices for Merchants*, (en anglais seulement) offert sur le site www.pcisecuritystandards.org.

INSPECTIONS VISUELLES PÉRIODIQUES DU TERMINAL

1. Procédez régulièrement à des inspections visuelles de chacun de vos terminaux pour y déceler d'éventuels signes d'altération. Ces signes incluent notamment :
 - a) Autocollant du fabricant manquant, endommagé ou altéré
 - b) Autocollants Do Not Remove (Ne pas enlever) manquants, endommagés ou altérés
 - c) Autocollant du numéro de série manquant, endommagé ou altéré
 - d) Mauvaises clés
 - e) Vis manquantes
 - f) Grilles de clavier incorrectes
 - g) Câbles externes
 - h) Trous dans le terminal
 - i) Étiquettes, peinture ou recouvrements qui pourraient camoufler des altérations
 - j) Tout élément inhabituel ou déplacé
2. Scrutez le plafond pour y déceler des caméras cachées.
3. Examinez les dimensions du terminal pour déterminer si un recouvrement a été ajouté. Le recouvrement peut contenir du matériel de numérisation de carte et



d'enregistrement du NIP. Les dimensions doivent être les suivantes :

MX 915 : 225 mm (8,9 po) de longueur × 182 mm (7,2 po) de largeur × 56 mm (2,2 po) de hauteur; poids de 0,6 kg (1,3 lb).

MX 925 : 230 mm (9,1 po) de longueur × 218 mm (8,6 po) de largeur × 56 mm (2,2 po) de hauteur; poids de 0,9 kg (2 lb).

4. Assurez-vous que les câbles n'ont pas été retirés ou changés.
5. Si vous notez quoi que ce soit qui sort de l'ordinaire, interrompez l'utilisation du terminal, que vous déconnecterez du PDV ou du réseau, mais **NE LE METTEZ PAS** hors tension.
6. Veuillez communiquer avec le service d'assistance de Solutions aux commerçants TD, au 1-800-363-1163 pour convenir des prochaines étapes.
7. Continuez d'exécuter les inspections visuelles avant tout changement de quart.
8. Utilisez les photos que vous avez prises après l'installation du clavier NIP à la section 3.2 ou reportez-vous à l'image de la section 3.1 lorsque vous effectuez l'inspection.

SURVEILLANCE DES PROBLÈMES DE PAIEMENT DU CLAVIER NIP

1. Mettez au point un processus pour surveiller les terminaux qui présentent constamment des problèmes de fonctionnement, notamment en affichant un nombre élevé d'échecs de lecture de carte ou de refus de carte. Ces symptômes pourraient indiquer des terminaux altérés ou compromis.
2. Veuillez communiquer avec le service d'assistance de Solutions aux commerçants TD, au 1-800-363-1163 pour convenir des prochaines étapes.

MONTAGE SÉCURITAIRE DES CLAVIERS NIP

Revoyez l'installation de vos claviers NIP. Ceux-ci doivent

- être installés sur le comptoir;
- Les câbles doivent être solidement fixés, de façon à ne pas se débrancher par le simple fait de retourner le clavier NIP.

Nous vous recommandons fortement d'envisager l'installation de stations verrouillées pour prévenir tout retrait non autorisé des terminaux.

5.2 Directives pour réagir à une altération évidente du terminal de paiement interactif

Si vous avez des raisons de croire que le terminal ou son emballage a été altéré pendant l'expédition, ou que le terminal a été compromis pendant son installation :

1. Ne procédez pas à l'installation ou à l'utilisation du terminal;
2. Communiquez avec le service d'assistance de Solutions aux commerçants TD au 1-800-363-1163 et signalez une activité douteuse, notamment :

- a) Un clavier NIP perdu, volé ou compromis
- b) Des changements non autorisés à la configuration ou aux contrôles d'accès du clavier NIP
- c) La déconnexion ou la reconnexion non autorisée d'un terminal
- d) Tout message indiquant un bris du mécanisme de chiffrement
- e) Tout message indiquant un bris du contrôle de sécurité du terminal
- f) La connexion d'un dispositif non reconnu

Si vous devez retourner un terminal P2PE, vous devez communiquer avec le service d'assistance de Solutions aux commerçants TD au 1-800-363-1163 pour obtenir des directives.

5.3 Directives pour confirmer que le terminal et son emballage n'ont pas été altérés et pour établir des communications sécurisées avec le fournisseur de solutions

Vérifiez que les sceaux inviolables de l'emballage de l'appareil sont intacts avant de les briser et d'ouvrir la boîte.

Si le sceau de sécurité ou les sceaux inviolables semblent avoir été altérés :

1. Cessez immédiatement le déballage du terminal;
2. Veuillez communiquer avec le service d'assistance de Solutions aux commerçants TD, au 1-800-363-1163 pour convenir des prochaines étapes.



5.4 Directives pour confirmer le besoin d'affaires et l'identité d'un membre de personnel tiers affirmant relever du service de soutien et de réparation avant de lui accorder l'accès aux terminaux de paiement interactifs

VÉRIFICATION ET CONSIGNATION DU TECHNICIEN RÉPARATEUR

1. Mettez en place une procédure qui obligera tous les techniciens réparateurs qui effectuent une visite à votre établissement à s'inscrire à votre registre et à montrer une pièce d'identité comportant une photo.
2. Les techniciens doivent être escortés par un membre du personnel du magasin pendant qu'ils travaillent sur des claviers NIP.

6. Problèmes de chiffrement du terminal

6.1 Directives pour répondre aux échecs de chiffrement du terminal de paiement interactif

Advenant un improbable cas d'échec de chiffrement ou de déchiffrement du clavier NIP :

1. Les opérations ne seront pas exécutées et l'écran affichera le message Transaction not completed (Opération non effectuée);
2. On vous invitera alors à entrer l'opération de nouveau;
Si vous voyez encore le message Transaction not completed (Opération non effectuée), veuillez communiquer avec le service d'assistance de Solutions aux commerçants TD au 1-800-363-1163 pour obtenir des directives.

N'UTILISEZ PAS le clavier NIP avant que le service d'assistance de Solutions aux commerçants TD ne vous y ait autorisé.

6.2 Directives pour demander formellement au fournisseur de solution P2PE d'interrompre le processus de chiffrement point à point des données du compte

Le terminal ne comporte pas d'option vous permettant de désactiver le processus de chiffrement. Par conséquent, vous ne disposez d'aucun moyen pour demander formellement l'interruption de chiffrement point à point des données du compte. Si vous, le commerçant (ou un dirigeant de l'entreprise) décidez que vous n'avez plus besoin de la solution P2PE, une personne autorisée de votre entreprise doit communiquer avec votre représentant des ventes pour en discuter.

7. Dépannage du terminal de paiement interactif

7.1 Directives pour le dépannage d'un terminal de paiement interactif

PCI requirements demand that PIN Pads must have built-in tamper detection capability
Les exigences de l'industrie des cartes de paiement prévoient que les claviers NIP soient dotés d'une capacité de détection de modifications frauduleuses; toute tentative d'intrusion se soldera par la désactivation du terminal, ce qui rendra l'exécution d'opérations impossible. Plusieurs raisons peuvent expliquer la désactivation du terminal, comme le fait d'appliquer un faux lecteur de carte au terminal, la tentative de l'ouvrir physiquement, le fait de l'échapper.

Si le terminal détecte une quelconque altération :

1. Il affichera un message d'effraction, qu'il ne sera pas possible d'effacer;
2. Veuillez communiquer avec le service d'assistance de Solutions aux commerçants TD, au 1-800-363-1163 pour connaître les étapes suivantes.

Lorsque vous appelez le service d'assistance de Solutions aux commerçants TD, assurez-vous d'avoir en main les renseignements suivants :

1. Le numéro de série du terminal, que vous trouverez à l'arrière de celui-ci
2. La marque et le modèle du terminal, p. ex. Verifone MX 925
3. Votre système PDV et votre solution intergicielle, ainsi que le numéro de version
4. La date et l'heure locale précises auxquelles le problème est survenu
5. Toute référence connexe à l'opération, p. ex. code d'autorisation ou numéro d'identification de l'opération
6. Constate-t-on le même problème avec d'autres terminaux?
7. Étapes permettant de reproduire le problème

Pour votre propre sécurité, nous veillons à ce que toutes les demandes proviennent du personnel autorisé et à ce que les renseignements sur les produits correspondent au contenu des dossiers de Solutions aux commerçants TD. Nous ne demanderons jamais aux commerçants de nous soumettre des numéros de carte pendant un appel de soutien.

8. Autres renseignements relatifs aux fournisseurs de solutions

Seuls les techniciens de Solutions aux commerçants TD sur le terrain sont autorisés à intervenir sur les claviers NIP aux fins de service et de réparation. C'est au marchand qu'il incombe de lancer la procédure de visite de service par l'intermédiaire du service d'assistance de Solutions aux commerçants au 1-800-363-1163. Pour assurer la surveillance adéquate de l'accès au clavier NIP, vous devez disposer d'un processus et de procédures appropriés pour permettre l'exécution des étapes suivantes :

1. Le personnel autorisé de votre établissement doit communiquer avec le service d'assistance de Solutions aux commerçants pour lancer la procédure de visite de service et de demande de désinstallation d'équipement.
2. Avant de donner accès à l'équipement aux techniciens de Solutions aux commerçants TD sur le terrain, le personnel doit vérifier leur identité et leur fournir les autorisations nécessaires dès leur arrivée.
3. Les techniciens de Solutions aux commerçants TD sur le terrain possèdent une carte d'accès avec photo délivrée par la TD, qu'ils doivent porter en tout temps.
4. Vous devez tenir un registre dans lequel seront consignés les détails quant à la date et à l'heure, au nom du technicien et au motif invoqué pour accéder à l'équipement.
5. Les techniciens de Solutions aux commerçants TD sur le terrain doivent être escortés et observés sans relâche.
6. Vous devez autoriser tout échange ou retrait d'équipement et mettre à jour la documentation d'inventaire en y consignant l'information relative au nouveau terminal.

