



Manuel d'instructions P2PE (PIM)
Un guide pour les commerçants pour le
déploiement et la maintenance de la
solution de réduction du périmètre P2PE de
FreedomPay

Version 3.4

1. Informations sur la solution P2PE et coordonnées du fournisseur de la solution P2PE

1.1 Informations sur la solution P2PE (telles que figurant dans la liste du site web du PCI SSC)	
Nom de la solution P2PE :	FreedomPay Commerce Platform P2PE
Numéro de référence de la solution P2PE dans la liste (Attribué par le PCI SSC)	2025-00909.016
https://listings.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions	

1.2 Coordonnées du fournisseur de la solution P2PE					
Nom de la société :	FreedomPay, Inc.	URL de la société :	http://corporate.freedompay.com		
Nom du contact :	Bernard Clary	Titre :	VP de la conformité		
Téléphone :	+1-610-902-9000	E-mail :	compliance@freedompay.com		
Adresse professionnelle :	FMC Tower at Cira Centre South 2929 Walnut Street · Floor 14	Ville :	Philadelphia		
État/Province :	Pennsylvanie	Pays :	États-Unis	Code postal :	19104

1.3 Instructions de communication
Instructions indiquant comment contacter le fournisseur de la solution P2PE, en tenant compte de l'établissement d'un canal/d'une session de communication de confiance.
<p>Les commerçants peuvent contacter leur Customer Success Manager (CSM) dédié, ou accounts@freedompay.com s'ils n'ont pas de CSM dédié, pour toute question générale relative à leur compte ou à leur mise en œuvre.</p> <p>Les questions d'assistance technique peuvent être adressées à techsupport@freedompay.com ou via le formulaire d'assistance de notre site web.</p> <p>Les questions de conformité peuvent être adressées à compliance@freedompay.com.</p>

PCI P2PE et PCI DSS

Les commerçants utilisant cette solution P2PE peuvent être tenus de valider leur conformité à PCI DSS. Les commerçants doivent contacter leur acquéreur ou les marques de paiement afin de déterminer leurs exigences de validation PCI DSS.

Consultez la [FAQ 1158](#) sur le site web du PCI SSC.

2. Informations sur les dispositifs PTS POI et les logiciels

2.1 Détails des dispositifs PTS POI

Les informations suivantes détaillent les dispositifs PTS POI approuvés pour être utilisés dans cette solution P2PE.

Toutes les informations sur les dispositifs PTS POI peuvent être vérifiées en consultant le lien suivant sur le site web du PCI SSC et en se référant au tableau 2.4 ci-dessous :

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

https://listings.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions

Pour les applications P2PE et les logiciels non liés au paiement, utilisez les numéros d'ID PIM pour effectuer un renvoi vers leurs tableaux respectifs ci-dessous. Les « ID PIM » sont des numéros créés et utilisés par le fournisseur de la solution P2PE uniquement dans le cadre de ce PIM, afin de faciliter le renvoi vers les applications P2PE et les logiciels non liés au paiement utilisés sur les dispositifs PTS POI indiqués ici. Les « ID PIM » ne sont pas attribués par le PCI SSC et ne sont pas reconnus par le programme PCI P2PE.

N° d'approbation PCI PTS	PTS POI Fournisseur du dispositif	Nom et numéro(s) de modèle du dispositif PTS POI	Matériel du dispositif PTS POI Numéro(s) de version	Micrologiciel du dispositif PTS POI Numéro(s) de version	Applications P2PE sur les dispositifs PTS POI (ID PIM du tableau 2.2)	Logiciels non liés au paiement sur les dispositifs PTS POI (ID PIM du tableau 2.3)
4-20324	Ingenico	Lane/5000	LAN51BA (une tête MSR), LAN51CA (deux têtes MSR), LAN51DA (une tête MSR et caméra), LAN51EA (deux têtes MSR et caméra)	820547v01.xx, 820376v01.xx, 820549v01.xx (SRED OnGuard FPE), 820556v01.xx (SRED OnGuard SDE), 820559v01.xx (SRED ANL), 820555v01.xx (SRED AWL)	App#1, App#2, App#3	S/O
4-30257	Ingenico	Lane/8000	LAN80AA, LAN80BA	820547v01.xx	App#1, App#2	S/O

4-30326	Ingenico	Link/2500	LIN25AA (version de base sans prise en charge CTLS), LIN25BA (version de base avec CTLS), LIN25CA (version Companion sans prise en charge CTLS), LIN25DA (version Companion avec CTLS), LIN25EA (version tactile sans prise en charge CTLS), LIN25FA (version tactile avec CTLS), LIN25GA (version à deux têtes sans prise en charge CTLS), LIN25HA (version à deux têtes avec CTLS), LIN25IA (version Companion avec connecteur arrière et sans prise en charge CTLS), LIN25JA (version Companion avec connecteur arrière et avec CTLS)	820547v01.xx	App#1, App#3	S/O
4-30237	Ingenico	Lane/7000	LAN70AA, LAN70AB, LAN70BB	820547v01.xx, 820376v04.xx (services de sécurité)	App#1, App#2	S/O

4-20316	Ingenico	Move/5000	<p>MOV50AC (sans CTLS)</p> <p>MOV50AQ (sans CTLS)</p> <p>MOV50AS (sans CTLS)</p> <p>MOV50BB (CTLS)</p> <p>MOV50BC (CTLS)</p> <p>MOV50BQ (CTLS)</p> <p>MOV50BR (CTLS) ; MOV50DR (CTLS + écran de confidentialité) ; MOV50JR (CTLS + écran de confidentialité + couvercle de boîtier de bureau) ; MOV50BE (CTLS) ; MOV50DE (CTLS + écran de confidentialité) ; MOV50JE (CTLS + écran de confidentialité + couvercle de boîtier de bureau)</p> <p>MOV50BS (CTLS)</p> <p>MOV50CB (sans CTLS + écran de confidentialité)</p> <p>MOV50CC (sans CTLS + écran de confidentialité)</p> <p>MOV50CQ (sans CTLS + écran de confidentialité)</p> <p>MOV50CS (sans CTLS + écran de confidentialité)</p> <p>MOV50DB (CTLS + écran de confidentialité)</p> <p>MOV50DC (CTLS + écran de confidentialité)</p> <p>MOV50DN (CTLS + écran de confidentialité)</p> <p>MOV50DQ (CTLS + écran de confidentialité)</p> <p>MOV50DS (CTLS + écran de confidentialité)</p> <p>MOV50JB (CTLS + écran de confidentialité + couvercle de boîtier de bureau)</p>	<p>820376v01.xx, 820547v01.xx, 820549v01.xx (SRED OnGuard FPE), 820555v01.xx (SRED), 820556v01.xx (SRED OnGuard SDE), 820559v01.xx (SRED ANL), 820565v01.xx (SRED FF1)</p>	App#1, App#2, App#3, App#5	S/O
---------	----------	---------------------------	--	--	--	---------------------

			<p>MOV50JC (CTLS + écran de confidentialité + couvercle de boîtier de bureau)</p> <p>MOV50JN (CTLS + écran de confidentialité + couvercle de boîtier de bureau)</p> <p>MOV50JQ (CTLS + écran de confidentialité + couvercle de boîtier de bureau)</p> <p>MOV50JS (CTLS + écran de confidentialité + couvercle de boîtier de bureau)</p> <p>MOV50AB (sans CTLS)</p> <p>MOV50BN (CTLS)</p>			
4-30310	Ingenico	<i>Lane/3000</i>	<p>LAN30AA, LAN30BA, LAN30CA, LAN30DA, LAN30EA, LAN30FA, LAN30GA, LAN30HA</p>	<p>820547v01.xx, 820561v01.xx (micrologiciel de base)</p>	<i>App#1, App#2, App#3</i>	<i>S/O</i>
4-20317	Ingenico	<i>DESK/5000</i>	<p>(CTLS) (sans CTLS + écran de confidentialité) (sans CTLS) DES50AB, DES50BB, DES50CB, DES50DB (CTLS + écran de confidentialité)</p>	<p>820376v01.xx, 820547v01.xx (micrologiciel principal), 820549v01.xx (SRED OnGuard FPE), 820555v01.xx (SRED), 820556v01.xx (SRED OnGuard SDE), 820559v01.xx (SRED ANL), 820565v01.xx (SRED FF1)</p>	<i>App#6</i>	<i>S/O</i>
4-30365	Ingenico	<i>Moby/5500</i>	<p>MOB55xBxAx, MOB55ABBBx (avec CTLS)</p> <p>MOB55BBABx (sans CTLS)</p> <p>MOB55BBBBx (avec CTLS)</p> <p>MOB55ABABx (sans CTLS)</p> <p>MOB55xBxAx</p>	<p>CTRL: xxxx-F-802-01xx-xxxx-xx</p> <p>BOOT: xxxx-F-801-01xx-xxxx-xx</p> <p>CTRL: xxxx-F-802-02xx-xxxx-xx BOOT: xxxx-F-801-02xx-xxxx-xx</p>	<i>S/O</i>	<i>S/O</i>

4-90307	Ingenico	<i>Moby/5500 CL3</i>	MOB55ABHAX (avec CTLS) MOB55BBGAX (sans CTLS) MOB55BBHAX (avec CTLS) MOB55ABGAX (sans CTLS)	BOOT: xxxx-F-001-01xx-xxxx-xx CTRL: xxxx-F-D02-01xx-xxxx-xx USER: xxxx-F-023-02xx-xxxx-xx		S/O
4-30263	Ingenico	<i>Moby/8500</i>	MOB85AAX (sans CTLS), MOB85ABX (sans CTLS), MOB85ACX (sans CTLS), MOB85BAX (avec CTLS), MOB85BBX (avec CTLS), MOB85BCX (avec CTLS)	Boot: xxxx-F-701-01xx-xxxx-xx, Boot: xxxx-F-701-02xx-xxxx-xx, Boot: xxxx-F-701-03xx-xxxx-xx, Ctrl: xxxx-F-702-01xx-xxxx-xx, Ctrl: xxxx-F-702-02xx-xxxx-xx, Ctrl: xxxx-F-702-03xx-xxxx-xx, Ctrl: xxxx-F-702-04xx-xxxx-xx	S/O	S/O
4-30481	Ingenico	<i>Lane/3600</i>	LAN36AA2-xxxx, LAN36AB2-xxxx, LAN36BA1-xxxx, LAN36BA2-xxxx, LAN36CA1-xxxx, LAN36CA2-xxxx, LAN36CB2-xxxx, LAN36DA1-xxxx, LAN36DA2-xxxx, LAN36DB2-xxxx, LAN36EA2-xxxx, LAN36FA2-xxxx, LAN36AA1-xxxx	820571v01.xx (micrologiciel principal), 820376v12.xx (services de sécurité), 820555v01.xx (SRED AWL), 820556V01.xx (SRED On-Guard SDE), 820549V01.xx (SRED On-Guard FPE), 820570V07.xx (protocoles ouverts), 820565V01.xx (SRED FF1)	App#2	<i>S/O</i>
4-30381	Ingenico	<i>Self/2000</i>	SEL20AA	820376v04.xx (services de sécurité) 820566v01.xx	App#2	<i>S/O</i>
4-30393	Ingenico	<i>Self/4000</i>	SEL40BA	820376v04.xx (services de sécurité) 820547v01.xx	App#2	<i>S/O</i>
4-30384	Ingenico	<i>Self/5000</i>	SEL50CA	820376v04.xx (services de sécurité) 820566v01.xx	App#2	<i>S/O</i>

4-30510	Ingenico	<i>Self/3000</i>	SEL30BA1-xxxx SEL30BA2-xxxx SEL30AA1-xxxx SEL30AA2-xxxx	820571v01.xx (micrologiciel de base), 820376v12.xx (services de sécurité), 820555v01.xx (SRED AWL), 820556v01.xx (SRED On-Guard SDE), 820549v01.xx (SRED On-Guard FPE), 820565v01.xx (SRED FF1)	App#2	<i>S/O</i>
4-30535	Ingenico	<i>Self/4000 LE</i>	SEL41AA1-xxxx SEL41AA2-xxxx	820571v01.xx (micrologiciel principal), 820376v12.xx (services de sécurité), 820556v01.xx (SRED On-Guard SDE), 820549v01.xx (SRED On-Guard FPE)	App#2	<i>S/O</i>
4-30532	Ingenico	<i>Self/5000 LE</i>	SEL51AA1-xxxx	820573v01.xx (micrologiciel principal), 820376v12.xx (services de sécurité), 820556v01.xx (SRED On-Guard SDE), 820549v01.xx (SRED On-Guard FPE)	App#2	<i>S/O</i>

4-20359	Ingenico	Move/5000	MOV50BE (CTLS) MOV50BQ (CTLS) MOV50BR (CTLS) MOV50BS (CTLS) MOV50DC (CTLS + écran de confidentialité) MOV50DE (CTLS + écran de confidentialité) MOV50DN (CTLS + écran de confidentialité) MOV50DQ (CTLS + écran de confidentialité) MOV50DR (CTLS + écran de confidentialité) MOV50DS (CTLS + écran de confidentialité) MOV50JC (CTLS + couvercle de boîtier de bureau) MOV50JE (CTLS + couvercle de boîtier de bureau) MOV50JN (CTLS + écran de confidentialité + couvercle de boîtier de bureau) MOV50JQ (CTLS + couvercle de boîtier de bureau) MOV50JR (CTLS + couvercle de boîtier de bureau) MOV50JS (CTLS + couvercle de boîtier de bureau) MOV50BC (CTLS) MOV50BN (CTLS)	820547v11.xx, 820549v01.xx (SRED OnGuard FPE), 820556v01.xx (SRED OnGuard SDE), 820547v11.xx (micrologiciel principal), 820376v12.xx (services de sécurité)	App#1, App#2, App#3, App#5, App#6	S/O
---------	----------	---------------------------	---	---	---	-----

4-30494	Ingenico	Lane/7000	LAN70AC LAN70BB LAN70BC LAN70BD LAN70AB	820547v11.xx (micrologiciel principal), 820376v12.xx (services de sécurité), 820555v01.xx (SRED AWL), 820556V01.xx (SRED On-Guard SDE), 820549V01.xx (SRED On-Guard FPE), 820565V01.xx (SRED FF1), 820548V07.xx (protocoles ouverts), 820572V01.xx (module complémentaire Tetra JVM), 820376v14.xx (services de sécurité)	App#2	S/O
4-30493	Ingenico	Lane/8000	LAN80BA LAN80BB LAN80AA	820547v11.xx (micrologiciel principal), 820376v12.xx (services de sécurité), 820556V01.xx (SRED On-Guard SDE), 820549V01.xx (SRED On-Guard FPE), 820548V07.xx (protocoles ouverts), 820376v14.xx (services de sécurité)	App#2	S/O
4-20375	Ingenico	Lane/5000	LAN52BA1-xxxx	820571v01.xx (micrologiciel principal) 820376v12.xx (services de sécurité) 820549v01.xx (SRED OnGuard FPE) 820556v01.xx (SRED OnGuard SDE) 820376v14.xx (services de sécurité)	App#2, App#3, App#5	S/O

4-30533	Ingenico	<i>Link/2500 LE</i>	LIN25AB1-xxxx LIN25BA1-xxxx LIN25CA1-xxxx LIN25DA1-xxxx LIN25AA1-xxxx	820571v01.xx (micrologiciel principal) 820376v12.xx (services de sécurité) 820556v01.xx (SRED On-Guard SDE) 820549v01.xx (SRED On-Guard FPE) 820565v01.xx (SRED FF1) 820376v14.xx (services de sécurité)	<i>App#2</i>	<i>S/O</i>
4-30498	Ingenico	<i>AXIUM RX7000</i>	R70411xxxx	02.03.11.xxxxx (La solution SRED prise en charge par le micrologiciel comprend SRED EP2, SRED C-TAP, SRED ZVT-H, SRED OnGuard FPE, SRED OnGuard SDE, SRED FF1)	<i>App#4</i>	<i>SW#1</i>
4-30444	Ingenico	<i>AXIUM EX8000</i>	E801x2	01.09.11.xxxxx (avec AP Solution 1, SRED EP2, SRED C-TAP, SRED ZVT-H, SRED OnGuard SDE, SRED OnGuard FPE, SRED FF1)	<i>App#4</i>	<i>SW#1</i>
4-30443	Ingenico	<i>AXIUM DX8000-2, AXIUM DX8000-5</i>	D851x3 (with AP Solution 1)	01.09.11.xxxxx (avec AP Solution 1 SRED EP2 SRED C-TAP SRED ZVT-H SRED OnGuard SDE SRED OnGuard FPE SRED FF1)	<i>App#4</i>	<i>SW#1</i>
4-30527	Ingenico	<i>AXIUM RX5000</i>	R50411xxxx (sans protège-PIN)	02.03.11.xxxxx (La solution SRED prise en charge par le micrologiciel comprend : SRED EP2 SRED C-TAP SRED ZVT-H SRED OnGuard SDE SRED OnGuard FPE SRED FF1)	<i>App#4</i>	<i>SW#1</i>
4-90075	ID Tech	<i>SREDKey 2</i>	80172001 (avec MSR), 80172002 (sans MSR), 80172004 (avec MSR), 80172005 (sans MSR)	SREDKEY2 FW v1.00.xxx.xxxx.S, SREDKey2 FW v1.01.xxx.xxxx.S	<i>S/O</i>	<i>S/O</i>

4-90385	ID Tech	SREDKey2	80172002 (sans MSR) 80172004 (avec MSR) 80172005 (sans MSR) 80172007 (sans MSR) 80172001 (avec MSR) 80172006 (avec MSR)	SREDKEY2 FW v1.03.xxx.xxx.S SREDKEY2 FW v2.01.xxx.xxx.S	S/O	
4-30432	Infinite Peripherals, Inc	QuantumPay Reader 250	06.00.xx.xx	3.0.xx.xx	S/O	S/O
4-30433	Infinite Peripherals, Inc	QuantumPay Reader 300	05.11.xx.xx	3.1.xx.xx, 3.2.xx.xx	S/O	S/O
4-30437	Infinite Peripherals, Inc	QuantumPay PIN 400	00xxxD1xxxxxx (version sans CTLS) CLxxxD1xxxxxx (version CTLS)	3.1.xx.xx, 3.2.xx.xx	S/O	S/O
4-30438	Infinite Peripherals, Inc	QuantumPay Connected 150	PRR05xxx PRR15xxx PXR05xxx PXR15xxx	3.0.xx.xx, 3.1.xx.xx	S/O	S/O
4-30511	Infinite Peripherals, Inc	QuantumPay Connected 250 and 252	51DxxxxNxxxx version sans CTLS 51DxxxxCxxxx version CTLS	3.0.xx.xx	S/O	S/O
4-30453	Infinite Peripherals, Inc	QuantumPay PIN 401	41D1xxxN0xxx 41D1xxxC0xxx	3.0.xx.xx	S/O	S/O
4-30464	Infinite Peripheral, Inc	QuantumPay PIN 451	41D1xxxN1xxx - version sans CTLS 41D1xxxC1xxx - version CTLS	3.0.xx.xx	S/O	S/O

4-30318	Datecs Ltd.	<i>BluePad-5000 (QuantumPay PIN 600)</i>	02.05.2x.0xxxxa (BluePad-5000 v2) 02.05.2x.1xxxxa (BluePad-5000 v2) 02.05.2x.2xxxxa (BluePad-5000 v2) 02.05.3x.0xxxxa (BluePad-5000 v3) 02.05.3x.1xxxxa (BluePad-5000 v3) 02.05.3x.1xxxxx (BluePad-5000 v3) 02.05.3x.2xxxxa (BluePad-5000 v3) 02.05.3x.xxxxxa (BluePad-5000 v3) 02.05.4x.0xxxxa (BluePad-5000 v4) 02.05.4x.1xxxxa (BluePad-5000 v4) 02.05.4x.1xxxxx (BluePad-5000 v4) 02.05.4x.2xxxxa (BluePad-5000 v4) 02.05.4x.xxxxxa (BluePad-5000 v4) 02.05.5x.0xxxxa (BluePad-5000 v5) 02.05.5x.1xxxxa (BluePad-5000 v5) 02.05.5x.1xxxxx (BluePad-5000 v5) 02.05.5x.2xxxxa (BluePad-5000 v5) 02.05.5x.xxxxxa (BluePad-5000 v5) 02.05.2x.1xxxxx (BluePad-5000 v2) 02.05.2x.xxxxxa (BluePad-5000 v2)	3.2.xx.xx 3.1.xx.xx	S/O	S/O
---------	-------------	--	--	------------------------	-----	-----

4-30475	Infinite Peripherals, Inc	<i>QuantumPay Pro Plus</i>	21.1x.xx.xxx	SP: 3.0.xx.xx, AP: 1.0.xx.xx	S/O	S/O
4-80037	Castles Technology Co. Ltd	<i>Saturn 1000-E</i>	SATURN1000E-HW- V1.20.xxxx	1.1.1.xxxxxx	S/O	<i>SW#1-22</i>
4-80033	Castles Technology Co. Ltd	<i>Saturn 1000</i>	SATURN1000-HW- V1.03.xxxx SATURN1000-HW- V1.01.xxxx SATURN1000-HW- V1.04.xxxx	1.1.2.xxxxxx 1.1.1.xxxxxx	S/O	<i>SW#1-22</i>
4-30416	Castles Technology Co. Ltd	<i>Saturn 1000</i>	SATURN1000-HW- V2.00.xxxx	1.3.1.xxxxxx 1.4.1.xxxxxx	S/O	<i>SW#1-22</i>
4-80075	Castles Technology Co. Ltd	<i>S1E2, S1E2-L, S1E2N</i>	HW-V1.00, S1E2: HW- V1.00	S1E2 & S1E2-L:	S/O	<i>SW#1-22</i>
4-80094	Castles Technology Co. Ltd	<i>S1F4 PRO</i>	HW-V-1G.00	1.6.1.xxxxxx	S/O	<i>SW#1-22</i>
4-80082	Castles Technology Co. Ltd	<i>S1P</i>	HW-V1.00	1.4.1.xxxxxx	S/O	<i>SW#1-22</i>
4-80092	Castles Technology Co. Ltd	<i>S1P2</i>	HW-V-1D.00	1.6.1.xxxxxx	S/O	<i>SW#1-22</i>
4-80091	Castles Technology Co. Ltd	<i>S1Mini2</i>	HW-V-1E.00	1.6.1.xxxxxx	S/O	<i>SW#1-22</i>
4-80118	Castles Technology Co. Ltd	<i>S1E4 PRO</i>	HW-V-1P.00	1.6.1.xxxxxx 13.0002.xxxx.xxxx.xxxx_xx xx.xxxx.xxxx	S/O	<i>SW#1-22</i>
4-80106	Castles Technology Co. Ltd	<i>S1U2-M4</i>	HW-V-1I.00	1.6.1.xxxxxx	S/O	<i>SW#1-22</i>

4-80084	Castles Technology Co. Ltd	S2L	HW-V1A.00	1.4.1.xxxxxx	S/O	SW#1-22
4-80077	Castles Technology Co. Ltd	S1U2	HW-V1.00	1.4.1.xxxxxx 1.4.2.xxxxxx	S/O	SW#1-22
4-30470	Elo Touch Solutions, Inc	EMC0600, EMC0600C, EMC0600SC' EMC0600S	A01.0EC.x A01.0NC.x A01.S00.x A01.SEC.x A01.SNC.x A01.000.x	5.xxx.xxx.xxx+ap 5.xxx.xxx.xxx+p 6.xxx.xxx.xxx+ap 6.xxx.xxx.xxx+p	S/O	S/O
4-90136	Ziosk	Z600	6.0.A 6.0.B	6201.29.xxxx.xxx.xxx 6201.30.xx.x.xxx	S/O	S/O
4-90335	Ziosk	Z600 Pro	6.0.A	6201.29.xxxx.xxx.xxx	S/O	S/O
4-30522	Verifone	M425 M450	H625-0007-0090-1xx-xxx-B0 (avec écran de confidentialité), H650-0007-0090-0xx-xxx-B0 (sans écran de confidentialité), H650-0007-0090-1xx-xxx-B0 (avec écran de confidentialité), H625-0007-0090-0xx-xxx-B0 (sans écran de confidentialité),	VOS3: 02.xx.xx, SPBL_01.02.xx.xx, SPFW_01.04.xx.xx, APFW_01.02.xx.xx, Android: 3.01D.xx	S/O	S/O
4-80062	Verifone	P630	H565-0007-xxxx-xxx-xxx-A1	Vault: APFW_01.02.xx.xx, VOS3: 01.xx.xx, Android: 3.01D.xx, Vault: SPFW_01.04.xx.xx	S/O	S/O

4-110000	Verifone	<i>V660P</i>	H660-0007-00D0-0Nx-xxx-B1, H660-0007-00D0-0Nx-xxx-B0	Vault: SPFW_01.06.xx.xx, Vault: APFW_01.03.xx.xx, Vault: SPFW_01.05.xx.xx, Vault: SPBL_01.02.xx.xx, Vault: SPFW_01.02.xx.xx, Vault: APFW_01.02.xx.xx, Android: 3.00D.xx, Vault: SPFW-01.04.xx.xx, Android: 3.01D.xx	S/O	<i>S/O</i>
4-30558	Verifone	<i>V660p-A</i>	H660-007-xxxx-xxx-xxx-A0	SPFW_01.05.xx.xx, SPBL_01.02.xx.xx, APFW_01.02.xx.xx, Android (VAOS):4.00F.xx, SPFW_01.06.xx.xx, APFW_01.03.xx.xx	S/O	<i>S/O</i>
4-80065	Verifone	<i>UX700</i>	U605-0007-xxxx-xxx-xxx-A0	Vault: SPBL_01.02.xx.xx, Vault: APFW_01.02.xx.xx, Vault: SPFW_01.06.xx.xx, Vault: APFW_01.03.xx.xx, Vault: SPFW_01.05.xx.xx, Android: 3.01D.xx, Vault: SPFW_01.04.xx.xx, VOS3: 02.xx.xx	S/O	<i>S/O</i>
4-40363	PAX Computer Technology (Shenzhen) Co Ltd	<i>A6650</i>	A6650-0xx-0x6-0xxx (NON-CTLS), A6650-0xx-0x6-1xxx (NON-CTLS), A6650-0xx-Rx6-0xxx (CTLS), A6650-0xx-Rx6-1xxx (CTLS),	26.00.01 xxxxx	S/O	<i>S/O</i>
4-30554	Toast Inc	<i>TG300, TG310</i>	REV1.xx	01.xx.xx.-10xxxxx	S/O	<i>SW#1</i>

2.2 Détails des applications P2PE

Les informations suivantes répertorient les applications P2PE approuvées pour être utilisées sur les dispositifs PTS POI du tableau 2.1 dans cette solution P2PE.

Par définition, les applications P2PE ont accès aux données de compte en clair. Ces applications **doivent** être indiquées dans la liste de la solution P2PE.

Les « ID PIM » sont des numéros créés et utilisés par le fournisseur de la solution P2PE uniquement dans le cadre de ce PIM, afin de faciliter le renvoi vers les applications P2PE indiquées ici qui sont utilisées sur les dispositifs PTS POI indiqués dans le tableau 2.1. Ils ne sont pas attribués par le PCI SSC et ne sont pas reconnus par le programme PCI P2PE.

Remarque: Les applications P2PE qui ont été évaluées dans le cadre de la solution P2PE et pour lesquelles il a été choisi de ne pas les répertorier séparément sont signalées comme telles dans la liste de la solution P2PE et n'auront pas de numéro de référence de liste d'application PCI P2PE indépendant.

https://listings.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions

ID PIM (p. ex., App#1, App#2, ...)	Éditeur de l'application P2PE	Nom de l'application P2PE	Version(s) de l'application P2PE	Numéro de référence de la liste d'applications PCI P2PE (Attribué par le PCI SSC)
App#1	Ingenico	UPP	1.1.x	2023-00470.045
App#2	Ingenico	UPP	2.0.x	2023-00470.051
App#3	Ingenico	RA1	20.x	2024-00470.056
App#4	Ingenico	Axium Retail Core Axium Payment Service (ARC APS)	1.0.x	2024-00470.059
App#5	Ingenico	IngeProtect	2.1.x.x.x	2025-01079.009
App#6	FreedomPay	FreeWay Standalone Application (FSA)	3.0.x	2025-00909.015

2.3 Détails des logiciels non liés au paiement

Les informations suivantes répertorient les logiciels non liés au paiement approuvés pour être utilisés sur les dispositifs PTS POI du tableau 2.1 dans cette solution P2PE.

*Par définition, les logiciels non liés au paiement P2PE **ne doivent pas** avoir accès aux données de compte en clair. Bien que ce type de logiciel soit évalué dans le cadre de l'évaluation de la solution P2PE, il n'est pas indiqué dans la liste des solutions PCI P2PE.*

Les « ID PIM » sont des numéros créés et utilisés par le fournisseur de la solution P2PE uniquement dans le cadre de ce PIM, afin de faciliter le renvoi vers les logiciels non liés au paiement indiqués ici qui sont utilisés sur les dispositifs PTS POI indiqués dans le tableau 2.1. Ils ne sont pas attribués par le PCI SSC et ne sont pas reconnus par le programme PCI P2PE.

ID PIM (p. ex., SW#1, SW#2, ...)	Éditeur du logiciel non lié au paiement	Nom du logiciel non lié au paiement	Version(s) du logiciel non lié au paiement	Informations supplémentaires (au besoin)
SW#1	FreedomPay	CX App	1.x.x	Composant middleware Android pour l'intégration avec les applications de point de vente sur les appareils tout-en-un
SW#2	MyVenue	mvPOS	2.71, 3.38	
SW#3	Tapin2	Tapin2 Web View App	2x.xx.xxx	
SW#4	Agilysys	rGuestPay	2x.xx.xxx	
SW#5	Up'n'Go	UpNGoPay	1.x.x	
SW#6	Agilysys	IG FLY	12.3.x.x	
SW#7	RetailCloud	6IX POS	3.x.x	
SW#8	HotelKey	RK Register	5.02, 6.01	
SW#9	Verteda	SwiftPOS	4.x	
SW#10	Zonal	iServe	2.x.x.x	
SW#11	Kappture	Kappture epos	1.10.x.x	
SW#12	OTG	Skywire Pay	1.0.2	
SW#13	RetailCloud	Inventory360	2.3.3	
SW#14	Tevalis	TevX	20xx.xx.xx	

2.3 Détails des logiciels non liés au paiement

SW#15	OutPay	OutPay FOH	1.x.x	
SW#16	Shiji	Infrasys	1.x.x	
SW#17	Axess	RetailPOS	3.0.0	
SW#18	Campana AXIS	FPConnector	1.0.7	
SW#19	Haven	SandCastles Pay	1.0.0	
SW#20	SmartQ	Time2Eat MPOS	1.08	
SW#21	OTG	floServe	1.0.7, 2.3.0	
SW#22	OTG	SkyWire Companion	0.1.3	

2.4 Vérification des informations du dispositif PTS POI

La vérification des informations du dispositif PTS POI est essentielle. Ces informations sont nécessaires pour valider les informations de ce PIM, pour les recouper avec les listes PCI PTS ainsi que la liste des solutions PCI P2PE, en plus de la gestion des stocks, du dépannage et de la déclaration des incidents.

Instructions pour confirmer le matériel, le micrologiciel du dispositif PTS POI, ainsi que les applications P2PE et les logiciels non liés au paiement présents

Les versions matérielles se trouvent au dos de tous les appareils, sur l'autocollant du fabricant qui contient le numéro de série. Des exemples d'emplacement de cet autocollant figurent à l'annexe C.

Appareils Ingenico :

Pour trouver la version du micrologiciel, suivez les étapes ci-dessous :

1. Débranchez l'appareil du système de point de vente ou de tout autre système frontal
2. Alimentez l'appareil à l'aide du câble d'alimentation ou en le branchant à un PC au moyen du câble USB
3. Pendant le démarrage de l'appareil, appuyez sur la séquence de touches suivante sur l'appareil Ingenico : 2634, [bouton vert], F
4. Si votre appareil n'a pas de touche « F », la séquence de touches sera 2634, [bouton vert], +
5. Si vous utilisez un Move/5000, utilisez le code 0001
6. Sélectionnez le menu suivant : *Control Panel/Terminal Information/Firmware PCI PTS/Display*

7. Notez les informations de micrologiciel associées à M1

La version de l'application chargée sur les appareils Ingenico peut être consultée sur l'écran d'accueil lors du démarrage de l'appareil. La valeur « PCI Version » doit correspondre au modèle de numéro de version indiqué sur le site web du PCI SSC.

Appareils ID Tech :

Les versions de micrologiciel de ces appareils ne peuvent être consultées qu'à l'aide d'une application fournie par ID Tech. Pour télécharger cette application, veuillez contacter compliance@freedompay.com pour obtenir de l'aide.

Appareils Castles/Elo :

Ouvrez le menu CX Application depuis l'écran principal, puis cliquez sur « About ». En bas de cet écran, vous verrez la version du micrologiciel.

Appareils Ziosk :

La version du micrologiciel peut être consultée dans le menu de l'appareil en allant à Settings > About device > Firmware version.

Appareils Infinite Peripheral :

Les versions de micrologiciel de ces appareils ne peuvent être consultées qu'à l'aide d'une application fournie par Infinite Peripherals. Pour télécharger cette application, veuillez contacter compliance@freedompay.com pour obtenir de l'aide.

Appareils PAX

Depuis l'écran d'accueil, sélectionnez Settings > About et notez le micrologiciel affiché.

Appareils Toast

Depuis l'écran d'accueil, sélectionnez Settings > About et notez le micrologiciel affiché.

Appareils Verifone

Depuis l'écran d'accueil, sélectionnez Settings > About et notez le micrologiciel affiché.

2.5 Inventaire et surveillance des dispositifs PTS POI

- Tous les dispositifs PTS POI doivent être documentés au moyen de procédures de contrôle et de surveillance des stocks, y compris l'état du dispositif (p. ex., déployé, en attente de déploiement, en réparation ou autrement inutilisé, ou en transit).
- Cet inventaire doit être réalisé au moins une fois par an.
- Tout écart d'inventaire, y compris les dispositifs PTS POI manquants ou remplacés, doit être signalé au fournisseur de la solution P2PE au moyen des coordonnées et des instructions de la section 1 ci-dessus.
- Le tableau d'inventaire type ci-dessous est fourni à titre d'illustration uniquement. L'inventaire réel doit être établi et tenu à jour par le commerçant dans un document externe.

Instructions pour documenter et tenir à jour un inventaire des dispositifs PTS POI.

Le commerçant doit mettre en œuvre et maintenir un système de suivi des dispositifs POI qui identifie chaque dispositif POI selon son état actuel. Les états possibles comprennent, par exemple :

- Déployé
- En attente de déploiement
- Hors service et/ou en réparation
- En transit
- Retiré et retourné

FreedomPay propose un système de tenue de registres de base via son Enterprise Reporting Portal, appelé Device Management Portal, qui peut être configuré lors de la mise en œuvre. Les commerçants peuvent également, s'ils le préfèrent, mettre en place leur propre système. Les inventaires électroniques des dispositifs POI doivent être stockés de manière sécurisée, avec un accès limité au personnel autorisé uniquement.

Le commerçant doit également établir un « système d'état de comptabilité et de contrôle » afin de suivre tous les dispositifs POI (quantité et type), de noter les changements dans les inventaires de matériel (entrées/sorties) et de surveiller tous les aspects du cycle de vie du dispositif POI tant qu'il est en la possession et sous le contrôle du commerçant. Consignez tous les écarts d'inventaire dans votre système de contrôle des stocks et signalez les dispositifs manquants ou perdus à FreedomPay dès qu'ils sont identifiés à l'adresse compliance@freedompay.com, ou au partenaire/revendeur FreedomPay désigné qui a fourni les dispositifs.

Si votre organisation est un exploitant multi-magasins, régional ou national, il est important d'employer des systèmes de gestion et de suivi des stocks aux niveaux local, régional et national afin de garantir que les connaissances et les capacités de gestion, de suivi et de déclaration des inventaires soient assurées à tous les niveaux.

Il est recommandé que l'inventaire des dispositifs contienne, au minimum, des informations similaires à celles du tableau d'inventaire type ci-dessous. Toutes les informations d'identification propres à chaque dispositif nécessaires au suivi de l'inventaire se trouvent sur un autocollant situé sur le panneau arrière ou dans le compartiment de la batterie de chaque dispositif POI (des images de l'emplacement du numéro de série pour un échantillon de dispositifs figurent à l'**annexe C de la section 9, Conseils supplémentaires** et/ou via l'interface logique du dispositif POI).

Le commerçant doit élaborer et tenir à jour des protocoles écrits pour le déplacement des dispositifs entre les sites du commerçant. Le commerçant doit surveiller et documenter le respect de ces protocoles. Les protocoles de déplacement des dispositifs POI du commerçant doivent être au moins aussi sécurisés que les protocoles définis dans ce PIM pour l'expédition des dispositifs POI vers et depuis les sites de fournisseurs approuvés. Pour plus d'informations sur le maintien de la chaîne de traçabilité lors du déplacement ou du stockage des dispositifs, veuillez contacter compliance@freedompay.com ou le partenaire/revendeur FreedomPay qui a fourni les dispositifs.

Le commerçant peut être invité à soumettre son inventaire annuel des POI à son acquéreur dans le cadre de sa conformité annuelle à PCI DSS. Le non-respect des contrôles énumérés dans le PIM peut entraîner une « désactivation par le commerçant » (Merchant Opt-Out), c'est-à-dire la suspension du programme de réduction du périmètre P2PE de la FreedomPay Commerce Platform.

Si un commerçant ne souhaite plus utiliser les dispositifs POI fournis par FreedomPay dans le cadre d'un programme de réduction du périmètre PCI P2PE, en raison d'une désactivation par le commerçant, d'une résiliation de contrat, d'une cessation d'activité, d'un retrait de service ou pour toute autre raison, il est tenu de détruire de manière sécurisée tous les dispositifs POI fournis par FreedomPay. La destruction sécurisée doit être effectuée au moyen du service de destruction sécurisée de FreedomPay, en soumettant une demande à devicedisposal@freedompay.com en indiquant le nombre de dispositifs et les numéros de série de chacun. Une fois la demande reçue, l'équipe Professional Services de FreedomPay répondra avec de plus amples détails. Pour plus d'informations sur les services de destruction possibles, veuillez contacter votre représentant FreedomPay.

Tableau d'inventaire type

Fournisseur du dispositif PTS POI	Nom(s) et numéro(s) de modèle du dispositif PTS POI	Emplacement du dispositif	État du dispositif	Numéro de série ou autre identifiant unique	Date de l'inventaire	Remarques supplémentaires (au besoin)

3. Réception des dispositifs PTS POI

3.1 Instructions pour s'assurer que les dispositifs PTS POI proviennent de sources/sites/emplacements de confiance

FreedomPay ou son KIF certifié enverra par e-mail au commerçant une notification préalable à l'expédition indiquant les numéros de série des dispositifs POI, le nom du transporteur, le numéro de suivi, le site d'où le colis a été expédié et l'emplacement de commerçant approuvé auquel le colis a été expédié.

À la réception de toute expédition de dispositifs POI, le commerçant doit :

- i. Inspecter l'emballage comme indiqué ci-dessus.
- ii. Vérifier que le transporteur indiqué sur le bordereau de livraison est un transporteur de confiance (Trusted Courier).
- iii. Vérifier que le colis a été expédié depuis un site de fournisseur associé à un ou plusieurs fournisseurs de composants répertoriés dans la FreedomPay Commerce Platform P2PE, ou depuis un site faisant partie de la chaîne de traçabilité préétablie du commerçant. Si vous n'êtes pas certain de l'adresse ou de l'emplacement d'où un dispositif doit provenir, veuillez contacter compliance@freedompay.com.
- iv. Vérifier que les numéros de série figurant sur le bordereau d'expédition correspondent aux numéros de série de l'e-mail de notification préalable à l'expédition.
- v. Mettre à jour le système de tenue de registres des dispositifs pour refléter le changement d'état et d'emplacement du dispositif.

Le commerçant doit immédiatement retourner à FreedomPay, comme indiqué ci-dessous, tout colis de dispositifs POI qui semble avoir été altéré, qui a été livré par toute personne autre qu'un transporteur de confiance ou qui a été expédié depuis un emplacement autre qu'un site attendu.

Avant de retourner un dispositif POI à un site de fournisseur approuvé, le commerçant doit envoyer un e-mail à poidevicereturns@freedompay.com afin de déterminer où le dispositif doit être expédié selon la situation.

3.2 Instructions pour confirmer que le dispositif PTS POI et son emballage n'ont pas été altérés

À la réception d'un dispositif POI FreedomPay, les commerçants doivent, au minimum :

- Vérifier le transporteur indiqué sur le bordereau de livraison
- Vérifier que le colis a été expédié depuis un site attendu.
- Vérifier que les numéros de série figurant sur le bordereau d'expédition correspondent aux numéros de série de l'e-mail de notification préalable à l'expédition.
- Vérifier que l'emballage n'est pas endommagé au point d'exposer l'intérieur du colis.
- Vérifier que l'emballage n'a pas été mouillé au point que l'humidité ait pénétré les parois de l'emballage.
- Vérifier que l'intégrité de l'emballage inviolable (tamper evident) est intacte.

Exemple de colis non altéré avec ruban inviolable :



Si le dispositif ou l'emballage ne réussit pas l'une des inspections ci-dessus, contactez votre représentant FreedomPay et retournez le dispositif comme décrit à la section 5.2.

3.3 Instructions pour confirmer la nécessité professionnelle et l'identité de tout personnel tiers se présentant comme du personnel de livraison, d'assistance et/ou de réparation, avant de lui accorder l'accès aux dispositifs PTS POI.

Dans la plupart des cas, FreedomPay pourra fournir une assistance à distance pour les dispositifs sans nécessiter d'intervention sur site. Toutefois, lors d'installations complexes ou de certains cas d'assistance, un technicien peut être envoyé sur un site du commerçant. Si un technicien FreedomPay est nécessaire sur site, veillez à ce que les étapes suivantes soient suivies avant, pendant et après l'intervention sur site.

- i. Un technicien de terrain sera affecté à un dossier et remplira une demande d'intervention.
- ii. Une fois qu'un technicien a été affecté, FreedomPay fournira au commerçant les détails de la demande.
- iii. Lorsque le technicien arrive sur site, et avant de lui permettre d'accéder au dispositif POI, le commerçant doit vérifier l'identité du technicien en tant qu'employé ou sous-traitant de FreedomPay. Toute autre personne doit se voir refuser l'accès sans validation appropriée de son identité.
- iv. Une fois l'identité du technicien vérifiée, le commerçant doit désigner un accompagnateur pour surveiller en permanence l'activité du technicien.
- v. Une fois l'intervention terminée, le commerçant doit répondre à l'e-mail d'intervention en indiquant les informations suivantes :
 - i. Type de pièce d'identité présentée pour la vérification

- ii. Temps passé sur site
- iii. (Pour les cas d'assistance uniquement) Numéro(s) de série du ou des terminaux touchés par le technicien

FreedomPay n'enverra jamais de techniciens sur site sans se coordonner au préalable avec les contacts du commerçant et sans fournir des informations sur le technicien envoyé à des fins de vérification. Toute personne se présentant comme technicien de réparation/d'assistance sans notification ou identification appropriée ne doit pas se voir accorder l'accès aux dispositifs POI.

Sécuriser physiquement les dispositifs POI en votre possession, y compris les dispositifs :

- En attente de déploiement
- En réparation ou autrement inutilisés
- En attente de transport entre sites/emplacements

4. Déploiement et installation des dispositifs PTS POI

Ne connectez pas et n'utilisez pas d'autres dispositifs de capture de données de compte de paiement non approuvés.

La solution P2PE est approuvée pour utiliser des dispositifs PTS POI spécifiques, comme détaillé ci-dessus dans le tableau 2.1, qui doivent être indiqués dans la liste de la solution P2PE.

Si des dispositifs ne figurant pas dans le tableau 2.1 sont utilisés pour accepter des données de compte de paiement, l'éligibilité du commerçant à utiliser le SAQ P2PE pourrait en être affectée – contactez votre acquéreur ou les marques de paiement.

Ne modifiez pas et ne tentez pas de modifier les configurations ou paramètres sécurisés des dispositifs PTS POI.

La modification des configurations ou paramètres sécurisés des dispositifs PTS POI peut invalider la mise en œuvre de la solution P2PE et l'éligibilité du commerçant à utiliser le SAQ P2PE pourrait en être affectée – contactez votre acquéreur ou les marques de paiement.

Les exemples comprennent, sans s'y limiter, les tentatives d'effectuer les actions suivantes sur les dispositifs PTS POI :

- Activer toute interface du dispositif ou tout mécanisme de capture de données désactivé
- Modifier les configurations de sécurité ou les contrôles d'authentification
- Ouvrir physiquement le dispositif
- Tenter d'installer des applications/logiciels non autorisés

4.1 Instructions d'installation et de connexion des dispositifs PTS POI

Il est recommandé de sécuriser chaque installation de dispositif POI à l'aide de l'une des méthodes suivantes ou d'une autre méthode approuvée par votre Qualified Security Assessor (QSA) :

- i. Le dispositif est monté physiquement ou attaché afin d'empêcher tout retrait, altération ou remplacement non autorisé. Les méthodes acceptables comprennent :
 - a. Fixer le dispositif sur un support de sécurité PIN approuvé
 - b. Fixer le dispositif à l'aide d'un câble antivol relié à l'emplacement de sécurité du dispositif POI et fixé de manière permanente au comptoir ou à un autre matériel sécurisé fixé physiquement à l'extrémité opposée du câble. Une grande variété de câbles antivol sont disponibles chez la plupart des revendeurs informatiques, en ligne ou auprès de FreedomPay. Veuillez contacter votre représentant FreedomPay si vous avez besoin d'aide pour trouver un câble antivol adapté.
- ii. Le dispositif doit être placé de manière à pouvoir être facilement observé/surveillé par le personnel autorisé et dans un environnement dissuadant les tentatives de compromission.

Les étapes de mise en œuvre supplémentaires comprennent :

- i. Lors de l'initialisation du dispositif, le commerçant doit effectuer les étapes suivantes :
 - a. Vérifier que le numéro de série affiché correspond au numéro de série situé sous le dispositif.
 - i. Pour obtenir de l'aide afin de localiser les numéros de série sur les dispositifs POI, veuillez consulter l' **annexe C de la section 9, Conseils supplémentaires** du présent document.
 - b. Mettre à jour le système de tenue de registres des dispositifs pour refléter le changement d'état et d'emplacement du dispositif.
- ii. Le dispositif doit utiliser l'un des types de communication/connexion suivants :
 - a. USB
 - b. Série
 - c. Ethernet
 - d. WiFi
 - e. Bluetooth
 - f. Cellulaire

Autre : pour les types de communication POI non répertoriés ci-dessus, le commerçant doit contacter compliance@freedompay.com afin d'obtenir l'approbation officielle de conformité de l'équipe de conformité de FreedomPay pour l'utilisation d'un tel dispositif. Le commerçant doit recevoir, par écrit, une attestation officielle de FreedomPay indiquant que le type de communication POI, non répertorié dans la liste ci-dessus, est une méthode de communication/connexion acceptée pour la solution FreedomPay Commerce Platform P2PE.

4.2 Conseils pour choisir les emplacements appropriés pour le déploiement des dispositifs PTS POI

FreedomPay recommande, et PCI DSS renforce cette recommandation, que tous les dispositifs déployés soient solidement fixés et facilement visibles par le personnel afin d'empêcher tout retrait ou altération non autorisé. Le dispositif doit être placé de manière à pouvoir être facilement observé/surveillé par le personnel autorisé et dans un environnement dissuadant les tentatives de compromission. Si une mise en œuvre est destinée à une utilisation sans surveillance, des procédures doivent être en place pour atténuer les risques associés. Cela peut inclure des caméras de sécurité, des inspections plus fréquentes, des contrôles de prévention des altérations ou d'autres méthodes approuvées par votre QSA.

Les dispositifs hors service doivent être stockés conformément à la méthodologie décrite à la section 3.3.

4.3 Conseils pour sécuriser physiquement les dispositifs PTS POI déployés afin d'empêcher tout retrait et/ou remplacement non autorisé

Les commerçants sont encouragés à fixer les dispositifs en service sur un support de sécurité PIN approuvé ou à sécuriser le dispositif à l'aide d'un câble antivol relié à l'emplacement de sécurité du dispositif POI et fixé de manière permanente à l'extrémité opposée du câble. Une grande variété de câbles antivol sont disponibles chez la plupart des revendeurs informatiques ou en ligne. Veuillez contacter votre

représentant FreedomPay ou votre QSA si vous avez besoin d'aide pour trouver un câble antivol adapté. Pour les mises en œuvre qui ne se prêtent pas à des dispositifs fixés (p. ex., dispositifs autonomes ou scénarios mobiles), des procédures doivent être mises en place pour atténuer le risque d'altération ou de compromission du dispositif. Cela peut inclure l'attribution du dispositif au personnel du site, des inspections plus fréquentes ou d'autres procédures approuvées par le QSA.

Le commerçant doit établir une zone de « stockage sécurisé » pour les dispositifs POI hors service. Ce stockage sera utilisé lorsque des dispositifs POI sont reçus de FreedomPay avant leur installation, transférés depuis d'autres emplacements de commerçant approuvés ou retirés de l'utilisation active. Le stockage sécurisé est défini par PCI comme un espace ou un emplacement désigné dont l'accès physique est contrôlé, pour lequel le personnel doit être autorisé à y accéder et où des mécanismes/politiques sont en place pour documenter tous les accès physiques à la zone de « stockage sécurisé », notamment :

- Identifier le personnel autorisé à accéder aux dispositifs
- Restreindre l'accès au personnel autorisé
- Tenir un journal de tous les accès comprenant le nom de la personne, l'entreprise, le motif de l'accès, l'heure d'entrée et de sortie

Le commerçant doit mettre en œuvre une politique d'accès au « stockage sécurisé » avant de mettre en œuvre la solution P2PE validée PCI de FreedomPay. Cette politique doit inclure une description de ce qu'est la zone de stockage sécurisé et de son emplacement, ainsi que les procédures établies pour se conformer aux exigences énoncées dans cette section.

5. Surveillance et inspection continues des dispositifs PTS POI déployés

5.1 Instructions pour inspecter les dispositifs PTS POI afin de détecter des signes d'altération et pour réagir aux incidents d'altération présumés

Les commerçants doivent inspecter les éléments suivants, au minimum, dans un délai approprié en fonction de leur profil de risque (généralement trimestriel) :

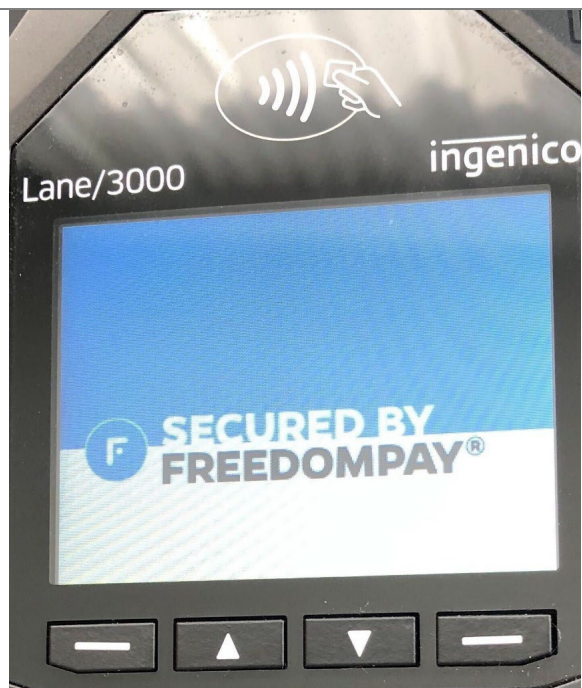
- Le câble USB/Ethernet a-t-il été endommagé ou modifié de quelque manière que ce soit ?
- Le numéro de série du dispositif correspond-il au numéro de série fourni par FreedomPay ? (Consultez l'annexe C pour l'emplacement du numéro de série)
- Les dispositifs POI actifs sont-ils sécurisés de manière appropriée conformément au PIM ?
- Les dispositifs POI inactifs sont-ils stockés de manière sécurisée conformément au PIM ?
- Le dispositif POI a-t-il été endommagé de quelque manière que ce soit ?
- L'écran « Secured by FreedomPay » est-il présent ?
- Les mesures supplémentaires de détection d'altération ajoutées par le commerçant et notées dans l'inventaire, telles que des scellés de sécurité, des étiquettes ou des marquages cachés, sont-elles intactes ?

Exemples de zones d'inspection :

Vérifier que les vis extérieures n'ont pas été retirées.



Vérifier que l'écran « Secured by FreedomPay » est présent.



Si un commerçant déploie un dispositif POI FreedomPay dans une zone non surveillée physiquement par un employé approuvé du commerçant, des procédures appropriées doivent être en place pour réduire la possibilité d'altération du dispositif et, dans les pires scénarios, le délai entre la compromission et la détection. Veuillez consulter votre Qualified Security Assessor (QSA) indépendant pour plus d'informations sur l'inspection et la surveillance des POI.

Toute altération d'un dispositif doit être signalée à FreedomPay, et tout dispositif qui a été altéré ou dont l'altération est suspectée doit être retiré immédiatement de l'environnement de point de vente et retourné à FreedomPay conformément aux instructions décrites à la section 5.2.

Le commerçant doit immédiatement retourner à FreedomPay, comme indiqué ci-dessous, tout dispositif POI, ou colis contenant un dispositif POI, qui semble avoir été altéré, qui a été livré par toute personne autre qu'un transporteur de confiance ou qui a été expédié depuis un emplacement autre qu'un site de fournisseur approuvé.

Expédition des dispositifs POI :

- i. Les dispositifs POI ne peuvent être transportés que par un transporteur de confiance vers un site de fournisseur approuvé indiqué à la section 4.2.
- ii. Les numéros de série des dispositifs retournés, ainsi que le motif du retour, doivent être communiqués à RMA@freedompay.com qui générera une étiquette d'expédition pour le retour.

iii. Tous les numéros de série des dispositifs POI doivent être imprimés sur le bordereau d'emballage ou sur l'étiquette d'expédition.

Le commerçant doit mettre à jour son système de tenue de registres des dispositifs pour refléter le changement d'état et d'emplacement du dispositif.

5.2 Instructions pour inspecter les dispositifs PTS POI afin de détecter des dispositifs de skimming et pour réagir à une détection présumée de skimming

Des conseils supplémentaires pour l'inspection des dispositifs PTS POI figurent dans le document intitulé *Skimming Prevention: Best Practices for Merchants*, disponible à l'adresse https://www.pcisecuritystandards.org/document_library/

Vérifier les points d'interaction pour détecter des surcouches ou des outils insérés.



Vérifier le point de connexion pour détecter des fils/connexions ou du matériel supplémentaires.



5.3 Instructions pour détecter les défaillances de chiffrement des données de compte du dispositif PTS POI et y réagir

En cas de défaillance du chiffrement indiquée par la présence d'un code d'erreur 266 ou d'un message « P2PE Encryption Error », il est recommandé que le commerçant :

- i. Examine tous les journaux du système de point de vente (POS) et les fonctions de traitement par lots pour l'autorisation de crédit, ainsi que tout signe de données de titulaire de carte en clair.
- ii. Examine tous les rapports de règlement du POS afin de s'assurer qu'aucune donnée de titulaire de carte non chiffrée n'est présente.

Si des données de titulaire de carte en clair sont détectées, ou en cas de défaillance d'un contrôle de sécurité du dispositif ou d'utilisation non autorisée avérée ou présumée de fonctions administratives sensibles, le commerçant doit contacter immédiatement l'assistance technique de FreedomPay et suivre les instructions de dépannage figurant à la section 7 du présent document. Tant que la fonctionnalité de chiffrement

appropriée n'a pas été rétablie sur le dispositif et que celui-ci n'a pas été réautorisé par FreedomPay, le dispositif défectueux ne peut pas être utilisé pour traiter des transactions, sauf si le commerçant demande formellement une suspension du chiffrement P2PE comme décrit à la section 6.2.

5.4 Instructions de dépannage d'un dispositif PTS POI

Si un dispositif POI est endommagé, détruit, semble mal fonctionner ou nécessite une intervention, le commerçant doit suivre le processus suivant lors de ses échanges avec le personnel de FreedomPay :

- i. Contactez l'assistance technique de FreedomPay au 888-495-2446 ou par e-mail à techsupport@freedompay.com.
- ii. Si le technicien d'assistance FreedomPay détermine qu'un technicien de terrain doit être envoyé, ce dernier remplira une demande d'intervention.
- iii. Une fois qu'un technicien a été affecté, FreedomPay fournira au commerçant les détails de la demande de déploiement.
- iv. Lorsque le technicien arrive sur site, et avant de lui permettre d'accéder au dispositif POI, le commerçant doit vérifier l'identité du technicien en tant qu'employé ou sous-traitant de FreedomPay. Toute autre personne doit se voir refuser l'accès sans validation appropriée de son identité.
- v. Une fois l'identité du technicien vérifiée, le commerçant doit désigner un accompagnateur pour surveiller en permanence l'activité du technicien.
- vi. Une fois l'intervention terminée, le commerçant doit répondre à l'e-mail d'intervention en indiquant les informations suivantes :
 - i. Type de pièce d'identité présentée pour la vérification
 - ii. Temps passé sur site
 - iii. Numéro(s) de série du ou des terminaux touchés par le technicien

Si un commerçant ne souhaite plus utiliser les dispositifs POI fournis par FreedomPay dans le cadre d'un programme de réduction du périmètre PCI P2PE, en raison d'une désactivation par le commerçant, d'une résiliation de contrat, d'une cessation d'activité, d'un retrait de service ou pour toute autre raison, il est tenu de détruire de manière sécurisée tous les dispositifs POI fournis par FreedomPay. La destruction sécurisée doit être effectuée au moyen du service de destruction sécurisée de FreedomPay, en soumettant une demande à devicedisposal@freedompay.com en indiquant le nombre de dispositifs et les numéros de série de chacun. Une fois la demande reçue, l'équipe Professional Services de FreedomPay répondra avec de plus amples détails. Pour plus d'informations sur les services de destruction possibles, veuillez contacter votre représentant FreedomPay.

6. Transport / expédition des dispositifs PTS POI

6.1 Instructions pour s'assurer que les dispositifs PTS POI ne sont expédiés qu'à des sites/emplacements de confiance, selon les besoins (p. ex., pour réparation)

Tous les dispositifs expédiés au commerçant par FreedomPay utiliseront un transporteur de confiance. Certains transporteurs utilisés par FreedomPay sont énumérés ci-dessous et peuvent également être utilisés par les commerçants pour les expéditions d'un site à l'autre :

- FedEx
- UPS
- USPS (dans certains scénarios)
- R&L Carriers
- DHL
- Ceva Logistics
- New World Transportation
- Purolator
- DPD
- Startrack
- APC

Ces transporteurs seront utilisés pour livrer les dispositifs aux adresses professionnelles fournies par le personnel du commerçant lors de l'intégration. Dans le cas d'une expédition entre des sites du commerçant, les dispositifs ne doivent être livrés qu'à des adresses professionnelles de confiance. Tous les dispositifs expédiés par et vers le commerçant (y compris les expéditions d'un site du commerçant à un autre) doivent être emballés dans un emballage résistant à l'effraction.

Les emballages inviolables comprennent par exemple les enveloppes ou sacs dotés d'étiquettes numérotées qui montrent de manière irréversible toute tentative d'ouverture du colis. Les emballages inviolables peuvent être achetés auprès de fournisseurs de fournitures de bureau et seront étiquetés spécifiquement « Tamper-Proof » ou « Tamper-Resistant » (inviolable ou résistant à l'effraction). Les colis peuvent également être sécurisés avec un ruban de sécurité inviolable autour de toutes les ouvertures.

6.2 Instructions pour sécuriser les dispositifs PTS POI destinés à être transportés vers d'autres sites (p. ex., vers un atelier de réparation) et pendant leur transport

Afin d'assurer la sécurité de la livraison des dispositifs, il est recommandé d'utiliser un transporteur de confiance permettant le suivi des colis et la confirmation de livraison. Des exemples de tels transporteurs sont énumérés ci-dessous, mais d'autres méthodes sécurisées sont autorisées :

- FedEx
- UPS
- USPS (dans certains scénarios)
- R&L Carriers
- DHL
- Ceva Logistics
- New World Transportation
- Purolator
- DPD
- Startrack
- APC

Tous les dispositifs expédiés par et vers le commerçant (y compris les expéditions d'un site du commerçant à un autre) doivent être emballés dans un emballage résistant à l'effraction.

Les emballages inviolables comprennent par exemple les enveloppes ou sacs dotés d'étiquettes numérotées qui montrent de manière irréversible toute tentative d'ouverture du colis. Les emballages inviolables peuvent être achetés auprès de fournisseurs de fournitures de bureau et seront étiquetés spécifiquement « Tamper-Proof » ou « Tamper-Resistant » (inviolable ou résistant à l'effraction). Les colis peuvent également être sécurisés avec un ruban de sécurité inviolable autour de toutes les ouvertures.

7. Conseils / instructions supplémentaires

7.1 Conseils supplémentaires pour les commerçants concernant la solution P2PE (au besoin).

Le présent manuel d'instructions P2PE est fourni conformément aux exigences de PCI DSS. La mise en œuvre des contrôles énoncés dans ce PIM est une exigence du SAQ-P2PE de PCI DSS et de l'attestation de conformité. L'utilisation de tout dispositif POI non approuvé par FreedomPay et/ou tout manquement aux exigences énoncées dans ce manuel se fait aux seuls risques du commerçant et peut entraîner une non-conformité au SAQ-P2PE de PCI DSS, la perte de l'admissibilité à la réduction du périmètre PCI DSS et/ou la compromission de la sécurité des données.

En utilisant la solution de réduction du périmètre P2PE de FreedomPay, le commerçant convient qu'il ne modifiera pas et ne tentera pas de modifier les configurations des dispositifs POI fournis par FreedomPay, y compris, sans s'y limiter :

- Tenter d'activer des interfaces de dispositif ou des mécanismes de capture de données qui ont été désactivés sur un dispositif fourni par Freedom Pay
- Tenter de modifier les configurations de sécurité ou les contrôles d'authentification
- Ouvrir physiquement un dispositif
- Tenter d'installer des applications sur un dispositif

Afin de conserver la réduction du périmètre offerte par la solution FreedomPay, le commerçant reconnaît que toutes les transactions par carte de crédit doivent être saisies/glissées via un dispositif POI approuvé pour rester dans le programme de réduction du périmètre P2PE. Les transactions saisies par tout autre moyen ne relèvent pas du programme P2PE validé de FreedomPay approuvé par le PCI SSC. FreedomPay a mis en œuvre sur sa passerelle de paiement (Freeway) un mécanisme visant à rejeter, avec une réponse « P2PE Device Error », également appelée erreur 266, les transactions envoyées non chiffrées depuis un dispositif non approuvé par FreedomPay. Ces transactions non chiffrées ne sont pas stockées dans l'environnement de FreedomPay, mais peuvent être stockées dans les journaux générés par le point de vente du commerçant, ce qui expose le commerçant au risque de perdre la réduction du périmètre PCI. Si un commerçant accepte un paiement par toute autre méthode en dehors de la solution PCI P2PE de FreedomPay ou s'il n'est pas en mesure de résoudre les occurrences régulières d'erreurs 266 dans les 30 jours suivant leur survenue, il doit se retirer du programme de réduction du périmètre PCI P2PE au moyen du formulaire de demande de désactivation par le commerçant (annexe A).

Restrictions par pays/région

Si un pays ou une région impose des restrictions sur la marque et le modèle de dispositif pouvant être utilisés sur son territoire, le tableau ci-dessous sera mis à jour :

Pays/région	Marque du dispositif	Modèle du dispositif
-------------	----------------------	----------------------

Australie	Ingenico	Lane 5000, Move 5000
Australie	IDTech	SREDKey v2

Annexe A : Demande de désactivation par le commerçant

Cette demande de désactivation doit être signée par un représentant autorisé du commerçant figurant dans les dossiers de FreedomPay. Avant de soumettre une demande de désactivation par le commerçant, veuillez contacter l'assistance technique de FreedomPay pour obtenir les instructions de désactivation. L'assistance technique vérifiera le représentant autorisé du commerçant et fournira un numéro d'incident.

Numéro d'incident (le cas échéant) : _____

Date de la demande de désactivation : _____

Le commerçant soussigné choisit par la présente de se retirer de la solution P2PE de FreedomPay. En signant cette demande, le commerçant reconnaît que :

1. Les transactions traitées pendant qu'une désactivation est en vigueur ne relèvent pas de la réduction du périmètre P2PE.
2. Le commerçant est seul responsable de la mise en œuvre de contrôles alternatifs pour protéger les données de compte en lieu et place de la solution P2PE de FreedomPay.
3. Le commerçant est tenu d'informer son acquéreur ou sa marque de paiement qu'il s'est retiré de la solution P2PE de FreedomPay.
4. FREEDOMPAY REJETTE TOUTE DÉCLARATION ET GARANTIE CONCERNANT LA SOLUTION P2PE DE FREEDOMPAY POUR CHAQUE TRANSACTION TRAITÉE PENDANT QU'UNE DÉSACTIVATION EST EN VIGUEUR.
5. FREEDOMPAY DÉCLINE TOUTE RESPONSABILITÉ, Y COMPRIS, SANS S'Y LIMITER, EN CAS DE VIOLATION DE DONNÉES RÉSULTANT DU TRAITEMENT DE PAIEMENTS PAR LE COMMERÇANT AUTREMENT QUE PAR L'UTILISATION DE LA SOLUTION P2PE VALIDÉE DE FREEDOMPAY ET DE LA FREEDOMPAY COMMERCE PLATFORM.
6. Le commerçant dispose de 60 jours à compter de la désactivation (« fenêtre de désactivation ») pour résoudre les conditions ayant motivé la désactivation et se réinscrire à la solution, sauf si une fenêtre de désactivation différente est convenue d'un commun accord par écrit entre FreedomPay et le commerçant. Après la fenêtre de désactivation, le commerçant peut se voir interdire de traiter des transactions sur la FreedomPay Commerce Platform pour une durée indéterminée.

Remarque : Après une désactivation, un commerçant peut choisir de se réinscrire à la solution de réduction du périmètre P2PE de FreedomPay, sous réserve du protocole de sécurité établi par FreedomPay, y compris une attestation du commerçant selon laquelle tous les résidus de données de titulaire de carte en clair ont été supprimés des systèmes du commerçant à l'aide de processus de suppression sécurisée des données.

Commerçant : _____

Signature: _____

(Nom du personnel autorisé du commerçant – en caractères d'imprimerie)

Nom : _____

Titre: _____

(Nom du personnel autorisé du commerçant – Signature)

Veuillez envoyer ce formulaire par e-mail à : compliance@freedompay.com

Annexe C : Exemples d'identification du numéro de série des dispositifs POI

Les images ci-dessous présentent quelques exemples de dispositifs POI de divers fabricants et l'emplacement physique des numéros de série apposés par les Key Injection Facilities à des fins d'inspection, de vérification ou de RMA du POI (qui peut fournir une aide supplémentaire pour localiser ou associer les numéros de série). Pour toute question supplémentaire concernant les numéros de série des dispositifs POI, veuillez contacter compliance@freedompay.com.

Ingenico Lane 3000



Quantum Pay Reader 250



Ziosk

