



P2PE-Bedienungsanleitung (PIM)
Ein Leitfaden für Händler zur Bereitstellung
und Wartung der FreedomPay® P2PE-
Lösung zur Reduzierung des
Geltungsbereichs

Version 3.4

1. P2PE-Lösung Informationen und P2PE Kontaktinformationen des Lösungsanbieters

1.1 Informationen zur P2PE-Lösung (gemäß dem Eintrag auf der PCI-SSC-Website)	
Name der P2PE-Lösung:	FreedomPay Commerce Platform P2PE
Listing-Referenznummer der P2PE-Lösung (Vergeben vom PCI SSC)	2025-00909.016
https://listings.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions	

1.2 Kontaktinformationen des P2PE-Lösungsanbieters					
Firmenname:	FreedomPay, Inc.	Firmen-URL:	http://corporate.freedompay.com		
Ansprechpartner:	Bernard Clary	Position:	VP of Compliance		
Telefon:	+1-610-902-9000	E-Mail:	compliance@freedompay.com		
Geschäftsadresse:	FMC Tower at Cira Centre South 2929 Walnut Street · Floor 14	Stadt:	Philadelphia		
Bundesstaat/Provinz:	Pennsylvania	Land:	USA	Postleitzahl:	19104

1.3 Kommunikationsanweisungen
Anweisungen, wie der P2PE-Lösungsanbieter kontaktiert werden kann, unter Berücksichtigung des Aufbaus eines vertrauenswürdigen Kommunikationskanals bzw. einer vertrauenswürdigen Sitzung.
Händler können sich an ihren zuständigen Customer Success Manager (CSM) wenden, oder an accounts@freedompay.com falls sie keinen zuständigen CSM haben, bei allgemeinen Fragen zu ihrem Konto oder zur Implementierung.
Fragen zum technischen Support können an techsupport@freedompay.com oder über das Support-Formular auf unserer Webseite gerichtet werden.
Fragen zur Compliance können an compliance@freedompay.com.

PCI P2PE und PCI DSS

Händler, die diese P2PE-Lösung verwenden, müssen gegebenenfalls die PCI-DSS-Konformität validieren. Händler sollten sich an ihren Acquirer oder die Zahlungsmarken wenden, um ihre PCI-DSS-Validierungsanforderungen zu ermitteln.

Siehe [FAQ 1158](#) auf der PCI-SSC-Website.

2. Informationen zu PTS-POI-Geräten und Software

2.1 Details zu PTS-POI-Geräten

Die folgenden Informationen listen die Details der PTS-POI-Geräte auf, die für die Verwendung in dieser P2PE-Lösung zugelassen sind.

Alle Informationen zu PTS-POI-Geräten können überprüft werden, indem Sie Folgendes auf der PCI-SSC-Website aufrufen und Tabelle 2.4 unten heranziehen:

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

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

Verwenden Sie für P2PE-Anwendungen und Nicht-Zahlungssoftware die PIM-ID-Nummern, um auf die jeweiligen Tabellen unten zu verweisen. Die „PIM-ID-Nummern“ sind Nummern, die vom P2PE-Lösungsanbieter ausschließlich für die Verwendung innerhalb dieses PIM erstellt und verwendet werden, um den Querverweis auf die P2PE-Anwendungen und Nicht-Zahlungssoftware zu erleichtern, die auf den hier aufgeführten PTS-POI-Geräten eingesetzt werden. Die „PIM-ID-Nummern“ werden nicht vom PCI SSC vergeben und vom PCI-P2PE-Programm auch nicht anerkannt.

PCI-PTS-Zulassungsnr.	PTS POI Gerätehersteller	Modellname und -nummer(n) des PTS-POI-Geräts	Hardware des PTS-POI-Geräts Versionsnr.	Firmware des PTS-POI-Geräts Versionsnr.	P2PE-Anwendungen auf PTS-POI-Geräten (PIM-ID-Nr. aus Tabelle 2.2)	Nicht-Zahlungssoftware auf PTS-POI-Geräten (PIM-ID-Nr. aus Tabelle 2.3)
4-20324	Ingenico	Lane/5000	LAN51BA (einzelner MSR-Kopf), LAN51CA (doppelter MSR-Kopf), LAN51DA (einzelner MSR-Kopf und Kamera), LAN51EA (doppelter MSR-Kopf und Kamera)	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	NA
4-30257	Ingenico	Lane/8000	LAN80AA, LAN80BA	820547v01.xx	App#1, App#2	NA

4-30326	Ingenico	Link/2500	LIN25AA (Basisversion ohne CTLS-Unterstützung), LIN25BA (Basisversion mit CTLS), LIN25CA (Companion-Version ohne CTLS-Unterstützung), LIN25DA (Companion-Version mit CTLS), LIN25EA (Touch-Version ohne CTLS-Unterstützung), LIN25FA (Touch-Version mit CTLS), LIN25GA (Version mit Doppelkopf ohne CTLS-Unterstützung), LIN25HA (Version mit Doppelkopf mit CTLS), LIN25IA (Companion-Version mit rückseitigem Anschluss und ohne CTLS-Unterstützung), LIN25JA (Companion-Version mit rückseitigem Anschluss und mit CTLS)	820547v01.xx	App#1, App#3	NA
4-30237	Ingenico	Lane/7000	LAN70AA, LAN70AB, LAN70BB	820547v01.xx, 820376v04.xx (Security Services)	App#1, App#2	NA

4-20316	Ingenico	Move/5000	MOV50AC (ohne CTLS) MOV50AQ (ohne CTLS) MOV50AS (ohne CTLS) MOV50BB (CTLS) MOV50BC (CTLS) MOV50BQ (CTLS) MOV50BR (CTLS); MOV50DR (CTLS + Sichtschutz); MOV50JR (CTLS + Sichtschutz + Tischgehäusedeckel); MOV50BE (CTLS); MOV50DE (CTLS + Sichtschutz); MOV50JE (CTLS + Sichtschutz + Tischgehäusedeckel) MOV50BS (CTLS) MOV50CB (ohne CTLS + Sichtschutz) MOV50CC (ohne CTLS + Sichtschutz) MOV50CQ (ohne CTLS + Sichtschutz) MOV50CS (ohne CTLS + Sichtschutz) MOV50DB (CTLS + Sichtschutz) MOV50DC (CTLS + Sichtschutz) MOV50DN (CTLS + Sichtschutz) MOV50DQ (CTLS + Sichtschutz) MOV50DS (CTLS + Sichtschutz) MOV50JB (CTLS + Sichtschutz + Tischgehäusedeckel) MOV50JC (CTLS + Sichtschutz + Tischgehäusedeckel)	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)	App#1, App#2, App#3, App#5	NA
---------	----------	---------------------------	---	---	--	--------------------

			MOV50JN (CTLS + Sichtschutz + Tischgehäusedeckel) MOV50JQ (CTLS + Sichtschutz + Tischgehäusedeckel) MOV50JS (CTLS + Sichtschutz + Tischgehäusedeckel) MOV50AB (ohne CTLS) MOV50BN (CTLS)			
4-30310	Ingenico	<i>Lane/3000</i>	LAN30AA, LAN30BA, LAN30CA, LAN30DA, LAN30EA, LAN30FA, LAN30GA, LAN30HA	820547v01.xx, 820561v01.xx (Basis- Firmware)	<i>App#1, App#2, App#3</i>	<i>NA</i>
4-20317	Ingenico	<i>DESK/5000</i>	(CTLS) (ohne CTLS + Sichtschutz) (ohne CTLS) DES50AB, DES50BB, DES50CB, DES50DB (CTLS + Sichtschutz)	820376v01.xx, 820547v01.xx (Core- Firmware), 820549v01.xx (SRED OnGuard FPE), 820555v01.xx (SRED), 820556v01.xx (SRED OnGuard SDE), 820559v01.xx (SRED ANL), 820565v01.xx (SRED FF1)	<i>App#6</i>	<i>NA</i>
4-30365	Ingenico	<i>Moby/5500</i>	MOB55xBxAx, MOB55ABBBx (mit CTLS) MOB55BBABx (ohne CTLS) MOB55BBBBx (mit CTLS) MOB55ABABx (ohne CTLS) MOB55xBxAx	CTRL: xxxx-F-802-01xx- xxxx-xx BOOT: xxxx-F-801-01xx- xxxx-xx CTRL: xxxx-F-802-02xx- xxxx-xx BOOT: xxxx-F-801- 02xx-xxxx-xx	NA	NA
4-90307	Ingenico	<i>Moby/5500 CL3</i>	MOB55ABHxAx (mit CTLS) MOB55BBGxAx (ohne CTLS) MOB55BBHxAx (mit CTLS) MOB55ABGxAx (ohne CTLS)	BOOT: xxxx-F-D01-01xx- xxxx-xx CTRL: xxxx-F-D02-01xx- xxxx-xx USER: xxxx-F-023-02xx- xxxx-xx		NA

4-30263	Ingenico	Moby/8500	MOB85AAx (ohne CTLS), MOB85ABx (ohne CTLS), MOB85ACx (ohne CTLS), MOB85BAx (mit CTLS), MOB85BBx (mit CTLS), MOB85BCx (mit 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	NA	NA
4-30481	Ingenico	Lane/3600	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 (Core- Firmware, 820376v12.xx (Security Services), 820555v01.xx (SRED AWL), 820556v01.xx (SRED On-Guard SDE), 820549v01.xx (SRED On- Guard FPE), 820570v07.xx (Open Protocols), 820565v01.xx (SRED FF1)	App#2	NA
4-30381	Ingenico	Self/2000	SEL20AA	820376v04.xx (Security Services) 820566v01.xx	App#2	NA
4-30393	Ingenico	Self/4000	SEL40BA	820376v04.xx (Security Services) 820547v01.xx	App#2	NA
4-30384	Ingenico	Self/5000	SEL50CA	820376v04.xx (Security Services) 820566v01.xx	App#2	NA
4-30510	Ingenico	Self/3000	SEL30BA1-xxxx SEL30BA2-xxxx SEL30AA1-xxxx SEL30AA2-xxxx	820571v01.xx (Basis- Firmware), 820376v12.xx (Security Services), 820555v01.xx (SRED AWL), 820556v01.xx (SRED On-Guard SDE), 820549v01.xx (SRED On- Guard FPE), 820565v01.xx (SRED FF1)	App#2	NA

4-30535	Ingenico	<i>Self/4000 LE</i>	SEL41AA1-xxxx SEL41AA2-xxxx	820571v01.xx (Core-Firmware), 820376v12.xx (Security Services), 820556v01.xx (SRED On-Guard SDE), 820549v01.xx (SRED On-Guard FPE)	App#2	<i>NA</i>
4-30532	Ingenico	<i>Self/5000 LE</i>	SEL51AA1-xxxx	820573v01.xx (Core-Firmware), 820376v12.xx (Security Services), 820556v01.xx (SRED On-Guard SDE), 820549v01.xx (SRED On-Guard FPE)	App#2	<i>NA</i>

4-20359	Ingenico	Move/5000	MOV50BE (CTLS) MOV50BQ (CTLS) MOV50BR (CTLS) MOV50BS (CTLS) MOV50DC (CTLS + Sichtschutz) MOV50DE (CTLS + Sichtschutz) MOV50DN (CTLS + Sichtschutz) MOV50DQ (CTLS + Sichtschutz) MOV50DR (CTLS + Sichtschutz) MOV50DS (CTLS + Sichtschutz) MOV50JC (CTLS + Tischgehäusedeckel) MOV50JE (CTLS + Tischgehäusedeckel) MOV50JN (CTLS + Sichtschutz + Tischgehäusedeckel) MOV50JQ (CTLS + Tischgehäusedeckel) MOV50JR (CTLS + Tischgehäusedeckel) MOV50JS (CTLS + Tischgehäusedeckel) MOV50BC (CTLS) MOV50BN (CTLS)	820547v11.xx, 820549v01.xx (SRED OnGuard FPE), 820556v01.xx (SRED OnGuard SDE), 820547v11.xx (Core-Firmware), 820376v12.xx (Security Services)	App#1, App#2, App#3, App#5, App#6	NA
---------	----------	---------------------------	--	--	---	----

4-30494	Ingenico	Lane/7000	LAN70AC LAN70BB LAN70BC LAN70BD LAN70AB	820547v11.xx (Core-Firmware), 820376v12.xx (Security Services), 820555v01.xx (SRED AWL), 820556V01.xx (SRED On-Guard SDE), 820549V01.xx (SRED On-Guard FPE), 820565V01.xx (SRED FF1), 820548V07.xx (Open Protocols), 820572V01.xx (Tetra JVM Addon), 820376v14.xx (Security Services)	App#2	NA
4-30493	Ingenico	Lane/8000	LAN80BA LAN80BB LAN80AA	820547v11.xx (Core-Firmware), 820376v12.xx (Security Services), 820556V01.xx (SRED On-Guard SDE), 820549V01.xx (SRED On-Guard FPE), 820548V07.xx (Open Protocols), 820376v14.xx (Security Services)	App#2	NA
4-20375	Ingenico	Lane/5000	LAN52BA1-xxxx	820571v01.xx (Core-Firmware) 820376v12.xx (Security Services) 820549v01.xx (SRED OnGuard FPE) 820556v01.xx (SRED OnGuard SDE) 820376v14.xx (Security Services)	App#2, App#3, App#5	NA

4-30533	Ingenico	<i>Link/2500 LE</i>	LIN25AB1-xxxx LIN25BA1-xxxx LIN25CA1-xxxx LIN25DA1-xxxx LIN25AA1-xxxx	820571v01.xx (Core-Firmware) 820376v12.xx (Security Services) 820556v01.xx (SRED On-Guard SDE) 820549v01.xx (SRED On-Guard FPE) 820565v01.xx (SRED FF1) 820376v14.xx (Security Services)	<i>App#2</i>	<i>NA</i>
4-30498	Ingenico	<i>AXIUM RX7000</i>	R70411xxxx	02.03.11.xxxxx (Die von der Firmware unterstützte SRED-Lösung umfasst 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 (mit 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 (mit AP Solution 1)	01.09.11.xxxxx (mit 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 (ohne Pinshield)	02.03.11.xxxxx(Die von der Firmware unterstützte SRED-Lösung umfasst: 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(mit MSR), 80172002(ohne MSR), 80172004(mit MSR), 80172005(ohne MSR)	SREDKEY2 FW v1.00.xxx.xxx.S, SREDKey2 FW v1.01.xxx.xxx.S	NA	NA

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

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	NA	NA
---------	-------------	--	--	------------------------	----	----

4-30475	Infinite Peripherals, Inc	<i>QuantumPay Pro Plus</i>	21.1x.xx.xxx	SP: 3.0.xx.xx, AP: 1.0.xx.xx	NA	NA
4-80037	Castles Technology Co. Ltd	<i>Saturn 1000-E</i>	SATURN1000E-HW- V1.20.xxxx	1.1.1.xxxxxx	NA	<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	NA	<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	NA	<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:	NA	<i>SW#1-22</i>
4-80094	Castles Technology Co. Ltd	<i>S1F4 PRO</i>	HW-V-1G.00	1.6.1.xxxxxx	NA	<i>SW#1-22</i>
4-80082	Castles Technology Co. Ltd	<i>S1P</i>	HW-V1.00	1.4.1.xxxxxx	NA	<i>SW#1-22</i>
4-80092	Castles Technology Co. Ltd	<i>S1P2</i>	HW-V-1D.00	1.6.1.xxxxxx	NA	<i>SW#1-22</i>
4-80091	Castles Technology Co. Ltd	<i>S1Mini2</i>	HW-V-1E.00	1.6.1.xxxxxx	NA	<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	NA	<i>SW#1-22</i>
4-80106	Castles Technology Co. Ltd	<i>S1U2-M4</i>	HW-V-1I.00	1.6.1.xxxxxx	NA	<i>SW#1-22</i>

4-80084	Castles Technology Co. Ltd	<i>S2L</i>	HW-V1A.00	1.4.1.xxxxxx	NA	<i>SW#1-22</i>
4-80077	Castles Technology Co. Ltd	<i>S1U2</i>	HW-V1.00	1.4.1.xxxxxx 1.4.2.xxxxxx	NA	<i>SW#1-22</i>
4-30470	Elo Touch Solutions, Inc	<i>EMC0600,</i> <i>EMC0600C,</i> <i>EMC0600SC'</i> <i>EMC0600S</i>	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	NA	NA
4-90136	Ziosk	<i>Z600</i>	6.0.A 6.0.B	6201.29.xxxx.xxx.xxx 6201.30.xx.x.xxx	NA	NA
4-90335	Ziosk	<i>Z600 Pro</i>	6.0.A	6201.29.xxxx.xxx.xxx	NA	NA
4-30522	Verifone	<i>M425</i> <i>M450</i>	H625-0007-0090-1xx-xxx-B0 (mit Sichtschutz), H650-0007-0090-0xx-xxx-B0 (ohne Sichtschutz), H650-0007-0090-1xx-xxx-B0 (mit Sichtschutz), H625-0007-0090-0xx-xxx-B0 (ohne Sichtschutz),	VOS3: 02.xx.xx, SPBL_01.02.xx.xx, SPFW_01.04.xx.xx, APFW_01.02.xx.xx, Android: 3.01D.xx	NA	NA
4-80062	Verifone	<i>P630</i>	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	NA	NA

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	NA	<i>NA</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	NA	<i>NA</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	NA	<i>NA</i>
4-40363	PAX Computer Technology (Shenzhen) Co Ltd	<i>A6650</i>	A6650-0xx-0x6-0xxx (OHNE CTLS), A6650-0xx-0x6-1xxx (OHNE CTLS), A6650-0xx-Rx6-0xxx (CTLS), A6650-0xx-Rx6-1xxx (CTLS),	26.00.01 xxxxx	NA	<i>NA</i>
4-30554	Toast Inc	<i>TG300, TG310</i>	REV1.xx	01.xx.xx.-10xxxxx	NA	<i>SW#1</i>

2.2 Details zu P2PE-Anwendungen

Die folgenden Informationen listen die P2PE-Anwendungen auf, die für die Verwendung auf den PTS-POI-Geräten in Tabelle 2.1 in dieser P2PE-Lösung zugelassen sind.

P2PE-Anwendungen haben per Definition Zugriff auf Klartext-Kontodaten. Diese Anwendungen **müssen** im Eintrag der P2PE-Lösung aufgeführt sein.

Die „PIM-ID-Nummern“ sind Nummern, die vom P2PE-Lösungsanbieter ausschließlich für die Verwendung innerhalb dieses PIM erstellt und verwendet werden, um den Querverweis auf die hier aufgeführten P2PE-Anwendungen zu erleichtern, die auf den in Tabelle 2.1 aufgeführten PTS-POI-Geräten eingesetzt werden. Sie werden nicht vom PCI SSC vergeben und vom PCI-P2PE-Programm auch nicht anerkannt.

Hinweis: P2PE-Anwendungen, die im Rahmen der P2PE-Lösung bewertet wurden und für die entschieden wurde, sie nicht separat aufzuführen, sind im Eintrag der P2PE-Lösung entsprechend gekennzeichnet und haben keine eigene Listing-Referenznummer für P2PE-Anwendungen.

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

PIM-ID-Nr. (z. B. App#1, App#2, ...)	Hersteller der P2PE-Anwendung	Name der P2PE-Anwendung	Version(en) der P2PE- Anwendung	Listing- Referenznummer der PCI-P2PE- Anwendung (Vergeben vom 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	Axiom Retail Core Axiom 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 Details zur Nicht-Zahlungssoftware

Die folgenden Informationen listen die Nicht-Zahlungssoftware auf, die für die Verwendung auf den PTS-POI-Geräten in Tabelle 2.1 in dieser P2PE-Lösung zugelassen ist.

*P2PE-Nicht-Zahlungssoftware darf per Definition **keinen** Zugriff auf Klartext-Kontodaten haben. Diese Art von Software wird zwar im Rahmen der Bewertung der P2PE-Lösung geprüft, ist jedoch nicht im PCI-P2PE-Lösungseintrag aufgeführt.*

Die „PIM-ID-Nummern“ sind Nummern, die vom P2PE-Lösungsanbieter ausschließlich für die Verwendung innerhalb dieses PIM erstellt und verwendet werden, um den Querverweis auf die hier aufgeführte Nicht-Zahlungssoftware zu erleichtern, die auf den in Tabelle 2.1 aufgeführten PTS-POI-Geräten eingesetzt wird. Sie werden nicht vom PCI SSC vergeben und vom PCI-P2PE-Programm auch nicht anerkannt.

PIM-ID-Nr. (z. B. SW#1, SW#2, ...)	Hersteller der Nicht-Zahlungssoftware	Name der Nicht-Zahlungssoftware	Version(en) der Nicht-Zahlungssoftware	Zusätzliche Informationen (nach Bedarf)
SW#1	FreedomPay	CX App	1.x.x	Android-Middleware-Komponente zur Integration mit POS-Anwendungen auf All-in-One-Geräten
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 Details zur Nicht-Zahlungssoftware

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 Überprüfen der Informationen zum PTS-POI-Gerät

Die Überprüfung der Informationen zum PTS-POI-Gerät ist von entscheidender Bedeutung. Diese Informationen sind erforderlich, um die Angaben in diesem PIM zu validieren, sie mit den PCI-PTS-Listings sowie dem PCI-P2PE-Lösungseintrag abzugleichen und sie für Bestandsverwaltung, Fehlerbehebung und Vorfälle zu nutzen.

Anweisungen zur Bestätigung der Hardware und Firmware des PTS-POI-Geräts sowie der vorhandenen P2PE-Anwendung(en) und Nicht-Zahlungssoftware

Die Hardwareversionen finden sich bei allen Geräten auf der Rückseite auf dem Herstelleraufkleber, der die Seriennummer enthält. Beispiele für die Position dieses Aufklebers finden sich in Anhang C.

Ingenico-Geräte:

Um die Firmwareversion zu ermitteln, führen Sie die folgenden Schritte aus:

1. Trennen Sie das Gerät vom POS-System oder einem anderen Front-End-System
2. Versorgen Sie das Gerät über das Netzkabel mit Strom oder schließen Sie es mit dem USB-Kabel an einen PC an
3. Drücken Sie während des Hochfahrens des Geräts die folgende Tastenfolge auf dem Ingenico-Gerät: 2634, [Grüne Taste], F
4. Wenn Ihr Gerät keine „F“-Taste hat, lautet die Tastenfolge 2634, [Grüne Taste], +
5. Wenn Sie ein Move/5000 verwenden, verwenden Sie den Code 0001
6. Wählen Sie das folgende Menü: *Control Panel/Terminal Information/Firmware PCI PTS/Display*

7. Notieren Sie die mit M1 verknüpften Firmwareinformationen

Die Version der auf Ingenico-Geräten geladenen Anwendung ist beim Hochfahren des Geräts auf dem Startbildschirm zu sehen. Der Wert „PCI Version“ sollte mit der Versionsnummernvorlage übereinstimmen, die auf der PCI-SSC-Website angezeigt wird.

ID-Tech-Geräte:

Die Firmwareversionen dieser Geräte können nur mit einer von ID Tech bereitgestellten Anwendung angezeigt werden. Für den Download dieser Anwendung wenden Sie sich bitte an compliance@freedompay.com für Unterstützung.

Castles-/Elo-Geräte:

Öffnen Sie im Hauptbildschirm das Menü „CX Application“ und klicken Sie dann auf „About“. Am unteren Rand dieses Bildschirms, sehen Sie die Firmwareversion.

Ziosk-Geräte:

Die Firmwareversion ist im Gerätemenü unter Settings > About device > Firmware version zu sehen.

Infinite-Peripheral-Geräte:

Die Firmwareversionen dieser Geräte können nur mit einer von Infinite Peripherals bereitgestellten Anwendung angezeigt werden. Für den Download dieser Anwendung wenden Sie sich bitte an compliance@freedompay.com für Unterstützung.

PAX-Geräte

Wählen Sie im Startbildschirm Settings > About und notieren Sie die angezeigte Firmware.

Toast-Geräte

Wählen Sie im Startbildschirm Settings > About und notieren Sie die angezeigte Firmware.

Verifone-Geräte

Wählen Sie im Startbildschirm Settings > About und notieren Sie die angezeigte Firmware.

2.5 Inventarisierung und Überwachung von PTS-POI-Geräten

- Alle PTS-POI-Geräte müssen über Bestandskontroll- und Überwachungsverfahren dokumentiert werden, einschließlich des Gerätestatus (z. B. im Einsatz, wartet auf Inbetriebnahme, in Reparatur oder anderweitig außer Betrieb oder im Transit).
- Diese Inventur muss mindestens jährlich durchgeführt werden.
- Alle Abweichungen im Bestand, einschließlich fehlender oder ausgetauschter PTS-POI-Geräte, müssen dem P2PE-Lösungsanbieter über die Kontaktinformationen und Anweisungen in Abschnitt 1 oben gemeldet werden.
- Die untenstehende Beispiel-Inventartabelle dient nur zur Veranschaulichung. Das tatsächliche Inventar sollte vom Händler in einem externen Dokument erfasst und geführt werden.

Anweisungen zur Dokumentation und Führung eines Inventars der PTS-POI-Geräte.

Der Händler muss ein System zur Nachverfolgung von POI-Geräten implementieren und pflegen, das jedes POI-Gerät entsprechend seinem aktuellen Status identifiziert. Beispiele für mögliche Status sind:

- Im Einsatz
- Wartet auf Inbetriebnahme
- Außer Betrieb und/oder in Reparatur
- Im Transit
- Entfernt und zurückgesendet

FreedomPay bietet über sein Enterprise Reporting Portal, das Device Management Portal, ein einfaches Aufzeichnungssystem an, das während der Implementierung konfiguriert werden kann. Alternativ können Händler auch ein eigenes System einsetzen, wenn sie dies bevorzugen. Elektronische POI-Geräteinventare sollten sicher gespeichert werden, und der Zugriff sollte ausschließlich auf autorisiertes Personal beschränkt sein.

Der Händler muss außerdem ein „staatliches Buchführungs- und Kontrollsystem“ einrichten, um alle POI-Geräte (Menge und Typ) nachzuverfolgen, Änderungen im Materialbestand (Eingang/Ausgang) zu erfassen und alle Aspekte des Lebenszyklus der POI-Geräte zu überwachen, solange sich das Gerät im Besitz und unter der Kontrolle des Händlers befindet. Erfassen Sie alle Inventurdifferenzen in Ihrem Bestandskontrollsystem und melden Sie fehlende oder verlorene Geräte nach ihrer Feststellung an FreedomPay unter compliance@freedompay.com oder an den benannten FreedomPay-Partner/Reseller, der die Geräte bereitgestellt hat.

Wenn Ihre Organisation mehrere Filialen betreibt oder regional bzw. landesweit tätig ist, ist es wichtig, Bestandsverwaltungs- und Nachverfolgungssysteme auf lokaler, regionaler und nationaler Ebene einzusetzen, damit das Wissen und die Fähigkeit zur Verwaltung, Nachverfolgung und Meldung von Beständen auf allen Ebenen gewährleistet sind.

Es wird empfohlen, dass das Geräteinventar mindestens Informationen enthält, die denen in der untenstehenden Beispiel-Inventartabelle ähneln. Alle gerätespezifischen Identifikationsinformationen, die für die Bestandsverfolgung erforderlich sind, finden sich auf einem Aufkleber auf der Rückseite bzw. im Batteriefach jedes POI-Geräts (Abbildungen zum Speicherort der Seriennummer für eine Auswahl von Geräten sind enthalten in **Anhang C in Abschnitt 9, Zusätzliche Hinweise** und/oder über die logische Schnittstelle des POI-Geräts).

Der Händler muss schriftliche Protokolle für die Verlagerung von Geräten zwischen Händlerstandorten entwickeln und pflegen. Der Händler muss die Einhaltung dieser Protokolle überwachen und dokumentieren. Die Protokolle des Händlers für die Verlagerung von POI-Geräten müssen mindestens so sicher sein wie die in diesem PIM festgelegten Protokolle für den Versand von POI-Geräten von und zu zugelassenen Lieferantenstandorten (Approved Supplier Facilities). Weitere Informationen zur Aufrechterhaltung der Verwahrkette bei der Verlagerung oder Lagerung von Geräten erhalten Sie bei compliance@freedompay.com oder beim FreedomPay-Partner/Reseller, der die Geräte bereitgestellt hat.

Der Händler kann aufgefordert werden, sein jährliches POI-Inventar im Rahmen seiner jährlichen PCI-DSS-Compliance bei seinem Merchant Acquirer einzureichen. Die Nichteinhaltung der im PIM aufgeführten Kontrollen kann zu einem „Merchant Opt-Out“ führen, d. h. zur Aussetzung des FreedomPay Commerce Platform P2PE Scope Reduction Program.

Wenn ein Händler die von FreedomPay bereitgestellten POI-Geräte aufgrund eines Merchant Opt-Out, einer Vertragsbeendigung, einer Geschäftsaufgabe, einer Außerbetriebnahme oder aus einem anderen Grund nicht mehr im Rahmen eines PCI P2PE Scope Reduction Program nutzen möchte, ist der Händler verpflichtet, alle von FreedomPay bereitgestellten POI-Geräte sicher zu vernichten. Die sichere Vernichtung muss über den sicheren Vernichtungsservice von FreedomPay erfolgen, indem eine Anfrage an devicedisposal@freedompay.com gesendet wird, die die Anzahl der Geräte und die Seriennummern der einzelnen Geräte enthält. Nach Eingang meldet sich das Professional-Services-Team von FreedomPay mit weiteren Details. Weitere Informationen zu möglichen Vernichtungsdiensten erhalten Sie von Ihrem FreedomPay-Ansprechpartner.

Beispiel-Inventartabelle

Hersteller des PTS-POI-Geräts	Modellname(n) und -nummer(n) des PTS-POI-Geräts	Gerätestandort	Gerätestatus	Seriennummer oder andere eindeutige Kennung	Datum der Inventur	Zusätzliche Hinweise (nach Bedarf)

3. Erhalt von PTS-POI-Geräten

3.1 Anweisungen, um sicherzustellen, dass PTS-POI-Geräte aus vertrauenswürdigen Quellen/Standorten/Orten stammen

FreedomPay oder sein zertifiziertes KIF sendet dem Händler per E-Mail eine Vorabversandbenachrichtigung mit den Seriennummern der POI-Geräte, dem Namen des Kuriers, der Sendungsverfolgungsnummer, der Einrichtung, von der das Paket versandt wurde, sowie dem zugelassenen Händlerstandort (Approved Merchant Location), an den das Paket versandt wurde.

Beim Erhalt einer POI-Gerätesendung muss der Händler:

- i. Die Verpackung wie oben beschrieben prüfen.
- ii. Überprüfen, ob der auf dem Lieferschein angegebene Kurier ein vertrauenswürdiger Kurier (Trusted Courier) ist.
- iii. Überprüfen, ob das Paket von einer Lieferanteneinrichtung versandt wurde, die einem oder mehreren der als Teil von FreedomPays Commerce Platform P2PE aufgeführten Komponentenanbieter zugeordnet ist, oder von einer Einrichtung, die Teil der vom Händler vorab festgelegten Verwahrkette ist. Wenn Sie sich bezüglich der Adresse oder des Standorts, von dem ein Gerät kommen sollte, nicht sicher sind, wenden Sie sich bitte an compliance@freedompay.com.
- iv. Überprüfen, ob die Seriennummern auf dem Lieferschein mit den Seriennummern in der Vorabbenachrichtigung per E-Mail übereinstimmen.
- v. Das Geräteverwaltungssystem aktualisieren, um die Änderung von Gerätestatus und -standort widerzuspiegeln.

Der Händler muss jedes POI-Gerätepaket, das den Anschein erweckt, manipuliert worden zu sein, von jemand anderem als einem vertrauenswürdigen Kurier geliefert wurde oder von einem anderen als dem erwarteten Standort versandt wurde, umgehend wie unten beschrieben an FreedomPay zurücksenden.

Bevor ein POI-Gerät an einen zugelassenen Lieferantenstandort (Approved Supplier Facility) zurückgesendet wird, muss der Händler eine E-Mail an poidevicereturns@freedompay.com senden, um je nach Situation zu klären, wohin das Gerät versandt werden soll.

3.2 Anweisungen zur Bestätigung, dass PTS-POI-Gerät und Verpackung nicht manipuliert wurden

Beim Erhalt eines FreedomPay-POI-Geräts sollten Händler mindestens Folgendes tun:

- Überprüfen, ob der auf dem Lieferschein angegebene Kurier
- Überprüfen, ob das Paket von einem erwarteten Standort versandt wurde.
- Überprüfen, ob die Seriennummern auf dem Lieferschein mit den Seriennummern in der Vorabbenachrichtigung per E-Mail übereinstimmen.
- Überprüfen, ob die Verpackung nicht so stark beschädigt ist, dass das Innere des Pakets freiliegt.
- Überprüfen, ob die Verpackung nicht so nass geworden ist, dass Feuchtigkeit durch die Verpackungswände gedrungen ist.
- Überprüfen, ob die Unversehrtheit der manipulationssicheren Verpackung gewährleistet ist.

Beispiel für ein nicht manipuliertes Paket mit manipulationssicherem Klebeband:



Wenn das Gerät oder die Verpackung eine der oben genannten Prüfungen nicht besteht, wenden Sie sich an Ihren FreedomPay-Ansprechpartner und senden Sie das Gerät wie in Abschnitt 5.2 beschrieben zurück.

3.3 Anweisungen zur Bestätigung des geschäftlichen Bedarfs und der Identität von Drittpersonal, das sich als Liefer-, Support- und/oder Reparaturpersonal ausgibt, bevor diesem Personal Zugang zu PTS-POI-Geräten gewährt wird.

In den meisten Fällen kann FreedomPay den Gerätesupport aus der Ferne leisten, ohne dass Unterstützung vor Ort erforderlich ist. Bei komplexen Installationen oder bestimmten Supportfällen kann jedoch ein Techniker an einen Händlerstandort entsandt werden. Falls ein FreedomPay-Techniker vor Ort benötigt wird, stellen Sie sicher, dass vor, während und nach den Arbeiten vor Ort die folgenden Schritte durchgeführt werden.

- i. Einem Fall wird ein Außendiensttechniker zugewiesen, der eine Entsendeanforderung (Dispatch Request) ausfüllt.
- ii. Sobald ein Techniker zugewiesen wurde, stellt FreedomPay dem Händler die Details der Anforderung zur Verfügung.
- iii. Wenn der Techniker vor Ort eintrifft und bevor Zugang zum POI-Gerät gewährt wird, sollte der Händler die Identität des Technikers als FreedomPay-Mitarbeiter oder -Auftragnehmer überprüfen. Allen anderen Personen muss der Zugang ohne ordnungsgemäße Identitätsprüfung verweigert werden.
- iv. Sobald die Identität des Technikers überprüft wurde, sollte der Händler eine Begleitperson bestimmen, die die Tätigkeiten des Technikers jederzeit überwacht.
- v. Sobald der Techniker die Arbeiten abgeschlossen hat, muss der Händler auf die Dispatch-E-Mail mit den folgenden Angaben antworten:
 - i. Zur Überprüfung vorgelegte Ausweisart

- ii. Am Standort verbrachte Zeit
- iii. (Nur bei Supportfällen) Seriennummer(n) der vom Techniker bearbeiteten Terminals

FreedomPay entsendet niemals Techniker vor Ort, ohne dies vorher mit den Händlerkontakten abzustimmen und Informationen zum entsandten Techniker zu Verifizierungszwecken bereitzustellen. Personen, die sich ohne ordnungsgemäße Benachrichtigung oder Identifikation als Reparatur-/Supporttechniker ausgeben, sollte kein Zugang zu POI-Geräten gewährt werden.

POI-Geräte, die sich in Ihrem Besitz befinden, physisch sichern, einschließlich Geräten, die:

- auf die Inbetriebnahme warten
- in Reparatur oder anderweitig außer Betrieb sind
- auf den Transport zwischen Standorten warten

4. Bereitstellung und Installation von PTS-POI-Geräten

Schließen Sie keine nicht zugelassenen Geräte zur Erfassung von Zahlungskontodaten an und verwenden Sie diese nicht anderweitig.

Die P2PE-Lösung ist für die Verwendung bestimmter PTS-POI-Geräte zugelassen, wie oben in Tabelle 2.1 aufgeführt, die im Eintrag der P2PE-Lösung aufgeführt sein müssen.

Wenn Geräte, die nicht in Tabelle 2.1 aufgeführt sind, zur Annahme von Zahlungskontodaten verwendet werden, kann dies die Berechtigung des Händlers zur Nutzung des SAQ P2PE beeinträchtigen – wenden Sie sich an Ihren Acquirer oder die Zahlungsmarken.

Ändern Sie die sicheren Konfigurationen oder Einstellungen des PTS-POI-Geräts nicht und versuchen Sie nicht, diese zu ändern.

Das Ändern sicherer Konfigurationen oder Einstellungen des PTS-POI-Geräts kann die Implementierung der P2PE-Lösung ungültig machen und die Berechtigung des Händlers zur Nutzung des SAQ P2PE beeinträchtigen – wenden Sie sich an Ihren Acquirer oder die Zahlungsmarken.

Beispiele hierfür sind unter anderem der Versuch, auf den PTS-POI-Geräten Folgendes durchzuführen:

- Aktivieren deaktivierter Geräteschnittstellen oder Datenerfassungsmechanismen
- Ändern von Sicherheitskonfigurationen oder Authentifizierungskontrollen
- Physisches Öffnen des Geräts
- Versuch, nicht autorisierte Anwendungen/Software zu installieren

4.1 Installations- und Anschlussanweisungen für die PTS-POI-Geräte

Es wird empfohlen, jede POI-Geräteinstallation mit einer der folgenden Methoden oder einer von Ihrem Qualified Security Assessor (QSA) genehmigten Alternative zu sichern:

- i. Das Gerät ist physisch montiert oder angebunden, um unbefugte Entfernung, Manipulation oder Austausch zu verhindern. Zulässige Methoden umfassen:
 - a. Montage des Geräts auf einem zugelassenen PIN-Sicherheitsständer
 - b. Sichern des Geräts mit einem Sicherungsschloss (Tether Lock), das am Sicherheitsschlitz des POI-Geräts befestigt und am anderen Ende des Kabels dauerhaft an der Theke oder anderer sicherer, physisch befestigter Hardware gesichert ist. Eine große Auswahl an Sicherungsschlössern ist bei den meisten Computerhändlern, online oder bei FreedomPay erhältlich. Bitte wenden Sie sich an Ihren FreedomPay-Ansprechpartner, wenn Sie Hilfe bei der Suche nach einem geeigneten Sicherungsschloss benötigen.

- ii. Das Gerät sollte so aufgestellt werden, dass es von autorisiertem Personal leicht beobachtet/überwacht werden kann, und in einer Umgebung, die Manipulationsversuche abschreckt.

Zusätzliche Implementierungsschritte umfassen:

- i. Bei der Inbetriebnahme des Geräts muss der Händler die folgenden Schritte durchführen:
 - a. Überprüfen, ob die angezeigte Seriennummer mit der Seriennummer auf der Unterseite des Geräts übereinstimmt.
 - i. Hilfe beim Auffinden der Seriennummern auf POI-Geräten finden Sie im Abschnitt **Anhang C in Abschnitt 9, Zusätzliche Hinweise**.
 - b. Das Geräteverwaltungssystem aktualisieren, um die Änderung von Gerätestatus und -standort widerzuspiegeln.
- ii. Das Gerät muss einen der folgenden Kommunikations-/Verbindungstypen verwenden:
 - a. USB
 - b. Seriell
 - c. Ethernet
 - d. WLAN
 - e. Bluetooth
 - f. Mobilfunk

Sonstige: Für nicht oben aufgeführte POI-Kommunikationstypen muss der Händler compliance@freedompay.com kontaktieren, um vom Compliance-Team von FreedomPay die offizielle Compliance-Freigabe für die Verwendung eines solchen Geräts zu erhalten. Der Händler muss von FreedomPay schriftlich eine offizielle Bestätigung erhalten, dass der POI-Kommunikationstyp, der nicht in der obigen Liste aufgeführt ist, eine akzeptierte Kommunikations-/Verbindungsmethode für die FreedomPay Commerce Platform P2PE-Lösung ist.

4.2 Hinweise zur Auswahl geeigneter Standorte für die Bereitstellung von PTS-POI-Geräten

FreedomPay empfiehlt, und der PCI DSS bekräftigt, dass alle bereitgestellten Geräte sicher montiert und für das Personal gut sichtbar sein sollten, um unbefugte Entfernung oder Manipulation zu verhindern. Das Gerät sollte so aufgestellt werden, dass es von autorisiertem Personal leicht beobachtet/überwacht werden kann, und in einer Umgebung, die Kompromittierungsversuche abschreckt. Wenn eine Implementierung für den unbeaufsichtigten Einsatz vorgesehen ist, sollten Verfahren vorhanden sein, um das mit der Implementierung verbundene Risiko zu mindern. Dies können Überwachungskameras, häufigere Inspektionen, Kontrollen zur Manipulationsverhinderung oder andere von Ihrem QSA genehmigte Methoden sein.

Geräte, die nicht im Einsatz sind, müssen gemäß der in Abschnitt 3.3 beschriebenen Methodik gelagert werden.

4.3 Hinweise zur physischen Sicherung bereitgestellter PTS-POI-Geräte, um unbefugte Entfernung und/oder Austausch zu verhindern

Händlern wird empfohlen, im Einsatz befindliche Geräte auf einem zugelassenen PIN-Sicherheitsständer zu montieren oder das Gerät mit einem Sicherungsschloss zu sichern, das am Sicherheitsschlitz des POI-Geräts befestigt und am anderen Ende des Kabels dauerhaft gesichert ist. Eine große Auswahl an Sicherungsschlössern ist bei den meisten Computerhändlern oder online erhältlich. Bitte wenden Sie sich an Ihren FreedomPay-Ansprechpartner oder QSA, wenn Sie Hilfe bei der Suche nach einem geeigneten Sicherungsschloss benötigen. Bei Implementierungen, die sich nicht für montierte Geräte eignen (z. B. eigenständige Geräte oder mobile Szenarien), sollten Verfahren implementiert werden, um das Risiko einer Manipulation oder Kompromittierung des Geräts zu mindern. Dies kann die Zuweisung von Geräten an Standortpersonal, häufigere Inspektionen oder andere vom QSA genehmigte Verfahren umfassen.

Der Händler muss einen Bereich für die „sichere Aufbewahrung“ von POI-Geräten einrichten, die nicht im Einsatz sind. Dieser Bereich wird verwendet, wenn POI-Geräte vor der Installation von FreedomPay eingehen, von anderen zugelassenen Händlerstandorten überführt oder aus dem aktiven Einsatz genommen werden. Sichere Aufbewahrung wird von PCI als ein ausgewiesener Raum oder Ort mit kontrolliertem physischem Zugang definiert, für den Personal zugangsberechtigt sein muss und für den Mechanismen/Richtlinien zur Dokumentation jedes physischen Zugangs zum Bereich der „sicheren Aufbewahrung“ vorhanden sind, einschließlich:

- Identifizierung des zum Gerätezugriff berechtigten Personals
- Beschränkung des Zugangs auf autorisiertes Personal
- Führen eines Protokolls über jeden Zugang mit Name der Person, Unternehmen, Zugangsgrund sowie Ein- und Austrittszeit

Der Händler muss vor der Implementierung der PCI-validierten P2PE-Lösung von FreedomPay eine Zugangsrichtlinie für die „sichere Aufbewahrung“ einführen. Diese Richtlinie muss eine Beschreibung enthalten, was und wo der Bereich für die sichere Aufbewahrung ist, sowie die festgelegten Verfahren zur Einhaltung der in diesem Abschnitt dargelegten Anforderungen.

5. Kontinuierliche Überwachung und Inspektion bereitgestellter PTS-POI-Geräte

5.1 Anweisungen zur Inspektion von PTS-POI-Geräten auf Anzeichen von Manipulation und zur Reaktion auf vermutete Manipulationsvorfälle

Händler müssen mindestens Folgendes in einem angemessenen Zeitrahmen inspizieren, der auf ihrem Risikoprofil basiert (in der Regel vierteljährlich):

- Wurde das USB-/Ethernet-Kabel in irgendeiner Weise beschädigt oder verändert?
- Stimmt die Seriennummer auf dem Gerät mit der von FreedomPay bereitgestellten Seriennummer überein? (Zum Speicherort der Seriennummer siehe Anhang C)
- Sind aktive POI-Geräte gemäß dem PIM angemessen gesichert?
- Sind inaktive POI-Geräte gemäß dem PIM sicher gelagert?
- Wurde das POI-Gerät in irgendeiner Weise beschädigt?
- Ist der Bildschirm „Secured by FreedomPay“ vorhanden?

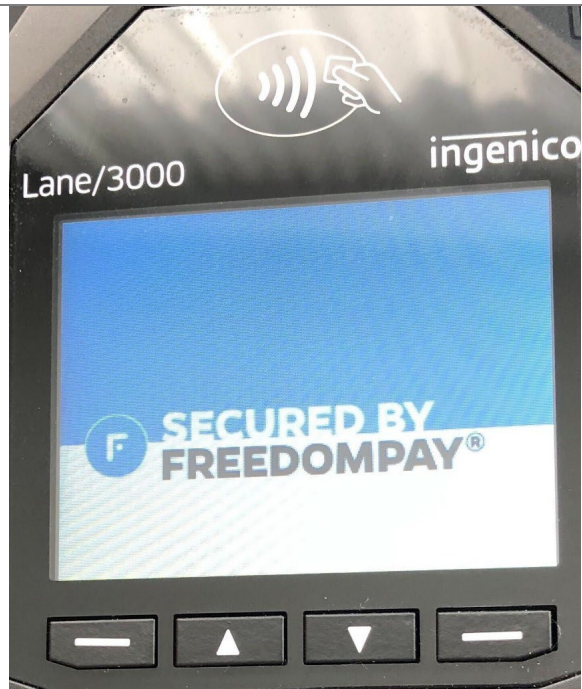
- Sind zusätzliche vom Händler angebrachte und im Inventar vermerkte Maßnahmen zur Manipulationserkennung, wie Sicherheitssiegel, Etiketten oder versteckte Markierungen, intakt?

Beispiele für Inspektionsbereiche:

Überprüfen, ob die äußeren Schrauben nicht entfernt wurden.



Überprüfen, ob der Bildschirm „Secured by FreedomPay“ vorhanden ist.



Wenn ein Händler ein FreedomPay-POI-Gerät in einem Bereich einsetzt, der nicht von einem zugelassenen Mitarbeiter des Händlers physisch überwacht wird, müssen geeignete Verfahren vorhanden sein, um die Möglichkeit einer Manipulation des Geräts und im schlimmsten Fall die Zeit zwischen Kompromittierung und Erkennung zu verringern. Bitte wenden Sie sich für weitere Informationen zur Inspektion und Überwachung von POI-Geräten an Ihren unabhängigen Qualified Security Assessor (QSA).

Jeder Fall von Gerätemanipulation muss FreedomPay gemeldet werden, und jedes Gerät, das manipuliert wurde oder bei dem der Verdacht auf Manipulation besteht, muss umgehend aus der POS-Umgebung entfernt und gemäß den Anweisungen in Abschnitt 5.2 an FreedomPay zurückgesendet werden.

Der Händler muss jedes POI-Gerät oder jedes Paket mit einem POI-Gerät, das den Anschein erweckt, manipuliert worden zu sein, von jemand anderem als einem vertrauenswürdigen Kurier geliefert wurde oder von einem anderen Ort als einem zugelassenen Lieferantenstandort (Approved Supplier Facility) versandt wurde, umgehend wie unten beschrieben an FreedomPay zurücksenden.

Versand von POI-Geräten:

- i. POI-Geräte dürfen nur von einem vertrauenswürdigen Kurier (Trusted Courier) zu einem in Abschnitt 4.2 aufgeführten zugelassenen Lieferantenstandort transportiert werden.

- ii. Die Seriennummern der zurückzusendenden Geräte sowie der Grund für die Rücksendung müssen an RMA@freedompay.com mitgeteilt werden, das ein Versandetikett für die Rücksendung erstellt.
- iii. Alle Seriennummern der POI-Geräte müssen auf dem Packzettel oder Versandetikett aufgedruckt sein.

Der Händler muss sein Geräteverwaltungssystem aktualisieren, um die Änderung von Gerätestatus und -standort widerzuspiegeln.

5.2 Anweisungen zur Inspektion von PTS-POI-Geräten auf Skimming-Geräte und zur Reaktion auf vermutete Skimming-Erkennung

Weitere Hinweise zur Inspektion von PTS-POI-Geräten finden sich im Dokument mit dem Titel *Skimming Prevention: Best Practices for Merchants*, verfügbar unter https://www.pcisecuritystandards.org/document_library/

Interaktionspunkte auf Overlays oder eingesetzte Werkzeuge prüfen.



Anschlusspunkt auf zusätzliche Kabel/Verbindungen oder Hardware prüfen.



5.3 Anweisungen zur Erkennung von und Reaktion auf Verschlüsselungsfehler bei Kontodaten auf PTS-POI-Geräten

Im Falle eines Verschlüsselungsfehlers, der durch einen Fehlercode 266 oder die Meldung „P2PE Encryption Error“ angezeigt wird, wird dem Händler empfohlen:

- i. Alle Protokolle des Point-of-Sale-(POS-)Systems und die Stapelverarbeitungsfunktionen für Kreditautorisierungen auf Anzeichen von Klartext-Karteninhaberdaten zu überprüfen.
- ii. Alle POS-Abrechnungsberichte zu überprüfen, um sicherzustellen, dass keine unverschlüsselten Karteninhaberdaten vorhanden sind.

Falls Klartext-Karteninhaberdaten gefunden werden oder ein Ausfall einer Gerätesicherheitskontrolle bzw. eine nachgewiesene oder vermutete unbefugte Nutzung sensibler Verwaltungsfunktionen vorliegt, muss der Händler umgehend den technischen Support von FreedomPay kontaktieren und die Anweisungen zur Fehlerbehebung in Abschnitt 7 dieses Dokuments befolgen. Bis die ordnungsgemäße Verschlüsselungsfunktion auf dem

Gerät wiederhergestellt wurde und das Gerät von FreedomPay erneut autorisiert wurde, darf das fehlerhafte Gerät nicht zur Verarbeitung von Transaktionen verwendet werden, es sei denn, der Händler beantragt formell eine Aussetzung der P2PE-Verschlüsselung wie in Abschnitt 6.2 beschrieben.

5.4 Anweisungen zur Fehlerbehebung bei einem PTS-POI-Gerät

Wenn ein POI-Gerät beschädigt, zerstört ist, eine Fehlfunktion aufzuweisen scheint oder anderweitig gewartet werden muss, muss der Händler bei der Interaktion mit dem Personal von FreedomPay den folgenden Prozess befolgen:

- i. Wenden Sie sich an den technischen Support von FreedomPay unter 888-495-2446 oder per E-Mail an techsupport@freedompay.com.
- ii. Wenn der Support-Techniker von FreedomPay feststellt, dass ein Außendiensttechniker entsandt werden sollte, füllt dieser eine Entsendeanforderung (Dispatch Request) aus.
- iii. Sobald ein Techniker zugewiesen wurde, stellt FreedomPay dem Händler die Details zur Einsatzanforderung zur Verfügung.
- iv. Wenn der Techniker vor Ort eintrifft und bevor Zugang zum POI-Gerät gewährt wird, sollte der Händler die Identität des Technikers als FreedomPay-Mitarbeiter oder -Auftragnehmer überprüfen. Allen anderen Personen muss der Zugang ohne ordnungsgemäße Identitätsprüfung verweigert werden.
- v. Sobald die Identität des Technikers überprüft wurde, sollte der Händler eine Begleitperson bestimmen, die die Tätigkeiten des Technikers jederzeit überwacht.
- vi. Sobald der Techniker die Arbeiten abgeschlossen hat, muss der Händler auf die Dispatch-E-Mail mit den folgenden Angaben antworten:
 - i. Zur Überprüfung vorgelegte Ausweisart
 - ii. Am Standort verbrachte Zeit
 - iii. Seriennummer(n) der vom Techniker bearbeiteten Terminals

Wenn ein Händler die von FreedomPay bereitgestellten POI-Geräte aufgrund eines Merchant Opt-Out, einer Vertragsbeendigung, einer Geschäftsaufgabe, einer Außerbetriebnahme oder aus einem anderen Grund nicht mehr im Rahmen eines PCI P2PE Scope Reduction Program nutzen möchte, ist der Händler verpflichtet, alle von FreedomPay bereitgestellten POI-Geräte sicher zu vernichten. Die sichere Vernichtung muss über den sicheren Vernichtungsservice von FreedomPay erfolgen, indem eine Anfrage an devicedisposal@freedompay.com gesendet wird, die die Anzahl der Geräte und die Seriennummern der einzelnen Geräte enthält. Nach Eingang meldet sich das Professional-Services-Team von FreedomPay mit weiteren Details. Weitere Informationen zu möglichen Vernichtungsdiensten erhalten Sie von Ihrem FreedomPay-Ansprechpartner.

6. Transport/Versand von PTS-POI-Geräten

6.1 Anweisungen, um sicherzustellen, dass PTS-POI-Geräte nur an vertrauenswürdige Standorte/Orte versandt werden, soweit erforderlich (z. B. zur Reparatur)

Alle von FreedomPay an den Händler versandten Geräte werden über einen vertrauenswürdigen Kurier zugestellt. Einige von FreedomPay verwendete Kuriere sind unten aufgeführt und könnten von Händlern auch für Sendungen von Standort zu Standort genutzt werden:

- FedEx
- UPS
- USPS (in bestimmten Szenarien)
- R&L Carriers
- DHL
- Ceva Logistics
- New World Transportation
- Purolator
- DPD
- Startrack
- APC

Diese Kuriere werden verwendet, um Geräte an Geschäftsadressen zu liefern, die vom Händlerpersonal während des Onboardings angegeben wurden. Bei Sendungen zwischen Händlerstandorten sollten Geräte nur an vertrauenswürdige Geschäftsadressen geliefert werden. Alle vom und an den Händler versandten Geräte (einschließlich Sendungen von Händlerstandort zu Händlerstandort) müssen in manipulationsgeschützter Verpackung verpackt sein.

Beispiele für manipulationssichere Verpackungen sind Umschläge oder Beutel mit nummerierten Etiketten, die jeden Versuch, das Paket zu öffnen, unumkehrbar sichtbar machen. Manipulationssichere Verpackungen können bei Büroartikelanbietern erworben werden und sind ausdrücklich als „Tamper-Proof“ oder „Tamper-Resistant“ gekennzeichnet. Pakete können zusätzlich mit manipulationssicherem Sicherheitsklebeband an allen Öffnungen gesichert werden.

6.2 Anweisungen zur Sicherung von PTS-POI-Geräten, die für den Transport an andere Standorte bestimmt sind (z. B. zu einer Reparaturreinrichtung), und während dieses Transports

Um eine sichere Lieferung der Geräte zu gewährleisten, wird ein vertrauenswürdiger Kurier empfohlen, der Sendungsverfolgung und Zustellbestätigung ermöglicht. Beispiele für solche Kurier sind unten aufgeführt, andere sichere Methoden sind jedoch zulässig:

- FedEx
- UPS
- USPS (in bestimmten Szenarien)
- R&L Carriers
- DHL
- Ceva Logistics
- New World Transportation
- Purolator
- DPD
- Startrack
- APC

Alle vom und an den Händler versandten Geräte (einschließlich Sendungen von Händlerstandort zu Händlerstandort) müssen in manipulationsgeschützter Verpackung verpackt sein.

Beispiele für manipulationssichere Verpackungen sind Umschläge oder Beutel mit nummerierten Etiketten, die jeden Versuch, das Paket zu öffnen, unumkehrbar sichtbar machen. Manipulationssichere Verpackungen können bei Büroartikelanbietern erworben werden und sind ausdrücklich als „Tamper-Proof“ oder „Tamper-Resistant“ gekennzeichnet. Pakete können zusätzlich mit manipulationssicherem Sicherheitsklebeband an allen Öffnungen gesichert werden.

7. Zusätzliche Hinweise/Anweisungen

7.1 Zusätzliche Hinweise für Händler zur P2PE-Lösung (nach Bedarf).

Dieses P2PE-Anleitungshandbuch wird gemäß den Anforderungen des PCI DSS bereitgestellt. Die Umsetzung der in diesem PIM dargelegten Kontrollen ist eine Voraussetzung für den PCI DSS SAQ-P2PE und die Konformitätsbescheinigung (Attestation of Compliance). Die Verwendung von POI-Geräten, die nicht von FreedomPay zugelassen sind, und/oder jede Nichteinhaltung der in diesem Handbuch dargelegten Anforderungen erfolgt auf alleiniges Risiko des Händlers und kann zu einer Nichtkonformität mit dem PCI DSS SAQ-P2PE, zum Verlust der Qualifikation für die Reduzierung des PCI-DSS-Prüfumfangs und/oder zu einer Beeinträchtigung der Datensicherheit führen.

Durch die Nutzung der FreedomPay P2PE Scope Reduction Solution erklärt sich der Händler damit einverstanden, keine der von FreedomPay bereitgestellten POI-Gerätekonfigurationen zu ändern oder dies zu versuchen, einschließlich, aber nicht beschränkt auf:

- Der Versuch, Geräteschnittstellen oder Datenerfassungsmechanismen zu aktivieren, die auf einem von Freedom Pay bereitgestellten Gerät deaktiviert wurden
- Der Versuch, Sicherheitskonfigurationen oder Authentifizierungskontrollen zu ändern
- Das physische Öffnen eines Geräts
- Der Versuch, Anwendungen auf einem Gerät zu installieren

Um die durch die FreedomPay-Lösung gebotene Reduzierung des Prüfumfangs aufrechtzuerhalten, bestätigt der Händler, dass alle Kreditkartentransaktionen über ein zugelassenes POI-Gerät eingegeben/durchgezogen werden müssen, um im P2PE Scope Reduction Program zu verbleiben. Transaktionen, die auf anderem Wege eingegeben werden, unterliegen nicht dem vom PCI SSC zugelassenen Validated P2PE Program von FreedomPay. FreedomPay hat auf seinem Zahlungs-Gateway (Freeway) einen Mechanismus implementiert, der Transaktionen, die unverschlüsselt von einem nicht von FreedomPay zugelassenen Gerät gesendet werden, mit einer Antwort „P2PE Device Error“, auch als Fehler 266 bezeichnet, ablehnt. Diese unverschlüsselten Transaktionen werden nicht in der Umgebung von FreedomPay gespeichert, können jedoch in den vom Point-of-Sale des Händlers erzeugten Protokollen gespeichert werden, wodurch der Händler Gefahr läuft, die Reduzierung des PCI-Prüfumfangs zu verlieren. Wenn ein Händler Zahlungen auf einem anderen Weg außerhalb der FreedomPay-PCI-P2PE-Lösung akzeptiert oder wiederkehrende Fehler 266 nicht innerhalb von 30 Tagen nach ihrem Auftreten beheben kann, muss er sich mit dem Formular „Merchant Opt Out Request“ (Anhang A) aus dem PCI P2PE Scope Reduction Program abmelden.

Einschränkungen nach Land/Region

Falls ein Land oder eine Region Einschränkungen dahingehend festlegt, welche Marke und welches Modell von Geräten innerhalb seiner Grenzen verwendet werden dürfen, wird die untenstehende Tabelle aktualisiert:

Land/Region	Gerätehersteller	Gerätemodell
-------------	------------------	--------------

Australien	Ingenico	Lane 5000, Move 5000
Australien	IDTech	SREDKey v2

Anhang A: Antrag des Händlers auf Opt-Out

Dieser Opt-Out-Antrag muss von einem autorisierten Händlervertreter unterzeichnet werden, wie in den Unterlagen von FreedomPay hinterlegt. Bevor ein Merchant-Opt-Out-Antrag eingereicht wird, wenden Sie sich bitte an den technischen Support von FreedomPay, um Anweisungen zum Opt-Out zu erhalten. Der technische Support überprüft den autorisierten Händlervertreter und stellt eine Vorgangsnummer (Incident Number) bereit.

Vorgangsnummer (falls zutreffend): _____

Datum des Opt-Out-Antrags: _____

Der unterzeichnende Händler entscheidet sich hiermit für den Opt-Out aus der FreedomPay P2PE Solution. Mit der Unterzeichnung dieses Antrags bestätigt der Händler, dass:

1. Transaktionen, die während eines wirksamen Opt-Outs verarbeitet werden, nicht der Reduzierung des P2PE-Prüfumfanges unterliegen.
2. der Händler allein dafür verantwortlich ist, anstelle der FreedomPay P2PE Solution alternative Kontrollen zum Schutz von Kontodaten zu implementieren.
3. der Händler verpflichtet ist, seinen Acquirer oder die Zahlungsmarke darüber zu informieren, dass der Händler aus der FreedomPay P2PE Solution ausgetreten ist (Opt-Out).
4. FREEDOMPAY SCHLIESST JEGICHE ZUSICHERUNGEN UND GEWÄHRLEISTUNGEN IN BEZUG AUF DIE FREEDOMPAY P2PE SOLUTION FÜR JEDE TRANSAKTION AUS, DIE WÄHREND EINES WIRKSAMEN OPT-OUTS VERARBEITET WIRD.
5. FREEDOMPAY SCHLIESST JEGICHE HAFTUNG AUS, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF EINE DATENPANNE, DIE DARAUS RESULTIERT, DASS DER HÄNDLER ZAHLUNGEN ANDERS ALS ÜBER DIE VALIDIERTE P2PE-LÖSUNG VON FREEDOMPAY UND DIE FREEDOMPAY COMMERCE PLATFORM VERARBEITET.
6. Der Händler hat ab dem Zeitpunkt des Opt-Outs 60 Tage („Opt-Out-Frist“), um die Bedingungen zu beheben, die den Opt-Out ausgelöst haben, und sich erneut für die Lösung anzumelden, sofern zwischen FreedomPay und dem Händler nicht schriftlich eine andere Opt-Out-Frist einvernehmlich vereinbart wird. Nach Ablauf der Opt-Out-Frist kann der Händler auf unbestimmte Zeit von der Verarbeitung von Transaktionen auf der FreedomPay Commerce Platform ausgeschlossen werden.

Hinweis: Nach dem Opt-Out kann sich ein Händler vorbehaltlich der von FreedomPay festgelegten Sicherheitsprotokolle erneut für die FreedomPay P2PE Scope Reduction Solution anmelden, einschließlich einer Bestätigung des Händlers, dass alle Reste von Klartext-Kartendaten mithilfe sicherer Datenlöschverfahren aus den Systemen des Händlers gelöscht wurden.

Händler: _____

Unterschrift: _____

(Name des autorisierten Händlerpersonals – in Druckschrift)

Name: _____

Position: _____

(Name des autorisierten Händlerpersonals – Unterschrift)

Bitte senden Sie dieses Formular per E-Mail an: compliance@freedompay.com

Anhang C: Beispiele zur Identifizierung der Seriennummern von POI-Geräten

Die untenstehenden Abbildungen zeigen einige Beispiele für POI-Geräte verschiedener Hersteller und die physische Position der Seriennummern, die von Key Injection Facilities zum Zweck der POI-Inspektion, -Verifizierung oder RMA angebracht werden (die bei der Suche oder Zuordnung der Seriennummer weiterhelfen können). Bei weiteren Fragen zu den Seriennummern von POI-Geräten wenden Sie sich bitte an compliance@freedompay.com.

Ingenico Lane 3000



Quantum Pay Reader 250



Ziosk

