xplor pay



P2PE
Instruction Manual
v3.

Release Date: 19-Jan-2024
Document Revision: 4.0

Revision History

The following details changes made to the PIM guide for the Xplor Pay P2PE Solution. This guide is updated for changes to the solution and for any changes to the P2PE standard as published by the PCI SSC. Changes to the PIM will be issued to a point of contact.

Document Version	Date of Change	Responsible Party	Change Description
1.0	08/2017	Juan Espinosa	Initial Release
2.3	11/2017	Juan Espinosa	• Updated for P2PE Audit ○ Added Glossary ○ Pics of P2PE devices ○ Skimming and tampering section
2.4	2/2019	Juan Espinosa	Added new ID Tech devices
2.5	09/2019	Juan Espinosa	Added new PAX & ID Tech devices
2.6	03/2020	Juan Espinosa	Added new PAX
2.7	12-Dec-2020	Juan Espinosa	Formatted into new P2PE 3.0 PIM layout
3.0	15-Jan-2021	Juan Espinosa	Updated post P2PE evaluation to address typos and formatting
3.1	04-Aug-2021	Hollie Brough	Added new PAX device
4.0	19-Jan-2024	Hollie Downen	General editing and clean up for P2PE 3.1 release. Added newly supported PAX and Wizarpos terminals. Removed unsupported devices.

Xplor Technologies - CONFIDENTIAL

1. P2PE Solution Information and Solution Provider Contact Details

1.1 P2PE Solution Information	
Solution name:	Xplor Pay P2PE Solution
Solution reference number per PCI SSC website:	2021-01151.002

1.2 Solution Provider Contact Information	
Company name:	*Xplor Pay LLC*
Company address:	*11330 Olive Blvd. Suite 200 Creve Coeur MO 63141*
Company URL:	*www.xplorpay.com*
Contact name:	*Hollie Downen*
Contact phone number:	*314.732.0515*
Contact e-mail address:	hollie.downen@xplortechnologies.com

P2PE and PCI DSS

Merchants using this P2PE solution may be required to validate PCI DSS compliance and should be aware of their applicable PCI DSS requirements. Merchants should contact their acquirer or payment brands to determine their PCI DSS validation requirements.

2. Confirm Devices were not tampered with and confirm the identity of any third-party personnel

2.1 Instructions for ensuring POI devices originate from trusted sites/locations only.

Xplor Pay and its partners take all necessary precautions to ensure devices are not tampered with or compromised prior to being shipped to you. However, there are steps that you must undertake to ensure that devices have not been tampered with during transit.

First you must confirm that shipment of devices originated from one of the following Key Injection Facility:

- The Phoenix Group
- PAX Computer Technology (Shenzhen) Co. LTD

All shipments of devices to you will be made through a shipping partner that provides tracking of packages. Primary shipping partners are FedEx and UPS.

To remain compliant, you may only deploy POI devices that are shipped from one of the PCI P2PE Component Solution Providers. Confirmation that devices were shipped from an authorized source may be performed by comparing the providers shipping information with the information listed above.

If you receive POI devices from another provider, you must contact us at support@xplorpay.com for confirmation. We will take necessary steps to communicate with you if our list of providers of POI devices has changed.

2.2 Instructions for confirming POI device and packaging were not tampered with, and for establishing secure, confirmed communications with the solution provider.

You must implement procedures for the detection of unauthorized alterations or replacement of devices prior to use and once deployed. This is imperative to maintaining the security of the P2PE solution and in enabling you to maintain your PCI DSS compliance.

Xplor Pay or our authorized KIF partners directly ship supported POI device directly to a merchant. No other location will be utilized to send P2PE supported POI Devices. To remain compliant, you may only deploy POI devices that are shipped from directly from an authorized source. If you receive POI device from somewhere else, you must contact us for confirmation. We will take necessary steps to communicate with you shipping origination changes. Regardless, if you cannot confirm the device was shipped from an authorized source, **DO NOT** deploy the device.

To ensure the POI device originate from and are only shipped to trusted sites and locations, the serial numbers on the terminal, the boxes the terminals are in, and the invoice provided for the terminals must all match. Signature upon receipt of the terminals should be required by the shipping method and the logistics provider. Only authorized signers should receive terminals. The addresses on all shipping labels should only match those of trusted sites and locations and should match those locations listed on the invoice.

In addition to confirm shipping origination, you must confirm that neither the packaging nor the device has been tampered with. All POI devices will be shipped using tamper-evident packaging. This packing will be evident on the shipping package itself and internally. See below for pictures depicting packaging materials:

- Sealed Silver Bags with tamper evident tape as shown below.



- Tamper Evident Tape used on all seams of the box





If you believe the packaging or the device has been tampered with, **DO NOT** deploy the device. You must also inspect the device. You should look for broken security seals and cracks around device's seals to determine if the POI device itself has been compromised. Pictures of each device type

supported are provided in Appendix B to aid in your inspections.

Prior to deployment of device for use, the deployment location must validate that the device received has not been tampered with or substituted. While awaiting deployment, the device must be deployed in a secure storage location with restricted access. Though the storage location of devices within your control is your responsibility, the location must include the following measures:

1) Device must be stored in locked room or container;
2) Device must remain in its original, tamper-evident packaging or in a physically secure storage until ready for use;
3) Storage location must support restricted access;
4) Must restrict access to authorized personnel. Example include:
    a. Door/Container requiring key access in which defined personnel have access to the key; or
    b. Door/Container required knowledge of cipherlock code in which defined personnel have knowledge of the cipherlock code.
5) Access to room or container storing device must be logged. This logging may be manual (written access log) or automatic (proximity card system that records access);
6) Access to room must be monitored (Cameras or physical sight).

Once the device is removed from storage and is being prepped for deployment, the following steps must be implemented:

1) The serial number on the devices must be matched with the recorded serial number of the device removed from storage and shipped to the location. This information must be recorded within inventory tracking at the deployment location and at the shipping location at the time of deployment;
2) A pre-installation of the device must be performed to ensure the device has not been tampered with. This must include physical inspection of the device to search for breakage of seal and security tampering seals; and
3) Prior to finally deployment into production, functionality must be tested to ensure that the device communicates and captures data properly.

Special Note: It is recommended that a list of device and serial numbers approved for a defined location be delivered to the location separate from the devices themselves. This will circumvent an individual from being able to substitute devices with differing serial numbers and updating the inventory list to reflect the compromised devices.

Once POI devices have been deployed, periodic inspection must be made at deployment locations to ensure devices have not been tampered with or substituted. The type of location for deployment will drive the frequency for inspections. For high traffic, visible areas such as storefronts, it is recommended inspections occur twice a year. For locations that are remote or unattended, it is recommended that inspections occur at least every ninety (90) days.

When inspecting devices, the first step should be to compare the serial number of the device with the serial number recorded for the location. If the serial numbers do not match, this could be the result of an unauthorized substitution. The individual should contact the personnel responsible for the storage, shipping, and installation of the POI device to confirm if the documentation is incorrect or if indeed a device has been substituted. Once the serial number has been confirmed, the device should undergo a physical inspection for tampering. Tamper and security seals should be examined to see if the seals are broken. The connection to the device should be inspected to ensure no extraneous devices are attached. The device should be inspected for missing screws, holes, or the addition of labels or covering that could be used to mask damage. Finally, the card DIP or magnetic stripe reader of the

POI device should be investigated to ensure a “skimmer” or other type of device has not been inserted.
Physically secure POI devices in your possession, including devices: ▪ Awaiting deployment ▪ Undergoing repair or otherwise not in use ▪ Waiting transport between sites/locations

2.3 Instructions to confirm the business need for, and identities of, any third-party personnel claiming to be support or repair personnel, prior to granting those personnel access to POI devices.

Access to POI devices by third-party personnel for repair/maintenance must be monitored. This monitoring is required to ensure there is no unauthorized access to device that could result in tampering, theft, or substitution of the device. To ensure proper third-party access monitoring, you must have a policy in place that requires the following steps:

1) Maintenance/repair of the device must be pre-arranged with date and timeframe of third-party personnel defined. Unexpected visits for repair/maintenance must be verified. If they cannot be verified, access to the device must be denied;
2) Prior to granting access to a device, personnel must be identified and authorized to access the device;
3) Third-party personnel access must be recorded and include personnel name, company, time of access, and purpose of access. Log must be maintained for no less than one year;
4) Personnel must be escorted and observed at all times; and
5) Personnel may not remove or replace a device without prior authorization. If authorized, new devices must be properly inspected and inventoried.

3. Approved POI Devices, Applications/Software, and the Merchant Inventory

3.1 POI Device Details

The following information lists the details of the PCI-approved POI devices approved for use in this P2PE solution.

All POI device information can be verified by visiting:
https://www.pcisecuritystandards.org/approved_companies_providers/approved_pin_transaction_security.php

See also Section 9.2, "Instructions for how to confirm hardware, firmware, and application versions on POI devices."

PCI PTS approval #:	POI device vendor:	POI device model name and number:	Hardware version #(s):	Firmware version #(s):
4-30301	PAX Computer Technology (Shenzhen) Co LTD	A80	A80-xxx-0x5-1xxx (without CTLS) A80-xxx-Rx5-1xxx (with CTLS)	25.02.xxxx
4-30224	PAX Computer Technology (Shenzhen) Co LTD	S300	S300-xxx-3x4-0xxx (with CTLS) S300-xxx-0x4-0xxx (w/o CTLS)	14.01.xx xxxx
4-30162	PAX Computer Technology (Shenzhen) Co LTD	Px5	0 no CTLS support) PX5-xxx-ax4-0xxx (a=R CTLS support	14.00.xx Boot: 2.0.x Boot: 3.0.xx.xxxx Firmware: 14.01.xx xxxx Firmware: 14.02.xx xxxx
4-40187	PAX Computer Technology (Shenzhen) Co LTD	SP30	CTLS SP30-xxx-0x4-0xxx Non CTLS SP30-xxx-2x4-0xxx	4.00.xx
4-40183	PAX Computer Technology (Shenzhen) Co LTD	A920	A920-xxx-xx4-0xxx	24.00.xxxx
4-40215	PAX Computer Technology (Shenzhen) Co LTD	A920	A920-xxx-Rx5-3xxx (CTLS) A920-xxx-0x5-3xxx (NON-CTLS)	25.03.xxxx
4-40184	PAX Computer Technology (Shenzhen) Co LTD	S80	S80-xxx-0x4-0xxx (Non CTLS) S80-xxx-3x4-0xxx (CTLS support)	4.01.xx
4-40305	PAX Computer Technology (Shenzhen) Co LTD	A35	A35-xxx-0x6-Axxx (No CTLS reader) A35-xxx-Rx6-Axxx (CTLS reader)	26.00.xxxx

4-40273	PAX Computer Technology (Shenzhen) Co LTD	A920pro	A920Pro-xxx-Rx5-3xxx (CTLS) A920Pro-xxx-Rx5-3xxx (NON-CTLS)	25.03.xxxx
4-40333	PAX Computer Technology (Shenzhen) Co LTD	A920pro	A920Pro-xxx-0x6-0xxx (NON-CTLS) A920Pro-xxx-Rx6-0xxx (CTLS)	26.00.xxxx
4-90100	PAX Computer Technology (Shenzhen) Co LTD	Q25	Q25-xxx-0x5-Axxx (Non CTLS) Q25-xxx-Rx5-Axxx (CTLS)	15.00.xx xxxx
4-40376	PAX Computer Technology (Shenzhen) Co LTD	Q25	Q25-xxx-Rx6-Bxxx	16.00.xx xxxxx
4-30371	PAX Computer Technology (Shenzhen) Co LTD	IM30	IM30-xxx-0x5-0xxx (without CTLS) IM30-xxx-Rx5-0xxx (with CTLS)	25.00.xxxx
4-40372	PAX Computer Technology (Shenzhen) Co LTD	IM30	IM30-xxx-0x6-Axxx (NON-CTLS) IM30-xxx-Rx6-Axxx (CTLS)	26.00.xx xxxxx
4-40195	Castles Technology Co. LTD	VEGA3000	VEGA3000-HW-v1.3.xxxx	xxxx-xxxx-xxxx-xxxx-0027
4-30332	Castles Technology Co. LTD	VEGA3000	VEGA3000-HW-V1.4.xxxx-A (Telit GPRS) VEGA3000-HW-V1.4.xxxx-E (Quectel GPRS)	002x-002x-003x-xx19 xx28-xx35-xx32-xx20
4-40159	Castles Technology Co. LTD	MP200	MP200-HW-v1.02	xxxx-xxxx-xxxx-0025
4-40173	Castles Technology Co. LTD	MP200	MP200-HW-v1.05	xxxx-xxxx-xxxx-0026
4-80053	Castles Technology Co. LTD	MP200	MP200-HW-v1.05	xx1x-xx1x-xx2x-xx23-0028
4-10156	ID Tech	SREDKey	IDSK-53XXXXXXX	SRED: 1.01
4-90075	ID Tech	SREDKey 2	80172006 (With MSR)	SREDKey2 FW v2.00.xxx.xxxx.S
4-10218	ID Tech	Augusta S	IDEM-8xxxx	V1.03.xxx.S
4-10184	ID Tech	SecuRED	IDSR-38xxxxxx	V2.01

Xplor Technologies - CONFIDENTIAL

4-30368	ID Tech	VP3320, VP3820	80173001	VP3320 FW v1.01.xxx.xxxx.S
4-90025	WIZARPOS International Co. Ltd.	WIZARPOS Q2	1.0	1.0.x

Xplor Technologies - CONFIDENTIAL

3.2 POI Software/Application Details

The following information lists the details of all software/applications (both P2PE applications and P2PE non-payment software) on POI devices used in this P2PE solution.

All applications with access to clear-text account data must be reviewed according to Domain 2 and are included in the P2PE solution listing. These applications may also be optionally included in the PCI P2PE list of Validated P2PE Applications list at vendor or solution provider discretion.

Application Vendor, Name, and Version #	POI Device Vendor	POI Device Model Name(s) and Number:	POI Device Hardware & Firmware Version #	Is Application PCI Listed? (Y/N)	Does Application Have Access to Clear-text Account Data (Y/N)
Xplor Pay LLC PAX_EMV 2.0	PAX Computer Technology (Shenzhen) Co LTD	A80	A80-xxx-0x5-1xxx (without CTLS) A80-xxx-Rx5-1xxx (with CTLS) 25.02.xxxx	N	N
Xplor Pay LLC PAX_EMV 2.0	PAX Computer Technology (Shenzhen) Co LTD	S300	S300-xxx-3x4-0xxx (with CTLS) S300-xxx-0x4-0xxx (w/o CTLS) 14.01.xx xxxx	N	N
Xplor Pay LLC PAX_EMV 2.0	PAX Computer Technology (Shenzhen) Co LTD	Px5	0 no CTLS support) PX5-xxx-ax4-0xxx (a=R CTLS support 14.00.xx Boot: 2.0.x Boot: 3.0.xx.xxxx Firmware: 14.01.xx xxxx Firmware: 14.02.xx xxxx	N	N
Xplor Pay LLC PAX_EMV 2.0	PAX Computer Technology (Shenzhen) Co LTD	SP30	CTLS SP30-xxx-0x4-0xxx Non CTLS SP30-xxx-2x4-0xxx 4.00.xx	N	N
Xplor Pay LLC PAX_EMV 2.0	PAX Computer Technology (Shenzhen) Co LTD	A920	A920-xxx-xx4-0xxx 24.00.xxxx	N	N
Xplor Pay LLC PAX_EMV 2.0	PAX Computer Technology	A920	A920-xxx-Rx5-3xxx (CTLS) A920-xxx-0x5-3xxx (NON-CTLS)	N	N

3.2 POI Software/Application Details					
	(Shenzhen) Co LTD		25.03.xxxx		
Xplor Pay LLC PAX_EMV 2.0	PAX Computer Technology (Shenzhen) Co LTD	S80	S80-xxx-0x4-0xxx (Non CTLS) S80-xxx-3x4-0xxx (CTLS support) 4.01.xx	N	N
Xplor Pay LLC PAX_EMV 2.0	PAX Computer Technology (Shenzhen) Co LTD	A35	A35-xxx-0x6-Axxx (No CTLS reader) A35-xxx-Rx6-Axxx (CTLS reader) 26.00.xxxx	N	N
Xplor Pay LLC PAX_EMV 2.0	PAX Computer Technology (Shenzhen) Co LTD	A920pro	A920Pro-xxx-Rx5-3xxx (CTLS) A920Pro-xxx-Rx5-3xxx (NON-CTLS) 25.03.xxxx	N	N
Xplor Pay LLC PAX_EMV 2.0	PAX Computer Technology (Shenzhen) Co LTD	A920pro	A920Pro-xxx-0x6-0xxx (NON-CTLS) A920Pro-xxx-Rx6-0xxx (CTLS) 26.00.xxxx	N	N
Xplor Pay LLC PAX_EMV 2.0	PAX Computer Technology (Shenzhen) Co LTD	Q25	Q25-xxx-0x5-Axxx (Non CTLS) Q25-xxx-Rx5-Axxx (CTLS) 15.00.xx xxxx	N	N
Xplor Pay LLC PAX_EMV 2.0	PAX Computer Technology (Shenzhen) Co LTD	Q25	Q25-xxx-Rx6-Bxxx 16.00.xx xxxxx	N	N
Xplor Pay LLC PAX_EMV 2.0	PAX Computer Technology (Shenzhen) Co LTD	IM30	IM30-xxx-0x5-0xxx (without CTLS) IM30-xxx-Rx5-0xxx (with CTLS) 25.00.xxxx	N	N
Xplor Pay LLC PAX_EMV 2.0	PAX Computer Technology	IM30	IM30-xxx-0x6-Axxx (NON-CTLS) IM30-xxx-Rx6-Axxx (CTLS)	N	N

Xplor Technologies - CONFIDENTIAL

3.2 POI Software/Application Details					
	(Shenzhen) Co LTD		26.00.xx xxxxx		
Xplor Pay LLC CASTLE_EMV 2.0	Castles Technology Co. LTD	VEGA3000	VEGA3000-HW-v1.3.xxxx xxxx-xxxx-xxxx-xxxx-0027	N	N
Xplor Pay LLC CASTLE_EMV 2.0	Castles Technology Co. LTD	VEGA3000	VEGA3000-HW-V1.4.xxxx-A (Telit GPRS) VEGA3000-HW-V1.4.xxxx-E (Quectel GPRS) 002x-002x-003x-xx19 xx28-xx35-xx32-xx20	N	N
Xplor Pay LLC CASTLE_EMV 2.0	Castles Technology Co. LTD	MP200	MP200-HW-v1.02 xxxx-xxxx-xxxx-0025	N	N
Xplor Pay LLC CASTLE_EMV 2.0	Castles Technology Co. LTD	MP200	MP200-HW-v1.05 xxxx-xxxx-xxxx-0026	N	N
Xplor Pay LLC CASTLE_EMV 2.0	Castles Technology Co. LTD	MP200	MP200-HW-v1.05 xx1x-xx1x-xx2x-xx23-0028	N	N
Xplor Pay LLC IDTECH_EMV 2.0	ID Tech	SREDKey	IDSK-53XXXXXXX SRED: 1.01	N	N
Xplor Pay LLC IDTECH_EMV 2.0	ID Tech	SREDKey 2	80172006 (With MSR) SREDKey2 FW v2.00.xxx.xxxx.S	N	N
Xplor Pay LLC IDTECH_EMV 2.0	ID Tech	Augusta S	IDEM-8xxxx V1.03.xxx.S	N	N
Xplor Pay LLC IDTECH_EMV 2.0	ID Tech	SecuRED	IDSR-38xxxxxx V2.01	N	N
Xplor Pay LLC IDTECH_EMV 2.0	ID Tech	VP3320, VP3820	80173001 VP3320 FW v1.01.xxx.xxxx.S	N	N
Xplor Pay LLC WIZARPOS_EMV 2.0	WIZARPOS International Co. Ltd.	WIZARPOS Q2	1.0 1.0.x	N	N

Xplor Technologies - CONFIDENTIAL

Xplor Technologies - CONFIDENTIAL

3.3 POI Inventory & Monitoring

- All POI devices must be documented via inventory control and monitoring procedures, including device status (deployed, awaiting deployment, undergoing repair or otherwise not in use, or in transit).
- This inventory must be performed annually, at a minimum.
- Any variances in inventory, including missing or substituted POI devices, must be reported to **Xplor Pay** via the contact information in Section 1.2 above.
- Sample inventory table below is for illustrative purposes only. The actual inventory should be captured and maintained by the merchant in an external document.

For you to maintain your compliance you must maintain an inventory of the provided POI devices. You must track which devices are deployed, which are awaiting deployment, those that have been removed from service for repair or otherwise not in use, and those in transit for deployment or return for repair. It is recommended that you designate Job Role or personnel responsible for maintaining the POI inventory and for inspection of devices.

For each area identified the following information must be recorded. It is recommended that you record this information upon receipt of your POI device and then update the location of each device as it transitions from storage, transit, deployment, and repair or return.

- Manufacturer of device
- Make and Model of device
- Serial Number of Device
- Internal Inventory Number; (if applicable)
- General Description of Device (Color, Secure Seals, Labels, Hidden Marking, etc.)
- Number and type of physical connections (Network, Serial, etc.)
- Firmware version
- Hardware version
- Device Location (Storage, Where Deployed, In Transit, Awaiting Repairs or Returned)
- Date of Location Inspection (Last Date device location was confirmed)
- Date of Last Inspection (last date device was inspected for tampering)
- Name of Job Role or personnel performing inspection
- Date inventory was last updated

Device identification can be found on the PTS POI device itself. Generally, this information is contained upon a manufacturer provided label located on the back or side of the device.

Device inventories are to be performed no less than annually to confirm that inventory of devices is being catalogued and performed correctly; however, inventory must be updated as device transition in and out of service and from one location to another. This inventory must also be completed to confirm that all devices identified as being within your environment are currently within your possession and not missing.

Access to device inventory and to the devices themselves must be restricted to authorized personnel. The method for maintaining a device inventory is determined by you; however, the method utilized must enable you to restrict access to the inventory tracking information and allow you to record who has had access to the inventory tracking information. Failure to do so will impact your PCI DSS compliance. In addition, you must be able to restrict access to stored devices and record who has accessed said devices and when access occurred.

During your inventory process, you must investigate the POI devices to identify unauthorized removal, tampering, or substitution of devices. Detection of these events may be an indication of a compromise of your environment. Inspection of device should compare information located on the device itself with the inventory information previously recorded. In addition, the inspection should look for indications that the device has been tampered with. Indications of tampering may include, but is not limited to, attachment of unauthorized devices to the POI device, breakage of security seals, cracks within the seal of the device itself, or insertion of a "skimmer" device within the Magnetic Stripe Reader (MSR) of the device. Skimmers are devices used by attackers to capture cardholder data prior to the POI device reading the card. Skimmers may be inserted in the MSR of the device or overlaid on the device itself. It is recommended that you train personnel (Cashiers/Managers) interfacing with the POI devices on a regular basis to inspect deployed POI devices daily.

Should you detect a compromised device or find that your inventory indicated a missing or substituted device, you must report this information to the device provider immediately.

For device being stored, be it prior to deployment, shipment, or awaiting repairs, they must be stored in a secure area with restricted access to ensure they are not tampered with. Though the storage location of devices within your control is your responsibility, the location must include the following measures:

1) Device must be stored in locked room or container
2) Storage location must support restricted access
3) Must restrict access to authorized personnel. Examples include:
    a. Door/Container requiring key access in which defined personnel have access to the key; or
    b. Door/Container required knowledge of cipherlock code in which defined personnel have knowledge of the cipherlock code.
4) Access to room or container storing device must be logged. This logging may be manual (written access log) or automatic (proximity card system that records access)
5) Access to room must be monitored (Cameras or physical sight).

In addition to keeping records of all device serial numbers and updating as needed, please follow the guidelines below. This includes installed devices and devices in storage.

- Take photographs from all angles of each device, including any labels or serial numbers on the device.
- Use the original photographs to compare the devices on future inventory reviews. If the devices appear to be tampered with, please contact your Solution provider immediately.
- Record the location a device is deployed and match to the device serial number
- Record the exact details of any security labels on the device
- Record how the terminal is connected, including the style, type, and color of each connector. A photograph of the connectors is recommended.
- Mark each terminal with an ultra-violet (UV) security pen to provide a unique identifier for that terminal.

A sample inventory table is provided as follows.

Xplor Technologies - CONFIDENTIAL

Sample Inventory Table

Device Vendor	Device Model Name(s) and Number	Device Location	Device Status	Serial Number or Other Unique Identifier	Date of Inventory
ID Tech	SREDKEY 2	Store 1	Installed	568748	21-Oct-2023
PAX	Px5	Store 3	Installed	908987	21-Oct-2023

4. POI Device Installation Instructions

Do not connect non-approved cardholder data capture devices.

The P2PE solution is approved to include specific PCI-approved POI devices. Only these devices denoted above in Table 3.1 are allowed for cardholder data capture.

If a merchant's PCI-approved POI device is connected to a data capture mechanism that is not PCI approved, (for example, if a PCI-approved SCR was connected to a keypad that was not PCI-approved):

- The use of such mechanisms to collect PCI payment-card data could mean that more PCI DSS requirements are now applicable for the merchant.
-

Do not change or attempt to change device configurations or settings.

Changing device configurations or settings may invalidate the PCI-approved P2PE solution in its entirety. Examples include, but are not limited to:

- Enabling any device interfaces or data-capture mechanisms that were disabled on the P2PE solution POI device.
- Altering security configurations or authentication controls on the POI device.
- Physically opening the POI device.
- Attempting to install unauthorized applications onto the POI device.

4.1 Installation and connection instructions

It is imperative that you follow the guidelines detailed below for the deployment of the P2PE solution. Failure to do so may impact your PCI DSS compliance and the protections afforded to you by the P2PE solution.

Prior to deployment, you must understand that any modification to the deployment can and will impact your compliance. Such modifications may include:

- Attempting to enable any device interfaces or data-capture mechanisms that were disabled on the P2PE solution POI device
- Attempting to alter security configurations or authentication controls
- Physically opening the device
- Attempting to install applications onto the device

Also, understand if a PCI-approved POI component is connected to another device or data-capture mechanism, the non-PCI-approved capture mechanism is not secured by the P2PE solution, and the use of any such mechanisms to collect PCI payment-card data would negate any PCI DSS scope reduction which might otherwise have been provided by the P2PE solution's device.

The P2PE solution provided by Xplor Pay or our partners only includes those devices previously identified in section 3.1 of this manual. It does not allow for POI components that are not PCI approved.

Xplor Technologies - CONFIDENTIAL

The solution is intended to be deployed in a network enabled environment to communicate with the Xplor Pay gateway over the Internet. Because of this you should ensure your network is secure and meets PCI DSS requirements for a secure network environment. For example, a firewall is to be deployed to segment and secure your network from the Internet.

The first step is to install the Xplor Pay POI Bridge software on a supported O/S (Windows 7 SP1 or later). To install simply double click on the Xplor Pay POI Bridge Microsoft Installer Program downloaded from our support site. This will setup the bridge software that enables communication with the POI device to our P2PE gateway. Once this is installed you will need to connect your POI device. Only those POI devices listed in section 2.2 of this guide are supported. Based on the type of POI device you selected, will determine needed POI device to Xplor Pay POI Bridge software connectivity steps.

For POI devices using Serial or USB connectivity to the system running the Xplor Pay POI Bridge Software, connect the POI device to the workstation prior to powering on the device. Once the POI device is connected, plug in the device's power cord. The POI device will power up and the POI device and the bridge software will sync.

For POI devices using BlueTooth connectivity to the system running the Xplor Pay POI Bridge Software, you will need to enable BlueTooth on your workstation and pair the POI device to the workstation. Once you have a successful pairing, start up the Xplor Pay POI Bridge Software. The bridge software and the POI device will sync.

For POI Devices using the network (Ethernet or WiFi) to communicate to the system running the Xplor Pay POI Bridge software, you will need to connect the POI device to your network first. For WiFi, you will need to enter in the WiFi network parameters into the POI device to include the SSID and WiFi password. Note: you WiFi should be set to WPA2 or stronger parameters to meet PCI DSS requirement. For Ethernet, connect an Ethernet cable to the device and power on the device. You will need to enter a Static IP address into the POI Device. In the Xplor Pay POI Bridge software, you must define the ip-address and device type within the device settings interface of the software. Once defined, the software will sync with the POI device.

If no error message appears on the bridge software or the POI device screen, then installation is complete and you may proceed with accepting of payments. If a connection error appears on the screen after connecting the device to your network and powering on, please contact Xplor Pay LLC support.

If you have any issues connecting your POI devices, installing the software, or configuring the software, please contact Xplor Pay support.

Note: *Only PCI-approved POI devices listed in the PIM are allowed for use in the P2PE solution for account data capture.*

Xplor Technologies - CONFIDENTIAL

4.2 Guidance for selecting appropriate locations for deployed devices

Select an installation location appropriate to the device and with protection measures in mind:

- Control public access to devices such that device access is limited to only parts of the device a person is expected to use to complete a transaction (for example, PIN pad and card reader).
- Locate devices so they can be observed/monitored by authorized personnel—for example, during daily store checks of the devices performed by store/security staff.
- Locate devices in an environment that deters compromise attempts—for example, through lighting, access paths, visible security measures, etc.
- Do not install devices outside that are designed for indoor use only.
- The location selected should provide adequate ventilation and protection. The location should be free from excessive heat, dust, oil and moisture. The location should not be near any water source, running or standing.
- The terminal should be placed on a flat surface or mounted on a manufacturer supplied stand or wall mount per the manufacturer's instructions. The terminal should not be in direct sunlight or within 24 inches of devices that cause excessive voltage fluctuations, electrical noise or radiate heat. The terminal should be at least 6 feet from anti-theft doorway units and at least 18 inches from surface mounted deactivator pads.
- Position the terminal on the check-stand in such a way as to make visual observation of the PIN-entry process infeasible. Examples include:
    - Visual shields designed into the check-stand. The shields may be solely for shielding purposes or may be part of the general check-stand design.
    - Position the PIN Entry Device (device) so that it is angled in such a way that PIN spying is difficult. Installing device on an adjustable stand that allows consumers to swivel the terminal sideways and/or tilt it forwards/backwards to a position that makes visual observation of the PIN-entry process difficult.
    - Position in-store security cameras so that the PIN-entry keypad is not visible.

The deployed POI devices should always be placed where the cardholder provides payment. For example, at a sales counter or a cashier lane. The POI device should always face the cardholder. For example, at a sales counter, the device would be placed on the counter facing away from the sales representative and towards where the customer would stand at the counter. The device should be in view of a surveillance camera, and staff should be able to see the device to prevent anyone from tampering with the device, **however,** steps should be taken to ensure surveillance/CCTV cameras and staff cannot see the screen or the PIN entry pad on the device.

Xplor Technologies - CONFIDENTIAL

4.3 Guidance for physically securing deployed devices to prevent unauthorized removal or substitution

Merchants should physically secure devices to prevent unauthorized removal or substitution while devices are deployed for use.

This includes both attended and unattended devices, as applicable to the P2PE solution (for example, kiosks, “pay-at-the-pump,” etc.).

If the devices cannot be physically secured (such as wireless or handheld devices):

- Secure devices in a locked room when not in use.
- Assign responsibility to specific individuals when device is in use.
- Always observe devices.
- Sign devices in/out, etc.

Merchants should physically secure devices when not deployed or being used. Including devices:

- Undergoing repair or maintenance while in the merchant’s possession.
- Awaiting deployment.
- Awaiting transport between sites/locations.

Merchants should prevent unauthorized physical access to devices undergoing repair or maintenance while in their possession, to include the following:

- Verify the identity and authorization of repair personnel.
- All repair personnel must be verified and authorized prior to granting access.
- Unexpected personnel must be denied access unless fully validated and authorized.
- Escort and always monitor authorized personnel.

5. POI Device Transit

5.1 Instructions for securing POI devices intended for, and during, transit

When you are shipping devices to your location for deployment or for return, devices must be shipped securely. They must be packed in tamper-evident packaging and shipped in a secure manner. All device either being shipped to a location for deployment or for return, must be shipped using a secure transport method such as a secure courier or bonded carrier. For deployment to sites, it is permissible to use employees for transport; however, they must be authorized to deliver the devices and the recipient must be notified of who will be delivering the devices to them. Be it a bonded carrier, secure courier, or internal employee, you must log the following information:

1) Personnel providing shipping (if employee, record name and job role);
2) Date of pickup
3) Device being shipped
4) Confirmation Date of Site delivery

When packaging devices for transit, they must be packed in tamper-evident packaging. You determine the type of packaging; however, the recipient must be notified as to how to determine if the package has been tampered with during transit. As with your inspection of POI device received from us, your deployment sites must perform the same inspection on device shipped from your storage location. They must be notified of authorized shipping locations, notified of how the device will be shipped, and trained in how to inspect the packaging and device for tampering. For example, they must be trained to investigate for breakage of tamper-evident seals on the external packaging and to investigate the device itself for cracks or breakage of security seals. Finally, they must be instructed that if they receive devices without prior confirmation from the shipping location or they are delivered in a manner unexpected, they must confirm prior to deployment of the devices.

Special Note: If using internal employees for device shipment, they must be instructed to not leave devices in public areas unattended, for example, in the front or back seat of a car. This may lead to unauthorized access or theft of the device.

Physically secure POI devices in your possession, including devices:

- Awaiting deployment
- Undergoing repair or otherwise not in use
- Waiting transport between sites/locations

Xplor Technologies - CONFIDENTIAL

5.2 Instructions for ensuring POI devices are shipped to, trusted sites/locations only

When devices are removed from service either for repair, being returned, being replaced, or being returned to storage, this must be done in a manner that allows for the tracking and security of the device. The following initial steps are required regardless of the reason a device is removed from service:

1) Removal of device must be pre-arranged prior to removal;
2) Location of device removal must confirm personnel removing device are authorized;
3) Personnel performing removal must be documented to include name, company, and time of removal; and
4) Inventory must be updated to indicate that the device was removed and reason for removal.

If the device is to remain at the deployment location for future deployment, the device must be securely stored at the location in a manner as described earlier within this manual.

If the device is to be returned to your shipping location, the device must be packed in a tamper-evident package and shipped using an authorized source that can be tracked. Methods for shipping and tracking are described in previous sections of this manual.

If the device is to be returned to us for repair or replacement, you must take the following steps:

1) Perform the Steps provided to you via the support contact below or the documentation you received with the device to wipe the device of all sensitive data.
2) Pack the device within a tamper-evident packaging; and
3) Notify us that the device is being returned. You will need to provide us the serial number of the device and a tracking number of the package as provided by the carrier. We can be contacted at: **Customer Support:** Support at 866.435.0666

6. POI Device Tamper & Modification Guidance

6.1 Instructions for physically inspecting POI devices and preventing skimming, including instructions and contact details for reporting any suspicious activity

Additional guidance for inspecting POI devices can be found in the document entitled *Skimming Prevention: Best Practices for Merchants,* available at www.pcisecuritystandards.org.

During your inventory process, you must investigate the POI devices to identify unauthorized removal, tampering, or substitution of devices. Detection of these events may be an indication of a compromise of your environment. Inspection of device should compare information located on the device itself with the inventory information previously recorded. In addition, the inspection should look for indications that the device has been tampered with. Indications of tampering may include, but is not limited to, attachment of unauthorized devices to the POI device, breakage of security seals, cracks within the seal of the device itself, or insertion of a "skimmer" device within the Magnetic Stripe Reader (MSR) of the device. Skimmers are devices used by attackers to capture cardholder data prior to the POI device reading the card. Skimmers may be inserted in the MSR of the device or overlaid on the device itself. It is recommended that your training personnel (Cashiers/Managers) interfacing with the POI devices on a regular basis to inspect deployed POI devices daily.

To prevent skimming, record the appearance, condition, and location of each terminal. It is recommended to take photographs of each terminal from all angles to make comparisons. In addition, it is recommended that you weigh POI devices upon receipt and record this weight and periodically compare the results with vendor specifications to aid in identifying potential insertion of skimmers or other taping mechanisms within the device. Note: proper device weight can be found documented with the device manufacture's manual shipped with the device.

Regularly check the terminals to make sure they have not been tampered with. Follow the guidelines above in section 3.3 to physically secure the terminals. Always return the terminals to an authorized dealer, never throw the terminals away in the trash or a dumpster. Never allow a service engineer to service the terminal on any unplanned or unannounced visits. Always confirm the identity of a service engineer by contacting your solution provider. Use Appendix C in the Skimming Prevention: Best Practices for Merchants document to perform regular inspections. Please contact your solution provider immediately using the contact information in section 1.2 of this document to report any suspicious activity.

Please see Appendix C of this document for visual examples of tampered devices. Note: Appendix C: Supported Devices provides visual examples of devices that have not been tampered with for comparison purposes.

6.2 Instructions for responding to evidence of POI device tampering

If tampering is suspected, one should contact the personnel responsible for the storage, shipping, and installation of the POI device to report the tampering. The device should be taken offline. You should contact us (Xplor Pay) to report the tampering and we will provide remote assistance regarding the removal and return of the device for further investigation. We can be contacted at:

Customer Support: Support at 866.435.0666

7. Device Encryption Issues

7.1 Instructions for responding to POI device encryption failures

In the event of a device encryption failure, that device must not be re-enabled for use until merchant has confirmed that either:

- The issue is resolved and P2PE functions are restored and re-enabled.

OR

- All applicable PCI DSS controls are enabled and enforced within the environment to protect account data, since the P2PE solution can no longer be used to reduce PCI DSS scope.
- The merchant has provided written notification (signed by a merchant executive officer) formally requesting stopping of P2PE protection.

Though highly unlikely, there may be occasions where a device encryption failure occurs. For this type of event, we will contact your primary point of contact regarding the failure and work with you to troubleshoot the device based on the guidelines detailed in the "Troubleshooting" section of this manual. Once contacted regarding a device encryption failure and troubleshooting has failed to remedy the situation, you have two options available to you that include removing the device from us or you may choose to opt-out of using the P2PE solution.

We do not support a method for disabling P2PE encryption for the deployed hardware. We can transition you to a non-P2PE environment outside of this solution. This involves moving you to accepting manual entry only transactions into our Virtual Terminal interface.

If you elect to remove the failing device, you must contact the location affected and instruct them to discontinue use of the device and inform that the device will be removed from service. The removal of the device from service must follow the steps describe previously within this manual. Once the device is removed, it must be returned to the device provider for repair or disposal. Please see instruction within this manual regarding the returning of devices.

As previously stated, you may choose to opt-out of using the protection of the P2PE solution. However, this involves transitioning you to differing solution that is not P2PE validated. This involves moving you to our PCI DSS validated Virtual Terminal interface that will allow you to manually enter cardholder data. You will not be able to accept any card swipe or chip transactions through this interface.

If you choose to opt out, understand you accept the following responsibility:

1. The security impact to your account data and potential risks associated with processing transactions without P2PE protection.
2. Responsibility for implementing alternative controls to protect account data in lieu of the P2PE solution
3. That you are no longer eligible for the PCI DSS scope reduction afforded by the P2PE solution
4. You must advise your acquirer that you are no longer using the P2PE solution
5. That processing transactions without P2PE protection may impact your PCI DSS compliance validation and you should confirm with their acquirer or payment brand, as applicable, for all PCI payment brands affected.

If you chose to accept the responsibilities outlined above, you must first fax or email to us the Opt-Out

Xplor Technologies - CONFIDENTIAL

Form included within this manual in Appendix A. Upon receipt of the form, we will walk your designated personnel through the process for moving to a non-P2PE acceptance method.

To formally request that encryption of account data be stopped, the following information will be needed:

- Merchant ID
- Total number of devices
- Make and Model of devices
- Serial Numbers of all devices

8. POI Device Troubleshooting

8.1 Instructions for troubleshooting a POI device

In the event of an issue, we will work with you remotely to troubleshoot the issue. Prior to any troubleshooting, we will confirm that the individual contacting us is an authorized individual within your organization for troubleshooting purposes as defined to us during the initial deployment of the solution.

Begin by contacting Support at: 866.435.0666

During our troubleshooting process:

1) Primary Account Number or Sensitive Authentication Data will never be outputted to your systems;
2) We will only collect the Primary Account Number or Sensitive Authentication Data as need to resolve the issue;
3) Data collected will be encrypted upon storage;
4) Data will be stored in specific, known locations with access restricted to those individuals charged with resolving your issue;
5) We will only collect limited amounts of data needed to solve the issue; and
6) All data will be securely removed from storage immediately after use and the issue is resolved.

Our troubleshooting process consists of the following steps:

STEP 1

1. If this is a P2PE device then confirm that the end user has been authorized to troubleshoot this device. If they have not, then escalate it to someone who does.

STEP 2

1. If Error Code is showing on the device's display screen, using the manufacture's resources follow the troubleshooting guidelines.
2. Restart Xplor Pay Bridge and test
3. If success stop else follow the manufacturer's device replacement procedures

STEP 3

1. Verify that the cables are securely connected to the correct port.
2. Confirm that the device's indicator lights are properly illuminated.
3. Stop Xplor Pay Bridge
4. Power cycle the device by unplugging all the cables and plugging them back in
5. Start Xplor Pay Bridge and test
6. If success stop else continue to STEP 4

STEP 4

1. Stop Xplor Pay Bridge
2. Unplug all cables from the device
3. Reboot workstation
4. Plug all cables back into the device
5. Start Xplor Pay Bridge and test

6. If success stop else continue to STEP 5

STEP 5

1. Follow the manufacturer's process for reinstalling the drivers
2. Start Xplor Pay Bridge and test
3. If success stop else continue to STEP 6

STEP 6

1. Review the Xplor Pay Bridge and the operating system's event logs
2. Contact device manufacture's support line and have them troubleshoot

9. Additional Guidance

9.1 Instructions for Disposal of POI devices

Disposal of devices will be handled by Xplor Pay or our authorized parties. If you have device for disposal, please follow the instruction regarding the removal of a device for repair and return the device to us.

9.2 Instructions for how to confirm hardware, firmware, and application versions on POI devices

As the instructions for confirming hardware, firmware, and application versions of POI devices vary by device and manufacturer, please refer to the device manual provided with your POI device on steps needed to access menu to allow one to check hardware, firmware, and application versions. Also, many models will display this information upon start up.

Appendix A – P2PE-Opt out Form

Name of Company: _____

Name of Requestor: _____

Date of Request: _____

Serial Number of Device: _____

At this time, we formally request to be transitioned to a non-P2PE solution through the use of the Xplor Pay Virtual Terminal interface. The device with the Serial Number above will be removed from service and returned to Xplor Pay. We formally agree to assume the responsibility for:

1. The security impact to our account data and potential risks associated with processing transactions without P2PE protection.
2. For implementing alternative controls to protect account data in lieu of the P2PE solution
3. That we are no longer eligible for the PCI DSS scope reduction afforded by the P2PE solution
4. We must advise our acquirer that we are no longer using the P2PE solution
5. That processing transactions without P2PE protection may impact our PCI DSS compliance validation and we should confirm with our acquirer or payment brand, as applicable, for all PCI payment brands affected.

Sincerely,

Customer Support: support@xplorpay.com

Appendix B – Visual Images of Supported Intact Devices

The following are images of supported intact devices to aid in your device inspections.

ID Tech Devices:		
SREDKey 2	SREDKey	Augusta S
		
SecuRED	VPP3320, VP3820	
		

Castles Technology Co. Ltd Device		
Vega3000	VEGA3000	MP200
		

Xplor Technologies - CONFIDENTIAL

PAX Computer Technology (Shenzhen) Co. Ltd devices		
A80	S300	Px5
		
A920	SP30	S80
		
A35	A920Pro	Q25
		

Xplor Technologies - CONFIDENTIAL

IM30		
		

Xplor Technologies - CONFIDENTIAL

WIZARPOS International Co. Ltd.		
WIZARPOS Q2		
		

Xplor Technologies - CONFIDENTIAL

Appendix C – Images of Tampered devices

The following are examples of tampered devices that will help identify if your devices have been tampered with.

<table>
<tr>
<td>The images to the right depict a layover device that can be placed over a POI device to hide a skimmer. You can note that the device will be bigger than normal in order to hide the skimmer.

During inspections, you can attempt to tug on device covers to see if a layover device has been applied.</td>
<td>

</td>
</tr>
<tr>
<td>The pictures here depict tampered devices where one has inserted a device into the POI device. The top depicts a wire that has been inserted and a fake label overlays the keypad to hide it.

The bottom depicts a wire inserted into the chip reader slot.

When inspecting devices, one should check labels to confirm they are supposed to be there. One can run their finger along them looking for bumps or tears. Inspecting the chip slot is a must as one can insert a skimmer into the slot.</td>
<td>

</td>
</tr>
</table>

Xplor Technologies - CONFIDENTIAL

The device to the right has been tampered with and had the back removed and a skimmer inserted. Always check the back of devices to look for tampering. Attacker will remove the back of devices and insert devices. Check of strange labels and check all screws to ensure none are removed. Around screw locations, check for scratches to see if someone may have opened the device.	
This is another example of a sticker hiding damage to a device. Always closely inspect stickers and labels to see if they have been removed. Run finger across the sticker to see if there are holes behind them.	 
Always check all security seals for wear and tear and tampering. Seals that look pulled back are an indication of tampering.	

These are just some examples of devices that have been tampered. Remember you POI device should only be physically connected to the network or a computer. Review the list of equipment that can be attached to a device and confirm that those are the only things connected. Strange device or wires attached to a device are a sign of tampering.

Appendix D – Glossary

Account Data - Account data consists of cardholder data and/or sensitive authentication data

Authorization - occurs when a merchant receives transaction approval after the acquirer validates the transaction with the issuer/processor.

BlueTooth - short-range wireless interconnection of mobile phones, computers, and other electronic devices.

Cardholder Data - At a minimum, cardholder data contains the full PAN. Cardholder data may also appear in the form of the full PAN plus any of the following: Cardholder name, Expiration date, Service code See Sensitive authentication data (SAD) for additional data elements that may be transmitted or processed as part of a payment transaction.

Cellular – Communication across mobile phone network requiring data connectivity.

Compromise - A violation of the security of a system such that an unauthorized disclosure of sensitive information may have occurred. This includes the unauthorized disclosure, modification, substitution, or use of sensitive data (including clear-text cryptographic keys and other keying material).

Encryption - The (reversible) transformation of data by a cryptographic algorithm to produce cipher text—i.e., hiding the information content of the data.

Firmware - Firmware is considered to be any code within the POI device that provides security protections needed to comply with PTS device security requirements or can impact compliance to these security requirements.

KIF – Key Injection Facility. Entities that perform cryptographic key injection for POI Devices.

PCI P2PE – Point to Point Encryption standard

PCI SSC – Payment Card Industry Security Standards Council

PED - A PED is a device for secure PIN entry and processing. The PED typically consists of a keypad for PIN entry, laid out in a prescribed format, a display for user interaction, a processor, and storage for PIN processing sufficiently secure for the key-management scheme used and firmware. A PED has a clearly defined physical and logical boundary and a tamper-resistant or tamper-evident shell.

PIM – P2PE Implementation Manual

POI Device – Point of Interaction Device. Device used to accept payment card data for payment purposes. The initial point where data is read from a card.

P2PE Solution - A combination of secure devices, applications, and processes that encrypt cardholder data from a PCI-approved point-of-interaction (POI) device through to decryption, assessed in accordance with PCI's P2PE standard and included on PCI's list of Validated P2PE Solutions.

SRED – A set of PTS POI requirements that provide a standardized approach to protecting account data in POI devices. SRED requirements cover all methods of account-data entry supported by the POI device, and include physically and logically protecting account data within the device, protecting any associated sensitive data or functions, and providing for the encryption of account data before transmission outside the device.

Xplor Pay POI Bridge – Software operating a workstation to aid in device communication

Tamper Evident Tape – Tape with a characteristic that provides evidence that an attack has been attempted such as trying to open a package.

WiFi – Wireless network