



Payment Card Industry (PCI) Point-to-Point Encryption



P2PE Instruction Manual (PIM) for the PAX A920 Pro Terminal

August 2023

Revision History

Version	Date	Author	Description of Change
1.0	September 2018	Jessica Brick	Initial Creation of Document
2.0	August 2020	Theresa Burch	Update to current CyberSource branding
3.0	December 2020	Theresa Burch	Migrate to Template Version 3.0
3.0	June 2021	David Barnet	Changed Card_Present_Support@cybersource.com to Terminals@Cybersource.com
1.0	August 2021	David Barnet	Converted to a A920 ProPIM, Version 1.0
1.1	August 2023	David Barnet	Document Updates

1. P2PE Solution Information and Solution Provider Contact Details

1.1 P2PE Solution Information

Solution name:	Cybersource Point-To-Point (P2PE) Solution
Solution reference number per PCI SSC website:	2021-00035.002

1.2 Solution Provider Contact Information

Company name:	Cybersource Corporation
Company address:	900 Metro Center Blvd Foster City, CA 94404
Company URL:	www.cybersource.com
Contact name:	Customer Support
Contact phone number:	US Toll Free: +1 855-477-1184 Europe Toll Free: +442039012015
Contact e-mail address:	Terminals@cybersource.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.

Europe (including United Kingdom)

Devices for Europe are shipped out to you using transport DHL services provided by Secure Retail.

Any documentation received from Secure Retail will include their trademarked logo and address:

Service and Support:

Secure Retail Ltd
Walker Road
Bardon Hill, Coalville
Leicestershire LE67 1TU
United Kingdom
Telephone: +44 (0)1530 511150
Email: customerservices@secure-retail.com

United States

Devices for United States are shipped out to you using transport FedEx services provided by POS Portal.

Any documentation received from POS Portal will include their trademarked logo and address:

Service and Support:

POS Portal, Inc.
180 Promenade Circle, Suite 215
Sacramento, CA 95834
United States
Telephone: +1 (866) 940-4767
Email: yourfriends@posportal.com

The shipment can be tracked via a tracking number you will receive via email.

When receiving any package, compare the providers shipping information with the information received.

If the solution provider changes, notification will be sent to the merchant ahead of time via email on record.

If devices are received from any other provider, you must immediately notify Cybersource, the solution provider, and remove the devices from your environment.

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

You will receive a delivery note via email before receiving the shipment of the devices. Upon receipt of the devices, make sure to compare the serial number of the device and tamper evident bag against the serial numbers on the delivery note.

Once you have checked all devices, make sure to respond back to the email with acknowledgement of devices delivery

All POI devices will be shipped using tamper-evident packaging:



Indications of tampering would include:

1. A bag that has been opened and reclosed
2. A missing bar code on bag
3. A torn bag

Check the bag upon receipt and confirm that it has not been tampered with. If tampering is confirmed or even suspected, **DO NOT** deploy the device. Contact Cybersource immediately.

We recommend keeping the device in the original, tamper-evident packaging until ready for deployment.

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.

- 1) All support or repair of devices must be performed by authorized personnel
- 2) All repair personnel must be verified and authorized prior to granting access
- 3) Call Cybersource to confirm that the person at the store was authorized to perform the repair
- 4) Cybersource will verify the identity of the person at the store
- 5) Unexpected personnel must be denied access unless fully validated and authorized
- 6) Escort and monitor authorized personnel at all times

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):
4-40273	PAX Computer Technology (Shenzhen) Co Ltd	PAX A920 Pro	A920Pro-xxx-Rx5-1xxx (CTLS)	25.03.xxxx

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)
PAX, BroadPOS P2PE P2PE Version: v3.1 Version BroadPOS P2PE 1.01.xx	PAX Computer Technology (Shenzhen) Co Ltd	PAX A920 PRO	A920Pro-xxx-Rx5-1xxx (CTLS) Firmware Version #: 25.03.xxxx	Yes	Yes

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 Cybersource 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.

Securing the devices used for payment acceptance is crucial for your overall security solution. It begins with tracking all devices from the time that they are received until they are removed from service. Cybersource recommends inventory monitoring at regular intervals, and an audit of all devices must be performed at least once a year.

Best practice for device inventory monitoring and management is to assign a person or to assign inventory management responsibilities to a job function within your organization. The responsibility of the person is to inventory and track all devices in stores and to manage and report any discrepancies to Cybersource. This practice ensures that inventory management is performed as Cybersource recommends.

The merchant can choose to automate device inventory tracking by using software tools or on paper. The chosen tracking method must contain at least the following information:

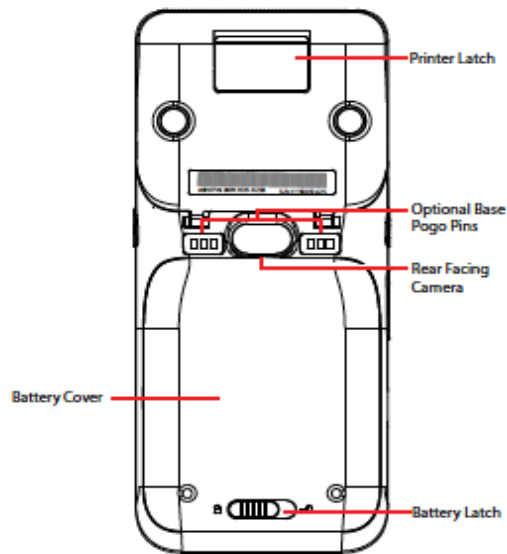
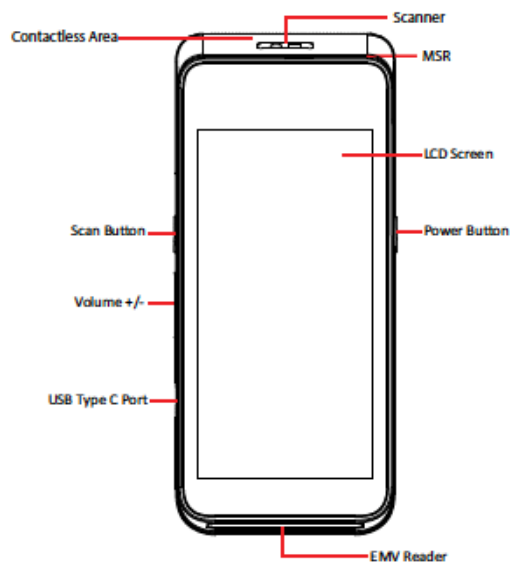
1. General product: the terminal product number, model, and power requirements
2. Serial number label: unique terminal serial number (S/N)
3. Tamper-evident bag serial number (in case the device is not deployed and is stored in one)
4. Status (deployed, in storage, in transit, or in repair)
5. Hardware version
6. Firmware version
7. Application version
8. Device location
9. Date of last inspection

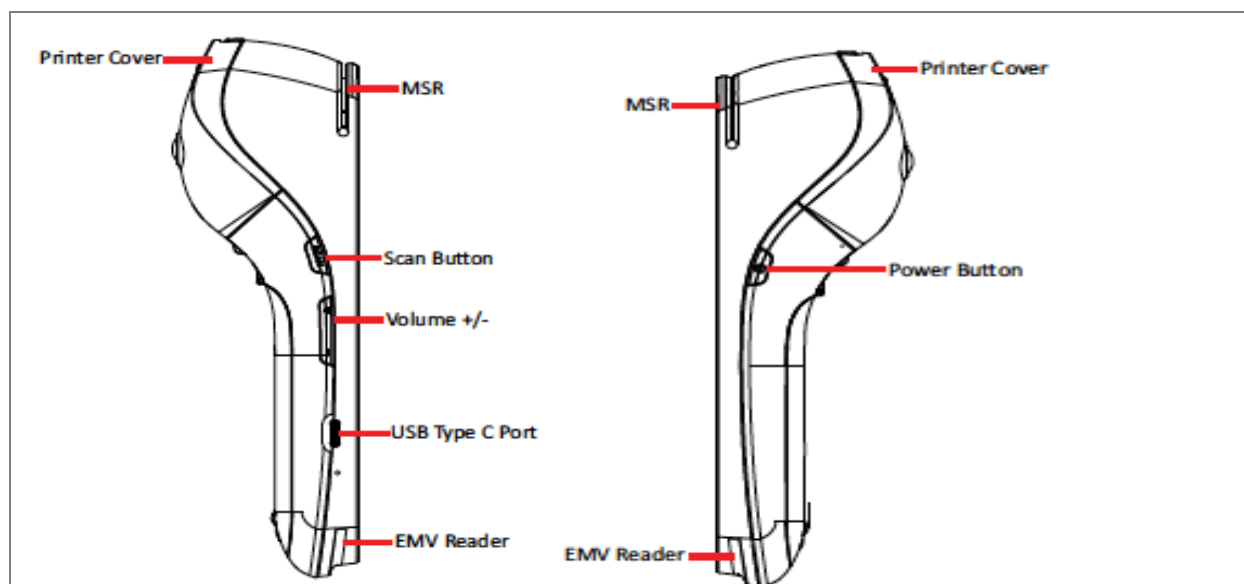
Images below indicate how to find the required inventory information listed above.



If the reader is not deployed in store and is stored in the tamper evident bag instead, locate the serial number on the tamper evident bag the device arrived in and include this as an inventory line item. Do not remove the device from the sealed bag.

The terminal details will also be provided on the back of the PAX A920 PRO and the terminal packaging shown below.





FIRMWARE CHECK

You must also verify that your A920 PRO product is running a PCI PED approved firmware. Shortly after powering up, a splash screen displays the version number for the Operating System. You must be able to find these numbers on the list of Approved PIN Transaction Security (PTS) Devices just as was done for the Hardware identifier. Listing can be found at https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices. If these numbers do not match, contact customer support number provided to you in section 1.0

In this example, the hardware identifier version number is:

- A920Pro-xxx-Rx5-1xxx (CTLS)

In this example, the firmware version number is:

- 25.03.xxxx

An example for a paper-based inventory is provided in the table below.

Date last updated: <Insert Date>

Updated by: <Insert Name>

Signature:

Device Vendor	Device Model Name(s) and Number	Device Location	Device Status	Serial Number or Other Unique Identifier	Date of Inventory
PAX	A920 PRO	Street 1 123456 City	Deployed	123-132-123	05.05.2017

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

Follow terminal installation guide provided to you for detailed terminal installation instructions. Images below are provided for your convenience to install PAX A920 PRO device.

SETTING UP DEVICE

- 1) Remove the device from its packing.
- 2) Insert the battery into the device.
- 3) Hold the power button to turn the device on.
- 4) Go to Android settings and enter the password. The password is included in the Instruction. Booklet that comes in the box with the A920 PRO.
- 5) Connect the device via Wi-Fi mode.
- 6) All software/ app updates are configured by our support team during fulfilment. The terminal will automatically download everything once it connects to wifi for the first time (incl. RKI, BroadPOS version, 3rd part POS app or ISV Hub app) Use the top the device to swipe a credit card.
- 7) Insert the card for EMV Contact transaction.
- 8) Tap the card for EMV Contactless transaction.
- 9) For refund transactions, the user will be promoted to enter the password again.
- 10) Please read the PAX A920 PRO user manual for detailed installation instructions.

SETTING UP WI-FI

A920 Pro Communications Setup

The A920 Pro supports Wi-Fi and Cellular for network and Internet access. Wi-Fi is a wireless computer network that links two or more devices using wireless communication to a local area network (LAN) within a limited area, such as a store or office building. Available access types of Wi-Fi on the A920 Pro are DHCP, Static IP, Manual Static IP, and Manual Proxy. The following sections include step-by-step procedures for setting up each of these communication types.

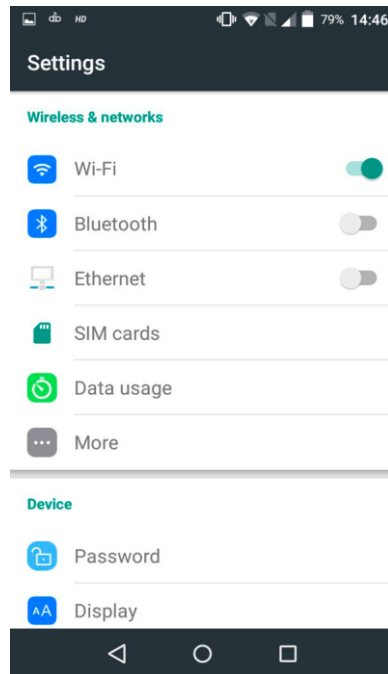
DHCP

The A920 Pro supports DHCP setup for network and Internet access. DHCP stands for Dynamic Host Configuration Protocol. DHCP is a network management protocol used in IP networks. The DHCP server dynamically assigns an IP address and other network configuration parameters to each device on the network.

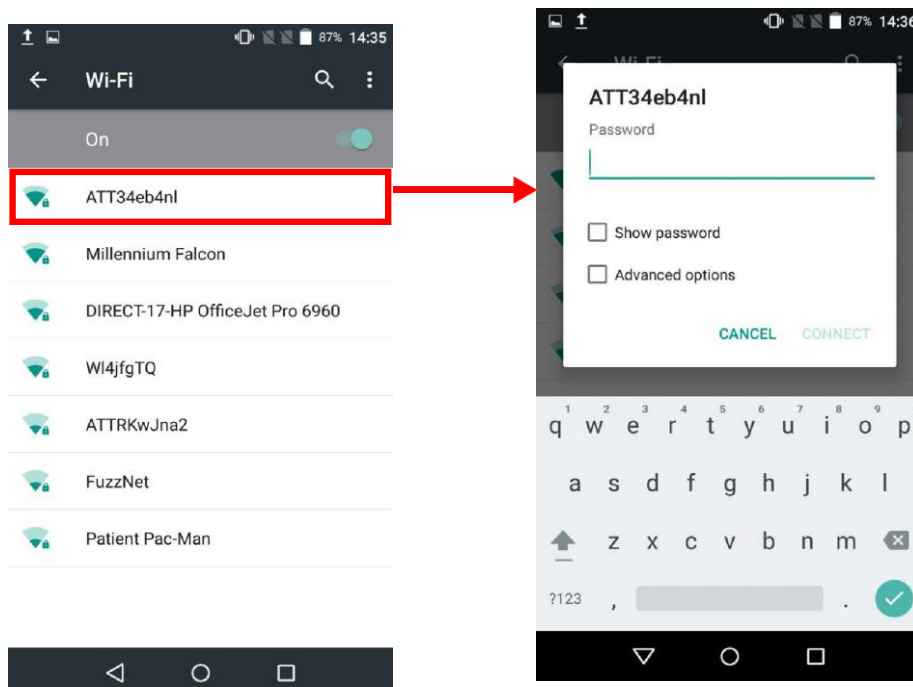
1. Select [Settings] and input the device password when prompted.



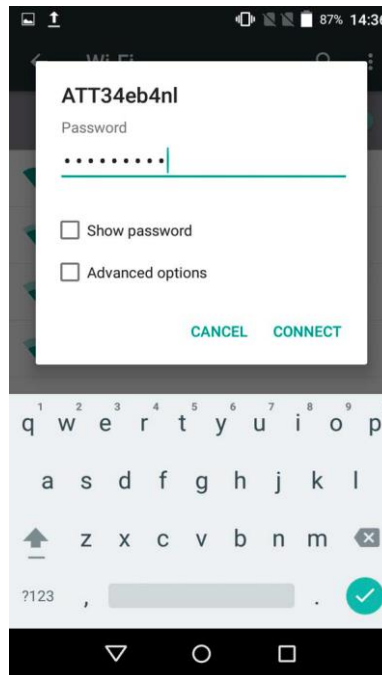
2. Slide the [Wi-Fi] tab to the right to enable Wi-Fi.



3. Select [Wi-Fi] and then select desired network. Input the network password when prompted.



4. Select [Connect].



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

4.2 Guidance for selecting appropriate locations for deployed devices

Choose an installation location appropriate for the device and with protection measures in mind:

- Control public access to devices so that it is limited to areas one is expected to use in order to complete a transaction (for example, PIN pad and card reader).
- Place devices so that authorized personnel can monitor them (for example, daily checks performed by store security staff).
- Place devices in an environment that deters compromise (for example, through lighting, access paths, visible security measures).
- Do not install devices outdoors that are designed for indoor use only.
- Ensure that the location is adequately ventilated and protected from excessive heat, dust, oil, and moisture. The device should not be near any running or standing water.
- Place the terminal on a flat surface, or mount it on the supplied stand or on the wall mount according to manufacturer's instructions.

- Keep the terminal away from direct sunlight and from devices that cause excessive voltage fluctuations, make electrical noise, or radiate heat, including high-power radios. The terminal should be a reasonable distance from anti-theft doorway units and from surface-mounted deactivator pads.
- Position the terminal on the check-stand so that the PIN-entry process is impossible to see.

For example:

- 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 PIN spying is difficult. Install the device on an adjustable stand that customers can swivel or tilt to a position that makes observation of the PIN-entry process difficult.
- Position in-store security cameras so that the PIN-entry keypad is not visible.

Place devices so that they can be handled only by authorized personnel who initiate transactions. In a retail environment, the unit should be placed on the counter where it can be observed, but not so close to customers that they could manipulate the device without being seen.

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

Merchants should physically secure devices to prevent substitution while devices are deployed. If devices cannot be physically secured because they are mobile:

- Secure devices in a locked room when not in use.
- Assign responsibility to specific individuals when device is in use.
- Observe devices at all times.
- Create a log to sign devices in and out.

Merchants should physically secure devices in a secure area with access for authorized personnel only when not deployed or being used, including devices:

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

Prior to deployment or shipment or while awaiting repairs, devices must be secured in restricted-access area to ensure that they are not tampered with. For example:

- Devices must be stored in locked room or container.
- The storage location must restrict access using a door or container with a physical key or numeric code.
- Access to the storage location must be logged. This logging may be manual with a written access log or automatic through electronic means.
- Access to the room must be monitored, such as with cameras or physical sight.

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

- 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 monitor authorized personnel at all times.

The following are best practices to ensure an adequate level of protection for devices:

- Merchants should be aware of the location of the devices at all times. When not in use, they should be securely locked away and out of reach.
- Devices in use should be visible to staff members at all times.

Ensure that devices are tracked at all times by assigning a job role or person to be responsible for watching the device while in use.

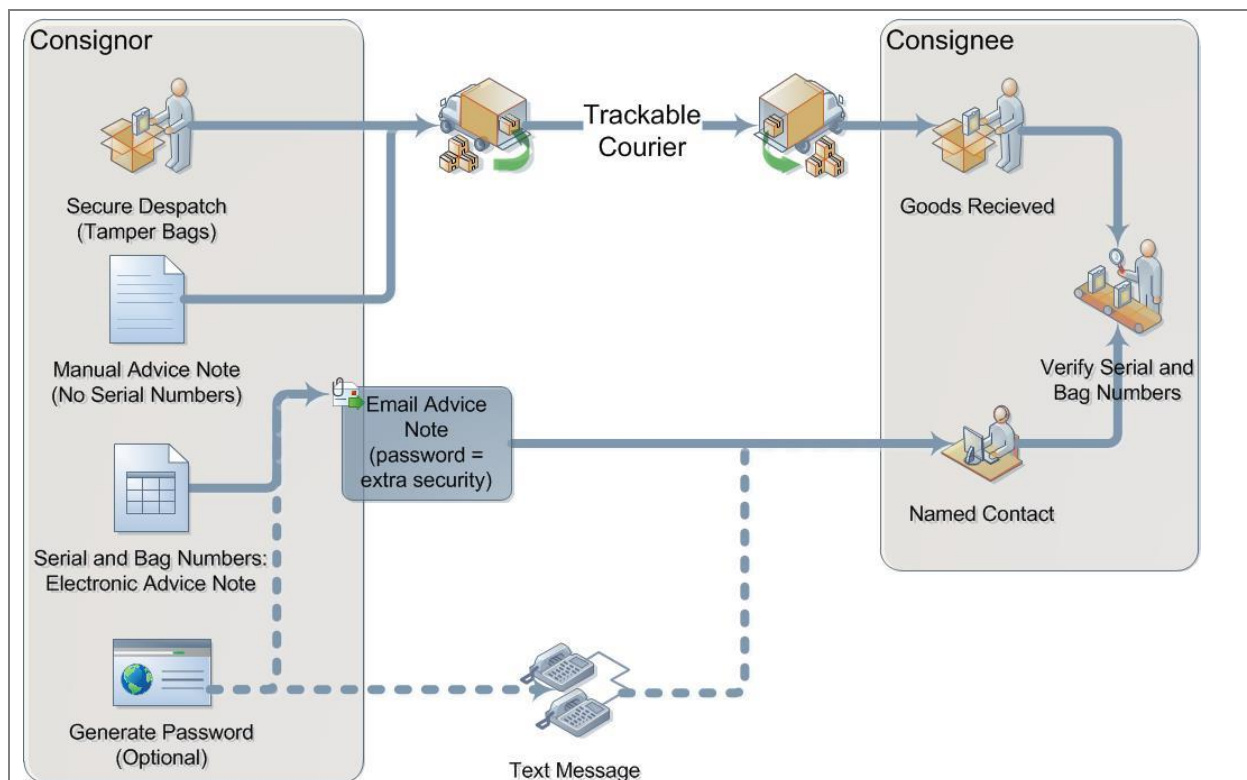
5. POI Device Transit

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

Devices Transported to Merchants

PAX A920 PRO will be shipped in following manner from Cybersource partner distribution center.

- 1) Cybersource deployment partner will ship the devices in tamper resistant bags with serial numbers listed on them.
- 2) An email will be generated to the merchant with tamper resistant bag serial number and terminal serial number to the client.
- 3) Upon receipt of the devices client must confirm the receipt of the terminals to CyberSource by calling support number or emailing back to CyberSource partner in step 2 above.



Devices Transported by Merchants

If you need to ship devices either to other locations or for repair / returns, devices must be shipped securely. This means that when packaging devices for transit, devices must be packed in tamper-evident packaging. Tamper evident packaging can either be independently obtained by merchant, or tamper evident packaging can be requested from CyberSource.

Additional Device Transport Instructions

All devices either being shipped to a location for deployment or for return, must be shipped using a secure transport method such as a trusted and trackable courier (e.g. FedEx, UPS, DHL, etc.)

For deployment to sites, internal employees may be used for device shipment; however, internal employees must be instructed and should understand that devices must be protected at all times. This means that devices may not be left in public areas unattended (for example, in the front or back seat of a car) as this may lead to unauthorized access or theft of the device.

In addition, employees 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, trackable 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 delivery to site

In the event devices are shipped from merchant storage locations, device recipients must be notified of authorized shipping, notified of how the device will be shipped, and trained in how to inspect the packaging and device for tampering. This includes training to recognize breakage of tamper-evident seals on the external packaging and training to investigate the device itself for cracks or breakage of security seals. Recipients of devices must also be instructed that if they receive devices without prior confirmation from the shipping location or if devices are delivered in an unexpected manner, recipients must request and receive definitive confirmation of the legitimacy of the shipment by calling Cybersource support.

Physically secure POI devices in your possession, including devices:

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

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

Devices Transported by Merchants

Devices must be shipped securely to other locations or for repair / returns. They must be packed in tamper-evident packaging, which can be independently obtained by the merchant or requested from Cybersource.

All devices being deployed or returned must be shipped using a secure transport method such as a trusted and trackable courier such as FedEx, UPS, or DHL.

For deployment to sites, internal employees may transport devices; however, internal employees must be instructed and understand that devices must be protected at all times. Devices may not be left in public areas unattended or in theft-prone areas such as the front or back seat of a car.

In addition, employees must be authorized to deliver the devices, and the recipient must be notified of who is delivering the devices.

Be it a bonded carrier, trackable courier, or internal employee, you must log the following information:

- 1) Personnel providing shipping (if employee, record name and job role)
- 2) Date of pick up
- 3) Device being shipped
- 4) Confirmation date of delivery to site

In the event devices are shipped from merchant storage locations, device recipients must be notified of authorized shipping, notified of how the device will be shipped, and trained in how to inspect the packaging and device for tampering. The training should include how to recognize breakage of tamper-evident seals on the external packaging and how to examine the device itself for cracks or breakage of security seals. Recipients of devices must also be instructed if they receive devices without prior confirmation from the shipping location or if devices are delivered in an unexpected manner, they must request and receive definitive confirmation of the legitimacy of the shipment by calling Cybersource support).

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.

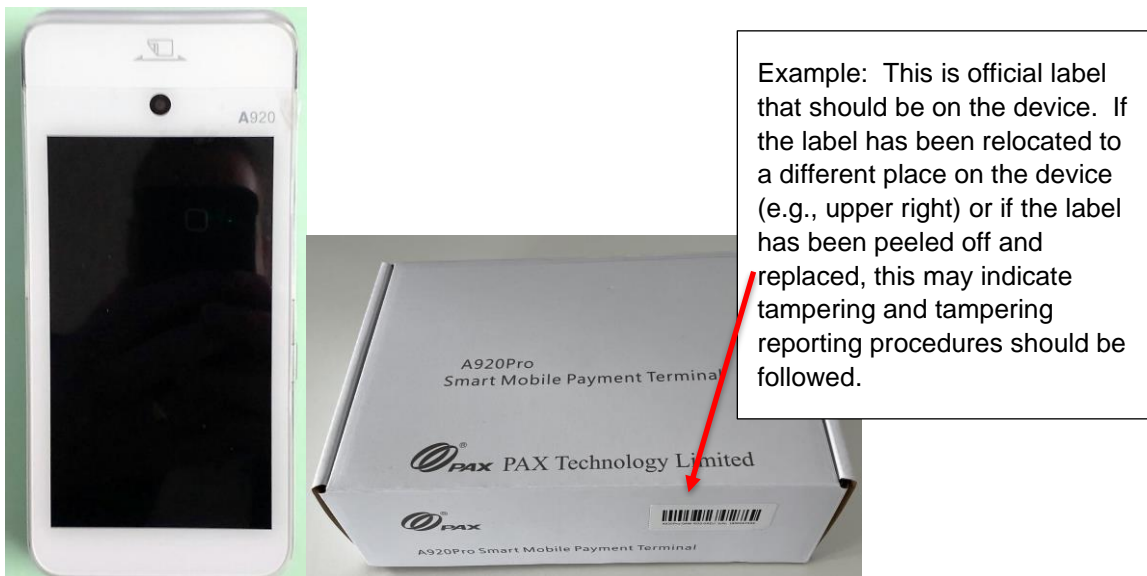
Prior to deployment:

- 1) Make sure to follow all instructions on how to receive and ship devices
- 2) Make sure the device is tracked in your inventory as described in section 2.3.
- 3) Perform pre-installation inspection procedures including:
 - a. Physical and functional tests
 - b. Visual inspection
 - c. Verify integrity of device

After deployment:

Merchants should perform physical inspections of devices, minimally every quarter, to detect tampering or modification, including steps such as:

- 1) Check for missing or altered seals or screws, extraneous wiring, holes in the device, or the addition of labels or other covering materials that could be used to mask damage from device tampering



- 2) Check the firmware version (confirm during boot up) and compare it to the inventory
- 3) Check the application version (on the idle screen) and compare it to the inventory
- 4) Monitor devices in remote or unattended locations (for example, via the use of video surveillance or other physical mechanisms to alert personnel)

- 5) If anything suspicious is detected, the device should not be used

Report tampered or missing devices and other suspicious activity to CyberSource Support immediately using the steps below.

How to Report Tampering

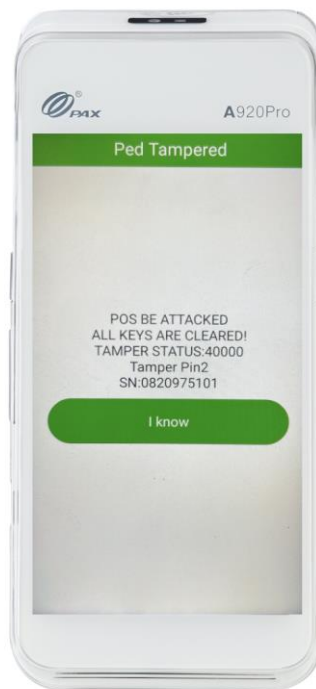
In the event that you believe your device has been tampered with, the following steps should be followed:

- 1) Notify Cybersource support:
 - a. Email Terminals@cybersource.com
- 2) Receive a confirmation number and use it in future correspondence related to the tampering report for this device.
- 3) Provide Cybersource with the serial number of the device and the device will be taken out of the system immediately. Please note: You will not be able to use the terminal anymore.
- 4) Physically remove the device from the area in which it was used.
- 5) Store out of service devices in a locked area (filing cabinet, secure storage room, etc.) until you take them out of service and return them.
- 6) Once the device is returned it will be subjected to inspection and if warranted, additional forensics will be conducted and/or the unit will be destroyed.
- 7) Merchants will need to coordinate with the CyberSource to secure a replacement unit.
- 8) Update inventory to reflect the device that has been removed.

6.2 Instructions for responding to evidence of POI device tampering

DEVICE SECURITY

- Security mechanisms employed within the terminal can detect physical tampering and trigger a tamper event. If the PAX A920 PRO chassis is opened, then the tamper mode will be triggered. This causes the terminal to cease performing transactions and indicates that it has been tampered as displayed in the “Ped Tampered” message in the figure below.



- Terminal security must not be compromised by altering the environmental conditions. The power and temperature operating ranges should be within the specifications specified in PAX A920 PRO Installation Guide. Operating the terminal outside of these ranges triggers a tamper event and causes the terminal to cease performing transactions and indicates that it has been tampered on the device display; see Figure above.
- If any device is found in tamper state, please remove it from service immediately, keep it available for potential forensics investigation, and notify your company security officer for tamper investigation and CyberSource support desk at provided number.
- Update your inventory to reflect the device has been removed from service.

SYSTEM SECURITY

- We automatically monitor the status of our solution on a continuous basis. This includes monitoring for any problems relating to encryption and decryption between the terminals and backend systems.
- Should you notice an unusual high rate of declines or errors related to encryptions are displayed on the terminal, remove the unit from service, contact the solution provider immediately and update your inventory to reflect the device has been removed from service.
- Do not use the terminal until you have received confirmation from support that the issue has been resolved.
- If the issue cannot be resolved, contact Cybersource support at Terminals@cybersource.com.

7. Device Encryption Issues

7.1 Instructions for responding to POI device encryption failures

In the event that merchant is getting encryption failure reported by the device it must be reported to Cybersource immediately. No further transactions will be authorized from the affected device and it must be removed from service. The merchant must update the inventory, to set the device status to 'Repair'.

8. POI Device Troubleshooting

8.1 Instructions for troubleshooting a POI device

If you encounter any problems with device and need help with troubleshooting, your first point of contact is the Cybersource support. For quick troubleshooting, please make sure to have the following information ready:

- 1) Serial number of the device as found on the back e.g. S/N: 1850000XXX



- 2) Make and model of the device, e.g. PAX A920 PRO
- 3) Accept app version in the app settings
- 4) Precise date and time the problem occurred in your time zone
- 5) Any transaction references, e.g. authorization code or transaction identifier
- 6) Are other devices experiencing the same issue?
- 7) Steps to reproduce the problem

For your own safety, we ensure that all inquiries come from authorized personnel and that product information matches Cybersource records. We will never ask merchants to submit clear text account numbers during support calls.

9. Additional Guidance

9.1 Additional Guidance for Merchants

Third Party Access to Devices

Depending on the service selected by the merchant, third-party contractors may be used to provide onsite support. Follow procedures below:

- 1) Confirm the identity of the person representing as third-party support personnel.
- 2) Confirm the identity of the person with Cybersource if the store is not notified ahead of time.
- 3) Do not allow access to the devices until identity of the support person is confirmed.

Removal from Service

Removing devices from service must be done securely and must allow for the tracking and security of the device. Regardless of the reason for removal, the following steps are required:

- 1) Removal of device must be arranged prior to shipping.
- 2) Personnel at the location from which the device will be removed must confirm that personnel removing device are authorized.
- 3) Names of personnel performing removal must be documented, including name, company, and time of removal.
- 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, it must be securely stored at the location in a manner as described in Section 3.3.

If the device is to be returned to a shipping location, it 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 Section 4.1 and 4.2.

If the device is to be returned to an authorized Deployment Center for repair or replacement, the following steps must be taken:

- 1) Place device in tamper-evident bag.
- 2) Call Cybersource support:
 - a. US Toll Free: +1 855-477-1184
 - b. UK: +44 2039012015
- 3) Include serial numbers and tamper bag numbers.
- 4) Email: Terminals@cybersource.com
- 5) Returned device must be accompanied by these forms:
 - a. RETURNS REQUEST FORM
 - b. REPAIR PROCEDURE ACCEPTANCE

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

FIRMWARE CHECK

You must also verify that your A920 PRO product is running a PCI PED approved firmware. Shortly after powering up, a splash screen displays the version number for the Operating System. You must be able to find these numbers on the list of Approved PIN Transaction Security (PTS) Devices just as was done for the Hardware identifier. Listing can be found at https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices. If these numbers do not match, contact customer support number provided to you in section 1.0

In this example, the hardware identifier version number is:

- A920Pro-xxx-Rx5-1xxx (CTLS)

In this example, the firmware version number is:

- 25.03.xxxx

