Payment Card Industry (PCI)

Point-to-Point Encryption (P2PE)®

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

For Use with PCI P2PE Standard v3.1

October 2025

Revision History

Version	Date	Author	Description of Change	Jira Ticket
1.0	April 2025	Kire Trajkovski	Initial Creation of Document	ADOPS-11
1.1	September 2025	David Barnet	Council updates	ADOPS-12
1.2	October 2025	David Barnet	Council approval and Reference Number update	ADOPS-12

1. P2PE Solution Information and P2PE Solution Provider Contact Information

1.1 P2PE Solution Information *(as per the listing on the PCI SSC website)*	
P2PE Solution Name:	Visa Acceptance Solutions P2PE
P2PE Solution Listing Reference Number (***Assigned by PCI SSC***)	**2025-01570.001**
https://listings.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions	
Entity Name Clarification For clarity, all references to Visa Acceptance Solution, Cybersource, and Payworks in this document refer to same entity. The names by be used interchangeably.	

1.2 P2PE Solution Provider Contact Information					
Company Name:	Cybersource Corporation		Company URL:	www.Cybersource.com	
Contact Name:	David Barnet or Customer Support		Title:	Director	
Telephone:	Customer Support: US Toll Free: +1 855-477-1184 Europe Toll Free: +442039012015		E-mail:	Terminals@cybersource.com inpersonacceptp2pemg@visa.com	
Business Address:	900 Metro Center Blvd		City:	Foster City	
State/Province:	CA	Country: USA		Postal Code:	94404

1.3 Communication Instructions
Instructions advising how to contact the P2PE Solution Provider, with consideration to establishing a trusted communication channel/session.
Please contact Customer Support at contact information in 1.2 above to advise of PTS POI device tampering or encryption issues, validating support/repair personnel, incident reporting, device troubleshooting, returning devices, or other concerns or issues related to P2PE.

PCI P2PE and PCI DSS

Merchants using this P2PE Solution may be required to validate PCI DSS compliance. Merchants should contact their acquirer or payment brands to determine their PCI DSS validation requirements.

Refer to FAQ 1158 on the PCI SSC Website.

2. PTS POI Device and Software Information

2.1 PTS POI Device Details

The following information lists the details of the PTS POI devices approved for use in this P2PE Solution.

All PTS POI device information can be verified by visiting the following on the PCI SSC Website and by referring to Table 2.4 below:
https://www.pcisecuritystandards.org/approved_companies_providers/approved_pin_transaction_security.php

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

For P2PE Applications and Non-Payment Software, use the PIM ID#s to cross reference to their respective tables below. The 'PIM ID#'s are numbers created and used by the P2PE Solution Provider solely for the purpose within this PIM to make it easier to cross reference the P2PE Applications and Non-payment Software that are used on the PTS POI devices denoted here. The 'PIM ID#'s are not assigned by the PCI SSC nor are they recognized by the PCI P2PE Program.

PCI PTS Approval #	PTS POI Device Vendor	PTS POI Device Model Name & Number(s)	PTS POI Device Hardware Version #(s)	PTS POI Device Firmware Version #(s)	P2PE Applications on PTS POI Devices *(PIM ID# from Table 2.2)*	Non-Payment Software on PTS POI Devices *(PIM ID# from Table 2.3)*
4-40350	***PAX Computer Technology (Shenzhen) Co Ltd***	***PAX A920 MAX***	***A920MAX-0xx-Rx6-0xxx (CTLS)***	***26.00.xxxx***	***APP#1***	

2.2 P2PE Application Details

The following information lists the P2PE Applications approved for use on the PTS POI devices in Table 2.1 for use in this P2PE Solution.

P2PE Applications by definition have access to clear-text account data. These applications **must** be denoted in the P2PE Solution listing.

The 'PIM ID#'s are numbers created and used by the P2PE Solution Provider solely for the purpose within this PIM to make it easier to cross reference the P2PE Applications denoted here that are used on the PTS POI devices denoted in Table 2.1. They are not assigned by the PCI SSC nor are they recognized by the PCI P2PE Program.

***Note**: P2PE Applications that have been assessed as part of the P2PE Solution and were chosen to not be separately listed are denoted as such as part of the P2PE Solution listing and will not have an independent PCI P2PE Application Listing Reference Number.*

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

PIM ID# (e.g., App#1, App#2, …)	P2PE Application Vendor	P2PE Application Name	P2PE Application Version(s)	PCI P2PE Application Listing Reference Number *(Assigned by PCI SSC)*
App#1	***Pax Technology Inc.***	***BroadPOS P2PE***	***1.01.xx***	***2022-00841.003***

2.3 Non-Payment Software Details

The following information lists the Non-Payment Software approved for use on the PTS POI devices in Table 2.1 for use in this P2PE solution.

*P2PE Non-payment Software by definition **must not** have any access to clear-text account data. While this type of software is assessed as part of the P2PE Solution assessment, this software is not denoted on the PCI P2PE Solution Listing.*

The 'PIM ID#'s are numbers created and used by the P2PE Solution Provider solely for the purpose within this PIM to make it easier to cross reference the Non-payment Software denoted here that is used on the PTS POI devices denoted in Table 2.1. They are not assigned by the PCI SSC nor are they recognized by the PCI P2PE Program.

PIM ID# (e.g., SW#1, SW#2, …)	Non-payment Software Vendor	Non-payment Software Name	Non-payment Software Version(s)	Additional Information (*as needed*)

<Insert additional rows above as necessary>

2.4 Verifying PTS POI Device Information

Verifying PTS POI device information is critical. This information is necessary to validate the information in this PIM, to cross-reference with the PCI PTS Listings as well as the PCI P2PE Solution Listing, in addition to inventory management, troubleshooting and incident reporting.

Instructions to confirm PTS POI device hardware, firmware, and the P2PE Application(s) and Non-payment Software present

FIRMWARE CHECK

You must also verify that your A920 MAX 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.

In this example, the hardware identifier version number is:

- A920MAX-0xx-Rx6-0xxx (CTLS)

In this example, the firmware version number is:

- 26.00.xxxx

2.5 PTS POI Device Inventory & Monitoring

- All PTS POI devices must be documented via inventory control and monitoring procedures, including device status (e.g., 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 PTS POI devices, must be reported to the P2PE Solution Provider via the contact information and instructions in Section 1 above.
- A sample inventory table below is for illustrative purposes only. The actual inventory should be captured and maintained by the merchant in an external document.

Instructions on documenting and maintaining an inventory of the PTS POI Devices.

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 MAX and the terminal packaging shown below.

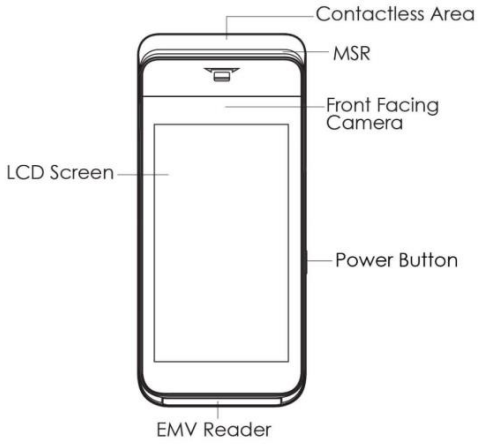


Figure 1: PAX A920 MAX Front side view

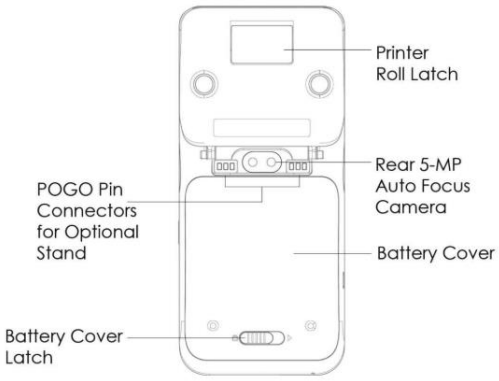


Figure 2: PAX A920 MAX Back side view

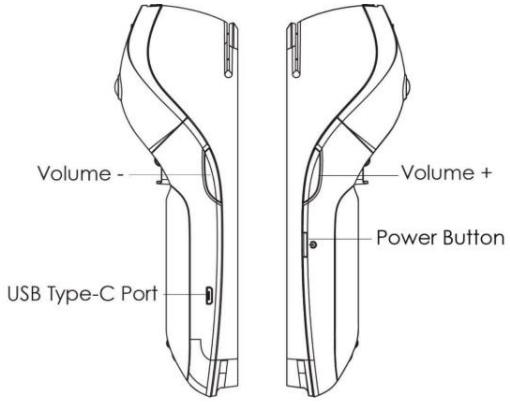


Figure 3: PAX A920 MAX Side views

FIRMWARE CHECK

You must also verify that your A920 MAX 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:

- A920MAX-0xx-Rx6-0xxx

In this example, the firmware version number is:

- 26.01.xxxx

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

Date last updated: ***<Insert Date>***

Updated by: ***<Insert Name>***

Signature:

Sample Inventory Table

PTS POI Device Vendor	PTS POI Device Model Name(s) and Number(s)	Device Location	Device Status	Serial Number or Other Unique Identifier	Date of Inventory	Additional Notes (as needed)
PAX	A920 MAX	Street 1, 123456 City	Deployed	123-123-123	19.03.2025	

3. Receipt of PTS POI Devices

3.1 Instructions for ensuring PTS POI devices originate from trusted sources/sites/locations

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 always protected. 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).

3.2 Instructions for confirming PTS POI device and packaging were not tampered with

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

Example: This is official label that should be on the device. If the label has been relocated to a different place on the device (e.g., upper right) or if the label has been peeled off and replaced, this may indicate tampering and tampering reporting procedures should be followed.

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.

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

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.

Physically secure POI devices in your possession, including devices:

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

4. Deployment and Installation of PTS POI Devices

Do not connect or otherwise use non-approved payment account data capture devices.

The P2PE Solution is approved to use specific PTS POI devices, as detailed above in Table 2.1, which must be denoted on the P2PE Solution Listing.

If any devices that are not in Table 2.1 are used to accept payment account data, it could affect the merchant eligibility to use SAQ P2PE – contact your acquirer or payment brands.

Do not change or attempt to change PTS POI device secure configurations or settings.

Changing secure PTS POI device configurations or settings may invalidate the P2PE Solution implementation and it could affect the merchant eligibility to use SAQ P2PE – contact your acquirer or payment brands.

Examples include, but are not limited to attempting to perform the following on the PTS POI devices:

- Enabling any device interfaces or data-capture mechanisms that are disabled
- Altering security configurations or authentication controls
- Physically opening the device
- Attempting to install unauthorized applications/software

4.1 Installation and connection instructions for the PTS POI devices

Follow terminal installation guide provided to you for detailed terminal installation instructions. Images below are provided for your convenience to install PAX A920 MAX 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) Connect the device via Wi-Fi or GPRS mode.
5) Go to Android settings and enter the password. The password is included in the Instruction. Booklet that comes in the box with the A920 MAX.
6) Go to PAX app and search for Accept app by Cybersource.
7) Download the app.
8) Open the app and login with the assigned username and password. This will be only required at the initial setup of the app. Once the app setup, no subsequent login is required to use the payment application except in the refund transaction flow.
9) Use the top the device to swipe a credit card.
10) Insert the card for EMV Contact transaction.
11) Tap the card for EMV Contactless transaction.
12) For refund transactions, the user will be promoted to enter the password again.

13) Please read the PAX A920 MAX user manual for detailed installation instructions.

SETTING UP WI-FI

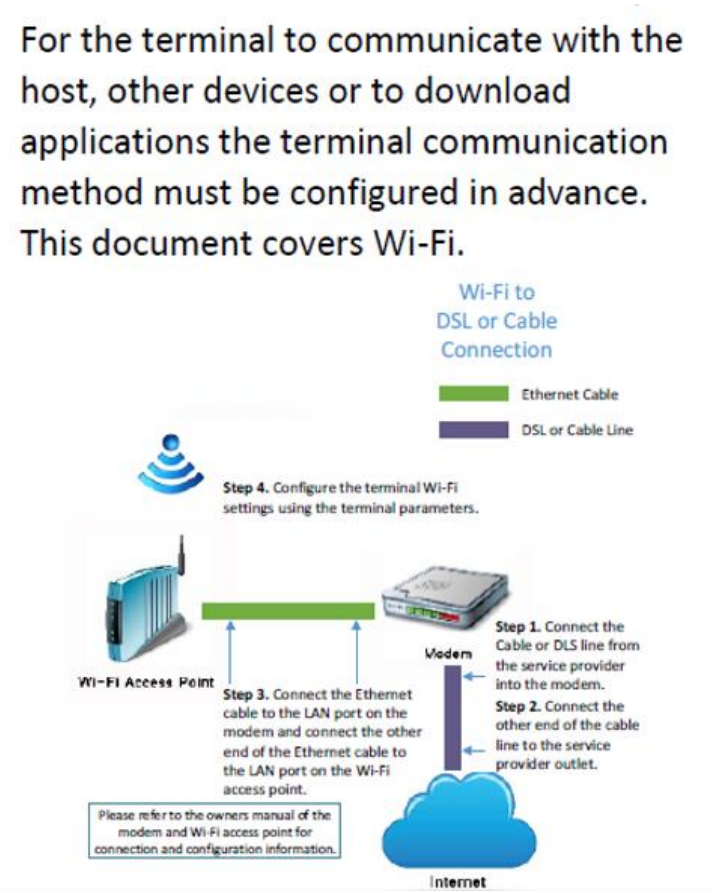


Figure 4: A920 MAX Communication Setup

Configuring Wi-Fi DHCP Access for the PAX Terminal

Using the DHCP configuration is one option for connecting the PAX terminal to your Wi-Fi network. In this configuration, the payment terminal is randomly assigned IP addresses by your service provider when you access the internet.

Enabling a Wi-Fi Network on the PAX Terminal

Follow these steps to enable a Wi-Fi network on the PAX terminal:

PAX Terminal Settings Screens

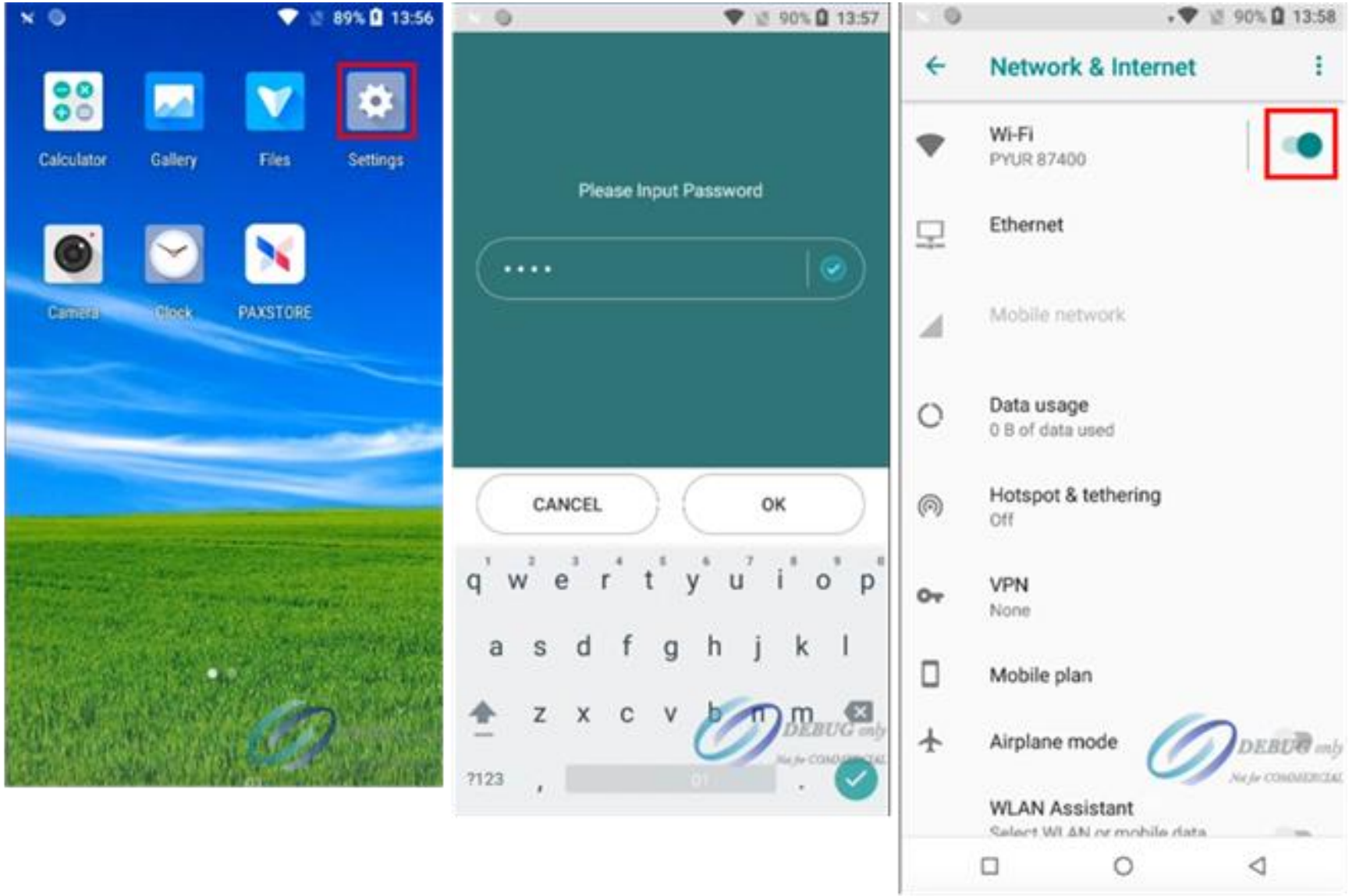


Figure 5: A920 MAX Wi-Fi Setup

1) On the terminal Home screen, tap the **Settings** icon. You are prompted to enter the system password.
    - If you are a first-time user, enter the default Settings password: pax9876@@
        - Tap the **Checkmark**. The Settings screen appears.
    - To change the default password, in the Device section, tap **Password**. Follow the prompts to change your password.
    - If you changed your password before, enter your system password. Tap the **Checkmark**. The Settings screen appears.
2) In the Wireless & networks section, tap the slider next to the **Wi-Fi** icon to enable Wi-Fi.
3) Tap the **Wi-Fi** icon. The Wi-Fi screen appears.
4) Choose your **Wi-Fi** network from the list. Enter the Wi-Fi network password.
5) Tap Connect. The device connects to your **Wi-Fi** network.
6) To exit the screen, tap the back arrow until you reach the Home screen.

Other Options for configuring WIFI on the A920 MAX

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 to deploy PTS POI 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 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 PTS POI devices to prevent unauthorized removal and/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.
- Always observe devices.
- 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.

- Always escort and monitor authorized personnel.

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

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

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

5. Continual Monitoring and Inspection of Deployed PTS POI Devices

5.1 Instructions for inspecting PTS POI devices for signs of tampering and responding to suspected tamper incidents

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

5) 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

Example: This is official label that should be on the device. If the label has been relocated to a different place on the device (e.g., upper right) or if the label has been peeled off and replaced, this may indicate tampering and tampering reporting procedures should be followed.

6) Check the firmware version (confirm during boot up) and compare it to the inventory

7) Check the application version (on the idle screen) and compare it to the inventory

8) Monitor devices in remote or unattended locations (for example, via the use of video surveillance or other physical mechanisms to alert personnel)

6) 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

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

9) Notify Cybersource support:
    a. Email Terminals@cybersource.com
10) Receive a confirmation number and use it in future correspondence related to the tampering report for this device.
11) 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.
12) Physically remove the device from the area in which it was used.
13) 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.
14) 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.
15) Merchants will need to coordinate with the CyberSource to secure a replacement unit.
16) Update inventory to reflect the device that has been removed.

5.2 Instructions for inspecting PTS POI devices for skimming devices and responding to suspected skimming detection

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

Prior to deployment:

4) Make sure to follow all instructions on how to receive and ship devices
5) Make sure the device is tracked in your inventory as described in section 2.3.
6) 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:

9) 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.

Example: This is official label that should be on the device. If the label has been relocated to a different place on the device (e.g., upper right) or if the label has been peeled off and replaced, this may indicate tampering and tampering reporting procedures should be followed.

10) Check the firmware version (confirm during boot up) and compare it to the inventory

11) Check the application version (on the idle screen) and compare it to the inventory

12) Monitor devices in remote or unattended locations (for example, via the use of video surveillance or other physical mechanisms to alert personnel)

7) 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

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

17) Notify Cybersource support:
    a. Email Terminals@cybersource.com
18) Receive a confirmation number and use it in future correspondence related to the tampering report for this device.

19) 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.
20) Physically remove the device from the area in which it was used.
21) 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.
22) 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.
23) Merchants will need to coordinate with the CyberSource to secure a replacement unit.
24) Update inventory to reflect the device that has been removed.

5.3 Instructions for detecting and responding to PTS POI device account data encryption failures

If 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'.

5.4 Instructions for troubleshooting a PTS 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. 400-200-123
2) Make and model of the device, e.g. PAX A920 MAX
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.

6. Transporting / Shipping PTS POI Devices

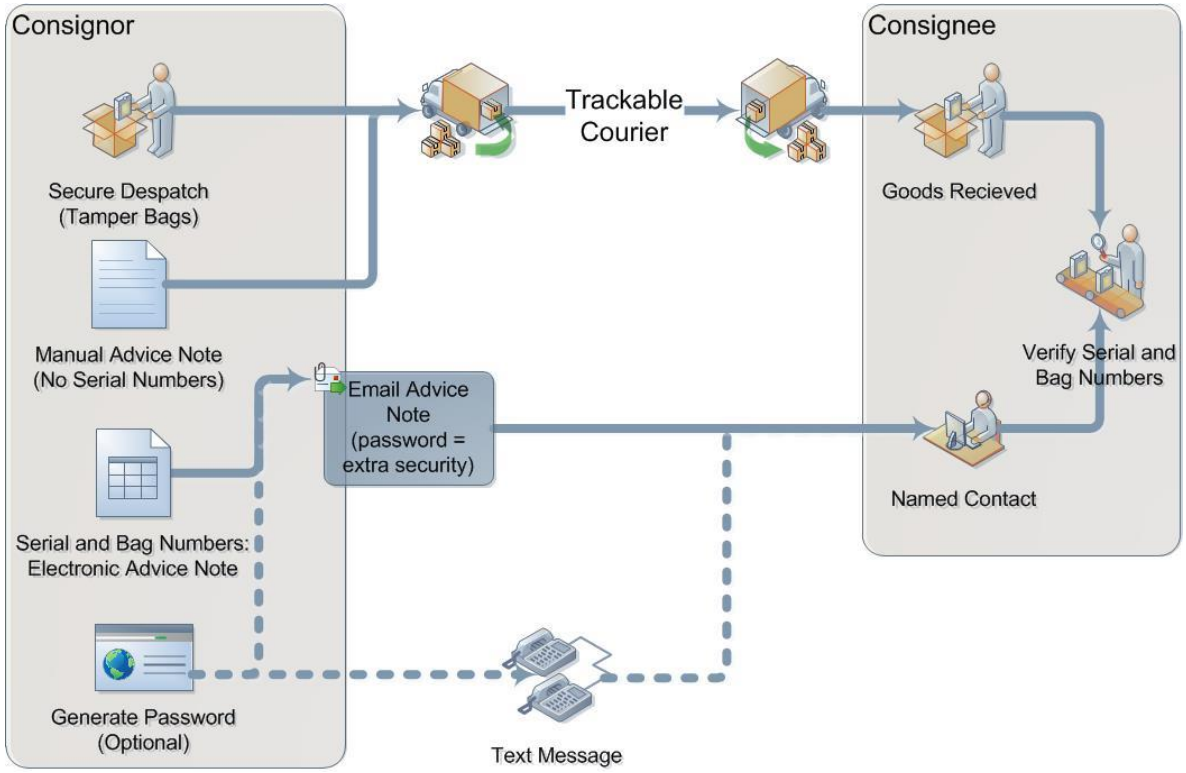
6.1 Instructions for ensuring PTS POI devices are shipped to trusted sites/locations only, as needed (e.g., for repair)
Devices Transported by Merchants Devices must be shipped securely to other locations or for repair / returns. They must be packed in tamper-evident packaging, which can be independently 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 always protected. 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: 5) Personnel providing shipping (if employee, record name and job role) 6) Date of pick up 7) Device being shipped 8) 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).

6.2 Instructions for securing PTS POI devices intended for, and during, transit to other locations (e.g., to a repair facility)

Devices Transported to Merchants

PAX A920 MAX 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 device's 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 always protected. 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.

7. Additional Guidance / Instructions

7.1 Additional guidance for merchants regarding the P2PE Solution (as needed).

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

REPAIR PROCEDURE ACCEPTANCE