Payment Terminals

P2PE Instruction Manual (PIM)

For Use with P2PE Version 3.1

Updated: January 2026

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: Payment Terminals

P2PE Solution Listing Reference number (**Assigned by PCI SSC**):

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

1.2. P2PE Solution Provider Contact Information

Company Name:	Market Pay Tech		Company URL:	market-pay.com	
Contact Name:	Sylvain Derin		Title:	Chief Information Security Officer	
Telephone:	+33 1591 31283		E-mail:	assist@market-pay.com	
Business Address:	120-122 rue Réaumur		City:	Paris	
State/Province:	Paris	Country:	France	Postal Code:	75002

1.3. Communication instructions

Our support team is available 24/24 and 7 days a week to assist you.

You will find all ways to reach us out on our dedicated page for assistance: assist.market-pay.com

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.

MARKET PAY

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 and number:	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)
4-40305	PAX	A35	A35-xxx-Rx6-0xxx	26.00.xxxx	App1	SW1, SW2, SW3, S4, SW5, SW6
4-40333	PAX	A920Pro	A920Pro-xxx-Rx6-0xxx	26.00.xxxx	App1	SW1, SW2, SW3, S4, SW5, SW6
4-40372	PAX	IM30	IM30-xxx-Rx6-0xxx IM30-xxx-Rx6-Axxx	26.00.xxxx	App1	SW1, SW2, SW3, S4, SW5, SW6

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#	P2PE Application Vendor	P2PE Applications Name	P2PE Application Version	PCI P2PE Application Listing Reference Number
App1	Market Pay Tech	Payment Terminals	4.x.y-zzzzzzzzz	

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#:	Non-payment Software Vendor	Non-payment Software Name	Non-payment Software Version	Additional Information
SW1	Market Pay Tech	Master App	1.x.y-zzzzzzz	ECR integration interface
SW2	Market Pay Tech	NTMS Agent	1.x.y-zzzzzzzz	Parameters and application management
SW3	Argentea	AMoneyAP	1.1.x	Alternative Payment method processing for Italy
SW4	Argentea	AMoneyBPE	1.1.x	Italian meal vouchers processing
SW5	Argentea	AMoneyLens	1.0.x	Activation of Argentea applications
SW6	Nepting	Payment	1.x.zzzz	Cheques processing

Only the user applications listed in the table above are allowed to be installed and run on the PTS POI, to be PCI P2PE compliant.

All software allowed have been verified and have to be signed by Market Pay to ensure its integrity after the above verification process.

PTS POI have a mechanism to authenticate Market Pay's signature. In case of signature verification failure, the software is rejected by the terminal firmware.

Merchants are not allowed to install and run any other software. Otherwise terminal is no longer P2PE compliant and cannot be use in this P2PE solution.

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.

You will find instructions for how to confirm PTS POI device hardware, firmware and the P2PE Application version and Non-payment Software present:

- Firmware and Hardware version
- Applications version

2.5. PTS POI Device Inventory & Monitoring

- All PTS 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 PTS POI devices, must be reported to *Market Pay* via the contact information 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.

You must monitor your PTS POI devices by tracking every event (installation, storage, repair…) in order to update your inventory database.

At least once per year, you must perform an inventory. During this inventory, you must check all PTS POI devices to identify any unauthorized removal, substitution of devices or tampering attempt (checking warranty seals are not damaged, “Device tampered” alert not displaying when terminal is on).

You will find below an inventory process proposition:

1. Obtain inventory results from each store and warehouse with a list of PTS POI devices available.
2. Compare the list of PTS POI devices reported with the list of PTS POI devices shipped by Market Pay
    a. Update the inventory with the status and audit date.
    b. For any discrepancies, investigate the issue to identify missing information or PTS POI devices. If you can’t solve this discrepancy, report immediately to Market Pay via the contact information in section 1.2.
3. For future auditing purposes, save the inventory results.

Do note, a customer can define its own inventory process as long as it matches all requirements defined in this section. If customer defines a custom inventory process, it should be communicated to and approved by Market Pay.

Market Pay can help in the inventory process by providing all PTS POI shipped and sharing an overview of all devices connected to Market Pay's platform at a given time.

PTS POI devices inventory table should contain the following information:

- Device vendor: PAX.
- Device model name(s) and number: one of the device model names mentioned in section 2.1.
- Device location: the location of the payment terminal.
- Device status: One of the following states:
    - At merchant's: PTS POI devices are in use in a store.
    - In depot: PTS POI devices are stored for further distribution, either at a store or at a warehouse.
    - Expected for repair: PTS POI devices have been sent back to Market Pay for repair…
    - Decommissioned: PTS POI devices have been removed from service.
    - In transport: shipment of the PTS POI devices to a different location, record location as planned destination.
    - Unknown: PTS POI devices location is not known (lost…).
- Serial Number: serial number of the PTS POI devices.

You will find below a sample inventory table:

Sample Inventory Table

PTS POI Device Vendor	PTS POI Device Model Name and Number	Device Location	Device Status	Serial Number	Date of inventory	Additional notes (as needed)
PAX	A35	120-122 rue Réaumur, 75002 Paris, France	In Storage	1852204107	23/08/2025	

3. Receipt of PTS POI Devices

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

You should ensure PTS POI devices shipped are coming from a Market Pay's address or from one of our trusted partners:

- ELTRONIC, Ul. Graniczna 12, 05-816 Michałowice, Poland
- Liem, 11, Rue de Pyrénées, 91090 Lisses, France
- MielPOS Services, ZAC Les Portes de l'Oise, 5264 Rue Isaac Newton, 60230 Chambly, France

If you happen to receive PTS POI devices from a different source, please reach out to us at assist.market-pay.com to verify the situation. PTS POI devices must not be used unless the source location is verified as trusted. We will promptly inform you in the event that our list of PTS POI device providers undergoes any changes.

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

After confirming PTS POI device(s) originate from a trusted location, you have to ensure PTS POI device and packaging were not tampered with. To do so, you can follow these online guides:

- PTS POI packaging was not tampered with.
- PTS POI device was not tampered with. You can follow our guide for each terminal:
  - PAX A35
  - PAX A920Pro
  - PAX IM30

If the package shows any sign it has been tampered with or if the delivery note does not match the package, immediately inform Market Pay and do not install the PTS POI device.

After confirming PTS POI packaging was not tampered with, you have to confirm PTS POI device(s) were not tampered with.

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.

Payment terminal issues are generally managed centrally without the necessity of on-site assistance. However, in exceptional circumstances, there may be a legitimate need for a technical support engineer to provide on-site assistance. We will engage in a discussion with you to determine whether this is required. Market Pay, or an authorized field service partner of Market Pay, will confirm the identity and expected arrival date of the technical support engineer in advance. When the technical support engineer arrives, please adhere to the following precautions:

- Verify the identity of the technical support engineer before granting access to the payment terminal.
- Do not allow access to the PTS POI device for individuals who are unexpected or unidentified.
- Accompany and oversee the technical support engineer while they have access to the PTS POI.

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

Installation is key to ensure a smooth and secure deployment. For a comprehensive guide on setting up each type of PTS POI devices, please refer to our online documentation, which can be accessed at

https://assist.market-pay.com/hc/en-us/sections/36532416870801-Terminals

This documentation provides step-by-step instructions along with visual aids and specifications.

If you encounter any challenges during the initial setup or have inquiries related to the installation process, reach out to Market Pay using the contact information provided in section 1.2.

Note: *Only PTS POI devices listed in the PIM are allowed for use in the P2PE solution.*

4.2. Guidance for selecting appropriate locations to deploy the PTS POI devices

PTS POI devices must be deployed in a location which allows to limit risk of unauthorized access. Use the recommendations below to identify an appropriate location:

- **Public Access Control**: limit public access to essential parts of the PTS POI devices, like the PIN pad and card reader. Position PTS POI devices facing the shopper and prevent observation by others in the queue.
- **Monitoring**: monitor PTS POI devices through methods like CCTV/security cameras, or daily checks by authorized staff. Ensure cameras don't capture the PIN-entry keypad.
- **Environment**: install PTS POI devices in environments with adequate lighting, appropriate access paths, and visible security measures like CCTV.
- **Unattended PTS POI**: secure unattended PTS POI devices with toughened, tamper-evident housings, and alarm systems to detect any tampering attempt.
- **Mobile PTS POI devices**: assign mobile devices to a staff member responsible for its security during use.

4.3. Guidance for physically securing deployed PTS POI devices to prevent unauthorized removal and/or substitution

All PTS POI devices used in a store must be physically secure to prevent any unauthorized operations. This can be accomplished by employing mounting plates or other security mechanisms.

In cases where PTS POI devices cannot be physically secured, you have to:

- Store the PTS POI devices in a secured location with controlled access when not in use
- Assign responsibility to an authorized employee when PTS POI devices is in use
- Monitor the PTS POI devices when in use

PTS POI devices which are not in use (in stock, under repair…) should also be stored in a secure location with controlled access (e.g. a locked room, a locked cupboard, or a safe…).

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

You will find below instructions for physically inspecting PTS POI devices and preventing tampering:

1. Conduct periodic inspections, which consist in visual inspections, to ensure the device's integrity. To guide you through the inspection, you can refer to manufacturer security policies (section *3.5 Periodic Inspection and Maintenance*):
    a. A35: https://listings.pcisecuritystandards.org/ptsdocs/4-40305A35%20Security%20Policy.pdf
    b. A920Pro: https://listings.pcisecuritystandards.org/ptsdocs/4-40333Security_Policy_A920Pro_v1.03-1657915855.25356.pdf
    c. IM30: https://listings.pcisecuritystandards.org/ptsdocs/4-40372%20IM30_Security_Policy-1690595139.75956.pdf
2. Record periodic inspections once performed. It should, at least, include inspection results and date associated with the serial number of the PTS POI device.

Report any suspicious activity immediately to Market Pay via the contact information in section 1.2.

If you find evidence of PTS POI device tampering, you must follow these instructions:

- Do not use the PTS POI device for payment anymore.
- Remove the PTS POI device from the counter, to avoid any payment.
- Report any tampering with PTS POI device immediately to the contact information in section 1.2
- Label the PTS POI device as tampered/compromised, to avoid limit risk using the device for payments.
- Return the PTS POI device to Market Pay as instructed in section 5.2.
- Keep a record of returning the payment terminal as described in section 5.2

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://pcisecuritystandards.org/document_library/.

You will find below instructions for physically inspecting PTS POI devices and preventing skimming:

1. Conduct periodic inspections, which consist in visual inspections, to ensure the device's integrity. To guide you through the inspection, you can refer to manufacturer security policies (section *3.5 Periodic Inspection and Maintenance*):
    a. A35: https://listings.pcisecuritystandards.org/ptsdocs/4-40305A35%20Security%20Policy.pdf
    b. A920Pro: https://listings.pcisecuritystandards.org/ptsdocs/4-40333Security_Policy_A920Pro_v1.03-1657915855.25356.pdf
    c. IM30: https://listings.pcisecuritystandards.org/ptsdocs/4-40372%20IM30_Security_Policy-1690595139.75956.pdf
2. Record periodic inspections once performed. It should, at least, include inspection results and date associated with the serial number of the PTS POI device.

Report any suspicious activity immediately to Market Pay via the contact information in section 1.2.

If you find evidence of skimming device, you must follow these instructions:

- Do not use the PTS POI device for payment anymore.
- Remove the PTS POI device from the counter, to avoid any payment.
- Report skimming and PTS POI devices immediately to the contact information in section 1.2
- Label the PTS POI device as compromised, to avoid limit risk using the device for payments.
- Send Skimming device and PTS POI device to Market Pay as instructed in section 6.2.
- Keep a record of returning the payment terminal as described in section 6.2

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

Encryption is displayed on Market Pay reporting trough a dedicated flag. In the event of an encryption failure at the device level, the incident must be reported to Market Pay or its partner for technical support and analysis. The device shall be removed from usage in the store as security is no longer ensured.

In case the issue cannot be solved remotely, the device must then be sent back to Market Pay or to its partner using the validated maintenance process.

5.4. Instructions for troubleshooting a PTS POI device

If a payment terminal experiences operational issues, you can access solutions for the most prevalent errors on Market Pay's knowledge base: https://assist.market-pay.com/hc/en-us/sections/36619236117905-Troubleshooting.

Market Pay Docs offers a detailed guide on the installation, updates, and configuration of PTS POI. Additionally, it provides instructions for troubleshooting common problems. If you are unable to resolve the issue through the Market Pay website, you can get in touch with Market Pay using the contact information specified in section 1.2.

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)

You should ensure PTS POI devices you are shipping to Market Pay (returns, repair, technical analysis…) are shipped exclusively to Market Pay or to one of its trusted partners:

- ELTRONIC, Ul. Graniczna 12, 05-816 Michałowice, Poland
- Liem, 11, Rue de Pyrénées, 91090 Lisses, France
- MielPOS Services, ZAC Les Portes de l'Oise, 5264 Rue Isaac Newton, 60230 Chambly, France

If you are shipping PTS POI devices to a different location, please reach out to us at assist@market-pay.com to confirm it is expected. We will promptly inform you in the event that our list of partners undergoes any changes.

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

Ensure you follow instructions below when preparing shipments of PTS POI devices:

- Store the PTS POI devices in a sealed box or a sealed package.
- Use a courier providing shipment tracking information.
- Send Serial Numbers of PTS POI devices being shipped and the shipment tracking number to the recipient in an electronic way.
- Ensure that the recipient controls the shipment as explained in section 2.2

In addition, ensure to comply with these two rules:

- Register all PTS POI devices shipments in order to be compliant with section 3.3
- Report any outstanding issue to Market Pay via the contact information in section 1.2.