P2PE PIM

axept®

September 2025

optomany
payment solutions

optomany
axept®

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:	*axept*
P2PE Solution Listing Reference Number (***Assigned by PCI SSC***)	*2025-01044.018*
https://listings.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions	

1.2 P2PE Solution Provider Contact Information					
Company Name:	*Optomany Ltd*	Company URL:	*https://dnapayments.com/*		
Contact Name:	*Optomany Helpdesk*	Title:			
Telephone:	*+44 (0)20 8102 8100*	E-mail:	*support@dnapaymentsgroup.com*		
Business Address:	*10 Lower Grosvenor Place, London, SW1W 0EN*	City:	*London*		
State/Province:	*London*	Country:	*UK*	Postal Code:	*SW1W 0EN*

1.3 Communication Instructions
Instructions advising how to contact the P2PE Solution Provider, with consideration to establishing a trusted communication channel/session.
Please direct all communication to the contact's name provided above.

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)*
4-40094	*PAX Technology Limited*	*S300 (MOS)*	*S300-abc-dx3-0xxx (where a=0, M b=0, G, C, T, W, E c=0, L, A and d=0, 3)*	*SRED (CTLS): Prolin 21.3xx.xxx.xxx.1xx (Boot 1.0.0 PED 001), 3.02.xx*	*App#2* *App#3*	*SW#1* *SW#2*
4-40088	*PAX Technology Limited*	*S800 (MOS)*	*S800-abc- dx3-0xxx (where a=0, M b=0, G, C, T, W, E, c=0, L, A and d=0, 3)*	*SRED (CTLS): Prolin 21.3xx.xxx.xx x.1xx (Boot 1.0.0 PED 001)* *3.02.xx*	*App#2*	*SW#1* *SW#2*
4-40089	*PAX Technology Limited*	*S900 (MOS)*	*S900-abc- dx3-0xxx (where a=0, M b=0, G, C, T, W, E c=0, W and d=0, 3)*	*SRED (CTLS): Prolin 21.3xx.xxx.xx x.1xx (Boot 1.0.0 PED 001)* *3.02.xx*	*App#2*	*SW#1* *SW#2*
4-30224	*PAX Technology Limited*	*S300*	*S300-xxx-0x4-0xxx (w/o CTLS), S300xxx-3x4-0xxx (with CTLS)*	*14.01.xx xxxx*	*App#2* *App#3*	*SW#1* *SW#2*
4-30225	*PAX Technology Limited*	*S800*	*S800-xxx-0x4-0xxx (w/o CTLS) S800-xxx-3x4-0xxx (with CTLS)*	*14.01.xx xxxx*	*App#2*	*SW#1* *SW#2*

4-30204	*PAX Technology Limited*	*S900 ECR*	*S900-xxx-0x4-0xxx (no CTLS support)* *S900-xxx-3x4-0xxx (with CTLS support)* *S901-0xa-bx4-0xxx (a=L Ethernet* *S901-0xa-bx4-1xxx (a=L Ethernet*	*14.00.xx xxxx* *14.01.xx xxxx*	*App#2*	*SW#1* *SW#2*
4-40269	*PAX Technology Limited*	*A77*	*A77-xxx-Rx5-0xxx* *A77-xxx-0x5-0xxx* *A77-xxx-Rx5-1xxx* *A77-xxx-0x5-1xxx* *A77-xxx-Rx5-2xxx (CTLS)* *A77-xxx-0x5-2xxx (NON-CTLS)*	*25.02.xxxx*	*App#1* *App#4*	*SW#1* *SW#2*
4-30301	*PAX Technology Limited*	*A80*	*A80-xxx-Rx5-0xxx (with CTLS)* *A80-xxx-0x5-0xxx (without CTLS)* *A80xxx-Rx5-1xxx (with CTLS)* *A80-xxx-0x5-1xxx (without CTLS)* *A80xxx-Rx5-1xxx (with CTLS)*	*25.02.xxxx*	*App#1* *App#4*	*SW#1* *SW#2*
4-40215	*PAX Technology Limited*	*A920*	*A920-xxx-0x5-0xxx (Non CTLS)* *A920xxx-Rx5-0xxx (CTLS)* *A920-xxx-0x5-1xxx* *A920-xxx-Rx5-1xxx (CTLS)* *A920-xxx-0x5-2xxx (NON-CTLS)*	*25.03.xxxx*	*App#1* *App#4*	*SW#1* *SW#2*

			A920-xxx-Rx5-2xxx (CTLS) *A920-xxx-0x5-3xxx (NON-CTLS)* *A920-xxx-Rx5-3xxx (CTLS)*			
4-40273	*PAX Technology Limited*	*A920 Pro*	*A920Pro-xxx-Rx50xxx* *A920Pro-xxx-0x50xxx* *A920Pro-1xx-Rx51xxx* *A920Pro-1xx-0x51xxx* *A920Pro-xxx-Rx5-2xxx (with contactless)* *A920Pro-xxx-0x52xxx (without contactless)* *A920Pro-xxx-0x53xxx (NON-CTLS)* *A920Pro-xxx-Rx5-3xxx (CTLS), A920Pro-xxx-0x51xxx (NON-CTLS)* *A920Pro-xxx-Rx51xxx (CTLS)*	*25.03.xxxx*	*App#1*	*SW#1* *SW#2* *SW#3* *SW#4* *SW#5*
4-30371	*PAX Technology Limited*	*IM30*	*IM30-xxx-Rx5-0xxx (with CTLS), IM30xxx-0x5-0xxx (without CTLS)*	*25.00.xxxx*	*App#1*	*SW#1* *SW#2*

4-30400	*Verifone*	*T650p*	*H561-07-aa-0Nxxxx-A1 (a=0-9; A to F)* *H561-07-xx-0Nxxxx-A1*	*SRED 1.x.x.xxx* *Android: 1A.x.x* *Android: 2.0C.x* *SP Driver: T650P-AS-1A.x.x* *SP Core: T650-A-P3A.x.x* *SP Core DLL: T650A-D-1A.x.x* *SRED 1.0.0.xxx*	*App#1*	*SW#1* *SW#2*
4-90100	*PAX Technology Limited*	*Q25*	*Q25-xxx-0x5-0xxx (Non CTLS)* *Q25-xxx-0x5-Axxx (Non CTLS)* *Q25-xxx-Rx5-0xxx (CTLS)* *Q25-xxx-Rx5-Axxx (CTLS)*	*15.00.xx xxxx*	*App#2* *App#3*	*SW#1* *SW#2*
4-40312	*PAX Technology Limited*	*A77*	*A77-xxx-Rx6-0xxx (CTLS reader), A77xxx-0x6-0xxx (No CTLS reader) A77xxx-0x6-1xxx (NONCTLS)* *A77-xxx-Rx6-1xxx (CTLS)* *A77-xxx-0x6-1xxx (NON-CTLS)*	*26.00.xxxx*	*App#1*	*SW#1* *SW#2*
4-90124	*ShenZhen Xinguodu Technology Co Ltd*	*N86*	*V1.0x* *V1.1x* *V1.2x*	*Z32020032.xxxxxx*	*App#1*	*SW#1* *SW#2*

			V1.3x V1.4x V1.5x V1.6x V1.7x V1.30xx V1.31xx V1.3A0xx V1.3A1xx V1.3A2xx V1.3A3xx V1.70x V1.71x			
4-40305	PAX Technology Limited	A35	A35-xxx-0x6-0xxx (No CTLS reader) A35-xxx-0x6-Axxx (No CTLS reader) A35-xxx-Rx6-Axxx (CTLS reader) A35-xxx-Rx6-0xxx (CTLS reader)	26.00.xxxx	App#1	SW#1 SW#2
4-40333	PAX Technology Limited	A920 Pro	A920Pro-xxx-Rx6-0xxx (CTLS) A920Pro-xxx-0x6-0xxx (NON-CTLS) A920Pro-2xx-0x6-1xxx (Non-CTLS) A920Pro-2xx-Rx6-1xxx (CTLS) A920Pro-2xx-0x6-2xxx (Non-CTLS) A920Pro-2xx-Rx6-2xxx (CTLS) A920Pro-3xx-0x6-2xxx (Non-CTLS) A920Pro-3xx-Rx6-2xxx (CTLS)	26.01.xxxx	App#1	SW#1 SW#2

4-90230	*ShenZhen Xinguodu Technology Co Ltd*	*UN20*	*V1.00xx* *V1.01xx*	*Z32010011.xxxxxx*	*App#1*	*SW#1* *SW#2*

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	*Optomany Ltd*	*a.2.01.XX.XX*	3.1	*2024-01044.016*
App#2	*Optomany Ltd*	*p.1.2.X*	3.1	2023-01044.015
App#3	*Optomany Ltd*	*p1.3.X*	3.1	2025-01044.017
App#4	*Pax Technology Europe Limited*	*eftp2pe, 2.0.X.X*	3.1	2024-01379.002

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*)

SW#1	*Optomany Ltd*	*axeptSvc*	*1.00.XX.XXXXX*	
2.3 Non-Payment Software Details				
SW#2	*Optomany Ltd*	axeptPro	*1.00.XX.XXXXX*	
SW#3	*Optomany Ltd*	positiveSvc	*0.00.XX*	
SW#4	*Optomany Ltd*	positiveSvc	*1.00.XX*	
SW#5	*Optomany Ltd*	positive	*1.00.XX*	

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
You can identify the POI device by examining specific details on the device itself. The model number is usually located near the screen, while the serial number is printed on a silver sticker on the underside of the device (please section 7). These details are also included in the email sent by our Order team. Additionally, you can compare the device with the POI device images provided in this manual for confirmation. *Identifying POI device firmware and application version varies for different devices. Please contact contact Optomany Helpdesk via the contact information in Section 1.2 above for guide for your device.* *If you observe any discrepancy in the software or hardware, contact Optomany Helpdesk via the contact information in Section 1.2 above*

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.

The POI inventory must be updated to reflect any changes to the payment devices status once installed. This will form a resource that can be used to identify the location of any device, e.g. warehouse, site address. Methods for keeping an inventory record include but are not limited to:

- *Spreadsheets*
- *Paper records*
- *CRM System or 3rd party stock management system*
- *Database*

The inventory record must document the following information about the devices when received and when completing any stock takes or device transfers to alternative locations:

- *Make / Model / product number and brief description*
- *Serial number of the device*
- *Deployed / Operational / Awaiting deployment / Maintenance / Not in Use / In transit*
- *Device location e.g. secure storage, merchant site*
- *Security seal integrity*
- *Number / Type of physical connections*
- *Firmware version*
- *Application version*
- *Date of last device inspection*

The inventory record must be secured to ensure only authorised personnel are permitted to review and update the device information. Security measures include but are not limited to:

- *Password controlled access to users for any electronic systems*
- *Regular password changes for electronic systems that apply a strong password requirement*
- *Regular checks of user access lists to limit access to be at a level required to maintain effective inventory keeping*
- *Any physical records e.g. paper, should be accessible only to authorised personnel and should be stored securely when not in use*
- *Updates and changes to any record should maintain an audit trail of all changes that can be traced back to an individual user and their activity*

Inventory Check Procedures

The inventory check must be completed annually at a minimum and should be completed with the following criteria under consideration:

- *Check all serial numbers are valid within the estate (device)*
- *Complete physical checks on the devices for any signs of tamper*
- *Any substitutions or lost devices must be reported to Optomany's Customer Services team for investigation.*
- *Verify all device serial numbers in the process of being repaired or replaced by Optomany do not exist at any trusted merchant site or storage location.*
- *Location of devices recorded in the central inventory should be crossed referenced with the devices' actual physical location.*
- *Inventory checks should only be completed by authorized personnel.*
- *Total number of devices should be checked against the total number contained within the inventory record. The description and device type should be checked to match the devices in the field.*
- *Date of last audit should be recorded against the device when checked.*

Any discrepancies found when auditing using the above criteria should be validated by a second, authorised person. Once verified Optomany must be contacted to investigate further

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)

3. Receipt of PTS POI Devices

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

Merchants may transport devices only to trusted sites / locations. Optomany will only ever ship devices to the merchant from the below facilities at the following addresses:

UKPR, Units 1 – 4 Alderston Way, Righead Industrial Park, Bellshill, ML43LT

Once a device is received by the merchant from Optomany or its approved partners, they may be transported to other locations within the merchant environment. If a device is received from any unknown location, it must not be installed for use.

In circumstances where devices are to be shipped from a central storage location to secondary trusted merchant site (e.g. head office/ to a store), all transportation of the devices must adhere to the same protocol as when the devices were received by the merchant.

Examples of trusted sites are head office, merchant stores, storage facilities or approved partner locations.

The merchant must maintain a list of trusted site location including addresses and any associated site ID numbers. The list should also contain authorised personnel names and contact details.

Optomany shall dispatch the devices in individually sealed tamper evident security bags inside a box, one device per box. The tamper evident bag will display a unique serial number. If there is any evidence or concern that the packaging has been tampered with the device must not be installed and you must contact Optomany to facilitate the return of the device for further investigation.

To validate the integrity and authenticity of the devices the merchant must observe the following:

- *Utilise the delivery confirmation email as the only reference point for all serial number validation. Any included documentation contained within the delivery packing must not be used to verify the serial numbers.*
- *Check and confirm that all device and security bag serial numbers received to site are present in the email list received from Optomany.*
- *Do not install any payment device whose serial numbers that have been received to the merchant site do not appear on the Optomany delivery confirmation email.*
- *Check the number of security bag and device serial numbers match in quantity e.g., 20 devices are in 20 security bags.*
- *Check the number of devices received matches the quantity detailed in the delivery confirmation email e.g., 20 devices dispatched, only 19 delivered to site*

If any of the above scenarios occur a query must be raised to Optomany for further investigation immediately. Additionally, any devices not fulfilling the above criteria must not be considered as a trusted device and you must contact Optomany immediately.

When devices are to be couriered to a second location, for storage or installation, a secure mode of transportation must be utilised e.g., trackable carrier. The shipment should be traceable and signed for at the delivery location by an authorised member of staff, e.g., duty manager. The inventory record should be updated to reflect the new location of devices

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

The device packaging must be inspected to verify no tampering before the device is removed. Then serial number on the tamper bag must be checked to match that which was communicated via email. If it does not match or signs of tamper, contact Optomany Helpdesk via the contact information in Section 1.2 above.

The following possible inspections should be considered as part of the tamper inspection. This list is not exhaustive:

- *Check all seals where the device may be opened to access internal parts.*
- *Check the material for any scrape marks or damage that may suggest forced entry into the device components.*
- *Check for software tamper mode when the device is powered up.*
- *Photographs to aid this process can be found in Section7 at the end of this document.*

If any devices are found to have been tampered with contact Optomany Helpdesk via the contact information in Section 1.2 above

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.

Optomany will not send engineers or third-party service providers to merchant site to inspect or repair POI devices without previously discussing with merchant. Please contact Optomany Helpdesk via the contact information in Section 1.2 above if you experience an unscheduled visit and do not permit access to your device(s).

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

Devices must NEVER be removed from the tamper evident packaging until they reach their destination and if devices are shipped to a central facility, they must be distributed to their final location via a bonded / trackable courier or similar secure method.

When installing the devices, the device packaging must be inspected to verify no tampering before the device is removed. If the packaging shows signs of tamper, the devices must not be installed and Optomany must be contacted for further investigation. Once removed from the packaging, the device must be inspected to ensure that there are no signs of tamper. The following possible inspections should be considered as part of the tamper inspection. This list is not exhaustive:

- *Check all seals where the device may be opened to access internal parts*
- *Check the material for any scrape marks or damage that may suggest forced entry into the device components*
- *Check for software tamper mode when the device is powered up*

If any devices are found to have been tampered with, contact Optomany for further investigation.

Provided the inspection of the devices has been completed successfully with no evidence of tampering, the installation of the device can continue as per the payment solution instructions which are detailed fully in the Optomany axept® Quick Start guide, supplied alongside this device.

4.2 Guidance for selecting appropriate locations to deploy PTS POI devices

When selecting a location for deploying devices the following guidelines should be considered:

- *Limit access to only the parts of the device that are required for payment processing, e.g. keypad, card reader access, mag stripe reader access*
- *Position devices so they can be readily observed and/ or monitored by authorised personnel. The position of the device should be chosen to deter any attempt to tamper or compromise it. Optomany recommend weekly device checks should be performed by store/ security staff*
- *If the devices are being installed in a remote or unattended location, tamper mechanisms must be put in place to monitor the device status. The use of monitoring equipment or other physical mechanisms should be put in place to alert staff/ personnel of a breach in device integrity, e.g. alarms. If a device is being installed in a remote location at a merchant site the device must either be monitored to an appropriate level (e.g. security camera), or the merchant must create a process to check the integrity of the device in a periodic basis (e.g. store security or staff checks).*

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

Deployed devices must be physically secure to prevent unauthorized removal or substitution. This can be achieved with the use of a locking pole mount or tether. However, if physical security mechanisms cannot be implemented because the payment device is wireless or handheld, the merchant must implement regular site checks to ensure the devices are installed and have not been removed or substituted.

Any such check must verify that the serial numbers of the devices are consistent against the merchant inventory as well as checking for signs of device tampering. These checks must be completed at regular intervals in line with the merchant's environment and must be completed by authorised personnel.

Any devices that cannot be physically secured (such as wireless or handheld devices), the merchant must:

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

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

The following possible inspections should be considered as part of the tamper inspection. This list is not exhaustive:

- *Check all seals where the device may be opened to access internal parts.*
- *Check the material for any scrape marks or damage that may suggest forced entry into the device components.*
- *Check for software tamper mode when the device is powered up.*

Photographs to aid this process can be found in Section 7 at the end of this document.

If any devices are found to have been tampered with, contact Optomany Helpdesk via the contact information in Section 1.2 above

In the case where a device has been inspected by the merchant and found to show signs of tampering, the merchant must contact Optomany's Helpdesk immediately. The following process will be initiated:

- *The Optomany Helpdesk will verify the device has been tampered with*
- *The merchant must remove this device from the payment environment immediately.*
- *Optomany shall raise a support call to return the tampered devices to a repair centre for further investigation.*
- *Merchant organises a replacement device*

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/

The following possible inspections should be considered as part of the tamper inspection. This list is not exhaustive:

- *Check all seals where the device may be opened to access internal parts.*
- *Check the material for any scrape marks or damage that may suggest forced entry into the device components.*
- *Check for software tamper mode when the device is powered up.*

Photographs to aid this process can be found in Section 7 at the end of this document.

If any devices are found to have been tampered with, contact Optomany Helpdesk via the contact information in Section 1.2 above

In the case where a device has been inspected by the merchant and found to show signs of tampering, the merchant must contact Optomany's Helpdesk immediately. The following process will be initiated:

- *The Optomany Helpdesk will verify the device has been tampered with*
- *The merchant must remove this device from the payment environment immediately.*
- *Optomany shall raise a support call to return the tampered devices to a repair center for further investigation.*
- *Merchant organises a replacement device*

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

To ensure cardholder data and the merchant are protected, the Optomany P2PE solution does not allow payments to be processed through a device that has suffered an encryption failure. Should an encryption failure occur the merchant must notify the Optomany helpdesk immediately using the details in section 1.2 as the device must be replaced with a secure payment device to allow the payment solution to continue to process card payments in a compliant manner.

5.4 Instructions for troubleshooting a PTS POI device

In the event of an issue occurring with Optomany's solution the merchant should check that all connections to the POI device are present and correct. If this is the case and the issue continues the merchant should contact the Optomany Helpdesk via the contact information in Section 1.2 above.

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)

Optomany Ltd will not send an engineer to your site to retrieve or replace any device without first contacting you to schedule. If your device is experiencing issues or is faulty, please contact Optomany Helpdesk via the contact information in Section 1.2 above.

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

The relocation of the payment devices must accommodate the following considerations:

- *Devices must be transported in tamper evident packaging via a trackable method such as a private courier. Optomany recommended the use of serialised, tamper evident security bags. The devices may already be in tamper evident packaging from the original Optomany delivery or replacements utilised by the merchant as part of any previous device testing or relocation efforts.*
- *A separate communication channel must be utilised to send a serial number list of the devices and security bags to the secondary site*
- *The secondary trusted site must validate the serial numbers of the devices and security bags (if serialised) against the separately communicated list and not against any documentation shipped with the devices.*
- *Do not install any devices that do not appear on the delivery communication list. The device serial numbers must be checked to ensure they match. • Check the number of security bag and device serial numbers match in quantity e.g., 20 devices dispatched = 20 devices delivered*
- *Complete tamper checks on the devices upon delivery and do not install any devices that show evidence of suspicious activity.*
- *Do not install any devices that have not been received from a trusted merchant site*

7. Additional Guidance / Instructions

7.1 PHOTOGRAPHS TO AID PHYISCAL INSPECTION OF POI DEVICES AND PREVENT SKIMMING	
S300 PIN PAD   	**Front:** The front l of the s300 houses the colour touch screen and keypad. **Back:** contains the device labels for general information, serial number and voltage information. The device power connections are also located on the back **Card Reader:** The bottom of the device houses the chip and pin card reader. There are no additional security marking or connector on the reader **Screw Positions**: There are eight screws positions on the back. Four are visible around the general information label. Four more are located under the back panel **Screen Pen**: This is located on the right of the device **S/N**: Unique device serial number **General Product**: Contain details of device manufacturer, model and power requirements **Power Connector**: device power connectors for USB and RS232 are located here
S800 Countertop Payment Terminal   	**Front:** The front l of the s800 houses the colour touch screen and receipt printer. **Back:** contains the device labels for general information, serial number and voltage information. The device power connections are also located on the back **Card Reader:** The bottom of the device houses the chip and pin card reader. There are no additional security marking or connector on the reader **Screw Positions**: There are five screws positions on the back. Three are visible around the general back area. Two more are located under the back panel **General Product:** Contains the device Manufacturer, Model and power requirements **S/N**: Unique device serial number

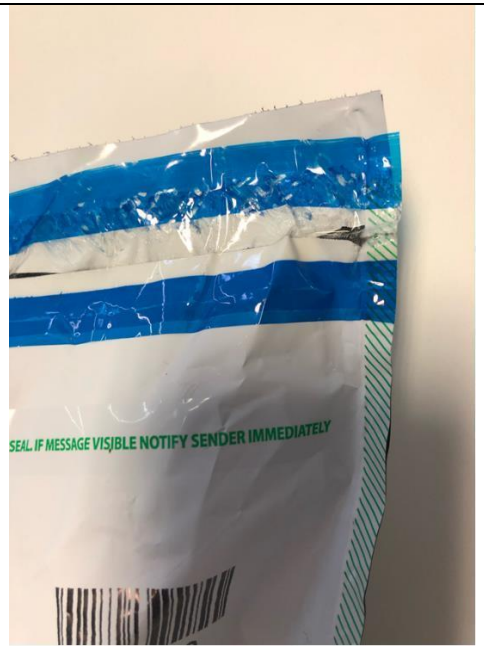
	Power: Device power adapter is connected to this socket **LAN/RS232B**: This is where the LAN/ RS2232 is connected **RS232**: This is where the RS2232 is connected **USB**: Single USB connector Line: Connects to the telephone line **PINPAD**: This is where the pin pad data cable is connected
S900 Mobile Payment Terminal 	**Front:** The front l of the s900 houses the colour touch screen and keypad **Back:** contains the device labels for general information, serial number and voltage information. The printer paper holder can be found on the back . The device cradle ports are also located on the back (bottom centre) **Card Reader:** The bottom of the device houses the chip and pin card reader. Additionally, underneath the card reader there is USB device port, serial port and external power adapter port. **Screw Positions:** There are six screw positions on the back . Two are visible by the paper chamber. Four more are located under the back panel. **General Product**: Contains the device Manufacturer, Model and power requirements **S/N**: Unique device serial number **SAM / SIM card locations:** The Cradle connector also shown here
Q25 Payment Terminal 	**Front:** houses the colour screen and keypad **Back**: contains the device labels for general information, serial number and voltage information. The device power connectors and SIM located are also located on the back. **Card Reader:** The bottom of the device houses the chip and pin card reader. There are no additional security marking or connectors on the reader. **Screw positions:** There are three screws on the back . Three are visible around the general back area **General Product**: Contains the device Manufacturer, Model and power requirements **S/N**: Unique device serial number

Payment Device - A920 Mobile Payment Terminal    	**Front :** houses the colour touch screen and keypad. **Back**: contains the device labels for general information, serial number and voltage information. The printer paper holder can be found on the back. **Card Reader:** The bottom of the device houses the chip and pin card reader. The top of the device is where contactless is located **Screw positions:** Back of the terminal can unlock for SIM cards etc. **General Product:** Contains the device Manufacturer, Model and power requirements, camera **S/N**: Unique device serial number
A920Pro Mobile Payment Terminal    	**Front**: houses the colour touch screen and keypad. **Back**: contains the device labels for general information, serial number and voltage information. The printer paper holder can be found on the back. **Card Reader:** The bottom of the device houses the chip and pin card reader. The top of the device is where contactless is located **Manufacturer Screw:** Back of the terminal can unlock for SIM cards etc. **General Product:** Contains the device Manufacturer, Model and power requirements, camera **S/N**: Unique device serial number
A77 Mobile Payment Terminal   	**Front:** houses the colour touch screen and keypad. **Back:** contains the device labels for general information, serial number and voltage information. The device ports are also located on the back (bottom centre) **Card Reader:** houses the chip and pin card reader. Additionally, underneath the card reader there is power point, headphones port **Manufacturer Screw:** There are no screws on back **General Product**: Contains the device Manufacturer, Model and power requirements **S/N**: Unique device serial number
A80 Mobile Payment Terminal	**Front:** houses the colour touch screen and keypad.

   	**Back:** contains the device labels for general information, serial number and voltage information. The device ports are also located in the middle of the back **Card Reader:** The bottom of the device houses the chip and pin card reader. The top of the reader houses the contactless reader **Manufacturer Screw** There are four screws on back . **General Product:** Contains the device Manufacturer, Model and power requirements **S/N:** Unique device serial number
IM30 Mobile Payment Terminal   	**Front:** The front of the IM30 houses the colour touch screen and keypad. **Back:** The back contains the device labels for general information, serial number and voltage information. The device ports are also located in the middle of the back **Card Reader:** The bottom of the device houses the chip and pin card reader. The top of the reader houses the contactless reader **Manufacturer Screw** There are eight screws on back . **General Product:** Contains the device Manufacturer, Model and power requirements **S/N:** Unique device serial number
Verifone T650p   	**Front:** houses the colour touch screen and keypad. **Back**: The back contains the battery **Card Reader:** The bottom of the device houses the chip and pin card reader. The top of the reader houses the contactless reader **Manufacturer Screw:** There are four screw positions on the back. four are visible by the battery chamber **Back Labels** - Serial cable connections , SIM card , Power
Nexgo UN20	**Front:** houses the colour touch screen and keypad.

	**Back:** The back contains the device labels for general information, serial number and voltage information. The device ports are also located in the middle of the back **Card Reader:** The bottom of the device houses the chip and pin card reader. The top of the reader houses the contactless reader **Manufacturer Screw** There are eight screws on back . **General Product:** Contains the device Manufacturer, Model and power requirements **S/N:** Unique device serial number
NexGo n86 	**Front :** The front of the n86 terminal houses the colour touch screen and keypad. **Back:** The back contains the battery **Card Reader:** The bottom of the device houses the chip and pin card reader. The top of the reader houses the contactless reader **Screw positions:** There are four screw positions on the back . Four are visible by the battery chamber **Back Labels:** Serial cable connections , SIM card, Power
Pax A35	**Front :** houses the colour touch screen and keypad.

	**Back:** The back contains the battery **Card Reader:** The bottom of the device houses the chip and pin card reader. The top of the reader houses the contactless reader **Screw positions:** There are seven screw positions on the back. **Back Labels:** Serial cable connections , SIM card, Power
Tamper Bag Examples 	The image to the left shows the tamper blue line intact – No visible breaks. Correctly sealed. Note the serial number is clearly visible

	The image to the left shows the tamper blue line is not intact and clear evidence of tampering