TDMS Point-to-Point Encryption (P2PE) Solution

Instruction Manual

This document is for Merchants that use the TD PCI Point-to-Point Encryption Solution. It is meant to aid you in better understanding the solution and to help you secure your business from fraud.

For the:

- Verifone MX 915 & MX 925

1. P2PE Solution Information and Solution Provider Contact Details

1.1 P2PE Solution Information

Solution Name: TDMSPoint to Point Encryption (P2PE) Solution

Solution reference number per PCI SSC website: 2020-01281.001

1.2 Solution Provider Contact Information

Company Name: TD Merchant Solutions

Company address: 77 King Street West, 15th Floor, Toronto, ON, M5K 1A2

Company URL: https://www.tdmerchantsolutions.com

Contact name: TD Merchant Solutions Help Desk

Contact phone number: 1-800-363-1163 TTY 1-888-670-6651

Contact e-mail address: Not applicable

P2PE and PCI DSS

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

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

2.1 POI Device Details

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

Note all POI device information can be verified by visiting:
https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices

POI device vendor: Verifone Inc.
POI device model name and number: MX 915
Hardware version #: P177-409-01-R (MX 915)
Firmware version #(s): Vault: 13.x.x, AppM: 7.x.x; SRED: 4.x.x, OP: 7.x.x
PCI PTS Approval #(s): 4-10177

POI device vendor: Verifone Inc.
POI device model name and number: MX 925
Hardware version #(s): P177-50x-xx-xxx (MX 925)
Firmware version #(s): Vault: 13.x.x, AppM: 7.x.x, SRED: 4.x.x.110, OP: 7.x.x
PCI PTS Approval #(s): 4-10177

2.2 POI Software / applicaiton Details

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

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

Application vendor, name and version #	POI device vendor	POI device model name(s) and number:	POI Device Hardware & Firmware Version #	Is application PCI listed? (Y / N)	Does application have access to clear-text account data (Y / N)
VeriFone, Formagent / XPI	VeriFone	MX 925	P177-50x-xx-xxx Vault: 13.x.x, AppM: 7.x.x, SRED: 4.x.x.1105300, OP: 7.x.x	Y	Y
		MX 915	P132-409-01-R Vault: 13.x.x, AppM: 7.x.x, SRED: 4.x.x.110, OP: 7.x.x		

2.3 POI Inventory & Monitoring

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

To remain compliant, you must inspect your devices upon delivery/install and maintain an inventory of your current PIN Pads.

The following information must be recorded after your PINPad device has been installed:

- device manufacturer (upper left corner on the front of the device – Verifone in this case),
- make and model of device (on the back of the device on the label),
- serial number of the device, (on the back of the device on the label – see image to the right)
- device location and status (storage, where deployed, in transit, awaiting repairs or returned),
- date of location inspection (the last date that the device location was confirmed),
- date of last inspection (last date device was inspected for tampering),
- name of the job role or the personnel performing inspection, and
- date inventory was last updated.

During your inspection process, you must determine whether devices have been substituted. If you see any indication of this, your business may be compromised. To determine whether a device has been substituted, you should compare the information located on the device itself with the inventory information that you collected previously.

Also, your inspection should look for any indications that the device has been tampered with. This may include:

- missing, damaged, or altered tamper seals,
- mismatched keys,
- missing screws,
- incorrect keyboard overlays,
- external wires,
- holes in the device,
- labels / paint / coverings that could mask tampering,
- anything else that looks unusual or out of place, or
- the insertion of a “skimmer” device within the Magnetic Stripe Reader (MSR) of the device. Skimmers are devices used by unauthorized personnel trying to capture cardholder data prior to the PIN Pad reading the card. Skimmers may be inserted in the MSR of the device or overlaid on the device itself.

NOTE: We recommend that you train anyone using your PIN Pads to inspect them daily for tampering.

If you believe a device has been compromised, or find that your inventory indicated a missing, or device has been substituted, you must report this information to TD Merchant Solutions Help Desk at 1-800-363-1163 immediately.

For maintaining your inventory, you must track the device location and designate an individual to be responsible for maintaining the inventory and inspecting the devices.

Device inventories must be performed:

- at least annually to confirm that your device inventory is being catalogued and performed correctly,
- when a device is moved in and out of service or from one location to another, and
- to confirm that all devices identified are currently within your possession and not missing.

The storage location must include the following:

- Devices which are not in service must be stored in locked room or container such as a cabinet or drawer.
- The storage location must support restricted access to authorized personnel such as: door / container requiring key access in which defined personnel have access to the key;

  OR
- door / container required knowledge of cipher lock code in which defined personnel have knowledge of the cipher lock code.
- Access to the storage location must be logged. This may be done manually (written log) or automatically (identity card system).
- Access to the storage room must be monitored via cameras or physical sight.
- DO NOT swap devices between different stores or locations without contacting TD Merchant Solutions Help Desk at 1-800-363-1163.

Sample Inventory Table

Device vendor	Device model name(s) and number:	Device Location	Device Status	Serial Number or other Unique Identifier

3. POI Device Installation Instructions

Do not connect non-approved cardholder data capture devices.

The P2PE solution is approved to include specific PCI-approved POI devices. Only these devices denoted above in table 2.1 are allowed for cardholder data capture.

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

- The use of such mechanisms to collect PCI payment-card data could mean that there may be more PCI DSS requirements to which you are now subject.
- Only P2PE approved capture mechanisms as designated on PCI's list of Validated P2PE Solutions and in the PIM can be used.

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

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

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

3.1 Installation and connection instructions

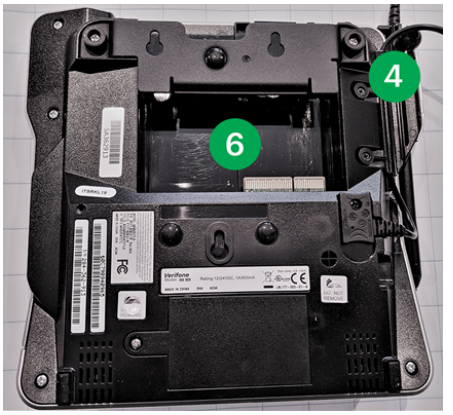
TD Merchant Solutions technicians will perform the installation, demo and training at your location(s).

MX 915

1. Chip card reader
2. Magnetic strip reader
3. Contactless card reader
   Tap the card on the touchscreen.
4. Stylus
5. Keypad
6. Data cable(s) to the register
   Please note that there can be more than one cable depending on the solution's connection type. In the image to the right, a USB connection is used, and a third cable would be used for power.

Cable connections on the device:

- USB to the electronic cash register (ECR)
- COM2
- Ethernet
- Audio
- Power



MX 925

7. Chip card reader

8. Magnetic strip reader

9. Contactless card reader
Tap the card on the touchscreen.

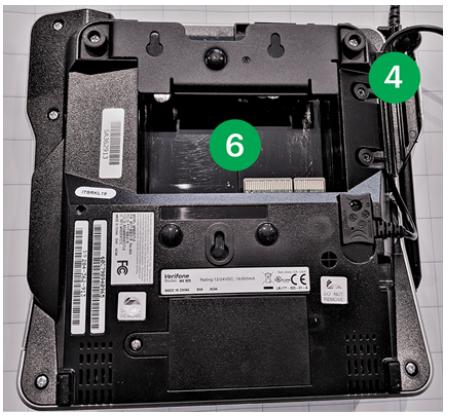
10. Stylus

11. Keypad

12. Data cable(s) to the register
Please note that there can be more than one cable depending on the solution's connection type. In the image to the right, a USB connection is used, and a third cable would be used for power.

Cable connections on the device:

- USB to the electronic cash register
- COM2
- Ethernet
- Audio
- Power



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

Physically secure POI devices in your possession, including devices:

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

3.2 Guidance for selecting appropriate locations for deployed devices

When determining where you will install your PIN Pad, you must take the following into account to find the ideal location.

PIN Pads should NOT be installed:

- in direct sunlight,
- within 60 cm (2 feet) of devices that cause excessive voltage fluctuations, electrical noise or radiate heat,
- within 2m (6.5 feet) from anti-theft doorway units,
- within 45 cm (1.5 feet) from surface mounted deactivator pads,
- outdoors when they are designed for indoor use only,
- in areas of excessive heat, dust, oil and moisture, or
- near any water.

PIN Pads should be installed:

- under good lighting, with a clear line of sight by authorized personnel, etc. to deter compromise attempts,
- in areas that provide adequate ventilation and protection from physical damage,
- to restrict physical access to devices such that device access is limited to only parts of the device a person is expected to use to complete a transaction, such as the PIN Pad and card reader,
- to restrict access to any part of the device that is not required for public use such as cables, power cords or access panels,
- in such a way that PIN spying is difficult, and
- so that the PIN-entry keypad is not visible by in-store security cameras.

We strongly suggest that you take photos of your PIN Pad (front and back) once it is installed. Then, use these as a reference whenever you perform a physical inspection for tampering.

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

We strongly suggest that you consider installing locking stands to prevent unauthorized removal.

The PIN Pad should be:

- mounted on the counter, and
- cables should not be easily unplugged such as by merely turning over the PIN Pad.

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

- secure devices in a locked room when not in use,
- sign devices in / out, etc. as necessary,
- assign responsibility to specific individuals when device is in use, and
- observe your devices at all times.

You should physically secure devices when not deployed or being used. This includes devices:

- undergoing repair or maintenance while in the merchant's possession, or
- awaiting deployment or transport between sites / locations.

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

- verifying the identity and authorization of repair personnel prior to granting access, and
- escorting and monitoring authorized personnel at all times.

4. POI Device Transit

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

A PIN Pad device must never be transported between merchant sites without the assistance of a TDMS technician.

You must call TD Merchant Solutions Help Desk at 1-800-363-1163 to create:

- a de-install request for an onsite Technician pick up, or
- a UPS Waybill and box drop off for courier shipping.

If you have any questions, please contact TD Merchant Solutions Help Desk at 1-800-363-1163.

4.2 Instructions for ensuring POI devices originate from, and are only shipped to, trusted sites / locations

A TDMS technician will install the PIN Pad device to your location for install.

Ensure that you validate their ID to verify they are who that they say they are.

If you have any questions, please contact TD Merchant Solutions Help Desk at 1-800-363-1163.

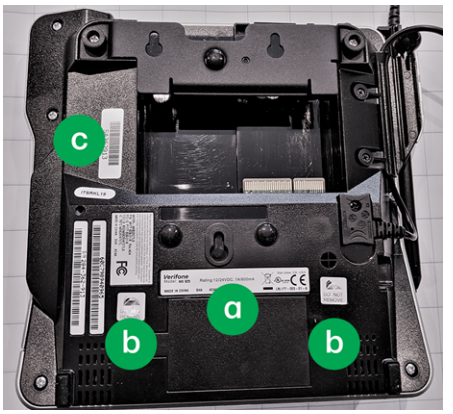
5. POI Device Tamper Monitoring and Skimming Prevention

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

Additional guidance for skimming prevention on POI devices can be found in the

document entitled Skimming Prevention: Best Practices for Merchants, available at www.pcisecuritystandards.org.

PERIODIC VISUAL DEVICE INPSECTIONS



1. Perform regular visual inspections on every device to look for potential signs of tampering. This includes anything such as:
   - **a)** missing, damaged, or altered manufacturer's sticker,
   - **b)** missing, damaged, or altered Do Not Remove stickers,
   - **c)** missing, damaged, or altered serial number sticker,
   - **d)** mismatched keys,
   - **e)** missing screws,
   - **f)** incorrect keyboard overlays,
   - **g)** external wires,
   - **h)** holes in the device,
   - **i)** labels / paint / coverings that could mask tampering, or
   - **j)** anything else that looks unusual or out of place.
2. Look for any hidden cameras in the ceiling.
3. Examine the dimensions of the terminal to detemrine if an overlay has been added. These overlays may contain equipment to scan cards and record PIN number. The dimensions should measure:

   MX 915: 225 mm (8.9 in.) Length × 182 mm (7.2 in.) Width × 56 mm (2.2 in.) Height; 0.6kg (1.3 lbs) weight.

   MX 925: 230 mm (9.1 in.) Length × 218 mm (8.6 in.) Width × 56 mm (2.2 in.) Height; 0.9kg (2.0 lbs) weight.
4. Verify that the cables have not been removed or changed.
5. If you notice anything out of the ordinary, stop using the device, disconnect it from the POS or network, but DO NOT power it down.
6. Contact the TD Merchant Solutions Help Desk at 1-800-363-1163 to determine the next steps.
7. Continue to perform visual inspections prior to any shift change.
8. Use the photos that you took, after the PIN Pad was installed in section 3.2, or refer to the image in Section 3.1, as a reference when you perform the inspection.

MONITOR PINPAD PAYMENT PROBLEMS

1. Develop a process to monitor devices that consistently do not work properly such as high card read failures or card declines. These can be indicators of tampered or compromised devices.
2. Contact the TD Merchant Solutions Help Desk at 1-800-363-1163 to determine the next steps.

MOUNT PINPADS SECURELY

Review the installation of your PINpads. They should be:

- mounted on the counter, and
- cables should not be easily unplugged such as by merely turning over the PIN Pad.

We strongly suggest that you consider installing locking stands to prevent unauthorized removal.

5.2 Instructions for responding to evidence of POI device tampering

If you have any suspicions that the device or packaging has been tampered with during shipping, or that a device has been compromised while deployed:

1. Do not deploy or use the device.
2. Contact the TD Merchant Solutions Help Desk at 1-800-363-1163 and report suspicious activity, including but not limited to:
    - **a)** a lost, stolen or compromised PIN Pad,
    - **b)** any unauthorized changes to PIN Pad configuration or access controls,
    - **c)** the unauthorized disconnection or reconnection of any devices,
    - **d)** any messages indicating encryption mechanism failure,
    - **e)** any messages indicating device security control failure, or
    - **f)** the connection of an unrecognized device.

If you need to return a P2PE device, you must call the TD Merchant Solutions Help Desk at 1-800-363-1163 for instructions.

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

Verify that the tamper evident seals on the device box are intact prior to breaking the seal to open the box.

If either the security seal, or the tamper evident seal, appear to have been tampered with:

1. Stop and do not unpackage the device any further.

2. Contact the TD Merchant Solutions Help Desk at 1-800-363-1163 to determine the next steps.

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

REPAIR TECHNICIAN VERIFICATION AND LOG

1. Implement a procedure to require all repair technicians who visit your stores sign in, and verify their identity by photo identification.
2. Technicians must be accompanied by store personnel during any work on PIN Pads.

6. Device Encryption Issues

6.1 Instructions for responding to POI device encryption failures

In the unlikely event the PIN Pad encryption and decryption fails:

1. Transactions will not be processed and display a Transaction not completed message.
2. You will be prompted to re-enter the transaction.

   If you see the Transaction not completed message again, please contact the TD Merchant Solutions Help Desk at 1-800-363-1163 for further instructions.

   DO NOT use the PIN Pad until you have been instructed by the TD Merchant Solutions Help Desk to do so.

6.2 Instructions for formally requesting of the P2PE solution provider that P2PE encryption of account data be stopped

There is no option available for you to turn off encryption within the device. Therefore, there are no process available to you for formally requesting that P2PE encryption of account data be stopped. Should you, the Merchant (or company executive), decide that the P2PE solution is no longer needed, then an authorized person from your business must contact your Sales Representative to discuss.

7. POI Device Troubleshooting

7.1 Instructions for troubleshooting a POI device

PCI requirements demand that PIN Pads must have built-in tamper detection capability and, if triggered, they will disable the device's ability to perform transactions. This can happen for a number of reasons, such as having a credit card skimmer applied to the device, someone attempting to physically break the device open, dropping the device, and many others.

If the device deems that it has been tampered with, it will:

1. Display a tamper message that cannot be turned off.
2. Please call the TD Merchant Solutions Help Desk at 1-800-363-1163 for the next steps.

When calling the TD Merchant Solutions Help Desk, ensure that you have the following information:

1. The serial number of the device as found on the back of the device.
2. The make and model of the device, e.g. Verifone MX 925.
3. Your POS System and middleware solution as well as version number.
4. The precise date and the local time when the problem occurred.
5. Any transaction references, e.g. authorization code or transaction identifier.
6. Are any other devices experiencing the same issue?
7. The steps to reproduce the problem.

For your own security, we ensure that all inquiries come from authorized personnel and that product information matches TD Merchant Solutions records. We will never ask merchants to submit card numbers during support calls.

8. Additional Solution Provider Information

Access to PIN Pads for service/repairs should be restricted to only TD Merchant Solution field technicians. A service call is initiated by the merchant through the TD Merchant Solutions Help Desk at 1-800-363-1163. To ensure proper monitoring of access to the PIN Pad, you should have proper process and procedures in place to ensure the following steps:

1. Authrorized personnel at your location must contact the TD Merchant Solutions Help Desk to initiate service calls and device de-install requests.
2. Personnel must authenticate and authrorize any TD Merchant Solutions field technicians upon arrival before they access the device.
3. TD Merchant Solutions field technicians have a TD issued photo ID badge clearly displayed at all times.
4. You should maintain a log with details of date, time, name and purpose for accessing devices.
5. TD Merchant Solutions field technicians must be escorted and observed at all times.
6. You must authorize any device swaps or removals, and you must update any inventory documentation with the new device information.