TranSafe® Payment Gateway

LockDown® P2PE Instruction Manual

Revision: 1.0.0
Publication date September 23, 2019

LockDown® P2PE Instruction Manual

Monetra Technologies, LLC

Revision: 1.0.0

Publication date September 23, 2019

Legal Notice

Table of Contents

1 P2PE Solution Information and Solution Provider Contact Details

1.1 P2PE Solution Information

Solution Name: `TranSafe® Lockdown®`

Solution Ref#: `2019-01232.001`

PCI Notice: The Solution Reference Number can be found on the PCI SSC web site: https://www.pcisecuritystandards.org/

1.2 Solution Provider Contact Information

Company name:	`Monetra Technologies, LLC` `d/b/a TranSafe`

Company address:	Physical:
	`2770 NW 43rd Street, Suite N`
	`Gainesville, FL 32606`
	
	Mailing:
	`PO Box 357548`
	`Gainesville, FL 32635`

Company URL:	`https://www.transafe.com/`
Contact name:	`Jessica Waddington`
Contact phone number:	`904-312-9592`
Contact e-mail address:	`p2pe@transafe.com`

PCI Notice: **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/approved_companies_providers/approved_pin_transaction_security.php

Note: Any device not listed cannot be used as part of a P2PE solution.

2.1.1 ID Tech: Augusta S

POI Device Vendor:	ID Tech
POI Device model name and number:	Augusta S
Hardware version #(s):	`IDEM-8xxx, IDEM-8xxxx, 80146001`
Firmware version #(s):	`V1.00, V1.01.xxx.S, V1.02.xxx.S, V1.03.xxx.S`
PCI PTS Approval #(s):	4-10218 [https://www.pcisecuritystandards.org/popups/pts_device.php?appnum=4-10218]

Security Policy:	https://www.pcisecuritystandards.org/ptsdocs/4-10218_IDTech_-_PCI-PTS_POI_Security_Policy_-Augusta_S-1510790891.36524-1542381400.01515.pdf

2.1.2 ID Tech: SREDKey

POI Device Vendor:	ID Tech
POI Device model name and number:	SREDKey
Hardware version #(s):	`IDSK-53XXXXXXX`
Firmware version #(s):	`SRED: 1.01, 1.02, 1.02.xxx.S`
PCI PTS Approval #(s):	4-10156 [https://www.pcisecuritystandards.org/popups/pts_device.php?appnum=4-10156]

2.2 POI Software/application Details

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

PCI Notice: 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.

The Lockdown® solution does not currently support the use of any software with access to clear text account data within the POI device. The currently supported devices utilize SRED readers which encrypt cardholder data in hardware thus not providing access to sensitive data within any software running on the device.

2.3 POI Inventory and 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 PO devices, must be reported to Monetra Technologies, LLC (Section 1.2) 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.

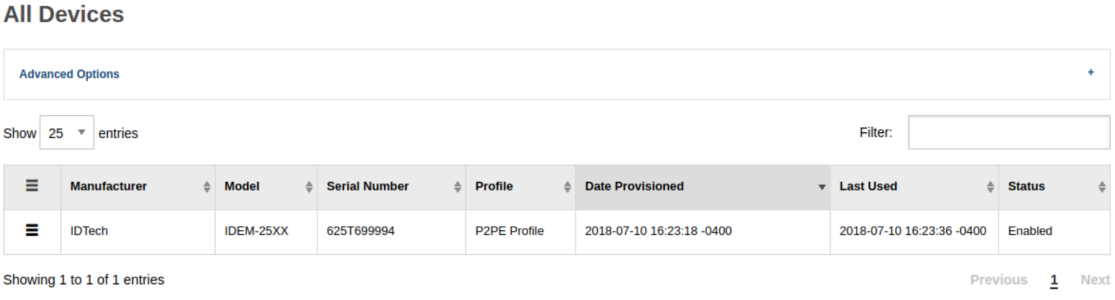
2.3.1 Sample inventory table

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

2.3.2 POI Inventory Tracking with TranSafe

TranSafe requires all devices are registered and tracked via the merchant management web interface: https://manage.transafe.com/merchant/devices. The table in the web interface can be used to assist merchants with the compliance requirements associated with inventory management.

Example inventory list in management web interface:



Note: The Profile column uniquely identifies a single merchant physical store, office, or other location.

The provided interface allows you to view all device event reports such as registration, activation, deactivation (manual or automatic), quarterly inspections, and decommissioning.

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 a merchants PCI-approved POI device is connected to a data capture mechanism that is not PCI approved, (for example, if a PCI-approved SCR was connected to a keypad that was not PCI-approved). • The use of such mechanisms to collect PCI payment-card data could mean that more PCI DSS requirements are now applicable for the merchant. • Only P2PE approved capture mechanisms as designated on the PCI list of Validated P2PE Solutions and in this 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 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

For detailed instructions on physically connecting devices, please consult with the UniTerm Guide available at https://www.monetra.com/docs/developer/UniTerm_Guide_v9.3.0.pdf, or contact your certified installer or the TranSafe help desk.

PCI Notice: 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

Public access to POI devices MUST BE CONTROLLED by the merchant so that public access is limited only to those parts of the POI a person is expected to use to complete a transaction (for example, PIN pad and card reader).

POI devices should be installed in such a manner that they can be easily observed and monitored by merchant operators at all times while in use.

When installing devices into the merchant environment, it is imperative to use tactics that deter compromise attempts (for example, through use of appropriate lighting, access paths, visible security measures, etc.). A means to physically secure the device(s) is a requirement for the prevention of unauthorized removal or substitution.

When using devices that are NOT customer facing (such as the IDTech Augusta) it is recommended that ONLY the merchant has physical access to the POI. If the device can be accessed by the customer then it is recommended the device be placed in such a manner that the merchant operator has a constant visual of the device while in use.

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

Merchants should physically secure deployed devices to prevent unauthorized removal or substitution while devices are in production use. The most common method is to purchase a stand (made specifically for the make/model of the POI device) and physically mount the stand to a flush counter top.

If the merchant has POI devices in their possession that are not being used (for example undergoing repair or maintenance) then those devices must be physically secured. An example of physically securing the device would be to lock it in a drawer or safe with restricted and logged access.

This includes both attended and unattended devices, as applicable to the P2PE solution (for example, kiosks, “pay-at-the-pump,” etc.). Note: In many un-attended solutions the POI device is embeded directly into the kiosk or pump itself.

If devices cannot be physically secured (such as wireless or handheld devices), or are being stored for future deployment, then the following guidance should be followed:

- Store devices in a locked room, or secure lock box only accessible to authorized personnel.
- Ensure devices are assigned to specific authorized individuals when in use and signed in and out of the secured area.
- Observe devices at all times, such as when handed to a customer for pay-at-the-table solutions.

4 POI Device Transit

There are times throughout the life-cycle of any POI device where the Merchant will be required to ship the POI device to or from a trusted location. Some examples of these events are as follows:

- A device must be forwarded to a specific Merchant location for final deployment.
- A device is defective and must be shipped back to the manufacturer/KIF facility.
- A location closed and the device(s) must be shipped back to headquarters, to be re-deployed.

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

POS devices being shipped, whether for repair or deployment, must be secured in tamper-evident packaging such as a TEA (Tamper Evident And Authenticatable) bag with a unique serial number. The device must also be shipped using a private bonded courier service or public shipping company with tracking information (e.g. UPS, USPS, DHL, FEDEX).

Additionally, you must be in contact with the company to which the package is being shipped and provide them with advanced notice and package tracking details and the means necessary to validate the shipment was not tampered during transport.

Note: Do not forget to update your device inventory with pertinent details when shipping a device.

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

POI devices will only be shipped to you DIRECTLY from a valid KIF facility (See approved KIF listings).

In addition to verifying the device has originated from a trusted source, you must also validate the integrity of the device. The first step would be to inspect the box to ensure the SECURE PACKING TAPE looks intact with no visible forced entry or removal across seams. Once opened, the device should be contained within a TAMPER EVIDENT BAG that again shows no sign of forced entry or tampering.

PCI Notice: If you receive a device from an unknown source OR you receive a device that you consider to be tampered with then DO NOT PUT THE DEVICE INTO PRODUCTION and notify Monetra Technologies LLC (Section 1.2) immediately of the incident.

5 POI Device Tamper Monitoring and Skimming Prevention

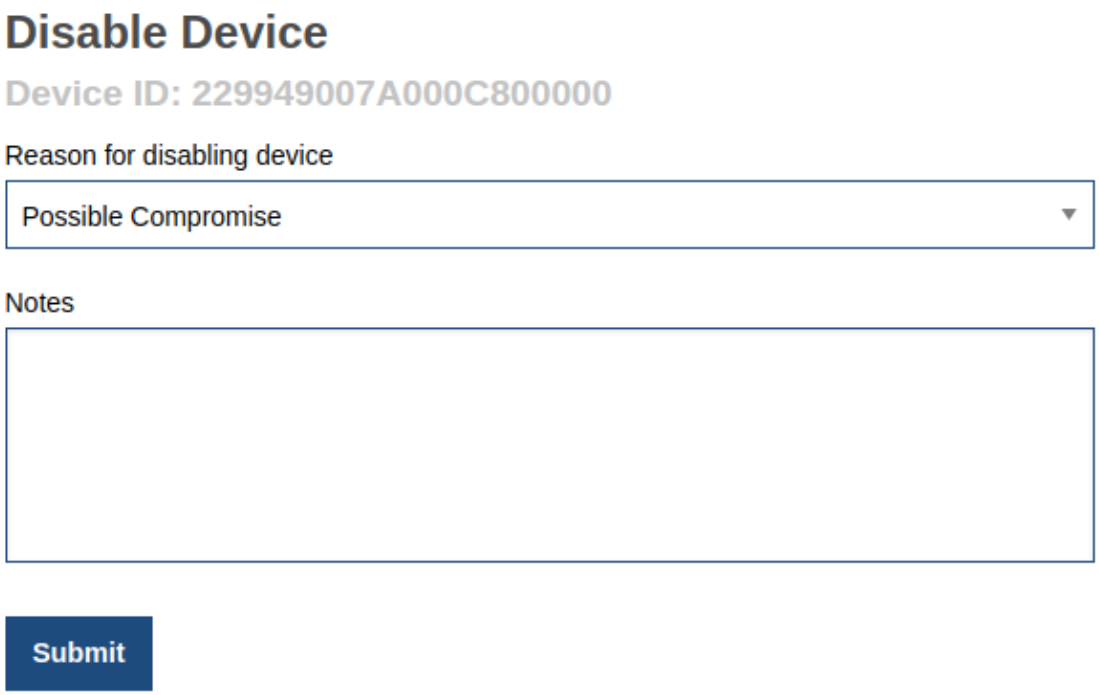
5.1 Instructions for physically inspecting POI devices and preventing skimming, including instructions and contact details for reporting any suspicious activity

PCI Notice: For more information regarding skimming the merchants should review the PCI SSCs Information Supplement Skimming Prevention: Best Practices for Merchants available at www.pcisecuritystandards.org.

After deployment, the merchant is responsible to perform periodic physical inspections of devices to detect tampering and/or modification, to include the following:

- Weigh and measure POI devices when received, compare to the specifications of the device vendor. Then during future inspection of deployed device, compare initial findings with findings of inspection to detect possible tampering or skimming devices.
- Check for missing or altered seals or screws, extraneous wiring, holes in the devices, or the addition of labels or other covering material that could be used to mask damage from device tampering.
- Monitor devices in remote or unattended locations, such as via the use of video surveillance or other physical mechanisms to alert personnel.
- Validate the serial number matches the expected value.

If any device is deemed to be suspicious STOP USING THE DEVICE immediately and disable the device via the merchant management portal at https://manage.transafe.com/merchant/devices. To disable a device, select the pancake menu next to the affected device and choose the `Disable` option and enter the appropriate details regarding the tampering suspected:



You may also contact Monetra Technologies LLC (Section 1.2), your reseller, or Key Injection Facility for further information about returning the affected device.

5.1.1 Additional Device Inspection Information

5.1.1.1 ID Tech August S

To check the tamper evidence

- Check the tamper evidence physical seals, make sure they are intact.
- Power on the device, check the beeper, making sure there is not non-interval beeping shows the tamper was triggered.

Check the hardware version on the label, power on the device, send a `deviceinfo` request to UniTerm to check the firmware version that conform to the version purchased.

5.1.1.2 ID Tech SREDKey

To check the tamper evidence

- Check the tamper evidence physical seals, make sure they are intact.
- Power on the device, check the beeper, making sure there is not non-interval beeping shows the tamper was triggered.

Check the hardware version on the label, power on the device, send a `deviceinfo` request to UniTerm to check the firmware version that conform to the version purchased.

5.2 Instructions for responding to evidence of POI device tampering

If the merchant EVER has any suspicion that the device or packaging has been tampered with during shipping, or that a device has been compromised while deployed then the device MUST NOT BE DEPLOYED OR USED, and marked as disabled as per the previous section.

Contact the device provider to report suspicious activity, and to return the affected device. Possible reasons include (but are not limited to):

- Physical device breach
- Logical alterations to device
- Failure of encryption mechanisms

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

5.3.1 Out of band communication

The Key Injection Facility that ships the POI device will communicate out of band from the device shipment a list of device serial numbers and tracking numbers for devices being shipped. Specifically, however, the Tamper Evident bag number is NOT provided in this communication. Valid communication methods include:

- e-mail
- fax
- Physical mailing: USPS, UPS, FEDEX, DHL

This communication must be kept on file for tamper verification.

5.3.2 POI Inspection upon reception

Immediately upon reception of the POI device, perform the following steps:

- Verify that any tamper evident tape or packaging is in-tact. If there is evidence of tampering, please follow steps in Section 5.2 regarding how to respond to and record POI tampering.
- Match tracking numbers and device serial numbers with those provided out of band.
- Provision the device with TranSafe via the management web portal.

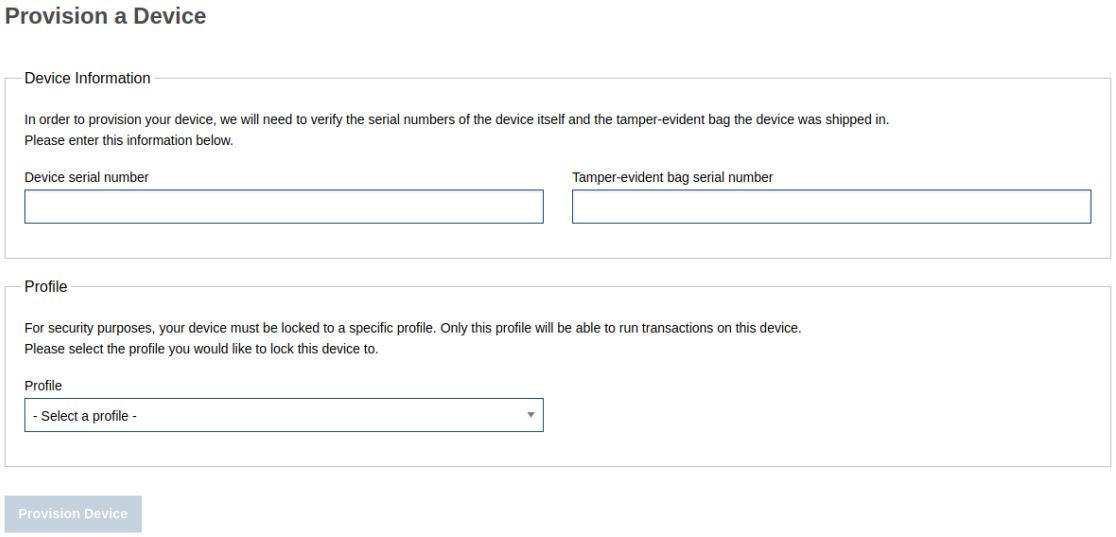
- Deploy the device to the intended location or securely store the device for future deployment. Please see Section 3.3 for information on secure storage of devices prior to deployment.

Example of outside of box with tamper evident tape:

Example of additional box inside of shipping container, again with tamper evident tape:

Example of tamper evident bag containing actual POI device:

In order to provision the device with TranSafe, open the management web portal at https://manage.transafe.com/merchant/devices/provision, and enter the device serial number, tamper evident bag number, and merchant profile (location) to associate the device with as seen in the screen shot below:



5.3.3 POI Deployment

Devices should be stored in original tamper-evident packaging and stored securely prior to deployment. Once the packaging has been opened, perform a pre-installation inspection using the same methods as described in Section 5.1.

Install the device in accordance with Section 3.2 and Section 3.3.

Finally, perform a functional test by powering on the device and attempting to run a transaction with a test card. This test must NOT result in any sort of decryption related failure, but will result in a decline due to the use of a test card.

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

Identification of Authorized Maintenance Personnel

All maintenance of the device is to be performed by the Key Injection Facility (KIF) where the device was ordered. The KIF will always be one listed within Appendix B, and is strictly serviced by shipping the device to and from the KIF. At no time will any representative ever visit a merchant location in order to service a POI device. Therefore, any third-party personnel who are on-site requesting access to the POI device for any purpose of maintenance shall be denied access. Access is denied even if the individual is identified as being from one of the listed Key Injection Facilities or Monetra Technologies, LLC.

6 Device Encryption Issues

6.1 Instructions for responding to POI device encryption failures

In the unlikely event that an encryption failure occurs, such as the inability to decrypt a payload from a device, or the device emits clear-text card holder data, the device will be immediately disabled in the TranSafe systems and will no longer be allowed to process new transactions until corrective action is taken. In such an event, an automatic email will be sent to the merchant email address on file in order to notify the merchant about this issue. The device must be immediately removed from service by the merchant.

The device must not be re-enabled for use until the merchant has confirmed the issue is resolved and P2PE-encryption functions are restored and re-enabled. To re-enable a device in TranSafe after taking corrective action, the merchant may do so via the web management portal at https://manage.transafe.com/merchant/devices by clicking on the pancake menu next to the affected device and re-enabling it and entering the corrective action taken in the notes.

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

The Lockdown® solution does not currently support the ability to suspend encryption of account data once a device is in production. We only provide the ability to suspend a DEVICE for trouble-shooting and/or security reasons. The only ability to deactivate P2PE support is to request complete termination of your current services and to re-sign up for new services without P2PE support.

7 POI Device Troubleshooting

7.1 Instructions for troubleshooting a POI device

In the event of an issue, we will work remotely with you to troubleshoot the issue. Prior to any troubleshooting, we will confirm that the individual contacting us is an authorized individual within your organization. During troubleshooting, PAN and/or SAD are never output to the merchant environment, nor are PAN and/or SAD data collected during the troubleshooting process.

Please contact us as listed in Section 1.2.

8 Additional Solution Provider Information

8.1 PIM updates

This PIM document will be updated on occasion, and may be updated to include clarifications, new requirements, new functionality, or new devices. Please ensure you always retrieve the latest PIM at https://www.transafe.com.

A Revision History

Version	Date	Changes
v1.0.0	2019-09-23	• Initial document creation

B LockDown Approved Key Injection Facilities

- JR's POS Depot http://www.jrposdepot.com/

  Order Here: https://www.jrorders.com/TRANSAFE-LockDown_c_409.html
- Scan Source http://www.scansource.com/
- The Phoenix Group https://tpgpos.com/