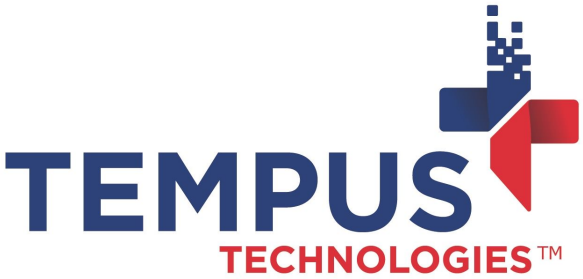

Tempus Technologies P2PE Instruction Manual

635 W. 11th St. | Auburn, IN 46706
www.TempusPayment.com
2024-04-01

Contents

P2PE Overview

Tempus Technologies, Inc. is a PCI SSC approved point-to-point encryption (P2PE) solution provider. As a P2PE solution provider, we have overall responsibility for the design and implementation of our P2PE solutions, and we manage the P2PE solutions for our customers.

A point-to-point encryption (P2PE) solution is a combination of secure devices, applications and processes that encrypts data from the point of interaction (e.g. at the point of swipe or dip) at your facilities until the data reaches the secure decryption environment.

Tempus Technologies offers two (2) P2PE solutions. Our primary solution is offered in conjunction with our partner First Data and is integrated with their TransArmor encryption and tokenization solution. Our secondary solution is fully managed my us, enabling transaction processing with our payment gateway and supported processors.

Use of a Tempus Technologies P2PE solution does not remove you from the scope of your own PCI DSS requirements. What our solution provides is a reduction of scope, by removing the systems and networks involved in card data capture and communication utilizing our solution from your CDE. This is because, when using a supported PinPad device, cardholder data is encrypted at the Point of Interaction and cannot be decrypted until it reaches our supported gateway devices. The PCI SSC has recognized that validated PCI P2PE solutions meet the necessary requirements to reduce your scope in this manner. If you capture cardholder data using other methods outside of the offered solution, the systems and environment utilized by these secondary POIs are fully within scope of PCI DSS and are solely your responsibility.

It is critical that you never store cardholder data in an insecure manner. Tempus Technologies recommends that you store only the minimum-necessary and use all appropriate controls to protect that data. Track data, pin blocks, or CVV values should NEVER be stored, under any circumstances. It is the user's responsibility to comply with all relevant PCI requirements. Please see https://www.pcisecuritystandards.org/ for more information.

Introduction

The purpose of this manual is to provide instruction to ensure your deployment of the P2PE solutions are performed in a manner consistent with PCI SSC P2PE guidelines. In addition, this manual will provide you with guidelines governing:

- Inventory Control and Monitoring Procedures
- Physical Security of Devices
- Detection of Unauthorized Alterations or Replacement of Devices
- Appropriate Deployment Locations for POI Devices
- Monitoring of Third-Party Personnel access to POI Devices
- Securing of Devices Removed from Service
- Disposal of Devices
- Guidance for Managing Device Failure
- Troubleshooting
- Detection of Tampering
- Installation and Connecting POI Devices

It is of utmost importance that you adhere to the guidelines detailed within this guide. Failure to do so will impact your PCI DSS compliance, and may impact the security of the deployed P2PE solution deployed within your environment.

Tempus Technologies provides two (2) P2PE solutions. Both solutions are P2PE Hardware-to-Hardware solutions. This information is critical in enabling you to complete the proper PCI DSS documentation, whether it be a Self-Assessment Questionnaire (SAQ) or a Report of Compliance generated by your PCI SSC QSA.

The first solution is delivered in conjunction with our partner First Data and utilizes their TransArmor Solution. With this solution your deployed POI devices will communicate directly with First Data's TransArmor HSM solution across the Internet. Cardholder data must be entered into the deployed POI device, upon which the data is encrypted by the POI device using an RSA cryptographic key that is delivered to the device and rotated annually. The POI device will securely transmit this information directly to First Data's TransArmor HSM. Upon receipt of the cardholder data, the HSM will decrypt the data and relay the information to your selected processor for authorization processing. The result of the request is returned to the POI device, which will indicate success or failure. The POI Device does not have the ability to decrypt cardholder data and does not store cardholder data post-authorization. The devices provided for this solution are PCI PTS SRED certified. RSA Keys are rotated annually via Tempus Technologies Key Management API.

The second solution is our in-house and fully Tempus-managed solution. With this solution your deployed POI devices will communicate directly with our deployed Hardware Security Module (HSM) across the Internet. Cardholder data must be entered into the deployed POI device, which is then encrypted by the POI device using a cryptographic key injected into the device prior to being shipped to you. The POI device will then securely transmit this information to the HSM deployed within our Data Center. Upon receipt of the cardholder data, the HSM will decrypt the data and relay the information to your selected processor for authorization processing. The result of the request is returned to the POI device, which will indicate success or failure. The POI Device does not have the ability to decrypt cardholder data and does not store cardholder data post-authorization.

Supported PTS devices approved by the PCI SSC for use with either solution are as follows:

Manufacturer	Device Make	Device Model	Firmware Version	Hardware Version	PCI PTS Approval Number
ID Tech	ID Tech	SREDKey	SRED: 1.01, 1.02, 1.02.xxx.S	IDSK-53xxxxxxx	4-10156
ID Tech	ID Tech	SREDKey 2	SREDKEY2 FW v1.00.xxx.xxxx.S, SREDKey2 FW v1.01.xxx.xxxx.S, SREDKey2 FW v1.02.xxx.xxxx.S, SREDKey2 FW v2.00.xxx.xxxx.S	80172001(With MSR), 80172002(Without MSR), 80172004(With MSR), 80172005(Without MSR), 80172006 (With MSR), 80172007 (Without MSR)	4-90075
Ingenico	Ingenico	Desk/3200 Desk/3500	820547v01.xx, 820376v01.xx, 820549v01.xx (SRED), 820549v01.xx, 820556v01.xx	DES32AA (Non CTLS), DES32BA (CTLS), DES35AA (Non CTLS), DES35BA (CTLS), DES32CA (Non CTLS), DES32DA (CTLS), DES35CA (Non CTLS), DES35DA (CTLS), DES32AB (Non CTLS), DES32BB (CTLS), DES32CB (Non CTLS), DES32DB (CTLS), DES35AB (Non CTLS), DES35BB (CTLS), DES35CB (Non CTLS), DES35DB (CTLS)	4-20283
Ingenico	Ingenico	Desk/3200 Desk/3500	820547v01.xx, 820376v01.xx, 820555v01.xx (SRED), 820549v01.xx, 820556v01.xx	DES32AB (without contactless), DES32BB (with contactless), DES32CB (without contactless, with PIN shield), DES32DB (with contactless, DES35AB (without contactless), DES35BB (with contactless), DES35CB (without contactless, DES35DB (with contactless)	4-20321
Ingenico	Ingenico	Desk/3200 Desk/3500	820376v01.xx, 820547v01.xx, 820549v01.xx, 820549v01.xx (SRED), 820556v01.xx, 820565v01.xx (SRED)	DES32AA (Non CTLS), DES32AB (Non CTLS), DES32BA (CTLS), DES32BB (CTLS), DES32CA (Non CTLS), DES32CB (Non CTLS), DES32DA (CTLS), DES32DB (CTLS), DES35AA (Non CTLS), DES35AB (Non CTLS), DES35BA (CTLS), DES35BB (CTLS), DES35CA (Non CTLS), DES35CB (Non CTLS), DES35DA (CTLS), DES35DB (CTLS)	4-20283
Ingenico	Ingenico	Desk/5000	820547v01.xx; 820376v01.xx, 820549V01.xx (SRED OnGuard FPE), 820555v01.xx (SRED AWL), 820556v01.xx (SRED OnGuard SDE), 820559v01.xx (SRED ANL)	DES50AA (non CTLS); DES50BA (CTLS), DES50CA (Non CTLS); DES50DA (CTLS), DES50AB (Non CTLS), DES50BB (CTLS), DES50CB (Non CTLS), DES50DB (CTLS)	4-20281
Ingenico	Ingenico	Desk/5000	820547v01.xx, 820376v01.xx, 820555v01.xx (SRED), 820559v01.xx (SRED ANL), 820549v01.xx (SRED OnGuard FPE), 820556v01.xx (SRED OnGuard SDE)	DES50AB, (Non CTLS), DES50BB, (CTLS), DES50CB, (Non CTLS + Privacy Shield), DES50DB(CTLS + Privacy Shield)	4-20317
Ingenico	Ingenico	iCMP	820305V01.xx, 820365V02.xx, SRED (CTLS): 820528V02.xx, 820539V01.xx	ICMxxx-01Txxxxx, ICMxxx-11Txxxxx, ICMxxx-21Txxxxx, ICMxxx-31Txxxxx	4-20235

Manufacturer	Device Make	Device Model	Firmware Version	Hardware Version	PCI PTS Approval Number
Ingenico	Ingenico	ICT220, ICT250	Non SRED (CTLS): 820305 V02.xx, 820375V01.xx, 820365 V02.xx, SRED (Non CTLS): 820528V02.x, 820073v01.xx	iCT2xx-11Txxxxx	4-20196
Ingenico	Ingenico	iPP310, iPP320, iPP350	820305V01.xx, 820365V02.xx, SRED (Non CTLS): 820157V01.xx	IPP3xx-01Txxxxx	4-20142
Ingenico	Ingenico	iPP310, iPP320, iPP350	SRED (CTLS): 820365 V02.xx, 820305V02.xx, 820528V02.xx, SRED (Non CTLS): 820375V01.xx, 820554v01.xx	IPP3xx-11Txxxxx	4-20184
Ingenico	Ingenico	iPP320, iPP350, iPP310, iPP315	820305 V11.xx, 820180 V01.xx	iPP3xx-21Txxxxx, iPP3xx-31Txxxxx, iPP3xx-41Txxxxx, iPP3xx-51Txxxxx	4-30176
Ingenico	Ingenico	iSC Touch 250	820365 V02.xx, 820518 V02.xx, 820528V02.xx	iSC2xx-21Txxxxx, iSC2xx-31Txxxxx	4-30135
Ingenico	Ingenico	iSC Touch 250	820518 V12.xx, SRED (CTLS): 820528V02.xx	iSC2xx-21Txxxxx, iSC2xx-31Txxxxx	4-30132
Ingenico	Ingenico	iSC Touch 480	820365 V02.xx, 820518V01.xx, 820518V02.xx, SRED (CTLS): 820528V02.xx	ISC4xx-01Txxxxx (no CTLS), ISC4xx-11Txxxxx (CTLS)	4-30098
Ingenico	Ingenico	iSC Touch 480	820518 V11.xx, 820518 V12.xx, 820528V02.xx	ISC4xx-01Txxxxx, ISC4xx-11Txxxxx	4-30125
Ingenico	Ingenico	iSC250	820518 V01.xx, 820518 V02.xx, SRED (Non CTLS): 820157 V01.xx	iSC2xx-01Txxxxx	4-30062
Ingenico	Ingenico	iSMP	820305V01.xx, 820365V02.xx, SRED (Non CTLS): 820528V02.xx	iMP3xx-01Txxxxx, iMP3x0-01Txxxxx (already approved hardware version), iMP3x2-01Txxxxx (new hardware version)	4-20183
Ingenico	Ingenico	iSMP4	820305v11.xx	IMP6xx-01Txxxxx (without contactless), IMP6xx-11Txxxxx (with contactless), IMP6xx-02Txxxxx, (without contactless), IMP6xx-12Txxxxx(with contactless)	4-30220
Ingenico	Ingenico	iUC150B	820168 v01.xx	iUC15x-01Txxxxx	4-30172
Ingenico	Ingenico	iUC250	820178 v01.xx, 820178 v11.xx	IUC25x-01Txxxxx	4-30164
Ingenico	Ingenico	iUC280	820176 v01.xx	IUC28x-01Txxxxx	4-30160
Ingenico	Ingenico	iUC285	820177V01.xx	IUC28x-01Txxxxx	4-30161
Ingenico	Ingenico	iUI120	820167 V11.xx	iUI1xx-01Txxxxx	4-30157
Ingenico	Ingenico	iUP250	820305 V01.xx, SRED: 820528V02.xx, 820305V03.xx	IUP2xx-01Txxxxx	4-30075
Ingenico	Ingenico	iUP250LE	820305V13.xx, 820305v12.xx	IUP2xx-11Txxxxx	4-30251
Ingenico	Ingenico	iUR250, iUR250P	SRED: 820514V01.xx, 820514V11.xx	iUR2xx-01Txxxxx, iUR2xx-11Txxxxx	4-30083
Ingenico	Ingenico	iUR250, iUR250P	820514v02.xx, 820514v12.xx	IUR2xx-01Txxxxx standard Ingenico product, IUR2xx-11Txxxxx specific bezel	4-30250

Manufacturer	Device Make	Device Model	Firmware Version	Hardware Version	PCI PTS Approval Number
Ingenico	Ingenico	IWL220, IWL250	Non SRED (CTLS): 820365 V02.xx, 820305V01.xx, 820375V01.xx, SRED (Non CTLS): 820073v01.xx, 820528v02.xx	IWL2xx-01Txxxxx	4-20181
Ingenico	Ingenico	Lane/3000, Desk/1500	820547v01.xx, 820561v01.xx (base firmware)	LAN30AA, LAN30BA, LAN30CA, LAN30DA, LAN30EA, LAN30FA, LAN30GA, LAN30HA	4-30310
Ingenico	Ingenico	Lane/3600, Desk/1700	820571v01.xx (Core Firmware), 820376v12.xx (Security Services), 820555v01.xx (SRED AWL), 820556V01.xx (SRED On-Guard SDE), 820549V01.xx (SRED On-Guard FPE), 820570V07.xx (Open Protocols), 820565V01.xx (SRED FF1), 820376V13.xx (Security Services), 820382V01.xx (Security Services (PinPad))	LAN36AA1-xxxx, LAN36BA1-xxxx, LAN36CA1-xxxx, LAN36DA1-xxxx, LAN36AA2-xxxx, LAN36BA2-xxxx, LAN36CA2-xxxx, LAN36DA2-xxxx, LAN36AB2-xxxx, LAN36CB2-xxxx, LAN36DB2-xxxx, LAN36EA2-xxxx, LAN36FA2-xxxx	4-30481
Ingenico	Ingenico	Lane/5000	820547v01.xx, 820376v01.xx, 820549V01.xx (SRED), 820555V01.xx (SRED), 820556V01.xx (SRED)	LAN50AB (non CTLS), LAN50BB (CTLS)	4-20286
Ingenico	Ingenico	Lane/5000	820547v01.xx, (Non SRED) 820376v01.xx (Non SRED), 820549V01.xx, 820556V01.xx (SRED OnGuard SDE), 820559V01.xx (SRED ANL)	LAN51BA, LAN51CA, LAN51DA, LAN51EA	4-20303
Ingenico	Ingenico	Lane/5000	820547v01.xx, 820376v01.xx, 820549v01.xx (SRED OnGuard FPE), 820556v01.xx (SRED OnGuard SDE), 820559v01.xx (SRED ANL), 820555v01.xx (SRED AWL)	LAN51BA (single MSR head), LAN51CA (dual MSR head), LAN51DA (single MSR head and camera), LAN51EA (dual MSR head and camera)	4-20324
Ingenico	Ingenico	Lane/7000	820547v01.xx	LAN70AA	4-30226
Ingenico	Ingenico	Lane/7000	820547v01.xx	LAN70AA, LAN70AB	4-30237
Ingenico	Ingenico	Lane/8000	820547v01.xx	LAN80AA	4-30257
Ingenico	Ingenico	Link/2500	820547v01.xx, 820555v01.xx (SRED AWL), 820556v01.xx (SRED On-Guard SDE)	CTLS, LIN25AA, LIN25BA, LIN25CA, LIN25DA, LIN25EA; Touchscreen version; no CTLS support, LIN25FA; Touchscreen version; with CTLS support, LIN25GA; Dual Head version; no CTLS support, LIN25HA; Dual Head version; with CTLS support, LIN25IA (Companion version with rear connector and no CTLS support), LIN25JA (Companion version with rear connector and with CTLS), Non CTLS	4-30230
Ingenico	Ingenico	Link/2500	820547v01.xx	LIN25AA (Basic version no CTLS support), LIN25BA (Basic version with CTLS), LIN25CA (Companion version no CTLS support), LIN25DA (Companion version with CTLS), LIN25EA (Touch version no CTLS support), LIN25FA (Touch version with CTLS), LIN25GA (Dual head version no CTLS support), LIN25HA (Dual head version with CTLS), LIN25IA (Companion version with rear connector and no CTLS support), LIN25JA (Companion version with rear connector and with CTLS)	4-30326
Ingenico	Ingenico	Move/3500	820547v01.xx, 820376v01.xx, 820549V01.xx (SRED), 820556v01.xx	MOV35AA, MOV35BA, MOV35CA, MOV35DA, MOV35AB, MOV35BB, MOV35CB, MOV35DB, MOV35EB, MOV35FB	4-20289

Manufacturer	Device Make	Device Model	Firmware Version	Hardware Version	PCI PTS Approval Number
Ingenico	Ingenico	Move/3500	820547v01.xx, 820376v01.xx, 820555v01.xx (SRED), 820549v01.xx, 820556v01.xx	MOV35AB (non CTLS), MOV35BB (CTLS), MOV35EB (CTLS), MOV35CB (non CTLS), MOV35DB (CTLS), MOV35FB (CTLS), MOV35JB (CTLS)	4-20320
Ingenico	Ingenico	Move/5000	820547v01.xx; 820376v01.xx; (SRED) CTLS: 820549V01.xx, 820555v01.xx (SRED), 820549v01.xx (SRED OnGuard FPE), 820556v01.xx (SRED OnGuard SDE), 820559v01.xx (SRED ANL)	(Non CTLS); MOV50BA (CTLS), MOV50JA (CTLS), MOV50CA, MOV50DA, MOV50AB, MOV50BB (CTLS), MOV50CB, MOV50DB (CTLS), MOV50JB (CTLS)	4-20282
Ingenico	Ingenico	Move/5000	820376v01.xx, 820547v01.xx, 820549v01.xx (SRED OnGuard FPE), 820555v01.xx (SRED), 820556v01.xx (SRED OnGuard SDE), 820559v01.xx (SRED ANL), 820565v01.xx (SRED FF1)	(CTLS + Privacy shield), (CTLS), (Non CTLS + Privacy shield), (Non CTLS), MOV50AB, MOV50BB, MOV50CB, MOV50DB, MOV50JB (CTLS + Privacy shield + Desktop case lid)	4-20316
Ingenico	Ingenico	Self/2000	820566v01.xx	SEL20AA	4-30381
Ingenico	Ingenico	Self/4000	820547v01.xx	SEL40BA	4-30393
Ingenico	Ingenico	Self/5000	820566v01.xx	SEL50CA	4-30384
Verifone	Verifone	Vx820	Non-SRED: QT82001x, SRED: QT8201xx, QT8202xx, QT820240.xxxxxxxx, QT820246.xxxxxxxx, QTyy0400.xxxxxxxx, QTyy0500.xxxxxxxx, QTyy520.xxxxxxxx, QTyy0530.xxxxxxxx, OP: 2.x.x, QTyy0540.xxxxxxxx	M282-xxx-xx-xxx-3	4-40054

Contact and Support Information

For support or general questions, please contact Tempus Technologies at:

Technical Installation & Support	800-225-8979 x 4	Support@TempusTechnologies.com

Inventory Control and Monitoring

PCI requires that you maintain an inventory of all deployed POI devices, including which devices are deployed, which are awaiting deployment, those that have been removed from service for repair or otherwise not in use, and those in transit for deployment or return for repair. It is recommended that you designate a Job Role or personnel whose duties include maintaining the POI inventory and inspecting devices.
The following is a list of information that you must record for each device. It is recommended that you record this information upon receipt of your POI device and then update the location of each device as it transitions from storage, transit, deployment, and repair or return.

- Manufacturer of device;
- Make and Model of device;
- Serial Number of Device;
- Internal Inventory Number; (if applicable);
- General Description of Device (Color, Secure Seals, Labels, Hidden Marking, etc.);
- Number and type of physical connections (Network, Serial, etc)
- Firmware version;
- Hardware version;
- Device Location (Storage, Where Deployed, In Transit, Awaiting Repairs or Returned);
- Date of Location Inspection (Last Date device location was confirmed);
- Date of Last Inspection (last date device was inspected for tampering);
- Name of Job Role of personnel performing inspection; and
- Date inventory was last updated

Device inventories are to be performed no less than annually to confirm that inventory of devices is being catalogued and performed correctly; however, inventory must be updated as devices transition in and out of service or from one location to another. This inventory must also be completed to confirm that all devices identified as being in your environment are currently within your possession, and not missing.

Access to device inventory and to the devices themselves must be restricted to authorized personnel. The method for maintaining a device inventory is determined by you; however the method utilized must enable you to restrict access to the inventory tracking information and allow you to record who has had access to the inventory tracking information. Failure to do so will impact your PCI DSS compliance. In addition, you must be able to restrict access to stored devices and record who has accessed said devices, including when access occurred.

During your inventory process, you must investigate the POI devices to identify unauthorized removal, tampering, or substitution of devices. Detection of these events may be an indication

of a compromise of your environment. Inspection should include a comparison of the information located on the device itself with the inventory information that was previously recorded. In addition, the inspection should look for indications that the device has been tampered with. Indications of tampering may include, but are not limited to, attachment of unauthorized devices to the POI device, breakage of security seals, cracks within the seal of the device itself, or insertion of a “skimmer” device within the Magnetic Stripe Reader (MSR) of the device. Skimmers are devices used by attackers to capture cardholder data prior to the POI device reading the card. Skimmers may be inserted in the MSR of the device or overlaid on the device itself. It is recommended that you train personnel (e.g. cashiers, managers) interfacing with the POI devices on a regular basis to inspect deployed POI devices daily. Should you detect a compromised device or find that your inventory indicated a missing or substituted device, you must report this information to Tempus Technologies immediately. For reporting compromised, missing, or substituted devices, contact Tempus Technologies at:

Technical Installation & Support	800-225-8979 x 4	Support@TempusTechnologies.com

Device Physical Security

Maintain proper physical security of POI devices is required for you to maintain your own PCI DSS compliance and for you to ensure that devices have not been tampered with. Physical security of devices must be addressed in four key areas prior to receiving, during storage, and while in transit.

Receiving

Tempus Technologies and its partners take all necessary precautions to ensure devices are not tampered with or compromised prior to be shipped to you. However, there are steps that you must undertake to ensure that devices have not been tampered with during transit. First you must confirm that shipment of devices originated from one of the following providers:

1. Tempus Technologies, Inc.
2. Ingenico North America
3. ID Tech
4. ScanSource
5. MagTek
6. UCP (vendor)

To remain compliant, you may only deploy POI devices that are shipped from one of the aforementioned locations. Confirmation that devices were shipped from an authorized source may be performed by comparing the providers shipping information with the information listed above. If you receive a POI device from another provider, you must contact us for confirmation. We will take necessary steps to communicate any change to our list of providers. Regardless, if you cannot confirm the device was shipped from an authorized source, **DO NOT** deploy the device.

In addition to confirming shipping origination, you must confirm that neither the packaging nor the device has been tampered with. All POI devices will be shipped using tamper-evident packaging. This packaging will be evident on the shipping package itself and/or internally. Examples of said packaging include:

- Sealed Tamper Evident Bags: like Tamper Evident Deposit Bags
- Tamper Evident Tape used on all seams of the box

You must also inspect the device. You should look for broken security seals and cracks around device's seals to determine if the POI device itself has been compromised. If you believe the packaging or the device has been tampered with, **DO NOT** deploy the device.

For device confirmation or reporting of tampering, you may contact us at:

Technical Installation & Support	800-225-8979 x 4	Support@TempusTechnologies.com

If it is determined that a device or package has been tampered with, we will provide you with an address for the return of the POI device for further investigation.

Storage

Devices being stored for any reason (e.g. prior to deployment, shipment, or awaiting repairs) must be stored in a secure area with restricted access to ensure they are not tampered with. Though the storage location of devices within your control is at your discretion, the location must, at a minimum, implement the following measures:

1. Devices must be stored in locked room or container;
2. Storage location must support restricted access;
3. Access must be restricted to only authorized personnel. Examples include:
    a. Door/Container requires key access in which only defined personnel have access to the key; or
    b. Door/Container requires knowledge of a cipherlock code, in which only defined personnel have knowledge of the code.
4. Access to room or container storage device must be logged. This logging may be manual (written access log) or automatic (proximity card system that records access);
5. Access to the room must be monitored (cameras or physical sight).

Transit

Devices being shipped to your location, whether for original deployment or return, must be shipped securely. Devices must be packed in tamper-evident packaging and must be shipped using a secure transport method such as a secure courier or bonded carrier. For deployment to sites, it is permissible to use employees for transport; however, they must be authorized to deliver the devices and the recipient must be notified with information about who will be delivering the devices to them. Be it a bonded carrier, secure courier, or internal employee, you must log the following information:

1. Personnel providing shipping (if employee, record name and job role);

2. Date of pickup
3. Device being shipped
4. Confirmation date of site delivery

When packaging devices for transit, they must be packed in tamper-evident packaging. You may determine the type of packaging; however, the recipient must be notified on how to determine if the package has been tampered with during transit. As with your inspection of POI devices received from us, your deployment sites must perform the same inspection on device shipped from your storage location. They must be notified of authorized shipping locations, notified on how the device will be shipped, and trained in how to inspect the packaging and device for tampering (e.g. how to investigate for breakage of tamper-evident seals on the external packaging, or how to investigate the device itself for cracks or breakage of security seals). Finally, they must be instructed that if they receive devices without prior confirmation from the shipping location, or if they are delivered in an unexpected manner, they must confirm prior to deployment of the devices.

Special Note: If using internal employees for device shipment, they must be instructed to not leave devices in public areas unattended (e.g. in the front or back seat of a car). This may lead to unauthorized access or theft of the device.

Detection of Unauthorized Alterations or Replacement of Devices

You must implement procedures for the detection of unauthorized alterations or replacement of devices both prior and post deployment. This is imperative for maintaining the security of the P2PE solution, as well as enabling you to maintain your PCI DSS compliance.

Prior to Deployment

Prior to deployment of a device for use, the deployment location must validate that the device received has not been tampered with or substituted. While awaiting deployment, the device must be kept in a secure storage location with restricted access. Though the storage location of devices within your control is your responsibility, the location must include the following measures:

1. Devices must be stored in locked room or container;
2. Device must remain in its original, tamper-evident packaging or in a physically secure storage until ready for use;
3. Storage location must support restricted access;
4. Access must be restricted to only authorized personnel. Examples include:
    a. Door/Container requires key access in which only defined personnel have access to the key; or
    b. Door/Container requires knowledge of a cipherlock code, in which only defined personnel have knowledge of the code.
5. Access to room or container storage device must be logged. This logging may be manual (written access log) or automatic (proximity card system that records access);
6. Access to the room must be monitored (cameras or physical sight).

Once the device is removed from storage and is being prepped for deployment, the following steps must be implemented:

1. The serial number on the devices must be matched with the recorded serial number of the device removed from storage and shipped to the location. This information must be recorded within inventory tracking at the deployment location and at the shipping location at the time of deployment;
2. A pre-installation inspection of the device must be performed to ensure the device has not been tampered with. This must include physical inspection of the device to search

for breakage of seal and security tampering seals; and
3. Prior to final deployment into production, functionality must be tested to ensure that the device communicates and captures data properly.

Special Note: It is recommended that a list of devices and serial numbers approved for a defined location be delivered to the location separate from the devices themselves. This will circumvent an individual from being able to substitute devices with differing serial numbers and updating the inventory list to reflect the compromised devices.

Post Deployment

Once POI devices have been deployed, periodic inspection must be performed at deployment locations to ensure devices have not been tampered with or substituted. The type of location for deployment will drive the frequency for inspections. For high traffic, visible areas such as storefronts, it is recommended inspections occur twice a year. For locations that are remote or unattended, it is recommended that inspections occur every ninety (90) days.

When inspecting devices the first step should be to compare the serial number of the device with the serial number recorded for the location. If the serial numbers do not match, this could be the result of an unauthorized substitution. The individual should contact the personnel responsible for the storage, shipping, and/or installation of the POI device to determine whether the documentation is incorrect or if indeed a device has been substituted. Once the serial number has been confirmed, the device should undergo a physical inspection for tampering. Tamper and security seals should be examined for signs of breakage. The connection to the device should be inspected to ensure that no extraneous devices are attached. The device should be inspected for holes, missing screws, or the addition of labels/ covering that could be used to mask damage. Finally, the card DIP or magnetic stripe reader of the POI device should be investigated to ensure that a “skimmer” or other type of device has not been inserted. If tampering is suspected, contact the personnel responsible for the storage, shipping, and/or installation of the POI device to report the tampering. The device should be taken offline, and Tempus Technologies should be contacted to report the tampering, which will allow us to provide remote assistance regarding the removal and return of the device for further investigation. We can be contacted at:

Technical Installation & Support	800-225-8979 x 4	Support@TempusTechnologies.com

Appropriate Deployment Locations

You must deploy POI devices in the most secure manner possible. The following are recommendations for secure deployment:

1. Public access (non-employee) to devices must be limited such that they only have access to the portion of the device needed to complete the transaction. For example, they should only have access to the card reader and/or PinPad for PIN entry.
2. If the devices are stationary, they should be physically secured to prevent theft (e.g. bolted down).
3. Finally, they should be placed in an area that is easily viewable by employees and/or management. This will reduce the chances that a device is tampered with.

If the devices are deployed in a remote location or unattended, it is recommended that the devices be monitored with a camera so that one may review footage to determine if someone has attempted to tamper with the device.
Though the devices provided by Tempus can be physically mounted to reduce theft, if you deploy a device where mounting is not possible the device should not be left unattended. In addition, during off-hours, the device should be moved to a secure location to reduce the chance of theft and/or tampering.

Third-Party Access Monitoring

Access to POI devices by third-party personnel for repair/maintenance must be monitored. This monitoring is required to ensure there is no unauthorized access that could result in tampering, theft, or substitution of the device. To ensure proper third-party access monitoring, you should have a policy that ensures the following:

1. Maintenance/repair of the device must be pre-arranged, with date and timeframe of third-party personnel defined. Unexpected visits for repair/maintenance must be verified. If they cannot be verified, access to the device must be denied;
2. Prior to granting access to a device, personnel must be identified and authorized to access the device;
3. Third-party personnel access must be recorded, and include personnel name, company, time of access, and purpose of access. This log must be maintained for a minimum of one year;
4. Personnel must be escorted and observed at all times; and
5. Personnel may not remove or replace a device without prior authorization. If authorized, new devices must be properly inspected and inventoried.

Securing Devices Removed From Service

When devices are removed from service either for repair, return, replacement, or storage, it must be done in a manner that allows for the tracking and security of the device. The following initial steps are required regardless of the reason a device is removed from service:

1. Removal of device must be pre-arranged prior to removal;
2. Location of device removal must confirm personnel removing device are authorized;
3. Personnel performing removal must be documented to include name, company, and time of removal; and
4. Inventory must be updated to indicate that the device was removed and the reason for removal.

If the device is to remain at the location for future deployment, the device must be securely stored at the location in the manner described earlier within this manual.

If the device is to be returned to your shipping location, the device must be packed in a tamper-evident package and shipped using an authorized source that can be tracked. Methods for shipping and tracking are described in previous sections of this manual.

If the device is to be returned to us for repair or replacement, you must take the following steps:

1. Wipe the device of all sensitive data by following the instructions provided via the support contact below, or the documentation you received with the device.
2. Pack the device within tamper-evident packaging if available.
3. When returning a mobile device (i.e. Desk, Move, Link), remove the battery before packaging and shipping; and
4. Notify us that the device is being returned. You will need to provide us the serial number of the device and the tracking number of the package (as provided by the carrier). You can contact us at:

Technical Installation & Support	800-225-8979 x 4	Support@TempusTechnologies.com

Disposal of Devices

Tempus offers secure disposal services, which can be arranged by contacting sales@tempustechnologies.com. If you are using Tempus disposal services, please follow the instructions in the section above (Securing Devices Removed From Service) when returning the devices to us.

If you choose to handle device disposal internally or through another third-party, you must ensure that disposal occurs in a manner consistent with industry best practices (e.g. NIST 800-88 Rev. 1).

Managing Device Encryption Failure

Though highly unlikely, there may be occasions where a device encryption failure occurs. For this type of event, it is your responsibility to report the problem to us. Tempus customer support will work with you to troubleshoot the issue, based on the guidelines detailed in the “Troubleshooting” section of this manual. If the encryption failure cannot be remedied through troubleshooting, Tempus will work with you to find an appropriate solution. It is strongly discouraged for merchants to choose to go without a device in the event that one fails. However, if you choose to continue to use the device without the P2PE protection you must complete and submit the P2PE Opt-Out Form provided in Appendix A.

Removing the Device

If you elect to remove the failing device, you must contact the location affected and instruct them to discontinue use of the device and inform that the device will be removed from service. The removal of the device from service must follow the instructions described previously within this manual. Once the device is removed, it must be returned to Tempus Technologies or a designated partner for repair or disposal. Please refer to the instruction within this manual regarding device return.

P2PE Opt-Out

As previously stated, you may choose to opt-out of using the protection of the P2PE solution and continue the use of the POI device in a non-P2PE mode. If you choose to opt out, understand that you accept the following responsibility:

1. Potential impact to the security of your account data and potential risks associated with processing transactions without P2PE protection.
2. Implementation of alternative controls to protect account data in lieu of the P2PE solution.
3. Loss of eligibility for the PCI DSS scope reduction afforded by the P2PE solution.
4. Advising your acquirer that you are no longer using the P2PE solution.
5. That processing transactions without P2PE protection may impact your PCI DSS compliance validation and you should confirm with their acquirer or payment brand, as applicable, for all PCI payment brands affected.

If you chose to accept the responsibilities outlined above, you must first fax or email to us the P2PE Opt-Out Form included within this manual in Appendix A. Upon receipt of the form, we will guide your designated personnel through the process for enabling the POI device to operate in a non-P2PE compliant mode.

Troubleshooting

In the event of an issue, we will work with you remotely to troubleshoot the issue. Prior to any troubleshooting, we will confirm that the individual contacting us is authorized within your organization for troubleshooting purposes, as defined to us during the initial deployment of the solution.
During our troubleshooting process:

1. Primary Account Number or Sensitive Authentication Data will never be outputted to your systems;
2. We will only collect the Primary Account Number or Sensitive Authentication Data as needed to resolve the issue;
3. Data collected will be encrypted upon storage;
4. Data will be stored in specific, known locations with access restricted to only those individuals charged with resolving your issue;
5. We will only collect the amount of data needed to solve the issue; and
6. All data will be securely removed from storage immediately after use and the issue resolved.

Our troubleshooting process consists of the following steps:

STEP 1

1. If this is a P2PE device, then we will confirm that the end user has been authorized to troubleshoot this device. If they have not, then escalate it to someone who does.

STEP 2

1. If an Error Code is showing on the device's display screen, follow the troubleshooting guidelines provided by the manufacturer.
2. Restart all payment applications and test.
3. If success then stop, else follow the manufacturer's device replacement procedures.

STEP 3

1. Verify that the cables are securely connected to the correct port.
2. Confirm that the device's indicator lights are properly illuminated.
3. Stop all payment applications.
4. Power cycle the device by unplugging all of the cables and plugging them back in.
5. Start all payment applications and test.
6. If success then stop, else continue to STEP 4

STEP 4

1. Stop all payment applications.
2. Unplug all cables from the device.
3. Reboot the workstation.
4. Plug all cables back into the device.
5. Start all payment applications and test.
6. If success then stop, else continue to STEP 5.

STEP 5

1. Follow the manufacturer's process for reinstalling the drivers.
2. Start all payment applications and test.
3. If success then stop, else continue to STEP 6.

STEP 6

1. Review the payment application operating system's event logs.
2. Contact Tempus for direction regarding the device manufacturer's troubleshooting guidelines.

Installation and Connecting of POI Devices

It is imperative that you follow the guidelines detailed below for the deployment of the P2PE solution. Failure to do so may impact your PCI DSS compliance and the protections afforded to you by the P2PE solution.
Prior to deployment, you must understand that any modification to the deployment can and will impact your compliance. Such modifications may include:

- 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

Also, understand that if a PCI-approved POI component is connected to another device or data-capture mechanism, the non-PCI-approved capture mechanism is not secured by the P2PE solution, and the use of any such mechanisms to collect PCI payment card data would negate any PCI DSS scope reduction which might otherwise have been provided by the P2PE solution's device.

The P2PE solution provided by Tempus Technologies or our partners only includes those devices previously identified in the "Introduction" section of this manual. It does not allow for POI components that are not PCI approved.

Tempus P2PE solutions may be deployed in either within a Windows Edition or Terminal Edition Model.

- **Windows Edition Model:**
  - Ensure that the POI device is attached to your PC and PaymentMate Windows Edition is configured for the device you own. Follow PaymentMate Windows Edition Setup Procedures.
- **Terminal Edition Model:**
  - The POI device will need network access and must be assigned an IP number by your IT staff (either static or DHCP assigned).
  - The POI device will need to be activated using pre-defined activation credentials to ensure that the device are ready for payment processing.

Appendix A: P2PE Opt-Out Form

Name of Company: _____

Name of Requestor: _____

Date of Request: _____

Serial Number of Device: _____

At this time we formally request the device with the Serial Number above be configured to operate in a non-P2PE mode. We formally agree to assume responsibility for:

1. The security impact to our account data and potential risks associated with processing transactions without P2PE protection.
2. Implementing compensating controls to protect account data in li eu of the P2PE solution
3. That we are no longer eligible for the PCI DSS scope reduction afforded by the P2PE solution
4. Notifying our acquirer that we are no longer using the P2PE solution
5. Processing transactions without P2PE protection, which may impact our PCI DSS compliance validation, and will confirm with our acquirer or payment brand, as applicable, for all PCI payment brands affected.

Sincerely,

Technical Installation & Support	800-225-8979 x 4	Support@TempusTechnologies.com