TransArmor from fiserv.

P2PE Validated

Point-to-Point Encryption (P2PE)

Instruction Manual

Ingenico RP45x

Version 1.4

1. P2PE Solution Information and Solution Provider Contact Details

1.1 P2PE Solution Information	
Solution name:	First Data TransArmor P2PE Solution – Ingenico On-Guard
Solution reference number per PCI SSC website:	*2022-00541.001*

1.2 Solution Provider Contact Information	
Company name:	*First Data*
Company address:	*5565 Glenridge Connector, Atlanta, GA 30342*
Company URL:	*www.fiserv.com*
Contact name:	*Marco Mabante*
Contact phone number:	*(912) 484-6660*
Contact e-mail address:	*TransArmorP2PE@firstdata.com*

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. Confirm Devices were not tampered with and confirm the identity of any third-party personnel

2.1 Instructions for ensuring POI devices originate from trusted sites/locations only.

Ingenico terminals used as part of the First Data TransArmor P2PE Solution can only be deployed by First Data Hardware Services or Ingenico.

Do not purchase any Ingenico devices online or from a Key Injection Facility (KIF) that is not a Component of the TransArmor P2PE Solution. You may use PCI Qualified Integrator Resellers to install and activate Ingenico POI devices. To request a return (RMA) for a POI that has been tampered with or defective, please contact one of the following:

- Your Banking/Acquiring Relationship or Account Manager
- First Data TransArmor: TransArmorP2PE@FirstData.com
- Ingenico: (800) 435-3014 or CSSRMARequesting@ingenico.com

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

Carefully inspect the shipping carton and its Tamper Evident packaging for damage. If the tamper evident packaging is damaged DO NOT put the device into service and follow the tamper package internal process and contact First Data or Ingenico Customer Support to report.

Inspect the Tamper Evident packaging to ensure no damage or an attempt made to reseal the package with clear tape.

- Photograph and retain pictures of the package (damaged or not).
- Confirm the serial number(s) of the devices against the serial numbers listed on the Advance Ship Notice (ASN) you should have received from the FDHS or Ingenico prior to receipt of the shipment.

NOTE: If serial numbers do not match do not put device into service and contact one of the following:

If you believe the packaging or the device has been tampered with, DO NOT deploy the device. You must also inspect the device. You should look for broken security seals and cracks around device' seals to determine if the POI device itself has been compromised. Pictures of each device type supported are provided below to help you identify the devices and for inspections:

To request a return (RMA) for a POI that has been tampered with or defective, please contact one of the following:

- Your Banking/Acquiring Relationship or Account Manager
- First Data TransArmor: TransArmorP2PE@FirstData.com
- Ingenico: (800) 435-3014 or CSSRMARequesting@ingenico.com

Physically secure POI devices in your possession, including devices:

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

2.3 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.

First Data does not contract with any third-party personnel to install, troubleshoot, or repair any Ingenico devices.

Merchants may use internally approved associates or PCI Qualified Integrator Resellers (QIR) to install their devices using this P2PE Instruction Manual.

https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_integrators_and_resellers

To request a return (RMA) for a POI that has been tampered with or defective, please contact one of the following:

- Your Banking/Acquiring Relationship or Account Manager
- First Data TransArmor: TransArmorP2PE@FirstData.com
- Ingenico: (800) 435-3014 or CSSRMARequesting@ingenico.com

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

3.1 POI Device Details

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

IMPORTANT NOTE: PCI-listed P2PE solutions (and applicable P2PE components) are allowed to revalidate and reassess their existing PCI P2PE approval with expired PTS POI devices for up to, but not exceeding, 5 years past the PTS POI device expiry dates (as listed on the PCI Approved PTS Devices list) for the POI device types used in the solution. In the case of the Ingenico RP45x the PCI PTS expiry date is April 30, 2023. This means you could use the device until April 30, 2028. Be aware that the hardware manufacturer may end support for the device earlier than April 30, 2028.

All POI device information can be verified by visiting:
https://www.pcisecuritystandards.org/approved_companies_providers/approved_pin_transaction_security.php

See also Section 9.2, "Instructions for how to confirm hardware, firmware, and application versions on POI devices."

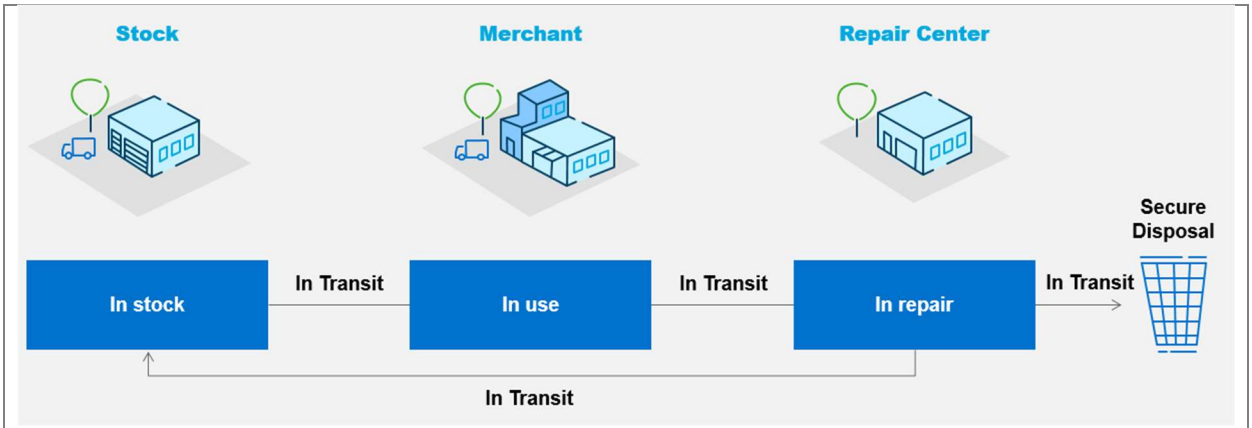
PCI PTS approval #:	POI device vendor:	POI device model name and number:	Hardware version #(s):	Firmware version #(s):

4-30202	*Ingenico*	*RP450, RP456, RP457, RP457 U*	*RP450b-01xxxxxx (Audio Jack)* *RP450b-02xxxxxx (Audio Jack)* *RP450b-03xxxxxxx (Audio Jack)* *RP450c-04xxxxxxx (for RP450; RP456; RP457; with CTLS)* *RP450n-04xxxxxxx (for RP450; RP456; RP457; no CTLS)* *RP456b-01xxxxxx (Audio Jack* *RP456b-02xxxxxx (Audio Jack; Bluetooth)* *RP456b-03xxxxxxx (Audio Jack; Bluetooth)* *RP456c-04xxxxxxx (for RP450; RP456; RP457; with CTLS)* *RP456n-04xxxxxxx (for RP450; RP456; RP457; no CTLS)* *RP457b-01xxxxxx (Audio Jack* *RP457b-02xxxxxx (Audio Jack; Bluetooth and MFI)* *RP457b-03xxxxxxx (Audio Jack; Bluetooth and MFI)* *RP457b-c3xxxxxxx (Bluetooth and MFI)* *RP457c-04xxxxxxx (for RP450; RP456; RP457; with CTLS)* *RP457c-M4xxxxxxx (for RP457 U; with CTLS)* *RP457c-R4xxxxxxx (for RP457 U; with CTLS)* *RP457c-U4xxxxxxx (for RP457 U; with CTLS)* *RP457n-04xxxxxxx (for RP450; RP456; RP457; no CTLS)* *RP457n-M4xxxxxxx (for RP457 U; no CTLS)* *RP457n-R4xxxxxxx (for RP457 U; no CTLS)* *RP457n-U4xxxxxxx (for RP457 U; no CTLS)*	*BOOT: xxxx-F-501-02xx-00xx-00 (SRED compliant)* *BOOT: xxxx-F-5x1-02xx-xxxx-xx (SRED compliant)* *BOOT: xxxx-F-5x1-03xx-xxxx-xx (SRED compliant)* *CTRL: xxxx-F-502-02xx-xxxx-00 (SRED compliant)* *CTRL: xxxx-F-502-03xx-xxxx-00 (SRED compliant)* *CTRL: xxxx-F-502-04xx-xxxx-00 (SRED compliant)* *CTRL: xxxx-F-5x2-04xx-xxxx-xx (SRED compliant)* *CTRL: xxxx-F-5x2-05xx-xxxx-xx (SRED complaint)*

3.2 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.
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)
N/A	*N/A*	*N/A*	*N/A*	No	No

3.3 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 *First Data* 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.
In order to maintain PCI P2PE compliance it is the Merchant's responsibility to keep track of all devices and regularly manage their inventory at the minimum of once per year. Merchants must track their POI devices for the following states: • In secure storage awaiting deployment • Deployed/In Service • Disabled / Out for repair • Decommissioned and returned for secure destruction • In transit



POI's held in storage awaiting deployment or for repair should be stored in a secure area that restricts access to authorized personnel only. In addition to the above states, the Merchant will also need to track the following items to ensure their POI's have not been tampered with:

- Physical connections to POI's
- Hardware and Firmware versions on POI's
- Dates and locations of inspections for each POI
- Name of authorized staff that performed the inspections

Below is the URL that will provide detailed instructions on reviewing Hardware and Firmware versions:

- https://www.pcisecuritystandards.org/ptsdocs/4-30202SPOL_RP45x_PCI_Security_Policy-20181113-1545247066.7392.pdf

Merchants may use an Inventory tracking spreadsheet to keep track of all their devices similar to this sample below:

Sample Inventory Table

Device Vendor	Device Model Name(s) and Number	Device Location	Device Status	Serial Number or Other Unique Identifier	Date of Inventory

4. 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 3.1 are allowed for cardholder data capture.

If a merchant's 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.
-

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

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

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

4.1 Installation and connection instructions

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 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.

RP45x

Usage

(a) Battery Status

A Red LED is present next to the USB connector for battery status.

-*Battery full*: Red LED is on all the time

-*Battery low*: Red LED On and Off for 1s every 3s alternatively

-*Battery very low*: Red LED On and Off for 1s every 6s alternatively

-*Battery out of capacity*: Red LED Off (and Green LED Off)

-*Battery charging*: Red LED On and Off every 1sec alternatively

Please ensure that the reader is charged every couple of months if not used on a regular basis.

(b) Reader during Swipe/Tap/Dip

There are 4 LEDs on the top of the reader to indicate progress of a contactless transaction. In addition, there is a buzzer inside the reader to prompt Swipe/Tap/Dip.

-*Reader ready:* The Red LED on the side of the reader will be On.

-*Reader waiting for card*: The reader will generate a beep prompting user to Swipe/Tap/Dip. One LED light on top of the reader will turn on (Only for Contactless).

-*Reader reading the card*: 2 LED lights turn On.

-*Card read successful*: 3 LED lights turn On.

-*Card Processing Error/Multiple Contactless Cards detected*: All lights are turned off to indicate that the contactless interface is not acceptable for this transaction.

-*Card Processing Error*: Only fourth LED light turns On indicating conditions for use of the contactless interface have not been satisfied (ex: As an added security measure, transaction amounts over a pre-set threshold may require a card swipe or insert.).

Pairing

Pairing of RP450c must be done from the mobile app that comes with the reader:

1. Open your mobile app
2. Tap on the **Menu** icon on the top left corner
3. Tap on **Settings**
4. Tap on **Bluetooth Readers**
5. If Bluetooth on your device is OFF, turn it ON
6. Tap on **'Pair a New Reader'** to start the pairing process.

Important: You will not be able to pair from your phone's Bluetooth Settings.

Connecting

You can connect this reader to your mobile app using an audio-jack or a Bluetooth connection. Once your reader has been paired with your mobile app, simply turn your reader ON to automatically connect to your app.

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

4.2 Guidance for selecting appropriate locations for deployed devices

When considering the prevention of theft once the device is installed, it is necessary to strike a balance between securing the asset and damaging usability and therefore, customer service. You should select a location for your POS that is secure, accessible by customers and always visible to staff.

It may be possible to attach the device to your payment station in such a way that prevents it being stolen but this will not necessarily deter the fraudulent engineer or collusive member of staff.

Therefore the physical location of the device and security of components should be considered. Can it be removed easily; are components hard wired together or physically protected to prevent easy tampering or theft?

You should ensure that you treat your RP45x as you do your cash till and make sure that it is safe and secure. It is the merchants' responsibility to ensure the devices are secure at all times.

- Do not place the RP45x device on a PC monitor, adjacent to an electronically active security tag deactivation system, or near other sources of magnetic fields. The RP45x device must be at least 12 inches away from an electronically active type of security tag deactivation pad. This is specifically defined as:
    - An electronically active system that sends out a powerful and potentially disruptive signal to deactivate the security tag. If the RP45x device is placed too close to the system's pad or placed too close above the pad, malfunction may occur.

- ***When selecting the device location, keep in mind that you must perform daily tasks to ensure the security and compliance of your device. Refer to section 5 POI Device Tamper Monitoring and Skimming Prevention for more information.***

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

Devices should be examined daily to check for suspicious attachments and any signs that they have been altered or interfered with. It is the merchants' responsibility to check the devices for any interference, unsecure devices, or scanning devices.

For POI devices located in areas away from merchant personnel, mechanism should be in place to ensure that suspicious attachments or alterations are be found and investigated. It is the merchants' responsibility to ensure the devices are checked regularly for the following items:

- Physical connections to POI's
- Hardware and Firmware versions on POI's
- Dates and locations of inspections for each POI
- Name of authorized staff that performed the inspections

You should also perform the following for devices that cannot be secured:

- Secure devices in a locked room, drawer or cabinet when not in use.
- Assign responsibility to specific individuals when device is in use.
- Observe devices at all times.
- Sign devices in/out, etc.

For lost or stolen devices:

How do I report a stolen device?

You can report a device as stolen to one of the following:

- Your Banking/Acquiring Relationship or Account Manager
- First Data TransArmor: TransArmorP2PE@FirstData.com
- Ingenico: (800) 435-3014 or CSSRMARequesting@ingenico.com

5. POI Device Transit

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

Each party involved in organizing the shipping should follow these security requirements:

- Ensure that devices are sealed with tamper-proof tape prior to shipment and during shipping process. This can be obtained at an office supply store
- Wherever the device is stored, it should be secured in an access-controlled area with sealed tamper-proof packaging
- Shipments are transported using Customs-Trade Partnership Against Terrorism (C-TPAT) approved common carriers such as FedEx, UPS or DHL
- Advance Ship Notice (ASN) including device serial numbers shall be provided to the receiving company at time of physical shipment via electronic method
- Receiving company should always verify physical receipt (part number, serial numbers, qty, etc.) with separately provided ASN information to ensure no en-route tampering
- Tracking number must be provided to track shipment status including locations at any given time
- Inspection should be conducted upon receiving the device (see Section 2.2 for instructions). If the device is tampered, it must be returned

Physically secure POI devices in your possession, including devices:

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

5.2 Instructions for ensuring POI devices are shipped to, trusted sites/locations only

Ingenico terminals used as part of the First Data TransArmor P2PE Solution can only be deployed by First Data Hardware Services or Ingenico.

Do not purchase any Ingenico devices online or from an unauthorized P2PE Solution Provider KIF. Only use PCI Qualified Integrator Resellers to install and activate Ingenico POI devices. To request a return (RMA) for a POI that has been tampered with or defective, please contact one of the following:

- Your Banking/Acquiring Relationship or Account Manager
- First Data TransArmor: TransArmorP2PE@FirstData.com
- Ingenico: (800) 435-3014 or CSSRMARequesting@ingenico.com

6. POI Device Tamper & Modification Guidance

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

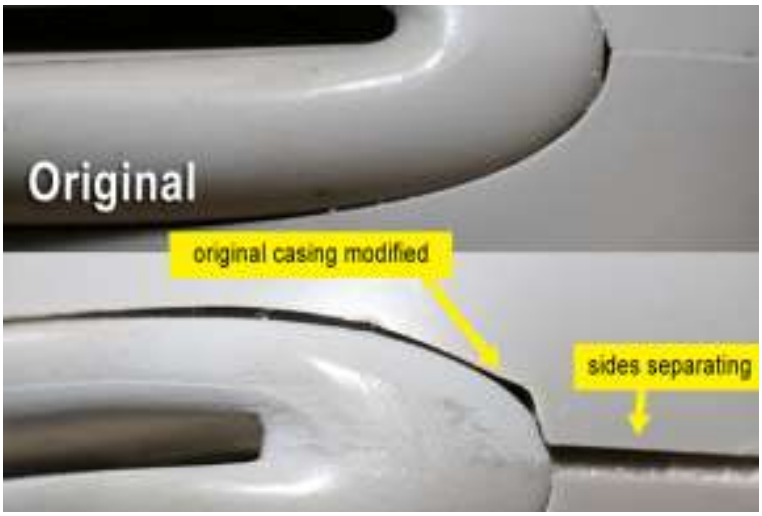
Additional guidance for inspecting POI devices can be found in the document entitled *Skimming Prevention: Best Practices for Merchants,* available at www.pcisecuritystandards.org.

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 of device should compare information located on the device itself with the inventory information previously recorded. In addition, the inspection should look for indications that the device has been tampered with. Indications of tampering may include, but is 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 (Cashiers/Managers) interfacing with the POI devices on a regular basis to inspect deployed POI devices daily.

To prevent skimming, record the appearance, condition, and location of each terminal. It is recommended to take photographs of each terminal from all angles to make comparisons. In addition, it is recommended that you weigh POI devices upon receipt and record this weight and periodically compare the results with vendor specifications to aid in identifying potential insertion of skimmers or other taping mechanisms within the device.

Regularly check the terminals to make sure they have not been tampered with. Follow the guidelines above in section 3.3 to physically secure the terminals. Always return the terminals to an authorized dealer, never throw the terminals away in the trash or a dumpster. Never allow a service engineer to service the terminal on any unplanned or unannounced visits. Always confirm the identity of a service engineer by contacting your solution provider. Use Appendix B in the Skimming Prevention: Best Practices for Merchants document to perform regular inspections. Please contact your solution provider immediately using the contact information in section 1.2 of this document to report any suspicious activity.

Inspect the EMV reader slot and MSR slot for obstructions and alterations



Inspect for case modifications, new stickers covering holes or signs of case separation

6.2 Instructions for responding to evidence of POI device tampering

The RP45x device detects any “tampered state”. In this state the PIN pad will repeatedly beep flash the 4 LED’s on and off and further use of the device will not be possible. If you observe the 4 LED’s flashing on and off and hear the beeping, you should contact one of the following immediately:

- Your Banking/Acquiring Relationship or Account Manager
- First Data TransArmor: TransArmorP2PE@FirstData.com
- Ingenico: (800) 435-3014 or CSSRMARequesting@ingenico.com

The reader contains tamper mechanisms that will trigger when a physical penetration attempt of the reader is detected. Merchants can easily detect a Tamper Response Event based on the lights flashing below.

What does it mean if my device has been tampered?

This can happen for a number of reasons, such as a credit card skimmer is applied to the device or someone has attempted to break the device open. This can also happen if the device is dropped hard enough during shipment or by the merchant or a customer.

What should I do if my device has been tampered?

To request a return (RMA) for a POI that has been tampered with or defective, please contact one of the following:

- Your Banking/Acquiring Relationship or Account Manager
- First Data TransArmor: TransArmorP2PE@FirstData.com
- Ingenico: (800) 435-3014 or CSSRMARequesting@ingenico.com

7. Device Encryption Issues

7.1 Instructions for responding to POI device encryption failures

If First Data has contacted the Merchant to inform them of encryption errors, OR the merchant experiences a Tamper Event the POI must be taken out of service immediately and replaced.

To request a swap (RMA) for a POI that has been tampered with or defective, please contact one of the following:

- Your Banking/Acquiring Relationship or Account Manager
- First Data TransArmor: TransArmorP2PE@FirstData.com
- Ingenico: (800) 435-3014 or CSSRMARequesting@ingenico.com

8. POI Device Troubleshooting

8.1 Instructions for troubleshooting a POI device

This section covers basic troubleshooting.

To request a return (RMA) for a POI that has been tampered with or defective, please contact 1 of the following:

1. Your Banking/Acquiring Relationship or Account Manager
2. First Data TransArmor: TransArmorP2PE@FirstData.com
3. Ingenico: (800) 435-3014 or CSSRMARequesting@ingenico.com

How to turn on the reader?
Start your mobile payment application and plug the reader to the audio jack. Make sure that the reader is not being charged. The reader should turn on with the Red LED on. If it does not, the common issues are low battery, audio jack hindrance, unsupported phone.
Developer: You can add a “Power On” status in troubleshooting section of the app. You can call Opendevice API call that you currently use. Based on the status, you can say whether the device is connected on not.
How to turn off the reader?
Removing the reader from the phone will automatically turn off the reader (after 5-10 seconds). If the reader is connected to the phone and no transactions are being processed, the reader turns off after set idle time (180 seconds). When powered off, all the LEDs are off.
Developer: Closing the device from the API will turn off the reader. It is ideal to turn off the reader when no transactions are under way. This will extend the reader battery per recharge.

How to check if the reader is charged?
Plug the reader to a wall USB charger without connecting to the phone's audio jack. Make sure that the Green LED light turns on. Make sure that the Red LED light is either blinking or solid. Blinking indicates that the reader is being charged and Solid indicates that the reader is fully charged.
Developer: Add battery level in troubleshooting section of the App. Selecting it should show the battery level. If it is below a threshold (say 10%), recommend to charge the reader.
How to check if the reader powers down on its own? How to perform a hardware reset?
Disconnect the reader from the phone and the Wall charger. Make sure that the LED lights turn off after 5-10 seconds. If the LED continues to remain on, reset the reader by pressing the reset button using a pin. The reset button is located below the micro USB. Pressing reset will not erase settings of the reader. It just performs a hard power off.

The RP45x device detects any "tampered state". In this state the PIN pad will repeatedly beep flash the 4 LED's on and off and further use of the device will not be possible. If you observe the 4 LED's flashing on and off and hear the beeping, you should contact one of the following immediately:

- Your Banking/Acquiring Relationship or Account Manager
- First Data TransArmor: TransArmorP2PE@FirstData.com
- Ingenico: (800) 435-3014 or CSSRMARequesting@ingenico.com

9. Additional Guidance

9.1 Additional Solution Provider Information

What should I do if I do not find the answer to my question or want to leave feedback?

Please contact one of the following:

- Your Banking/Acquiring Relationship or Account Manager
- First Data TransArmor: TransArmorP2PE@FirstData.com
- Ingenico: (800) 435-3014 or CSSRMARequesting@ingenico.com

9.2 Instructions for how to confirm hardware, firmware, and application versions on POI devices

Below is the URL that will provide detailed instructions on reviewing Hardware and Firmware versions:

- https://www.pcisecuritystandards.org/ptsdocs/4-30202SPOL_RP45x_PCI_Security_Policy-20181113-1545247066.7392.pdf