cardconnect®

P2PE Instruction Manual (PIM)

V3.8

March 2024

Revision History

Version	Date	Contributors
1.0	Oct 2014	Rush Taggart
1.1	Nov 2014	Andy Liaskos
1.2	Dec 2014	Justin Shipe
1.3	Jan 2016	Rush Taggart
2.0	Aug 2016	Justin Shipe
2.1	Jan 2017	Dave Gouger, Justin Shipe, Andy Liaskos
2.2	Mar 2017	Dave Gouger, Justin Shipe, Andy Liaskos
2.3	Jun 2017	Justin Shipe
2.4	Dec 2017	Justin Shipe
2.5	Apr 2018	Chris Kemmerer
2.6	May 2018	Chris Kemmerer
2.7	June 2018	Chris Kemmerer
2.8	March 2019	Chris Kemmerer, Christopher Edmundowicz
2.9	June 2019	Ken Groninger
3.0	November 2019	Ken Groninger
3.1	March 2020	Ken Groninger
3.2	October 2020	Ken Groninger
3.3	November 2020	Ken Groninger
3.4	January 2021	Ken Groninger
3.5	March 2021	Ken Groninger
3.6	November 2022	Ken Groninger
3.7	January 2023	Ken Groninger
3.8	March 2024	Ken Groninger

Table of Contents

1. P2PE Solution Information and Solution Provider Contact Details

1.1 P2PE Solution Information	
Solution name:	CardSecure P2PE
Solution reference number per PCI SSC website:	2024-00113.023

1.2 Solution Provider Contact Information	
Company name:	CardConnect, LLC
Company address:	1000 Continental Drive, Suite 300, King of Prussia PA 19406
Company URL:	www.cardconnect.com
Contact name:	CardPointe Support
Contact phone number:	877-828-0720
Contact e-mail address:	cardpointesupport@fiserv.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.

Devices are shipped from CardConnect's trusted sources. When receiving device shipments, ensure that the shipper address matches one of the following:

- **CardConnect**
  1000 Continental Dr
  Suite 300
  King of Prussia, PA 19406
- **Ingenico Inc.**
  6190 Shiloh Crossing
  Suite C
  Alpharetta, GA 30005
- **Fiserv Hardware Solutions**
  1169 Canton Rd
  Marietta, GA 30066
- **ID TECH**
  10721 Walker Street
  Cypress, CA 90630

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

When you receive a terminal shipment, verify that packages have not been tampered before or during shipment. Inspect the tape to ensure no seals are broken or cracked. If the package shows signs of tampering, contact CardPointe Support for further instructions.

You can confirm that your original terminal device is in place by comparing:

- Make and Model
- Serial number
- General description
- Security seals, labels, hidden markings, etc. You may dab a dot of nail polish inconspicuously on one corner, for instance.
- Number and type of physical connections to device (ONE)
- Date of last inspection

You must maintain a log of these security checks for each device and provide it to your PCI auditor for inspection. A handwritten notebook is sufficient. It should be kept in a secure location.

You can also contact CardPointe Support to provide an inspection record, including the device serial number, inspection result, and optionally a photograph. CardPointe Support will maintain this record.

The CardPointe Retail Terminal firmware included in the PCI PTS-approved Telium 2 and Tetra devices has been configured and programmed to communicate only over IP with TLS 1.2 communication channels. External communications via IP with TLS 1.2 are used to send encrypted transaction information directly to the CardPointe Retail Terminal P2PE decryption environment for processing. The protocol stack is provided by Ingenico as part of the Link Layer

module. The CardPointe Retail Terminal firmware does not implement its own open protocol stack. No other communication methods are used or programmed into the CardPointe Retail Terminal firmware for use.

To verify that your CardPointe Retail Terminal has established secure communications, do the following:

1. Press pound (#), then 4 to access the Setup menu.
2. Press 2 to access the Communications menu.
3. Press 4 to display the parameters.
4. Check the HostURL1 and HostURL2 parameters. These values should match, and should point to <site>.cardconnect.com.

CardPointe Integrated Terminal devices maintain a persistent secure socket connection to the terminal service over IP with TLS 1.2. For Ingenico terminals, the PanPad application implements the Ingenico Communication Link Layer (CLL) protocol, to enable secure Ethernet and Wi-Fi network communications. For Clover terminals, the CardPointe Integrated Terminal App uses SSL to enable secure Ethernet, Wi-Fi, and cellular communications. These external communications via IP are used to send encrypted transaction information directly to the CardSecure P2PE environment for processing. Both applications are configured to use only these methods, and no other communication channels are permitted. Enabling additional communication methods requires development work by CardConnect.

To verify that your terminal has established secure communications, check the terminal display. The terminal displays “Connected” when it has established a secure connection to the terminal service.

Physically secure POI devices in your possession, including devices:

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

2.3 Instructions for confirming 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.

At no time will CardConnect send a technician to perform on-site terminal repair. All staff at merchant locations must be trained to check the personal identification and credentials of any person that claims to be a terminal repair technician. Before allowing any person physical access to a payment terminal for troubleshooting or maintenance purposes, contact CardPointe Support.

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.

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

See also *9.1 Determining POI Device Hardware and Firmware Versions.*

POI device vendor:	Clover
POI device model name and number:	Flex
Hardware version #(s):	3.XX, 4.01
Firmware version #(s):	0 01.XX.XXXX 01.XX.XXXX (01.XXXXX) (SRED), 0 02.XX.XXXX 02.XX.XXXX (01.XXXXX) (SRED), 0 02.xx.xxxx 03.xx.xxxx (01.xxxxx) (SRED)
PCI PTS Approval #(s):	4-40209 (PTS v5.x)

POI device vendor:	Clover
POI device model name and number:	Mini (2nd Generation)
Hardware version #(s):	3.XX, 4.01
Firmware version #(s):	0 02.XX.XXXX 02.XX.XXXX (01.XXXXX) (SRED)
PCI PTS Approval #(s):	4-10248 (PTS v5.x)

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 (PTS v4.x)

POI device vendor:	ID TECH
POI device model name and number:	SecurRED
Hardware version #(s):	IDSR-33x1xxxxx
Firmware version #(s):	SRED: 1.07, 1.08, 2.00
PCI PTS Approval #(s):	4-10144 (PTS v3.x)

POI device vendor:	ID TECH
POI device model name and number:	SREDKey 2
Hardware version #(s):	80172004 (With MSR)
Firmware version #(s):	SREDKey2 FW v1.01.xxx.xxxx.S
PCI PTS Approval #(s):	4-90075 (PTS v5.x)

POI device vendor:	ID TECH
POI device model name and number:	SREDKey
Hardware version #(s):	IDSK-53XXXXXXX
Firmware version #(s):	SRED: 1.01
PCI PTS Approval #(s):	4-10156 (PTS v3.x)

POI device vendor:	ID TECH
POI device model name and number:	VP5300
Hardware version #(s):	80152001
Firmware version #(s):	VP5300 FW v1.01.xxx.xxxx.S, VP5300 FW v1.00.xxx.xxxx.S, VP5300 FW v1.02.xxx.xxxx.S
PCI PTS Approval #(s):	4-10245 (PTS v5.x)

POI device vendor:	Ingenico
POI device model name and number:	Desk/1500
Hardware version #(s):	LAN30AA, LAN30AN, LAN30BA, LAN30BN, LAN30CA, LAN30DA, LAN30EA, LAN30EN, LAN30FA, LAN30FN, LAN30GA, LAN30HA
Firmware version #(s):	820547v01.xx, 820561v01.xx (base firmware), 820376v01.xx, 820555v01.xx (SRED), 820548V02.xx (OP), 820556v01.xx (SRED On-Guard SDE), 820549v01.xx (SRED On-Guard FPE), 820548V03.xx (OP), 820565V01.xx (SRED FF1), 820548v06.xx (OP)
PCI PTS Approval #(s):	4-30310 (PTS v5.x)

POI device vendor:	Ingenico
POI device model name and number:	Desk/3500
Hardware version #(s):	DES35BA (CTLS)
Firmware version #(s):	820547 V01.xx
PCI PTS Approval #(s):	4-20283 (PTS v4.x)

POI device vendor:	Ingenico
POI device model name and number:	Desk/5000
Hardware version #(s):	DES50BA (CTLS)
Firmware version #(s):	820547 V01.xx
PCI PTS Approval #(s):	4-20281 (PTS v4.x)

POI device vendor:	Ingenico
POI device model name and number:	Desk/5000
Hardware version #(s):	DES50BB
Firmware version #(s):	820547v01.xx; 820376v01.xx, 820549V01.xx (SRED OnGuard FPE), 820555v01.xx (SRED AWL), 820556v01.xx (SRED OnGuard SDE), 820559v01.xx (SRED ANL), 820565v01.xx (SRED FF1), 820547v01.xx (Core Firmware), 820376v01.xx (Security Services), 820376v02.xx (Security Services)
PCI PTS Approval #(s):	4-20317 (PTS v5.x)

POI device vendor:	Ingenico
POI device model name and number:	iCT220, iCT250
Hardware version #(s):	iCT2xx-11Txxxxx
Firmware version #(s):	820305V02.xx, 820375V01.xx, 820365 V02.xx, SRED (Non CTLS): 820528V02.x
PCI PTS Approval #(s):	4-20196 (PTS v3.x)

POI device vendor:	Ingenico
POI device model name and number:	iPP310, iPP320, iPP350
Hardware version #(s):	iPP3xx-11Txxxxx
Firmware version #(s):	SRED (CTLS): 820365 V02.xx, 820305 V02.xx, 820528 V02.xx, SRED (Non CTLS): 820375 V01.xx, 820554 V01.xx
PCI PTS Approval #(s):	4-20184 (PTS v3.x)

POI device vendor:	Ingenico
POI device model name and number:	iPP320, iPP350, iPP310, iPP315
Hardware version #(s):	iPP3xx-21Txxxxx, iPP3xx-31Txxxxx, iPP3xx-41Txxxxx, iPP3xx51Txxxxx
Firmware version #(s):	820305 V11.xx, 820180 V01.xx
PCI PTS Approval #(s):	4-30176 (PTS v4.x)

POI device vendor:	Ingenico
POI device model name and number:	iSC Touch 250
Hardware version #(s):	iSC2xx-21Txxxxx, iSC2xx-31Txxxxx
Firmware version #(s):	820518 V12.xx, SRED (CTLS): 820528 V02.xx
PCI PTS Approval #(s):	4-30132 (PTS v4.x)

POI device vendor:	Ingenico
POI device model name and number:	iSMP4
Hardware version #(s):	IMP6xx-01Txxxxx (without contactless), IMP6xx-11Txxxxx (with contactless), IMP6xx-02Txxxxx, (without contactless), IMP6xx-12Txxxxx(with contactless)
Firmware version #(s):	820305 V11.xx
PCI PTS Approval #(s):	4-30220 (PTS v4.x)

POI device vendor:	Ingenico
POI device model name and number:	Lane/3000
Hardware version #(s):	LAN30AA, LAN30AN, LAN30BA, LAN30BN, LAN30CA, LAN30DA, LAN30EA, LAN30EN, LAN30FA, LAN30FN, LAN30GA, LAN30HA
Firmware version #(s):	820547v01.xx, 820561v01.xx (base firmware), 820376v01.xx, 820555v01.xx (SRED), 820548V02.xx (OP), 820556v01.xx (SRED On-Guard SDE), 820549v01.xx (SRED On-Guard FPE), 820548V03.xx (OP), 820565V01.xx (SRED FF1), 820548v06.xx (OP)
PCI PTS Approval #(s):	4-30310 (PTS v5.x)

POI device vendor:	Ingenico
POI device model name and number:	Lane/5000
Hardware version #(s):	LAN51BA, LAN51CA, LAN51DA, LAN51EA
Firmware version #(s):	820547v01.xx, (Non SRED) 820376v01.xx (Non SRED), 820547v01.xx, 820549V01.xx, 820556V01.xx (SRED OnGuard SDE), 820559V01.xx (SRED ANL), 820565v01.xx (SRED FF1), 820548V02.xx (Open Protocol), 820548v03.xx (Open Protocol)
PCI PTS Approval #(s):	4-20303 (PTS v4.x)

POI device vendor:	Ingenico
POI device model name and number:	Lane/5000
Hardware version #(s):	LAN51BA (single MSR head), LAN51CA (dual MSR head), LAN51DA (single MSR head and camera), LAN51EA (dual MSR head and camera)
Firmware version #(s):	20376v01.xx, 820547v01.xx, 820549v01.xx (SRED OnGuard FPE), 820555v01.xx (SRED AWL), 820556v01.xx (SRED OnGuard SDE), 820559v01.xx (SRED ANL), 820565v01.xx (SRED FF1), 820548V02.xx (Open Protocol), 820548v03.xx (Open Protocol)
PCI PTS Approval #(s):	4-20324 (PTS v5.x)

POI device vendor:	Ingenico
POI device model name and number:	Lane/7000
Hardware version #(s):	LAN70AA, LAN70AB
Firmware version #(s):	820547v01.xx, 820376v01.xx, 820549v01.xx (SRED), 820548V02.xx (OP), 820556v01.xx (SRED On-Guard SDE), 820556v01.xx (SRED On-Guard SDE), 820548V03.xx (OP), 820565v01.xx (SRED FF1), 820565v01.xx (SRED FF1), 820555v01.xx (SRED AWL), 820548v06.xx (OP)
PCI PTS Approval #(s):	4-30237 (PTS v5.x)

POI device vendor:	Ingenico
POI device model name and number:	Lane/8000
Hardware version #(s):	LAN80AA
Firmware version #(s):	820547v01.xx, 820376v01.xx, 820549v01.xx (SRED), 820548V02.xx (OP), 820556v01.xx (SRED On-Guard SDE), 820548V03.xx (OP), 820565V01.xx (SRED FF1), 820565V01.xx (SRED FF1), 820565V01.xx (SRED FF1)
PCI PTS Approval #(s):	4-30257 (PTS v5.x)

POI device vendor:	Ingenico
POI device model name and number:	Link/2500
Hardware version #(s):	LIN25BA CTLS, LIN25CA, LIN25DA
Firmware version #(s):	820547v01.xx, 820556v01.xx (SRED On-Guard SDE), 820555v01.xx (SRED AWL)
PCI PTS Approval #(s):	4-30230 (PTS v4.x)

POI device vendor:	Ingenico
POI device model name and number:	Move/5000
Hardware version #(s):	MOV50BB
Firmware version #(s):	820547v01.xx, 820376v02.xx, 820548v02.xx, 820556v01.xx (SRED OnGuard SDE), 820549V01.xx (SRED OnGuard FPE)
PCI PTS Approval #(s):	4-20316 (PTS v5.x)

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.

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)
CardPointe Integrated Terminal (for Clover) v1.x.x ***Note:*** *This non-P2PE application does not handle unencrypted cardholder data; this application only facilitates communication with the terminal web service.*	Clover	Flex	**Hardware Version:** 3.XX, 4.01 **Firmware Version:** 0 01.XX.XXXX 01.XX.XXXX (01.XXXXX) (SRED), 0 02.XX.XXXX 02.XX.XXXX (01.XXXXX) (SRED), 0 02.XX.XXXX 03.XX.XXXX (01.XXXXX) (SRED)	No	No
		Mini (2nd Generation)/ C302	**Hardware Version:** 3.XX, 4.01 **Firmware Version:** 0 02.XX.XXXX 02.XX.XXXX (01.XXXXX) (SRED)	No	No

CardPointe Integrated Terminal v2.1.x	Ingenico	Lane/3000 (PTS v5.x)	**Hardware Version:** LAN30AA, LAN30AN, LAN30BA, LAN30BN, LAN30CA, LAN30DA, LAN30EA, LAN30EN, LAN30FA, LAN30FN, LAN30GA, LAN30HA **Firmware Version:** 820547v01.xx, 820561v01.xx (base firmware), 820376v01.xx, 820555v01.xx (SRED), 820548V02.xx (OP), 820556v01.xx (SRED On-Guard SDE), 820549v01.xx (SRED On-Guard FPE), 820548V03.xx (OP), 820565V01.xx (SRED FF1), 820548v06.xx (OP)	Yes	Yes
		Lane/5000 (PTS v4.x)	**Hardware Version:** LAN51BA, LAN51CA, LAN51DA, LAN51EA **Firmware Version:** 820547v01.xx, (Non SRED), 820376v01.xx (Non SRED), 820547v01.xx, 820549V01.xx, 820556V01.xx (SRED OnGuard SDE), 820559V01.xx (SRED ANL), 820565v01.xx (SRED FF1),	Yes	Yes

			820548V02.xx (Open Protocol), 820548v03.xx (Open Protocol)		
		Lane/5000 (PTS v5.x)	**Hardware Version:** LAN51BA (single MSR head), LAN51CA (dual MSR head), LAN51DA (single MSR head and camera), LAN51EA (dual MSR head and camera) **Firmware Version:** 20376v01.xx, 820547v01.xx, 820549v01.xx (SRED OnGuard FPE), 820555v01.xx (SRED AWL), 820556v01.xx (SRED OnGuard SDE), 820559v01.xx (SRED ANL), 820565v01.xx (SRED FF1), 820548V02.xx (Open Protocol), 820548v03.xx (Open Protocol)	Yes	Yes
		Lane/7000 (PTS v5.x)	**Hardware Version:** LAN70AA, LAN70AB **Firmware Version:** 820547v01.xx, 820376v01.xx, 820549v01.xx (SRED), 820548V02.xx (OP), 820556v01.xx (SRED On-Guard SDE), 820556v01.xx (SRED On-Guard SDE),	Yes	Yes

			820548V03.xx (OP), 820565v01.xx (SRED FF1), 820565v01.xx (SRED FF1), 820555v01.xx (SRED AWL), 820548v06.xx (OP)		
		Lane/8000 (PTS v5.x)	**Hardware Version:** LAN80AA **Firmware Version:** 820547v01.xx, 820376v01.xx, 820549v01.xx (SRED), 820548V02.xx (OP), 820556v01.xx (SRED On-Guard SDE), 820548V03.xx (OP), 820565V01.xx (SRED FF1), 820565V01.xx (SRED FF1), 820565V01.xx (SRED FF1)	Yes	Yes
		Link/2500 (PTS v4.x)	**Hardware Version:** LIN25BA (CTLS), LIN25CA, LIN25DA **Firmware Version:** 820547v01.xx, 820556v01.xx (SRED On-Guard SDE), 820555v01.xx (SRED AWL)	Yes	Yes
CardPointe Integrated Terminal v2.0.x	Ingenico	iPP320, iPP350, iPP310, iPP315 (PTS v4.x)	**Hardware Version:** iPP3xx-21Txxxxx, iPP3xx-31Txxxxx, iPP3xx-41Txxxxx, iPP3xx-51Txxxxx **Firmware Version:** 820305 V11.xx, 820180 V01.xx	Yes	Yes
		iSC Touch 250 (PTS v4.x)	**Hardware Version:** iSC2xx-21Txxxxx,	Yes	Yes

			iSC2xx-31Txxxxx **Firmware Version:** 820518 V12.xx, SRED (CTLS): 820528 V02.xx		
		iSMP4 (PTS v4.x)	**Hardware Version:** IMP6xx-01Txxxxx (without contactless), IMP6xx-11Txxxxx (with contactless), IMP6xx-02Txxxxx, (without contactless), IMP6xx12Txxxxx (with contactless) **Firmware Version:** 820305 V11.xx	Yes	Yes
CardPointe Integrated Terminal v1.6.x	Ingenico	iPP310, iPP320, iPP350 (PTS v3.x)	**Hardware Version:** iPP3xx-11Txxxxx **Firmware Version:** SRED (CTLS): 820365 V02.xx, 820305V02.xx, 820528V02.xx SRED (Non CTLS): 820375 V01.xx, 820554 V01.xx	Yes	Yes
		iPP320, iPP350, iPP310, iPP315 (PTS v4.x)	**Hardware Version:** iPP3xx-21Txxxxx, iPP3xx-31Txxxxx, iPP3xx-41Txxxxx, iPP3xx-51Txxxxx **Firmware Version:** 820305 V11.xx, 820180 V01.xx	Yes	Yes
		iSC Touch 250 (PTS v4.x)	**Hardware Version:** iSC2xx-21Txxxxx, iSC2xx-31Txxxxx **Firmware Version:** 820518 V12.xx, SRED (CTLS): 820528 V02.xx	Yes	Yes
		iSMP4 (PTS v4.x)	**Hardware Version:** IMP6xx-01Txxxxx (without contactless), IMP6xx-11Txxxxx	Yes	Yes

			(with contactless), IMP6xx-02Txxxxx, (without contactless), IMP6xx12Txxxxx (with contactless) **Firmware Version:** 820305 V11.xx		
CardConnect PANpad v5.3.x	Ingenico	iPP310, PP320, PP350 (PTS v3.x)	**Hardware Version:** iPP3xx-11Txxxxx **Firmware Version:** 820305 V02.xx, 820528 V02.xx	Yes	Yes
		iPP320, iPP350, iPP310, iPP315 (PTS v4.x)	**Hardware Version:** iPP3xx-21Txxxxx, iPP3xx-31Txxxxx, iPP3xx-41Txxxxx, iPP3xx-51Txxxxx **Firmware Version:** 820305 V11.xx, 820180 V01.xx	Yes	Yes
		iSC Touch 250 (PTS v4.x)	**Hardware Version:** iSC2xx-21Txxxxx, iSC2xx-31Txxxxx **Firmware Version:** 820518 V12.xx, 820528 V02.xx	Yes	Yes
CardConnect PANpad v5.2	Ingenico	iPP310, iPP320, iPP350 (PTS v3.x)	**Hardware Version:** iPP3xx-11Txxxxx **Firmware Version:** 820305 V02.xx, 820528 V02.xx	Yes	Yes
		iPP320, iPP350, iPP310, iPP315 (PTS v4.x)	**Hardware Version:** iPP3xx-21Txxxxx, iPP3xx-31Txxxxx, iPP3xx-41Txxxxx, iPP3xx-51Txxxxx **Firmware Version:** 820305 V11.xx, 820180 V01.xx	Yes	Yes
		iSC Touch 250 (PTS v4.x)	**Hardware Versions:** iSC2xx-21Txxxxx, iSC2xx-31Txxxxx	Yes	Yes

			Firmware Versions: 820518 V12.xx, 820528 V02.xx		
CardPointe Retail Terminal v3.1.x	Ingenico	Desk/1500 (PTS v5.x)	**Hardware Version:** LAN30AA, LAN30AN, LAN30BA, LAN30BN, LAN30CA, LAN30DA, LAN30EA, LAN30EN, LAN30FA, LAN30FN, LAN30GA, LAN30HA **Firmware Version:** 820547v01.xx, 820561v01.xx (base firmware), 820376v01.xx, 820555v01.xx (SRED), 820548V02.xx (OP), 820556v01.xx (SRED On-Guard SDE), 820549v01.xx (SRED On-Guard FPE), 820548V03.xx (OP), 820565V01.xx (SRED FF1), 820548v06.xx (OP)	Yes	Yes
		Desk/3500 (PTS v4.x)	**Hardware Version:** DES35BA (CTLS) **Firmware Version:** 820547v01.xx, 820376v01.xx, 820549v01.xx (SRED), 820549v01.xx, 820556v01.xx, 820565v01.xx (SRED)	Yes	Yes
		Desk/5000 (PTS v5.x)	**Hardware Version:** DES50BB **Firmware Version:** 820547v01.xx,	Yes	Yes

			820376v01.xx, 820549V01.xx (SRED OnGuard FPE), 820555v01.xx (SRED AWL), 820556v01.xx (SRED OnGuard SDE), 820559v01.xx (SRED ANL), 820565v01.xx (SRED FF1), 820547v01.xx (Core Firmware), 820376v01.xx (Security Services), 820376v02.xx (Security Services)		
		Desk/5000 (PTS v4.x)	**Hardware Version:** DES50BA (CTLS) **Firmware Version:** 820547v01.xx, 820376v01.xx, 820549V01.xx (SRED OnGuard FPE), 820555v01.xx (SRED AWL), 820556v01.xx (SRED OnGuard SDE), 820559v01.xx (SRED ANL), 820565v01.xx (SRED FF1)	Yes	Yes
		iPP315 (PTS v4.x)	**Hardware Version:** iPP3xx-31Txxxxx **Firmware Version:** 820305 V11.xx, 820180 V01.xx	Yes	Yes
		Move/5000 (PTS v5.x)	**Hardware Version:** MOV50BB **Firmware Version:** 820547v01.xx, 820376v02.xx, 820548v02.xx, 820556v01.xx (SRED OnGuard SDE), 820549V01.xx (SRED OnGuard FPE)	Yes	Yes
CardPointe	Ingenico	Desk/3500 (PTS v4.x)	**Hardware Version:**	Yes	Yes

Retail Terminal v2.3.x			DES35BA (CTLS) **Firmware Version:** 820547v01.xx, 820376v01.xx, 820549v01.xx (SRED), 820549v01.xx, 820556v01.xx, 820565v01.xx (SRED)		
		Desk/5000 (PTS v4.x)	**Hardware Version:** DES50BA (CTLS) **Firmware Version:** 820547v01.xx; 820376v01.xx, 820549V01.xx (SRED OnGuard FPE), 820555v01.xx (SRED AWL), 820556v01.xx (SRED OnGuard SDE), 820559v01.xx (SRED ANL), 820565v01.xx (SRED FF1)	Yes	Yes
		iCT220, iCT250 (PTS v3.x)	**Hardware Version:** iCT2xx-11Txxxxx **Firmware Versions:** 820305V02.xx, 820375V01.xx, 820365V02.xx SRED (Non CTLS): 820528V02.x	Yes	Yes
		iPP315 (PTS v4.x)	**Hardware Version:** iPP3xx-31Txxxxx **Firmware Version:** 820305 V11.xx, 820180 V01.xx	Yes	Yes
		iPP320 (PTS v3.x)	**Hardware Version:** IPP3xx-11Txxxxx **Firmware Version:** SRED (CTLS): 820365V02.xx, 820305V02.xx, 820528V02.xx SRED (Non CTLS): 820375V01. xx, 820554v01.xx	Yes	Yes

ID TECH Payment Application Engine (PAE) v1.5.x.x ***Note:*** *This non-P2PE application does not handle unencrypted cardholder data; this application only facilitates communication with the terminal web service.*	ID TECH	VP5300 (PTS v5.x)	**Hardware Version:** 80152001 **Firmware Version:** VP5300 FW v1.01.xxx.xxxx.S, VP5300 FW v1.00.xxx.xxxx.S, VP5300 FW v1.02.xxx.xxxx.S	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 CardConnect directly via CardPointe Support.
- The sample inventory table below is for illustrative purposes only. The actual inventory should be captured and maintained by the merchant in an external document.

Secure Inventory Control

Merchants are responsible for maintaining inventory and monitoring inventory of all terminals in your charge. This includes terminals that are in use, devices that are waiting to be used and devices that are in the process of being repaired. A missing or unaccounted for device could indicate that a terminal has been intercepted by an unauthorized party.

The CardConnect Terminal Management System provides reports of all devices shipped to a location. This must match the devices in use at that location.

Annual Audit of Terminal Inventory

Merchants are responsible for maintaining inventory and monitoring inventory of all devices processing cardholder data. This includes terminals that are in use, devices that are waiting to be used and devices that are in the process of being repaired. For this reason, CardConnect recommends any terminal not in active use or in the installation process be securely stored on premises, or returned to CardConnect. The CardConnect TMS will record returned terminals and remove them from merchant responsibility. CardConnect grants program managers' access to the Terminal Management System to review device inventory information.

At least once a year, a full inventory of all terminals (POI devices) must be conducted to ensure that all devices are accounted for and match the serial numbers documented in your inventory. All merchants should be familiar with their terminal models, including security markings, screws, and tamper seals so that inspections are effective at detecting tampered or compromised devices.

If a discrepancy is found during the annual inventory, the following steps must be taken:

1. Isolate the missing device or devices.
2. Determine the last known location of the device and if possible the last known use.
3. Determine the serial number/type of device.
4. Verify what state the device was in (deployed, spare/backup, undergoing repair).

5. Contact CardPointe Support with all the information collected about the missing device.
6. Work with CardPointe Support to verify if cardholder data has been compromised.

If you determine that cardholder data has been compromised, follow the steps outlined by Visa at: http://www.visaeurope.com/en/businesses__retailers/payment_security/downloads__resources.aspx

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 additional PCI DSS requirements are now applicable for the merchant.
- Only PCI-approved capture mechanisms, as designated on the PCI Council'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 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

4.1 Installation and Connection Instructions

CardConnect Ingenico Device Installation

Your CardConnect device is shipped to you pre-programmed and ready to use. There is no need for you to perform any update or download once you receive your device. Perform the following upon receiving the device:

1. Unpack the device from the box.
2. Connect the included cabling.
3. Connect the USB, Ethernet or Serial cable to your network, and then plugin the power supply to a wall outlet to power up your device.

   Your device will now go through a boot cycle to power up.

For PANpad devices, once your device completes booting up it should display “Panpad No Connection.”

For CardPointe Integrated Terminal devices, the display should read “Connected.”

If your device displays another message, or if you are unable to process a transaction, contact CardPointe Support for immediate support.

After initial installation, it is considered best practice to disconnect and securely store your devices when unattended.

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

It is important that your devices are placed in secure and well-lit locations that are not left unattended for extended periods of time. Devices that are not in use should be stored in a secured location.

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

We recommended physically securing POI devices with security tethers to prevent the terminal(s) from being compromised. Devices should be placed in a location that allows customers to use them in a manner that obscures their PIN entry from other customers. In addition, it is a best practice to block ports on the device to prevent tampering.

5. POI Device Transit

5.1 Instructions for securing POI devices intended for, and during, transit
Terminals must be secured before and during transportation. When developing your transportation procedure, be sure to cover the following areas: • Package the device in such a way that is tamper-evident. Use tamper tape on boxes. Track the device number and shipping details together. • Verify the packages have not been tampered before shipment. Inspect the tape to ensure no seals are broken or cracked. If the package shows signs of tampering, do not ship it. Review your access log for information on the last person to access the area and contact CardPointe Support for further instructions. Terminal shipments must use only secure courier services that provide tracking services.
Physically secure POI devices in your possession, including devices: ▪ Awaiting deployment ▪ Undergoing repair or otherwise not in use ▪ Awaiting transport between sites/locations

5.2 Instructions for ensuring POI devices shipped to trusted sites/locations
As a P2PE merchant, you are responsible for maintaining all information regarding the chain of custody of your P2PE terminals. The intent of this control is to clearly identify which devices are in your possession, the device status, and location. If a terminal is not correctly encrypting card data, you, the merchant, must be able to locate a device in your possession using a Hardware Serial Number (HSN). Devices are shipped from CardConnect's trusted sources. When sending device shipments, ensure that the receiving address matches one of the following: ▪ **CardConnect** 1000 Continental Dr Suite 300 King of Prussia, PA 19406 ▪ **Ingenico Inc.** 6190 Shiloh Crossing Suite C Alpharetta, GA 30005 ▪ **Fiserv Hardware Solutions** 1169 Canton Rd Marietta, GA 30066 ▪ **ID TECH** 10721 Walker Street Cypress, CA 90630

Transporting Devices
Terminals must be secured before and during transportation. Ensure that you do the following:

- **Establish Trusted Locations**
  Establish a list of trusted locations for which you are storing or deploying devices.
- **Use Tamper Evident Packaging**
  Use tamper tape on boxes, and sign/initial over the edge of the tape.
- **Track Device and Shipment Details**
  Track the device quantity, make, model, serial numbers, and shipping details together.
- **Inspect Packages Before Shipping**
  Verify the packages have not been tampered before shipment. Inspect the tape to ensure no seals are broken or cracked. If the package shows signs of tampering, do not ship it. Review your access log for information on the last person to access the area and contact CardPointe Support for further instructions.
- **Secure Shipping Services**
  Terminal shipments must use only secured courier services such as FedEx and UPS.

6. POI Device Tamper Monitoring and Skimming Prevention

6.1 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 terminals can be found in the document titled *Skimming Prevention: Best Practices for Merchants,* available at www.pcisecuritystandards.org.

Step 1
Inspect the terminal daily and make sure that there are no unusual scratches, marks, or damage that were not present the previous day.

- If using a base or stand, ensure that the base is firmly mounted to the countertop and that the terminal is firmly attached to the base.
- Ensure that there are no unusual marks or scratches on the terminal.
- Ensure that the card reader is clean and an undamaged and that nothing is protruding from the opening. Verify that a card fits tightly in the opening.
- Ensure that no case or cover has been placed over the device.

Step 2
Inspect all wires and cables to ensure that they are securely connected.

- Verify that the terminal cable is securely attached to the device and there is nothing in-between it and the device.
- Verify that the connecting USB, Serial, or Ethernet cable is securely plugged in.

- Verify that no device is placed between the terminal and the USB, Serial, or Ethernet cable.
- Verify that all wires and cables are in good condition with no tears or ripping.

Following these steps will help maintain the integrity of your credit card terminals. If you feel that your terminal has been tampered with in any way, stop processing credit cards and immediately contact CardPointe Support.

6.2 Instructions for responding to evidence of POI device tampering

In the event devices show physical signs of tampering, stop using the device immediately. Contact CardPointe Support with the following information:

- The date and time when you initially noticed the tampering
- The suspected the cause of the tampering (for example, missing screws, holes, or additional seals in the device, the device weights too much, etc.)
- Last status of the device in your asset inventory
- Date of last inspection

Your CardConnect contact will assist you in gathering information, troubleshooting, and responding to the incident. Contact CardPointe Support to report any other suspicious activity of POI devices for investigation and resolution.

7. Device Encryption Issues

7.1 Instructions for responding to POI device encryption failures

In the case of an encryption failure, merchants should identify all POI devices that have encryption or tokenization errors and contact CardPointe Support with details of the devices and error(s) received. CardPointe Support will facilitate any troubleshooting necessary to diagnose an encryption error and coordinate device replacements as necessary.

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

A request to the P2PE Solution Provider, CardConnect, to stop encryption of account data would require the merchant to stop the use of the P2PE solution and return all devices to CardConnect. Such a request can be made to CardPointe Support.

8. POI Device Troubleshooting

8.1 Instructions for troubleshooting a POI device

The CardConnect terminal management and fulfilment partners cannot facilitate any on-site terminal repairs. Troubleshooting takes place only between the merchant and CardConnect. When a POI device presents an issue that requires troubleshooting, the merchant should contact CardPointe Support. CardPointe Support will triage the issue and attempt to provide resolution. CardConnect will contact their fulfilment partners for troubleshooting and/or replacement when necessary. No one outside of CardConnect, and their fulfilment partners, is authorized to troubleshoot or repair terminals.

9. Additional Guidance

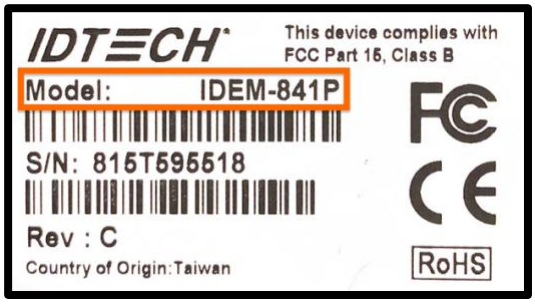
9.1 Determining POI Device Hardware and Firmware Versions

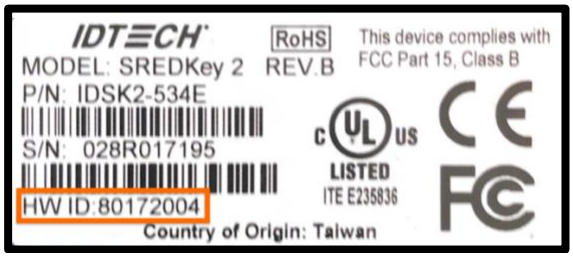
Each POI device included in this solution has specific hardware and firmware versions which have been validated for use with this P2PE solution, as described in *3.1 POI Device Details.*

To determine the firmware version installed on your device, contact CardPointe Support for assistance.

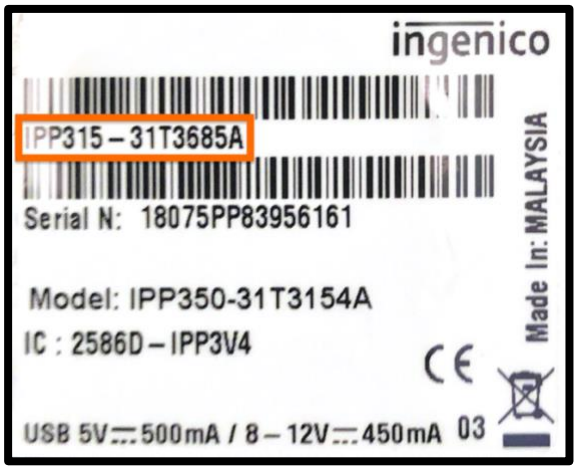
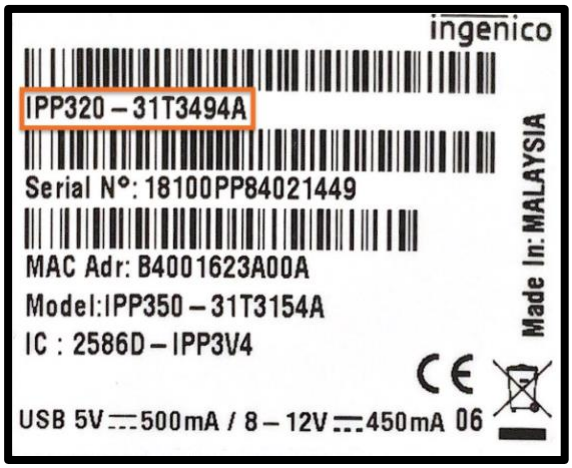
Each device includes a manufacturer label bearing the specific hardware version of the device. To determine the hardware version, check the label, typically located on the underside of the device.

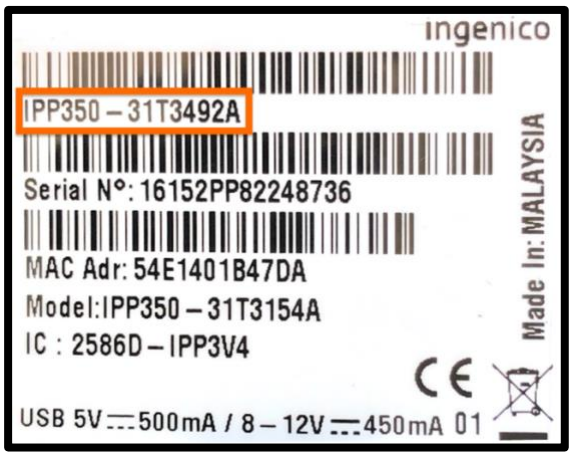
The following table provides an example of the label for each device:

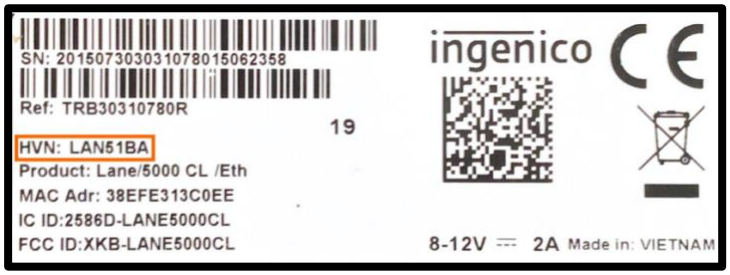
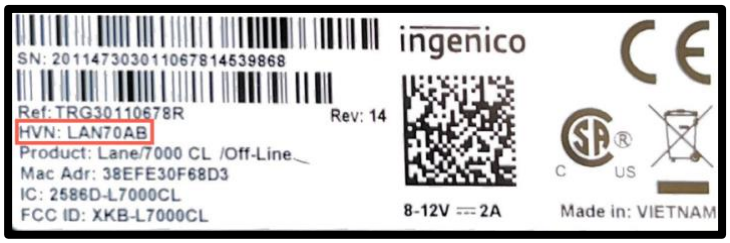
POI Device	Sample Label
Clover Flex	
Clover Mini	
ID TECH Augusta	

ID TECH SecuRED	
ID TECH SREDKey	
ID TECH SREDKey 2	
ID TECH VP5300	
Ingenico DESK/3500	

Ingenico DESK/5000	
Ingenico iCT220	
Ingenico iCT250	

Ingenico iPP315	
Ingenico iPP320 (v3)	
Ingenico iPP320 (v4)	

Ingenico iPP350 (v3)	
Ingenico iPP350 (v4)	
Ingenico iSMP4	
Ingenico iSC Touch 250	

Ingenico Lane/3000	
Ingenico Lane/5000	
Ingenico Lane/7000	
Ingenico Lane/8000	
Ingenico Link/2500	

9.2 Additional Solution Provider Information

Please contact CardPointe Support with any questions or concerns regarding your POI device.

Appendix A – Supplemental Information for Ingenico Devices running PANpad

A.1 Setup and Installation

Your CardConnect device is shipped to you pre-programmed and ready to use. There is no need for you to perform any update or download once you receive your device. Simply unpack the device from the box, connect the included cabling, connect the USB, Ethernet, or Serial cable to your network, and then plug the power supply into a wall outlet to power up your device.

Your device will now go through boot cycle to power up. Once your device has completed booting up it will display "PANpad No Connection." If your device displays another message, or you are unable to process a transaction contact CardPointe Support.

A.2 Troubleshooting

Misconfigured device from supplier:

If keys are wrong or missing, the device should be returned to Ingenico for a replacement.

Device is not communicating with the gateway:

1. Ensure that the Ethernet cable is plugged in properly between the device and the router/switch.
2. Ensure that TCP ports 443, 8443, 8553 are open on your firewall from your device to the gateway.

Device is communicating but not processing transactions:

Contact CardPointe Support.

Device does not start:

1. Ensure that the power supply is securely connected to your device.

ISC Touch 250

IPP320

2. Ensure that the power cable is securely connected to the power supply and plugged into the wall.

You will hear an audible chime when the device is powered on.

If the device still does not power on, please contact CardPointe Support.

A.3 Anti-Tampering Inspection

Below is a photo of an anti-tamper seal. Verify that the seal is not broken and has not been replaced or masked over.

Appendix B – Supplemental Information for CardPointe Retail Terminal Devices

B.1 Setup and Installation

Your CardPointe Retail Terminal is shipped to you pre-programmed and ready to use. There is no need for you to update or download software once you receive your terminal. Simply unpack the terminal from the box, connect the included cabling, connect the Ethernet cable to your network, and then plugin the power supply to a wall outlet to power up your device.

Your terminal will now go through boot cycle to power up. Depending on the model of terminal you have, either one of two idle screens should display. Telium 2 series devices will say “CardPointe” in plain text. Tetra terminals will have a blue CardPointe image as the idle screen. If your terminal displays another message, or you are unable to process a transaction contact CardPointe Support.

B.2 Troubleshooting

Device is not communicating with the gateway:

1. Ensure the Ethernet cable is plugged in properly between the device and the router/switch.
2. Ensure that TCP ports 443, 8443, 8553 are open on your firewall from your device to the gateway.

Device is communicating but not processing transactions:

Contact CardPointe Support via email, or by calling 877-828-0720.

Device does not start:

1. Ensure that the power supply is securely connected to your device.

ICT220/ICT250	DESK 3500	DESK 5000
		

2. Ensure that the power cable is securely connected to the power supply and plugged into the wall.

You will hear an audible chime when the device is powered on. If the device still does not power on, please contact CardPointe Support.

Appendix C – Supplemental Information for ID TECH SREDKey Devices

C.1 Setup and Installation

1. Connect the device to a USB port.
2. Verify that the device is ready to transact. The device will display “Swipe Card or Key-in Card Number” when ready.

C.2 Troubleshooting

Admin Settings

Selecting the Admin button opens a menu with various settings. By default, the Admin mode is set to "1." If you inadvertently change it to another mode number, you must change it back to "1," otherwise the device will not work properly.

Device is Faulty

If the device's screen blue and nothing else displays on the screen, please return it to CardConnect for a replacement. Contact CardPointe Support for assistance.

C.3 Anti-Tampering Inspection

The following photo illustrates the anti-tamper seal. Verify that the seal is not broken and has not been replaced or masked over.

ID TECH SREDKey	ID TECH SREDKey 2
	

Appendix D – Supplemental Information for CardPointe Integrated Terminal Devices (Ingenico)

D.1 Setup and Installation

1. Once your equipment is unboxed, plug the power supply connector into the jack on the Multipoint Interface Cable.
2. Connect the Multipoint Interface Cable into the Multipoint Port on the back of the device.
3. Connect the other end of the Multipoint Interface Cable to an ethernet port (POS, PC, modem, etc.).
4. Plug the power supply adapter into an available power outlet.

Confirming Connectivity

1. Once power is supplied to the device, an initiation process begins.
2. Once the device has successfully established its IP Address, it will attempt to call the terminal service.
3. If the connection is successful, the device displays Connected.
4. If the connection is unsuccessful, the device displays Disconnected, at which point you can contact CardPointe Support for troubleshooting.
5. Once Connected, the device is ready for use. The device may be left on indefinitely or may be disconnected from power as necessary.

D.2 Troubleshooting

Restarting the Device

1. To restart, press Clear and pound (#) simultaneously.
   Note: *For iSC Touch 250, press Clear and minus (-) simultaneously.*
2. Alternatively, disconnect and reconnect the power supply to power cycle the device.

Device is Faulty

If the device's screen blue and nothing else displays on the screen, please return it to CardConnect for a replacement.

D.3 Anti-Tampering Inspection

The device includes pressurized tamper detectors. If a tamper detector is triggered, the device enters an 'Alert Irruption' state and the keys installed on the device are erased. In this case, the device must be returned for repair and reactivation before it can be used again.

If the device shows any signs of tampering, contact CardPointe Support for assistance.

iSMP4 Front	iSMP4 Rear
	

Appendix E – Supplemental Information for CardPointe Integrated Terminal Devices (Clover)

E.1 Setup and Installation

Installing your device

When you unbox and power on the device for the first time, the device downloads and installs the required software and any necessary updates. Once the installation is complete, you must register the device using a registration key provided by CardConnect.

For more information on setting up the device, see https://support.cardpointe.com/cardpointe-clover-device-support.

E.2 Troubleshooting

Anti-Tampering Inspection

When inspecting the device, look for the following, which may indicate that the device has been tampered:

- The exterior of the device shows evidence of cutting, disassembly, broken seals, or damaged ports.
- There are unusual wires or overlays connected inside the chip card slot or on or near the PIN-entry area.
- Wires are loose or connectors are broken.
- The number of connections to the device are different.
- The cables are a different color.
- There are apparent changes to the resistance when inserting or removing a card from the chip card slot.
- The device is in a different location.
- The device has scratches or gouges around the seams of the terminal display.
- Clover labels are missing or show signs of peeling.

Device has malfunctioned

Sensors on your device will indicate when the device has been tampered with. Note that the tamper sensors can be triggered by excessive shaking or dropping of the device.

If your device has malfunctioned, the same protection mechanisms such as encryption and anti-tamper are still working to safeguard cardholder data when processing payments. However, the most sensitive type of transactions involving PIN-entry payments is disabled.

You can still accept transactions that do not require a PIN.

To request a replacement device, contact CardPointe Support.

Appendix F – Supplemental Information for ID TECH Augusta S Devices

F.1 Setup and Installation

The Augusta S uses a single USB connection for power and communication with the POS system. To install the Augusta S, place the device on the countertop and connect the supplied USB cable to a working USB port on the POS system.

LED Management

The Augusta includes two LED lights, which provide user interface and status information.

The EMV card slot includes a blue LED that tells the user when to insert or remove a card.

EMV Slot LED

Color	Activity	Description
Blue	Solid	Insert card.
Blue	Flashing (1s interval)	Remove card.

Additionally, a second tri-color (red/green/blue) LED located toward the rear of the device provides additional user interface and detailed status information.

Tri-color LED

Color	Activity	Description
Blue	Solid	The device is idle and ready for use.
Blue	Flashing (500ms interval)	Device ready for MSR or EMV card.
Blue	Flashing (1s interval)	Remove card.
Green	Solid	Card seated.
Green	Solid (2s)	EMV transaction successful
Red	Solid (2s)	One of the following: • MSR read unsuccessful. • EMV read unsuccessful. • Card seated incorrectly.
Red	Solid (until card removed)	Read or transaction unsuccessful, remove card.
Red	Solid	Device tamper detected.

F.2 Anti-Tampering Inspection

Below is a photo of the Augusta S device. To check for evidence of tampering:

- Inspect the device for signs of physical damage or alterations.
- Connect the device and check the LED display. A solid red LED indicates that the device has been tampered with.
- Check the hardware version on the label and power on the device to check the firmware/hardware version that conform to the version purchased.
- Check the ICC and ensure there is no overlay adaptor in the slot or ICC acceptor for shim devices.

The device uses multiple “active tamper” detection mechanisms that will detect physical intrusion into the device, and invoke a “tamper event”. A tamper event causes immediate erasure of all sensitive data and cryptographic keys. Once tampered, the device enters a non-operational state and the tri-color status LED remains solid red.

If the device shows any signs of tampering, contact CardPointe Support.