

globalpayments

Genius Smart P2PE™

P2PE Instruction Manual

Public Use

Doc no: CO-PUB-0101

Version 2.0 - November 17, 2023

Copyright notice

Copyright © 2023 Global Payments, Inc. All rights reserved.

No part of this publication may be reproduced, copied, manipulated, altered, or transmitted in any form or by any means, electronic or mechanical, including, without limitation, by photocopy, imaging, or recording, without the express prior written consent in each case of the copyright owner. The names, trademarks, logos, and service marks displayed in this publication will be protected by the owner to the fullest extent of the law, and any use without the express prior written permission of the trademark owner is strictly prohibited. The information contained in this publication is current when published; however, the publisher reserves the right to update and modify the specifications or other product information at any time without notice.

Table of contents

Table of contents	3
1. P2PE Solution Information and Solution Provider Contact Details	4
1.1 P2PE Solution Information	4
1.2 Solution Provider Contact Information	4
2. Confirm devices were not tampered with and confirm the identity of any third party personnel	5
2.1 Instructions for ensuring POI devices originate from trusted sites/locations only	5
2.2 Instructions for confirming POI device and packaging were not tampered with, and for establishing secure, confirmed communications with the solution provider	5
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.	8
3 Approved POI Devices, Applications/Software, and the Merchant Inventory	9
3.1 POI Device Details	9
3.2 POI Software/Application Details	14
3.3 POI Inventory & Monitoring	20
4 POI Device Installation Instructions	22
4.1 Installation and connection instructions	22
4.2 Guidance for selecting appropriate locations for deployed devices	23
4.3 Guidance for physically securing deployed devices to prevent unauthorized removal or substitution	23
5. POI Device Transit	25
5.1 Instructions for securing POI devices intended for, and during, transit	25
5.2 Instructions for ensuring POI devices are shipped to trusted sites/locations only	25
6 POI Device Tamper & Modification Guidance	26
6.1 Instructions for physically inspecting POI devices and preventing skimming, including instructions and contact details for reporting any suspicious activity	26
6.2 Instructions for responding to evidence of POI device tampering	30
7 Device Encryption Issues	31
7.1 Instructions for responding to POI device encryption failures	31
8 POI Device Troubleshooting	32
8.1 Instructions for troubleshooting a POI device	32
9 Additional Guidance	33
9.1 Additional Guidance for the Genius Smart P2PE solution	33
9.2 Instructions for how to confirm hardware, firmware, and application versions on POI devices	33
10. Appendix: Checklist for Remote Key Injection	36

1. P2PE Solution Information and Solution Provider Contact Details

1.1 P2PE Solution Information

Solution name:	Genius Smart P2PE
Solution reference number per PCI SSC website:	2021.00056.002

1.2 Solution Provider Contact Information

Company name:	Global Payments Direct, Inc.
Company address:	5995 Winward Pkwy, Alpharetta, GA 30005
Company URL:	
Contact name:	Contact Center Services
Contact phone number:	(1) (888) 249-3220
Contact e-mail address:	

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

To confirm that your device was shipped from a trusted location, do the following:

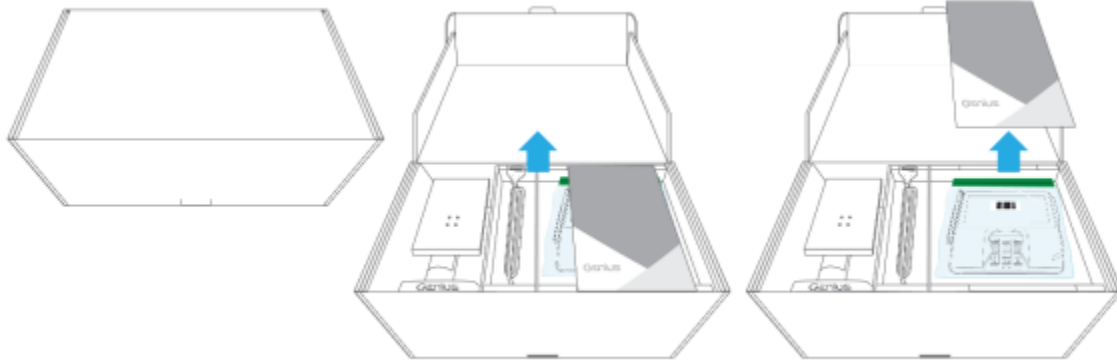
- Check the shipping label to confirm that the device was shipped from one of the following two secure sites:
 - POS Portal, 1627 Main Ave, Sacramento, CA 95838
 - POS Portal, 1920 Watterson Trail # A, Louisville, KY 40299

Important: If you receive your device from any other site or location, do NOT use the device. Contact our Customer Support Team at (1) (888) 249-3220

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

To confirm that your device was not tampered with during shipping, complete the following checks:

1. Open the shipping box and remove the packing slip and the Genius box.
2. Open the Genius box.



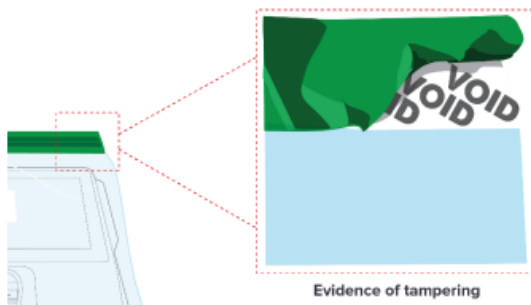
3. Check that the Genius device is packed in a tamper-evident bag.



Example: Countertop MX925 device

4. Confirm that the tamper-evident bag has no rips or evidence of tampering.

5. Check the tape that seals the top of the bag for evidence of tampering. If anyone has tried to remove the tape, the word "VOID" is displayed.



Evidence of tampering

6. . Check that the serial number of the tamper-evident bag matches the serial number printed on the packing slip. – The serial number of the tamper-evident bag is located underneath the barcode on the front of the bag.



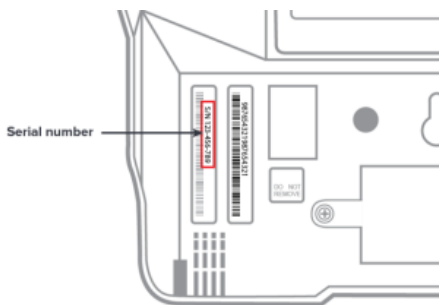
The corresponding serial number is printed in the rightmost column of the packing slip, after the letters TE.

Name				
ime				
1456789				
Quantity				
Lot	Ordered	Shipped		
Ea.	1	1	123-456-789	TE 12345

7. Check that the serial number of the device matches the serial number printed on the packing slip.

The serial number of the Genius device is located on the back of the device:

- If you have a Wireless e285, the serial number is under the back cover.
- If you have a Genius Handheld, the serial number is under the battery.



Example: Countertop MX925 device

The corresponding serial number is printed in the rightmost column of the packing slip.

Order No. 1234567
Ordered On: 01/01/2017 10:00 AM
MID: 123456789
DBA: Cayan LLC

Ship Method: FedEx Ground Service

SHIP TO				
Company Name Contact Name Address 1 Address 2				
Phone: 123456789				
		Quantity		
		Lot	Ordered	Shipped
ew	Ea.		1	1
				123-456-789

Serial number

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.

We do not repair deployed devices; therefore, you should NOT grant access to any person that claims to be repair or support personnel.

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. Note: 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” on page 30.

PCI PTS approval #:	POI device vendor:	POI device model name and number:	Hardware version #(s):	Firmware version #:
4-10177	Verifone	MX915: M177-40xxx-xxx, Version 4.x	P177-40x-xx-xxx	Vault: 11.x.x; 12.x.x, 13.x.x, AppM: 5.x.x; 5A.x.x; 6.x.x; 7.x.x, SRED: 4.x.x; 5.x.x, OP: 5.x.x; 6.x.x; 7.x.x, Vault: 14.x.x; AppM: 8.x.x; SRED: 7.x.x, Vault: 16.x.x; AppM: 10.x.x, Vault: 17.x.x
4-10177	Verifone	MX925: M177-50xxx-xxx, Version 4.x	P177-50x-xx-xxx	Vault: 11.x.x; 12.x.x, 13.x.x, AppM: 5.x.x; 5A.x.x; 6.x.x; 7.x.x, SRED: 4.x.x; 5.x.x, OP: 5.x.x; 6.x.x; 7.x.x, Vault: 14.x.x; AppM: 8.x.x; SRED: 7.x.x, Vault: 16.x.x; AppM: 10.x.x,

				Vault: 17.x.x
4-10110	Verifone, Inc.	MX915: M132-40xxx-xxx, Version 3.x	P132-40x-xx-xxx, Vault: 14.x.x; AppM: 8.x.x; SRED: 7.x.x, Vault: 16.x.x; AppM: 10.x.x	Vault: 1.x.x, 3.x.x, 4.x.x, 11.x.x, 12.x.x, AppM: 1.x.x; 3.x.x; 4.x.x; 5.x.x, 5A.x.x, 6.x.x, SRED: 1.x.x, 3.x.x; 4.x.x; 5.x.x, OP: 1.x.x, 3.x.x; 4.x.x; 7.x.x, SRED 5.x.x.xxx, Vault: 13.x.x, AppM: 7.x.x, Vault: 17.x.x, AppM: 10.x.x, SRED: 7.x.x, OP: 7.x.x
4-10110	Verifone, Inc	MX925: M132-50xxx-xxx, Version 3.x	P132-50x-xx-xxx, Vault: 14.x.x; AppM: 8.x.x; SRED: 7.x.x, Vault: 16.x.x; AppM: 10.x.x	Vault: 1.x.x, 3.x.x, 4.x.x, 11.x.x, 12.x.x, AppM: 1.x.x; 3.x.x; 4.x.x; 5.x.x, 5A.x.x, 6.x.x, SRED: 1.x.x, 3.x.x; 4.x.x; 5.x.x, OP: 1.x.x, 3.x.x; 4.x.x; 7.x.x, SRED 5.x.x.xxx, Vault: 13.x.x, AppM: 7.x.x, Vault: 17.x.x, AppM: 10.x.x, SRED: 7.x.x,
4-10239	Verifone, Inc	P400, P400 Plus, P400 DMSR	H435-07-02-xxx-x 0- B0, H435-07-32-xxxx 0-B0, H435-07-02- xx0-x0-A0, H435- 07-02-xx0-x0-A1 (P400), H435-07-32- xx0-x0-A0, H435- 07-32-xx0-x0-A1 (P400 Plus), H435- 07-02-xxx-x0-B0	Vault: 7.x.x.x, AppM: 11.x.x.x, SRED: 7.x.x.x, OP: 1.x.x, VAULT: 8.x.x, AppM: 12.x.x, VFSRED: 9.x.x, Vault: 10.x.x, AppM: 14.x.x, SRED: 11.x.x, OP: 2.x.x, Vault: 11.x.x, AppM: 15.x.x, SRED: 12.x.x

			(P400), H435-07-32- xxx-x0-B0 (P400 Plus), H435-07-02- xx0-x0-A0 (P400), H435-07-32-xx0-x 0- A0 (P400 Plus), H435-07-02-xxx-x 0- A2 (P400), H435-07- 02-xxx-x0-B1 (P400), H435-07-32- xxx-x0-A2 (P400 Plus), H435-07-32- xxx-x0-B1 (P400 Plus), H435-17-02- xxx-x0-B1 (P400 DMSR), H435-07- 02-xxx-x0-B2 (P400), H435-07-32- xxx-x0-B2 (P400 Plus), H435-17-02- xxx-x0-B2 (P400 DMSR)	
4-30276	Verifone, Inc	e285	H445-07-30-0xx-0 0- B0 (BT/WiFi), H445- 07-34-0xx-00-B0 (2G/BT/WiFi), H445- 07-38-0xx-00-B0 (3G/BT/WiFi), H445- 07-30-0xx-xx-B0 (BT/WiFi), H445-07- 34-0xx-xx-B0 (2G/BT/WiFi), H445- 07-38-0xx-xx-B0	VAULT: 6.x.x, AppM: 10.x.x, VFSRED: 7.x.x, VFOP: 1.x.x, VAULT: 7.x.x, AppM: 11.x.x, VAULT: 8.x.x, AppM: 12.x.x, VFSRED: 9.x.x, VAULT: 10.x.x, AppM: 14.x.x, VFSRED: 11.x.x, VFOP: 2.x.x, VAULT: 11.x.x, AppM: 15.x.x, VFSRED: 12.x.x

			(3G/BT/WiFi), H445- 07-98-0xx-xx-B1 (BT/3G/512MB/M Fi 3.0/Dual SIM/Dual Band WiFi), H445- 07-90-0xx-xx-B1 (BT/512MB/MFi 3.0/Dual Band WiFi), H445-07-38- 0xx-xx-B1 (BT/Single Band WiFi/3G/512MB/ MFi 3.0/Dual SIM), H445-07-30-0xx-x xB1 (BT/Single Band WiFi/512MB/MFi 3.0), H445-07-30- 0xx-xx-B2 (BT/Single Band WiFi/512MB/MFi 3.0), H445-07-38- 0xx-xx-B2 (BT/Single Band WiFi/3G/512MB/ MFi 3.0/Dual SIM), H445-07-90-0xx-x xB2 (BT/512MB/MFi 3.0/Dual Band WiFi), H445-07-98- 0xx-xx-B2 (BT/3G/512MB/M Fi 3.0/Dual SIM/Dual Band WiFi)	
4-10231	Verifone, Inc	M400	H405-07-00-xx0-0 0- B2 (M400; No Wi-Fi; No Bluetooth),	Vault: 10.x.x; 8.x.x; 7.x.x, AppM: 14.x.x; 12.x.x; 11.x.x,

			<p>H405-07-30-xx0-0 0- B2 (M400; Wi-Fi; Bluetooth), H405- 07-10-xx0-00-B2 (M400; Bluetooth), H405-07-00-xx0-0 0- B1 (M400; No Wi-Fi; No Bluetooth), H405-07-30-xx0-0 0- B1 (M400; Wi-Fi; Bluetooth), H405- 07-00-xx0-00-B0 (M400; No Wi-Fi; No Bluetooth), H405-07-30-xx0-0 0- B0 (M400; Wi-Fi; Bluetooth), H405- 07-x0-xx0-00-B0 (M400), H405-07- 00-xx0-00-B3 (M400; No Wi-Fi; No Bluetooth), H405-07-30-xx0-0 0- B3 (M400; Wi-Fi; Bluetooth), H405- 07-10-xx0-00-B3 (M400; Bluetooth)</p>	<p>VFSRED: 11.x.x; 9.x.x; 7.x.x.xxx, VFOP: 2.x.x; 1.x.x</p>
--	--	--	---	---

4-30260	Verifone, Inc.	V400m	H475-07-38-xxx-x1- B0 (V400m Plus 3G), H475-07-70-xxx-x1-B0 (V400m Plus 4G), H475-07-F0-xxx-x1-B0 (V400m Plus 4G WW)	VAULT: 6.x.x, AppM: 10.x.x, VFSRED: 7.x.x, VFOP: 1.x.x, VAULT: 7.x.x, AppM: 11.x.x, VAULT: 8.x.x, AppM: 12.x.x, VFSRED: 9.x.x, VAULT: 10.x.x, AppM: 14.x.x, VFSRED: 11.x.x, VFOP: 2.x.x, VAULT: 11.x.x, AppM: 15.x.x, VFSRED: 12.x.x
4-10204	BBPOS International Limited	WSX2	WSX2XXX-XX-XXX (WSX2)	WSX1.002-08.x.xx.xx.xx.xx (WSX2)

3.2 POI Software/Application Details

Important: The Genius application is installed and sold on terminals distributed only by Global Payment Direct, Inc. 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)
Global Payments, Inc., Genius version 5.2.x.x	Verifone, Inc	MX915, MX925, MX915 ECR	Hardware version: P177- 40x-xx-xxx (Mx915), P177-50x-xx-xxx (Mx925),	Y	Y

			<p>P177- 409-xx-xxx (Mx915 ECR) Firmware version: Vault: 11.x.x; 12.x.x, 13.x.x, AppM: 5.x.x; 5A.x.x; 6.x.x; 7.x.x, SRED: 4.x.x; 5.x.x, OP: 5.x.x; 6.x.x; 7.x.x, Vault: 14.x.x; AppM: 8.x.x; SRED: 7.x.x, Vault: 16.x.x; AppM: 10.x.x, Vault: 17.x.x, Vault: 14A.x.x, AppM: 8A.x.x, Vault: 12A.x.x, AppM: 6A.x.x</p>		
Global Payments, Inc., Genius version 6.4.x.x	Verifone, Inc	MX915, MX925, MX915 ECR	<p>Hardware version: P177- 40x-xx-xxx (Mx915), P177- 50x-xx-xxx (Mx925), P177- 409-xx-xxx (Mx915 ECR) Firmware version: Vault: 11.x.x; 12.x.x, 13.x.x, AppM: 5.x.x; 5A.x.x; 6.x.x; 7.x.x, SRED: 4.x.x; 5.x.x, OP: 5.x.x; 6.x.x; 7.x.x, Vault: 14.x.x; AppM: 8.x.x; SRED: 7.x.x, Vault: 16.x.x; AppM: 10.x.x, Vault: 17.x.x, Vault: 14A.x.x, AppM: 8A.x.x, Vault: 12A.x.x, AppM: 6A.x.x</p>	Y	Y
Global Payments, Inc., Genius versions 6.4.x.x and 6.5.x.x	Verifone, Inc	P400, P400 Plus, P400 DMSR	<p>Hardware version: H435-07-02-xxx-x0-B0, H435-07-32-xxx-x0-B0, H435-07-02-xx0-x0-A0,</p>	Y	Y

			<p>H435-07-02-xx0-x0-A1 (P400), H435-07-32-xx0-x0-A0, H435-07-32-xx0-x0-A1 (P400 Plus), H435-07-02-xxx-x0-B0 (P400), H435-07-32-xxx-x0-B0 (P400 Plus), H435-07-02-xx0-x0-A0 (P400), H435-07-32-xx0-x0-A0 (P400 Plus), H435-07-02-xxx-x0-A2 (P400), H435-07-02-xxx-x0-B1 (P400), H435-07-32-xxx-x0-A2 (P400 Plus), H435-07-32-xxx-x0-B1 (P400 Plus), H435-17-02-xxx-x0-B1 (P400 DMSR), H435-07-02-xxx-x0-B2 (P400), H435-07-32-xxx-x0-B2 (P400 Plus), H435-17-02-xxx-x0-B2 (P400 DMSR)</p> <p>Firmware version: Vault: 7.x.x.x, AppM: 11.x.x.x, SRED: 7.x.x.x, OP: 1.x.x, VAULT: 8.x.x, AppM: 12.x.x, VFSRED: 9.x.x, Vault: 10.x.x, AppM: 14.x.x, SRED: 11.x.x, OP: 2.x.x, Vault: 11.x.x, AppM: 15.x.x, SRED: 12.x.x</p>		
Global	Verifone,	e285	Hardware version:	Y	Y

<p>Payments, Inc., Genius versions 6.4.x.x and 6.5.x.x</p>	<p>Inc</p>		<p>H445-07-30-0xx-00-B0 (BT/WiFi), H445-07-34-0xx-00-B0 (2G/BT/WiFi), H445-07-38-0xx-00-B0 (3G/BT/WiFi), H445-07-30-0xx-xx-B0 (BT/WiFi), H445-07-34-0xxxx-B0 (2G/BT/WiFi), H445-07-38-0xx-xx-B0 (3G/BT/WiFi), H445-07-98-0xx-xx-B1 (BT/3G/512MB/MFi 3.0/Dual SIM/Dual Band WiFi), H445-07-90-0xx-xx-B1 (BT/512MB/MFi 3.0/Dual Band WiFi), H445-07-38-0xx-xx-B1 (BT/Single Band WiFi/3G/512MB/MFi 3.0/Dual SIM), H445-07-30-0xx-xx-B1 (BT/Single Band WiFi/512MB/MFi 3.0), H445-07-30-0xx-xx-B2 (BT/Single Band WiFi/512MB/MFi 3.0), H445-07-38-0xx-xx-B2 (BT/Single Band WiFi/3G/512MB/MFi 3.0/Dual SIM), H445-07-90-0xx-xx-B2 (BT/512MB/MFi 3.0/Dual Band WiFi), H445-07-98-0xx-xx-B2</p>		
--	------------	--	---	--	--

			(BT/3G/512MB/MFi 3.0/Dual SIM/Dual Band WiFi) Firmware version: VAULT: 6.x.x, AppM: 10.x.x, VFSRED: 7.x.x, VFOP: 1.x.x, VAULT: 7.x.x, AppM: 11.x.x, VAULT: 8.x.x, AppM: 12.x.x, VFSRED: 9.x.x, VAULT: 10.x.x, AppM: 14.x.x, VFSRED: 11.x.x, VFOP: 2.x.x, VAULT: 11.x.x, AppM: 15.x.x, VFSRED: 12.x.x		
Global Payments, Inc., Genius versions 6.4.x.x and 6.5.x.x	Verifone, Inc	M400	Hardware version: H405-07-00-xx0-00-B2 (M400; No Wi-Fi; No Bluetooth), H405-07-30-xx0-00-B2 (M400; WiFi; Bluetooth), H405-07-10-xx0-00-B2 (M400; Bluetooth), H405-07-00-xx0-00-B1 (M400; No Wi-Fi; No Bluetooth), H405-07-30-xx0-00-B1 (M400; Wi-Fi; Bluetooth), H405-07-00-xx0-00-B0 (M400; No Wi-Fi; No Bluetooth), H405-07-30-xx0-00-B0 (M400; Wi-Fi; Bluetooth), H405-07-x0-xx0-00-B0 (M400), H405-07-	Y	Y

			<p>00-xx0-00-B3 (M400; No Wi-Fi; No Bluetooth), H405-07-30-xx0-00-B3 (M400; WiFi; Bluetooth), H405-07-10-xx0-00-B3 (M400; Bluetooth)</p> <p>Firmware version: Vault: 10.x.x; 8.x.x; 7.x.x, AppM: 14.x.x; 12.x.x; 11.x.x, VFSRED: 11.x.x; 9.x.x; 7.x.x.xxx, VFOP: 2.x.x; 1.x.x</p>		
<p>Global Payments, Inc., Genius versions 6.4.x.x and 6.5.x.x</p>	<p>Verifone, Inc</p>	<p>V400m</p>	<p>Hardware version: H475-07-38-xxx-x1-B0 (V400m Plus 3G), H475-07-70-xxxx1-B0 (V400m Plus 4G), H475-07-F0-xxx-x1-B0 (V400m Plus 4G WW) Firmware version: VAULT: 6.x.x, AppM: 10.x.x, VFSRED: 7.x.x, VFOP: 1.x.x, VAULT: 7.x.x, AppM: 11.x.x, VAULT: 8.x.x, AppM: 12.x.x, VFSRED: 9.x.x, VAULT: 10.x.x, AppM: 14.x.x, VFSRED: 11.x.x, VFOP: 2.x.x, VAULT: 11.x.x, AppM: 15.x.x, VFSRED: 12.x.x</p>	<p>Y</p>	<p>Y</p>

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 Global Payments, Inc. 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.

You must maintain an inventory of all your P2PE devices, and include at least the following information about each device:

- **Make and model** – The make and model information of the Genius device is located on the back of the device.
 - If you have a Wireless e285, the make and model information is under the back cover.
 - If you have a Genius Handheld, the make and model information is under the battery. For more information about how to remove the battery of a Genius Handheld device, refer to the Quick Start Guide for the Genius Handheld.
- **Serial number** – The serial number of the Genius device is located on the back of the device.
 - If you have a Wireless e285, the serial number is under the back cover.
 - If you have a Genius Handheld, the serial number is under the battery. For more information about how to remove the battery of a Genius Handheld device, refer to the Quick Start Guide for the Genius Handheld.
- **Location** – Where you physically located the device in your business. If you have a Wireless Genius device, you should record where you store the device when it is not in use.
- **Status** – Description of the device’s status, which can be one of the following:
 - **Awaiting deployment** – The device is working correctly, and you are currently storing the device before using it in your business.
 - **Deployed** – The device is working correctly, and you are using it in your business.
 - **Not in use** – The device is working correctly, but you do not need to use it in your business. You must securely store any devices that are not in use. –
 - **Awaiting replacement** – The device is not working correctly, and you are waiting for us to send you a replacement device. You must securely store any devices that are awaiting replacement.



Important: You must use only PCI-approved P2PE devices to process transactions. If you process any transactions using devices that are not P2PE validated, you are no longer considered P2PE compliant.

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

Genius Countertop MX915, Countertop MX925, Wireless V400m, and Wireless M400 devices

To use Genius Smart P2PE, you can either purchase new devices from us or we can remotely inject keys into your existing devices.

Existing devices

To use existing devices:

- Complete "Appendix: Checklist for Remote Key Injection" and send it to Deployment@cayan.com
- After we remotely inject keys into your devices, make sure that your Genius device is ready by running a test transaction. For more information about how to run a test transaction, refer to the Quick Start Guide for the Genius device.
- All other sections of the PIM apply when you are using existing devices, except for section 2.2.

Genius Handheld devices

To use Genius Smart P2PE, you must purchase Handheld devices from us.

Genius Countertop P400 and Wireless e285 devices

To use Genius Smart P2PE, contact us.

Setting up your Genius device

To view instructions about how to set up your device, refer to your Quick Start Guide for your device.



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

You must install your device in a secure location to reduce the risk of criminals targeting the device for skimming. We recommend that you consider the following when selecting installation locations:

- Control public access to the device, so that people have access only to the parts of the device that they need to complete a transaction. For example, PIN pad and card reader.
- Locate the device where authorized personnel can easily observe and monitor it, for example during daily checks by store or security staff.
- Locate the device in a secure environment that deters compromise attempts, including, but not limited to:
 - Visible security measure
 - Video surveillance
 - Adequate lighting
 - Access paths
- Physically secure the device so that criminals cannot easily remove it. For example, when using Genius Countertop devices, install them on the stand that we provide or when using Wireless Genius devices, store them in a lockable area when they are not in use
- Enforce operational security processes to make sure that members of staff or security regularly inspect the device.

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

Genius Countertop devices

You must physically secure a deployed device to prevent unauthorized removal or substitution. For example, install the device securely on the stand that we provide. You must prevent unauthorized access to devices awaiting replacement while in your possession.



Important: If your device develops a fault, we arrange for you to return the device to us, and we ship a replacement device to you. We do not repair deployed devices; therefore, you should NOT grant access to any person that claims to be repair or support personnel.

Genius stands

To view instructions about how to install your Genius device onto a stand, refer to your Quick Start Guide for your stand.

Wireless Genius devices

You must ensure that when your Wireless Genius devices are in use, they are kept under the supervision of authorized employees. Whenever possible, your authorized employees should remain in possession of the device. If a cardholder needs to directly interact with the device, we recommend your authorized employees do the following:

- Remain with the cardholder during the interaction
- Keep the device in their sight
- Visually inspect the device after a cardholder interaction, they should ensure the cardholder has not:
 - Opened the device
 - Interfered with the card readers
 - Substituted the device for another

As the Wireless Genius devices do not have any physical fasteners, you should have a lockable area where authorized employees store the devices when not in use. Authorized employees should sign out devices when they need them and sign in devices when returning them for storage. The lockable area should be in view of a camera system to ensure any unauthorized access to the devices is captured.

You should also enforce operational security processes to make sure that members of staff or security regularly inspect the device.

5. POI Device Transit

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

Anytime you transport devices between locations, you must:

- Pack the devices in tamper-evident packaging before transit. For example, using tamper-evident bags, tamper seals, or security tape
- Ship devices using a trusted, trackable courier or shipping company.
- Notify the company or site that you are shipping the devices to, including package tracking details and tamper-seal serial numbers.

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

Transport devices to and from trusted locations only. To help manage this process, you must:

- Maintain a list of trusted sites that you may accept devices from and send them to.
- Use only devices that you receive from trusted sites.

If you receive a device from an unknown or untrusted location:

- Do not use the device until you verify that the source is trusted.
- Contact us at (1) (888) 249-3220 to verify that the device is authorized for use with your P2PE solution.

Trusted locations

We ship devices from one of two secure facilities:

- POS Portal, 1627 Main Ave, Sacramento, CA 95838
- POS Portal, 1920 Watterson Trail # A, Louisville, KY 40

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 skimming prevention on POI terminals can be found in the document entitled “Skimming Prevention: Best Practices for Merchants”, available at www.pcisecuritystandards.org.

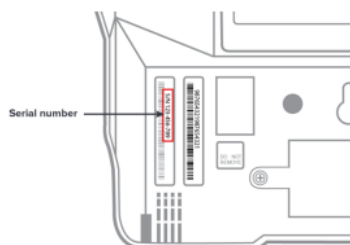
Before deploying a device

Note: When using devices that we have remotely injected with keys, skip to “

- 6.1.2 After deploying a device” on page 29.

After deploying a device All other sections of the PIM apply when using existing devices, except for section 2.2 on page 5 to page 7.

- Keep your device in its tamper-evident bag and store it securely until immediately before deployment.
- Check that the serial number of the device matches the serial number printed on the packing slip
- The serial number of the Genius device is located on the back of the device.
 - If you have a Wireless e285, the make and model information is under the back cover.
 - If you have a Genius Handheld, the make and model information is under the battery. For more information about how to remove the battery of a Genius Handheld device, refer to the Quick Start Guide for the Genius Handheld.



Example: Countertop MX925 device

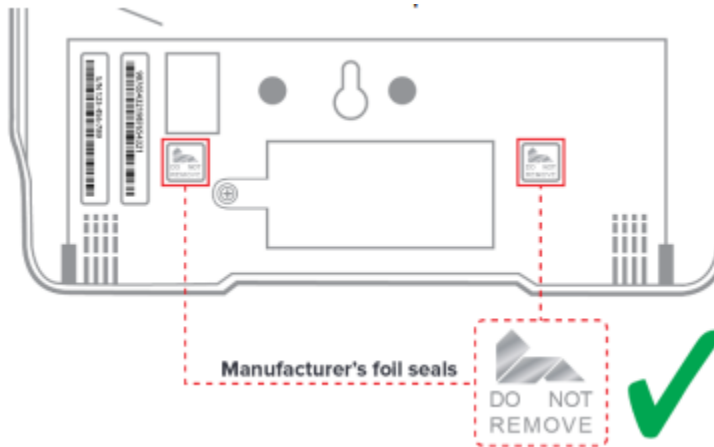
- The corresponding serial number is printed in the rightmost column of the packing slip

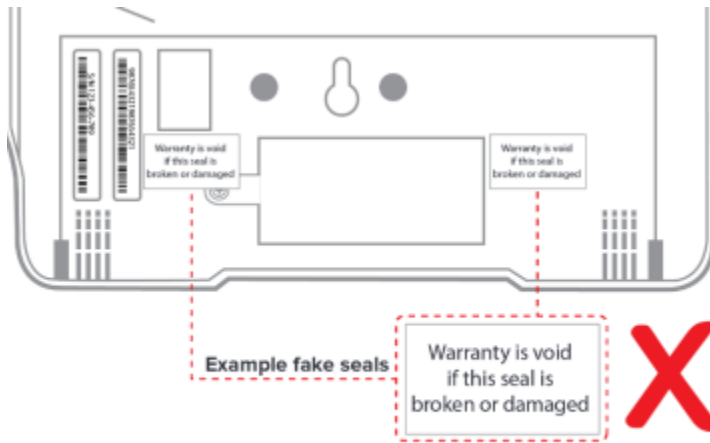
Order No. **1234567**
 Ordered On: 01/01/2017 10:00 AM
 MID: 123456789
 DBA: Cayan LLC

 Ship Method: FedEx Ground Service

SHIP TO				
Company Name				
Contact Name				
Address 1				
Address 2				
Phone: 123456789				
		Quantity		
	Lot	Ordered	Shipped	
ew	Ex	1	1	123-456-789 ← Serial number

- Record the device in your inventory.
- Inspect the device:
 - If the device has foil seals, inspect the device to make sure that the foil seals covering the screws are intact and have not been replaced with non-manufacturer seals.





Example: Countertop MX925 device

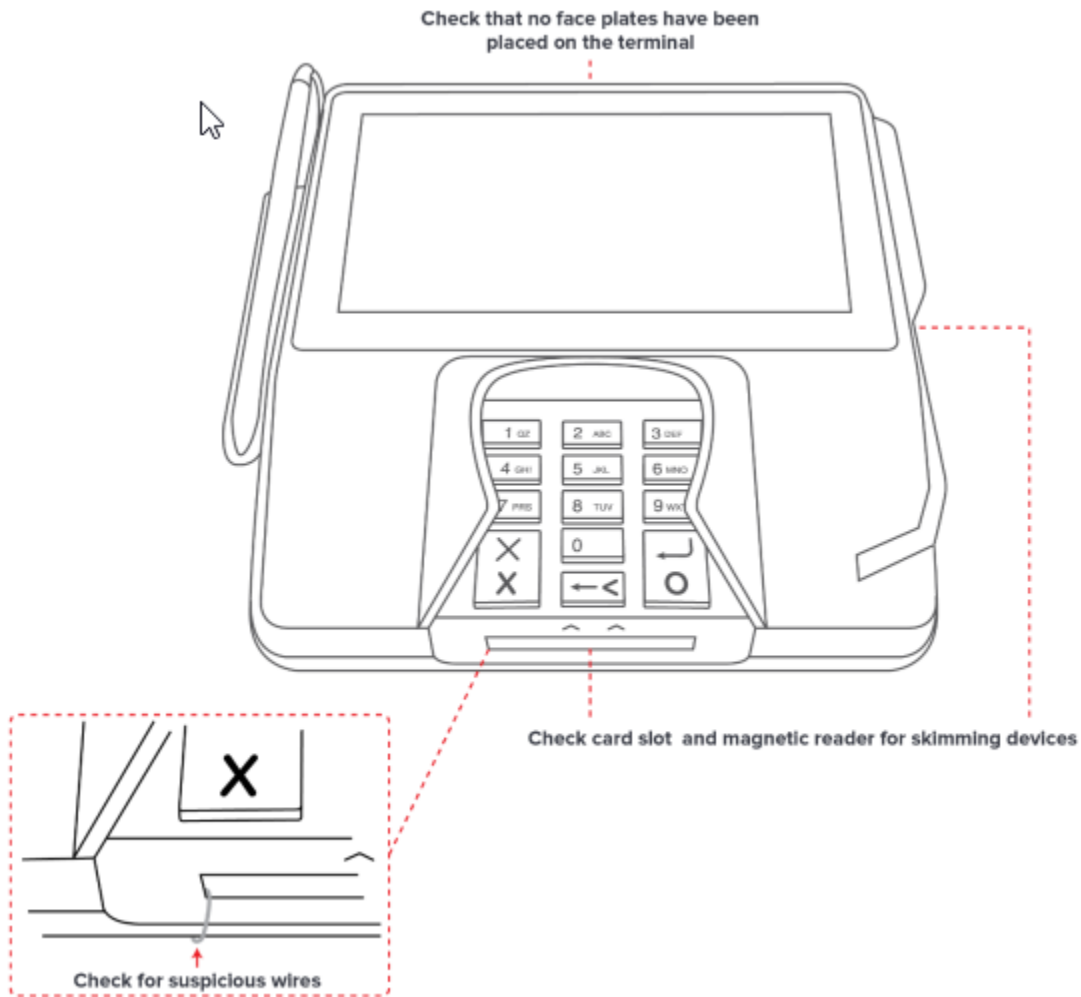
- Inspect the device for any signs of attempts to open it. Check for puncture marks, prize marks, and damage to the screws.
- Weigh your device when you first receive it and check the weight of the device as part of your regular device inspections.
 - MX915 weight as specified by Verifone: 0.6 kg
 - MX925 weight as specified by Verifone: 0.9 kg
 - P400 weight as specified by Verifone: 0.31 kg
 - M400 weight as specified by Verifone: 0.492 kg
 - e285 weight as specified by Verifone: 0.169 kg
 - V400m weight without paper roll as specified by Verifone: 0.388 kg
 - WS2 weight as specified by BBPOS International Ltd:
- Excluding battery: 0.185 kg
- Including battery: 0.235 kg
- Inspect the device before deployment to verify that the device has not been tampered with. If you notice anything suspicious, do not use the device, and immediately report your suspicions to our Customer Support Team at (1) (888) 249-3220.

After deploying a device

Check that the device meets the security standards described by the manufacturer. You can download the manufacturer's security standards from https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices

- Inspect your device regularly for signs of tampering, including:
 - A change in weight
 - Missing or changed screws - Broken or changed tamper seals
 - Holes in the device
 - Additional wires or components, or other covering material that could be used to mask evidence of tampering
 - Serial number changes
 - Broken or differently colored casing
 - Additional faceplate or casing that may conceal a skimming device

- SIM card or memory card inserted in the card slots



Example: Countertop MX925 device

Additional guidance for skimming prevention on POI terminals can be found in the document entitled "Skimming Prevention: Best Practices for Merchants", available at www.pcisecuritystandards.org



Note: The required frequency of inspections depends on factors such as the location of the device and whether it is attended or unattended. For example, devices left in a public area with little supervision should be inspected more regularly than devices that are kept in secure areas or that are supervised.

- If you cannot remove your device from its stand to weigh it, take alternative steps to monitor whether the device has been tampered with. For example, using tamper-seals or stickers to indicate if a device has been removed and replaced.
- Monitor devices in remote or unattended locations, for example, using video surveillance or other physical mechanisms to alert personnel of suspicious behavior.

Genius devices installed on stands

- If you cannot remove your device from its stand to check the printed serial number, you can check it in the Admin menu as follows:
 1. When Genius is displaying the splash screen, press 0 on the keypad three times.
 2. Using the keypad type the password, then press Enter (green button). The default password is 9416557.
 3. Check that the serial number matches the entry in your inventory.



Reporting suspicious activity

If you detect suspicious activity:

- Do not use the device
- Immediately contact our Customer Support Team at (1) (888) 249-3220 and give a full description of the suspected activity.
- Follow the instructions of our Customer Support Team for returning the device



Important: If your device develops a fault, we arrange for you to return the device to us, and we ship a replacement device to you. We do not repair deployed devices; therefore, you should NOT grant access to any person that claims to be repair or support personnel

6.2 Instructions for responding to evidence of POI device tampering

If you suspect that someone has tampered with your device:

- Do not use the device
- Immediately contact our Customer Support Team at (1) (888) 249-3220 and give a full description of the suspected tampering.
- Follow the instructions of our Customer Support Team for returning the device.

7 Device Encryption Issues

7.1 Instructions for responding to POI device encryption failures

In the event of a device encryption failure, you must immediately stop using the device. Do not re-enable the device until you confirm that full P2PE-encryption functions are restored and re-enabled.

8 POI Device Troubleshooting

8.1 Instructions for troubleshooting a POI device

To view instructions about how to troubleshoot your Genius device, refer to the Quick Start Guide for your device.

9 Additional Guidance

9.1 Additional Guidance for the Genius Smart P2PE solution



Important: We cannot share cardholder data with merchants who are using our P2PE solution, under any circumstances.

For more useful help articles and troubleshooting information, visit <https://help.globalpaymentsintegrated.com>.

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

Genius v5.2.x.x devices

Use the Verifone Administration menu to confirm the following:

- Hardware number
 - Firmware number
 - Application version number
1. Ensure that the Genius is displaying the Splash screen.
 2. On the keypad, press 1, 5, and 9 at the same time to enter System Mode. The Genius device displays a login screen.
 3. Use the keypad to type the supervisor password, then press Enter. The default supervisor password is 166832.
 4. Tap Info > Basic System
 5. Confirm the values for the following fields:
 - Hardware P/N
 - Vault Version
 - AppM Version
 - SRED Version
 - Open Protocol
 6. Tap Home.
 7. On the Home screen, tap Run App to restart the Genius application.

MX915 and MX925 devices running Genius v6.4.x.x

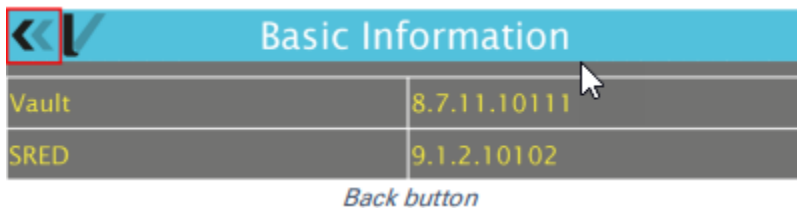
Use the Verifone Administration menu to confirm the following:

- Hardware number
 - Firmware number
 - Application version number
-
1. Ensure that the Genius is displaying the Splash screen.
 2. On the keypad, press 1, 5, and 9 at the same time to enter System Mode. The Genius device displays a login screen.
 3. Use the keypad to type the supervisor password, then press Enter. The default supervisor password is 166832.
 4. Tap Info > Basic System
 5. Confirm the values for the following fields:
 - Hardware P/N
 - Vault Version
 - AppM Version
 - SRED Version
 - Open Protocol
 6. Tap Home.
 7. On the Home screen, tap Run App to restart the Genius application.

Genius M400, P400, e285, and V400m devices

Use the Verifone Administration menu to confirm the following:

- Hardware number
 - Firmware number
 - Application version number
-
1. Ensure that the Genius is displaying the Splash screen.
 2. On the keypad, press 1, 5, and 9 at the same time to enter System Mode. The Genius device displays a login screen.
 3. Use the keypad to type the supervisor password, then press Enter. The default supervisor password is 166832.
 4. Tap Info > Basic Information
 5. Confirm the values for the following fields:
 - Part Number
 - Vault
 - Application Manager
 - SRED
 - Open protocol
 6. Tap the back button.

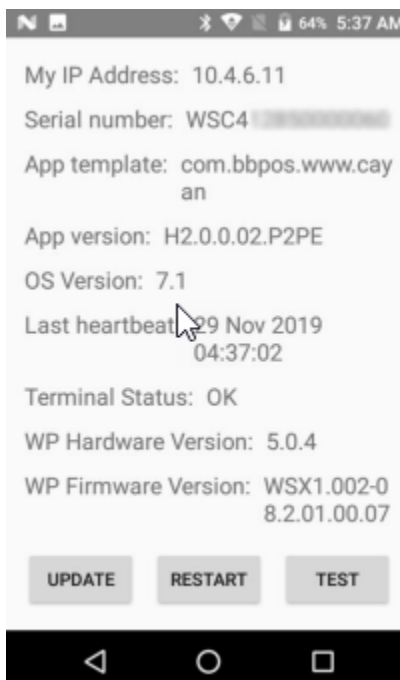



7. On the Information screen, tap the back button again.
8. Tap Run App to restart the Genius application.

Genius Handheld devices

Use the Genius Admin screen to confirm the following:


- Hardware number
 - Firmware number
 - Application version number
1. Tap O, then open the Genius app.
 2. Tap to open the Admin screen.
 3. Confirm the values for the following fields:
 - App version
 - WP Hardware Version
 - WP Firmware Version



4. Tap  to return to the Genius app screen.

10. Appendix: Checklist for Remote Key Injection

We can remotely inject P2PE keys into your existing Genius devices. This process allows you to use our Genius Smart P2PE solution without purchasing new devices or sending your existing devices to us. Your devices must be either version three or version four of Verifone’s hardware and be listed as a PCI approved PTS device. Before we can remotely inject P2PE keys into your devices, you need to inspect them to ensure that no one has tampered with or fitted skimming devices to them.



Important: You must include all the devices that you want to use with our Genius Smart P2PE solution on this form.

Sample Table of Devices for use with Genius Smart P2PE

Device vendor	PCI ID	Device model name(s) and number:	Serial number (S/N)

Attestation Checklist

Complete the following checklist to confirm the suitability of the devices that you want to use with Genius Smart P2PE.

Check	For more information	Complete
Devices are versions listed in the PCI PTS approval	Visit https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices	
Foil seals on the rear of the devices are intact, if applicable	See “6.1.1 Before deploying a device” on page 23 to page 25.	

Devices are the correct weight	See "6.1.1 Before deploying a device" on page 23 to page 25.	
Devices do not have any holes or signs of attempted access to the internal components	-	
Devices do not have any additional wires or components, or other material that could be used to mask evidence of tampering.	See " 6.1.2 After deploying a device" on page 25 to page 27.	
Devices do not have any broken or different colored casings -	-	

Attesting the suitability of your devices

By signing this attestation, I confirm the following:

- By completing this checklist, I confirm that I have visually and physically inspected each of the devices I have listed in the table of devices I want to use for Genius Smart P2PE.
- I have checked each of the devices I want to use with Genius Smart P2PE, and I have accurately recorded the results on this checklist.
- I understand that I must treat these devices like any other P2PE devices and that I must keep an up-to-date inventory.
- I understand that I will be held responsible should I use devices that are not suitable for use with Genius Smart P2PE and that any transactions I process using these devices will not be considered compliant with our P2PE solution

Merchant: _____

Signature: _____

Name: _____

Title: _____

Date: _____

globalpayments