ANDERSONZAKS

Device Appendix AM

Verifone P400/P400 Plus

Appendix AM, Verifone P400/P400 Plus V1.1
Issued on 3/24/2020

Appendix AM: Verifone P400/P400 Plus

This Appendix AM is intended to be used in conjunction with the P2PE Version 2.0 Anderson Zaks PIM Template document. Please make sure to review both documents in order to ensure proper compliance and usage for Anderson Zaks P2PE product offering.

The number used in the different sections of this appendix document directly correlates to general usage points in the P2PE Version 2.0 Anderson Zaks PIM core document.

3.0 Remote Device Administration

The following guidance is intended to communicate PCI's rules around merchants performing any actions while in the custody of the device that could invalidate the effectiveness of their P2PE solution.

For each of the two compliance points from PCI, the combination of the architecture of the Verifone P400/P400 Plus devices and Anderson Zaks P2PE Solution should prevent the merchant from accidently performing any of the PCI banned activities.

Do not connect non-approved cardholder data capture devices.

The P2PE solution is approved to include specific PCI-approved POI devices. Only those devices denoted in the Core PIM document in section 2.1 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.

The Anderson Zaks P2PE solution does not currently support any proprietary Verifone or third-party PIN pads for the P400/P400 Plus.

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

Verifone devices are designed to only accept applications and configuration files that have been signed by Verifone. Anderson Zaks will work with our customers to make sure that the Custom Data

Package (CDP) for their application load is configured to the merchant's requirements. All changes to the CDP will be coordinated and reviewed by Anderson Zaks, and issued by Verifone. CDP files can only be loaded at a Anderson Zaks approved KIF. All White List Bin range exclusion files must be reviewed and authorized by Anderson Zaks prior to their inclusion in any Verifone issued signed files.

For more information on the security around VeriFone's application loading process, please contact your Anderson Zaks support representative.

3.1 Installation and Connection Instructions

Physical Ports supported from the device:
Ethernet, RS-232, USB

Non-Physical connections supported:
The Verifone P400/P400 Plus series supports both Bluetooth and Wifi.

Activation instructions:
This device requires no special actions to activate the device outside of the standard P2PE device activation practices covered in the PIM sections 3.1 and 4.2. Your point of sale software provider may require additional actions, but no actions are required by Anderson Zaks.

Additional instructions:
For any additional instructions for the installation of the POI device, please reference any guidance from the hardware manufacturer. Additionally, reference any guidance provided to you by the hardware or application software provider of your point of sale device.

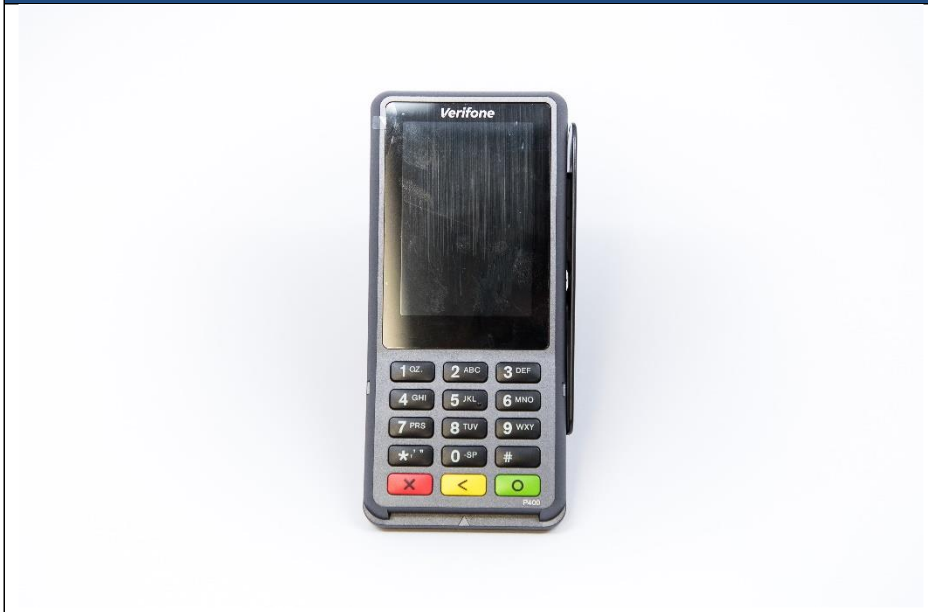
Hardware mounting guidance can be obtained from the device manufacturer, Verifone.

5.1 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.

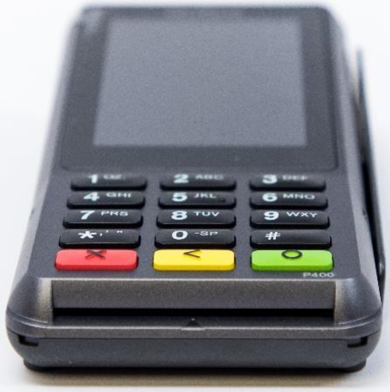
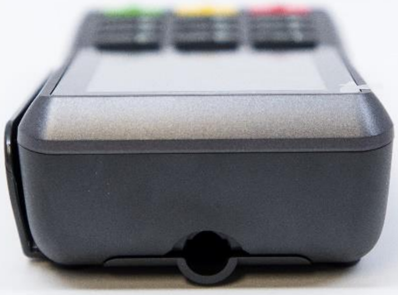
Visual Inspection – P400/P400 Plus

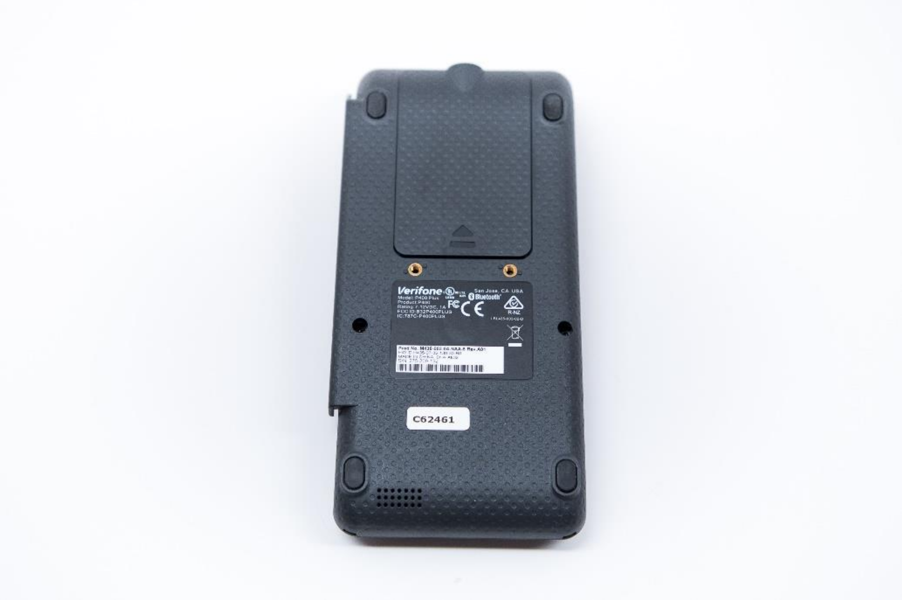
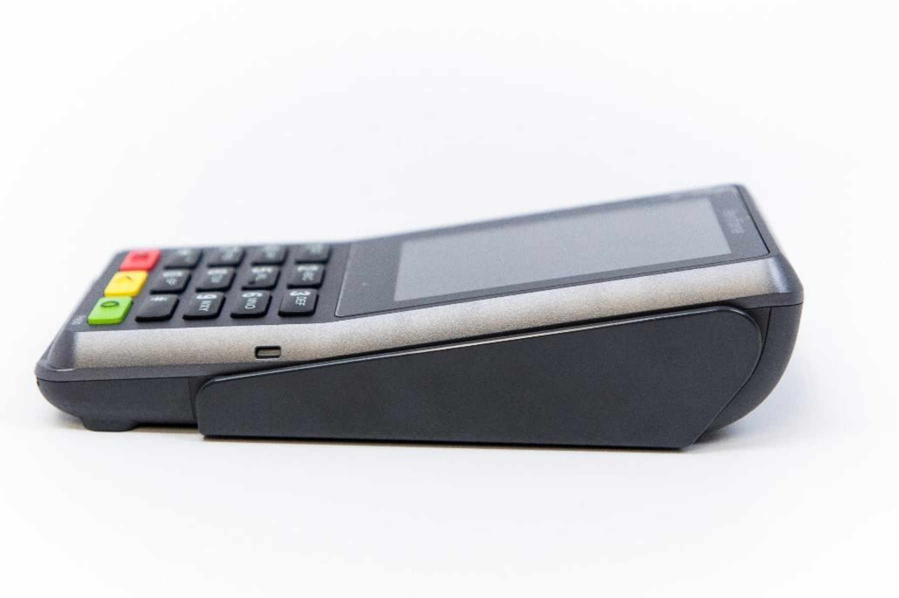
Front of device

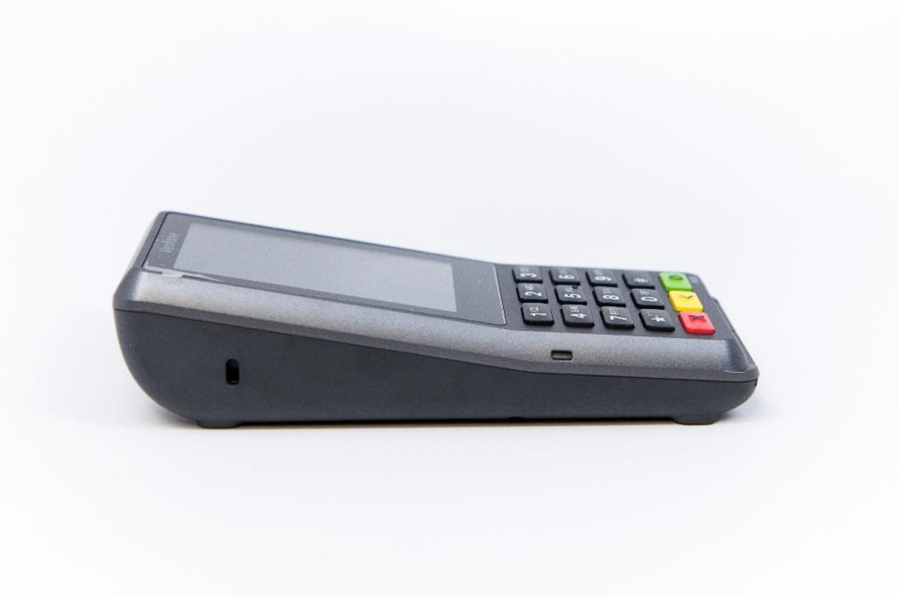


Housing inspection: Your device should fit together snugly. There should be no uneven gaps in the housing, or major scrapes or gouges that may indicate tool marks. Small blemishes are to be expected with the device over time, and concern should only be given to major physical damages in the housing in the area of the seals and seams. Other than the MSR slot for swiping the card on the right of the device and chip card insertion slot at the bottom, there should be no additional holes or slots found on the device.

Bottom of device

	The EMV slot is located on bottom of the device. Please inspect it to make sure that no foreign devices are attached or inserted, and ensure that the area is free of any obvious tamper marks such as tool marks.
Top of device	
	The rear of the device. Hole is for Power/data cable
Back of device	

	The back of the device contains the device model and serial number as well as a removable compartment for the units power/data cable and MicroSD memory optional components.
Right side of device	
	The right side of the device the MSR slot. Please inspect it to make sure that no foreign devices are attached or inserted, and ensure that the area is free of any obvious tamper marks such as tool marks
Left Side	

	The left side of the device.

Weight Verification

Weight verification: In the event that the merchant would like to verify the weight of their device as a method of tamper investigation, the following weight information is provided. Please keep in mind that the listed device weight does not include attachment cables, or accessories. The devices should weigh approximately 310g according to factory specifications. To improve accuracy in documentation, it is suggested that when the unit arrives and is first deployed, the weight of the device should be recorded and compared against the factory specification. The device should be weighed on a postal scale or similar device, with both the POI unit and cord resting fully on the scale. Over time, the device weight may fluctuate slightly, but any noticeable weight increase could be an indicator that the device has been tampered with, and that the device may contain additional malicious hardware.

Application Interface

The P400/P400 Plus supports multiple payment applications. However, the only supported applications for use in Anderson Zak's P2PE solution is the Verifone Point Secure Commerce Application Engage (SCA) version # 4.x.y-z, and Verifone's Integrated Payment Application (VIPA) versions 6.8.1.x and 6.8.2.x.

Guidance for usage and formatting of third party gateways or services that utilize the P2PE solution can be provided by the third party service provider. Merchants unsure of their third party provider can contact a representative via the contact information provided in the main PIM document in section 1.2.