



Opayo P2PE
(formerly SagePay P2PE)

Title	Opayo P2PE Implementation Manual
Version	4.00
Document Author	Damaris Amyes
Document Approver	Patrick Doyle
Last updated	20th December 2024

U.S. Bank Europe DAC. Registered in Ireland – Number 418442. Registered Office: Block F1, Cherrywood Business Park, Dublin 18, D18 W2X7, Ireland. U.S. Bank Europe DAC, trading as Elavon Merchant Services, is regulated by the Central Bank of Ireland.

U.S. Bank Europe DAC. Registered in Ireland with Companies Registration Office. The liability of the member is limited. United Kingdom branch registered in England and Wales under the number BR022122. U.S. Bank Europe DAC, trading as Elavon Merchant Services, is a credit institution authorised and regulated by the Central Bank of Ireland. Authorised by the Prudential Regulation Authority. Subject to regulation by the Financial Conduct Authority and limited regulation by the Prudential Regulation Authority. Details about the extent of our regulation by the Prudential Regulation Authority are available from us on request.

Version History:

Version	Date	Changes	Initials
3.01	01-Nov-21	Draft P2PE v3.01 PIM, based on old v2.0 PIM v 1.15.	DT
3.011	04-Nov-21	Rebranded Solution label back to SagePay, as official name change from SagePay to Opayo hasn't been initiated with PCI SSC yet. Removed V200c device as we don't support it.	DT
3.2	06-Mar-23	Tidied up some text, updated solution reference number, POI updates/refresh and renamed approved partner Lantec to CXM as they have rebranded in the interim. Corrected some original labels that should have stayed as SagePay (not Opayo) while the transition of the P2PE Solution, certifications and branding references are progressing with the PCI SSC.	KMC
3.21	07-Mar-23	Opayo.io email domain migrating to elavon.com (new email for customer service opayoterminalsupport@elavon.com)	KMC
4.00	20-Dec-24	Updated PIM details using the PCI SSC's new template version (released Sept 2024). Added additional PTS approval details to Section 3.1. Updated branding and company name	DA

1. P2PE Solution Information and P2PE Solution Provider Contact Information

1.1 P2PE Solution Information (as per the listing on the PCI SSC website)	
P2PE Solution Name:	SagePay P2PE
P2PE Solution Listing Reference Number (Assigned by PCI SSC)	2021-00240.010
https://listings.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions	

1.2 P2PE Solution Provider Contact Information					
Company Name:	U.S. Bank Europe DAC t/a Elavon Merchant Services (formerly SagePay Ireland)			Company URL:	https://www.elavon.co.uk https://www.elavon.ie
Contact Name:	Opayo Helpdesk			Title:	Opayo Helpdesk
Telephone:	Ireland: +353 (0)1 240 8779 UK: +44 (0)191 313 0296			E-mail:	opayoterminalsupport@elavon.com
Business Address:	Building F1, Cherrywood Business Park			City:	Loughlinstown
State/Province:	Dublin 18	Country:	Ireland	Postal Code:	D18 W2X7

1.3 Communication Instructions
Instructions advising how to contact the P2PE Solution Provider, with consideration to establishing a trusted communication channel/session.
<p>If at any point support is required the Opayo helpdesk is available 24 hours a day, 365 days a year. Support can be provided for POI device tampering or encryption issues, validating support / repair personnel, incident reporting, device troubleshooting, returning devices and many other topics. Please see the contact details referenced in section 1.2. of this Implementation Manual. If the support required is urgent, please contact via phone.</p> <p>Merchants with a relationship to their reseller / deployment partner should contact them directly where possible. These contact details may be listed in section 3.1 of this Implementation Manual.</p>

PCI P2PE and PCI DSS
<p>Merchants using this P2PE Solution may be required to validate PCI DSS compliance. Merchants should contact their acquirer or payment brands to determine their PCI DSS validation requirements.</p> <p>Refer to FAQ 1158 on the PCI SSC Website.</p>

2. PTS POI Device and Software Information

2.1 PTS POI Device Details						
<p>The following information lists the details of the PTS POI devices approved for use in this P2PE Solution.</p> <p>All PTS POI device information can be verified by visiting the following on the PCI SSC Website and by referring to Table 2.4 below: https://www.pcisecuritystandards.org/approved_companies_providers/approved_pin_transaction_security.php https://listings.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions</p> <p>For P2PE Applications and Non-Payment Software, use the PIM ID#s to cross reference to their respective tables below. The 'PIM ID#'s are numbers created and used by the P2PE Solution Provider solely for the purpose within this PIM to make it easier to cross reference the P2PE Applications and Non-payment Software that are used on the PTS POI devices denoted here. The 'PIM ID#'s are not assigned by the PCI SSC nor are they recognized by the PCI P2PE Program.</p>						
PCI PTS Approval #	PTS POI Device Vendor	PTS POI Device Model Name & Number(s)	PTS POI Device Hardware Version #(s)	PTS POI Device Firmware Version #(s)	P2PE Applications on PTS POI Devices (PIM ID# from Table 2.2)	Non-Payment Software on PTS POI Devices (PIM ID# from Table 2.3)
4-80023	Verifone Inc	V240m, V240m Plus 3GBWC, V240m Plus 3GBWCU	H474-07-xx-xxx-xx-B0, H474-07-xx-xxx-xx-B1, H474-07-xx-xxx-xx-B2, H474-07-xx-xxx-xx-B3, H474-07-xx-xxx-xx-B4, H474-07-xx-xxx-xx-B5, H474-07-xx-xxx-xx-B6, H474-07-xx-xxx-xx-B7, H474-07-xx-xxx-xx-B8 (V240m Plus 3GBWCU), H474-07-xx-xxx-xx-B8 (v240m, v240m Plus 3GBWC), H474-07-xx-xxx-xx-B9 (V240m Plus 3GBWCU)	Vault: 6.x.x AppM: 10.x.x VFSRED: 7.x.x.xxx 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, AppM 16.x.x, VFOP: 3.x.x, VFSRED: 13.x.x, Vault: 12.x.x, AppM: 17.x.x, VFOP: 4.x.x, VFSRED: 14.x.x, Vault: 13.x.x	Application 1	None

4-30306	Verifone Inc	V400c, V400c Plus	H425-07-03-xxx-xx-B0, H425-07-03-xxx-xx-B1 (V400c), H425-07-33-xxx-xx-B0, H425-07-33-xxx-xx-B1 (V400c Plus)	VAULT: 7.x.x, AppM: 11.x.x, VFSRED: 7.x.x, VFOP: 1.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, AppM: 16.x.x, VFSRED: 13.x.x, Vault: 12.x.x, VFOP: 3.x.x, AppM: 17.x.x, VFSRED: 14.x.x, Vault: 13.x.x, VFOP: 4.x.x	Application 1	None
---------	--------------	----------------------	---	--	---------------	------

4-10239	Verifone Inc	P400, P400 Plus, P400 DMSR	H435-07-02-xxx-x0-B0, H435-07-32-xxx-x0-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 (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), H435-07-02-xxx-x0-B3 (P400), H435-07-32-xxx-x0-B3 (P400 Plus), H435-17-02-xxx-x0-B3 (P400 DMSR), H435-07-02-xxx-x0-B4 (P400), H435-07-32-xxx-x0-B4 (P400 Plus), H435-17-02-	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, Vault: 12.x.x, AppM: 16.x.x, SRED: 13.x.x, OP: 3.x.x, Vault: 13.x.x, AppM: 17.x.x, SRED: 14.x.x, OP: 4.x.x	Application 2 & 3	None
---------	--------------	----------------------------------	---	--	-------------------	------

			xxx-x0-B4 (P400 DMSR)			
--	--	--	-----------------------	--	--	--

2.2 P2PE Application Details

The following information lists the P2PE Applications approved for use on the PTS POI devices in Table 2.1 for use in this P2PE Solution.

P2PE Applications by definition have access to clear-text account data. These applications **must** be denoted in the P2PE Solution listing.

The 'PIM ID#'s are numbers created and used by the P2PE Solution Provider solely for the purpose within this PIM to make it easier to cross reference the P2PE Applications denoted here that are used on the PTS POI devices denoted in Table 2.1. They are not assigned by the PCI SSC nor are they recognized by the PCI P2PE Program.

Note: P2PE Applications that have been assessed as part of the P2PE Solution and were chosen to not be separately listed are denoted as such as part of the P2PE Solution listing and will not have an independent PCI P2PE Application Listing Reference Number.

https://listings.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions

PIM ID# (e.g., App#1, App#2, ...)	P2PE Application Vendor	P2PE Application Name	P2PE Application Version(s)	PCI P2PE Application Listing Reference Number (Assigned by PCI SSC)
Application 1	SagePay Ireland	PRClient	15.00	2022-00240.011
Application 2	SagePay Ireland	SmartManager P2PE	15.00	2022-00240.012
Application 3	SagePay Ireland	SmartManager P2PE	15.01	2022-00240.013

2.3 Non-Payment Software Details

The following information lists the Non-Payment Software approved for use on the PTS POI devices in Table 2.1 for use in this P2PE solution.

*P2PE Non-payment Software by definition **must not** have any access to clear-text account data. While this type of software is assessed as part of the P2PE Solution assessment, this software is not denoted on the PCI P2PE Solution Listing.*

The 'PIM ID#'s are numbers created and used by the P2PE Solution Provider solely for the purpose within this PIM to make it easier to cross reference the Non-payment Software denoted here that is used on the PTS POI devices denoted in Table 2.1. They are not assigned by the PCI SSC nor are they recognized by the PCI P2PE Program.

PIM ID# (e.g., SW#1, SW#2, ...)	Non-payment Software Vendor	Non-payment Software Name	Non-payment Software Version(s)	Additional Information (as needed)
N/A - Non – payment software not present	N/A - Non – payment software not present	N/A - Non – payment software not present	N/A - Non – payment software not present	N/A - Non – payment software not present

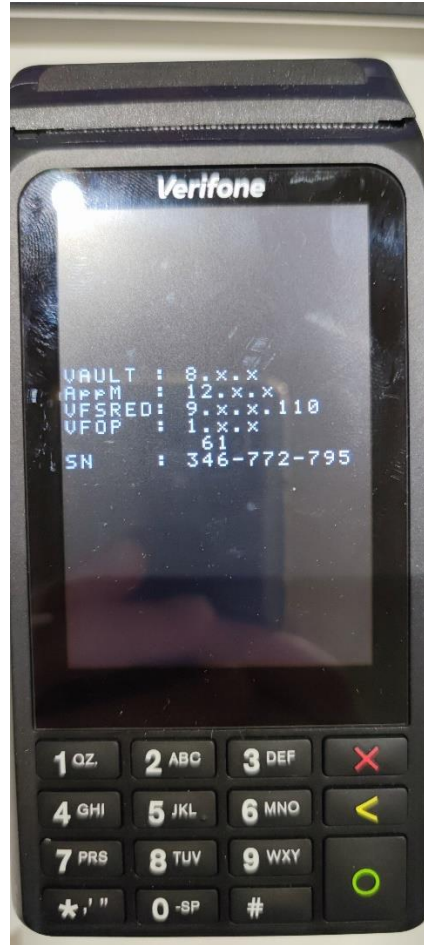
2.4 Verifying PTS POI Device Information



Verifying PTS POI device information is critical. This information is necessary to validate the information in this PIM, to cross-reference with the PCI PTS Listings as well as the PCI P2PE Solution Listing, in addition to inventory management, troubleshooting and incident reporting.

Instructions to confirm PTS POI device hardware, firmware, and the P2PE Application(s) and Non-payment Software present

V240m / V240m Plus 3GBWC / V240m Plus 3GBWCU (PCI PTS Approval # 4-80023)



1. The boot screen should correspond to information on the PCI SSC listing and section 2.1 of this manual.



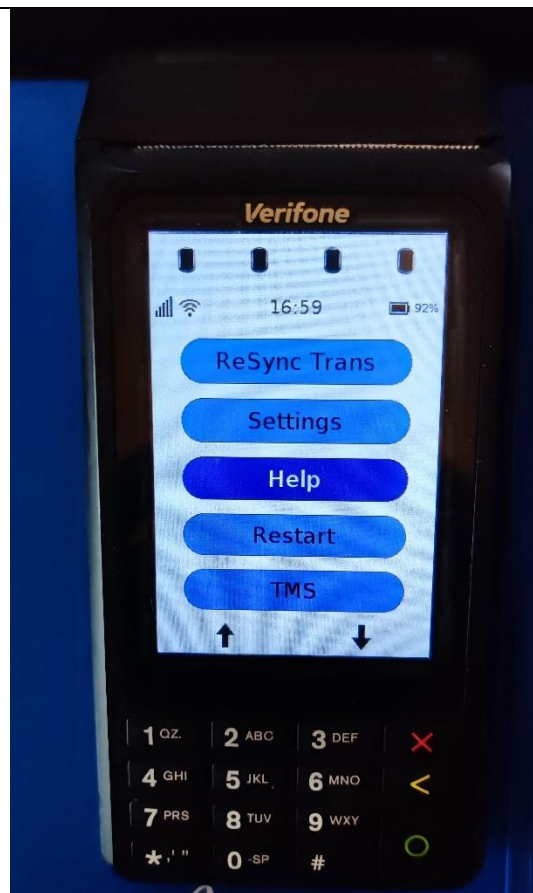
Company	Approval Number 
Verifone, Inc.	
V240m, V240m Plus 3GBWC, V240m Plus 3GBWCU	
Hardware #: H474-07-xx-xxx-xx-B0, H474-07-xx-xxx-xx-B1, H474-07-xx-xxx-xx-B2, H474-07-xx-xxx-xx-B3, H474-07-xx-xxx-xx-B4, H474-07-xx-xxx-xx-B5, H474-07-xx-xxx-xx-B6, H474-07-xx-xxx-xx-B7, H474-07-xx-xxx-xx-B8 (V240m Plus 3GBWCU), H474-07-xx-xxx-xx-B8 (v240m, v240m Plus 3GBWC), H474-07-xx-xxx-xx-B9 (V240m Plus 3GBWCU)	4-80023
Firmware #: Vault: 6.x.x AppM: 10.x.x VFSRED: 7.x.x VFO: 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, AppM 16.x.x, VFOP: 3.x.x,	
VFSRED: 13.x.x, Vault: 12.x.x, AppM: 17.x.x,	
VFOP: 4.x.x, VFSRED: 14.x.x, Vault: 13.x.x	
Applic #:	
Approved Components  :	

2. The back of the device should show the hardware ID (HW ID) and correspond to information on the PCI SSC listing and section 2.1 of this manual.

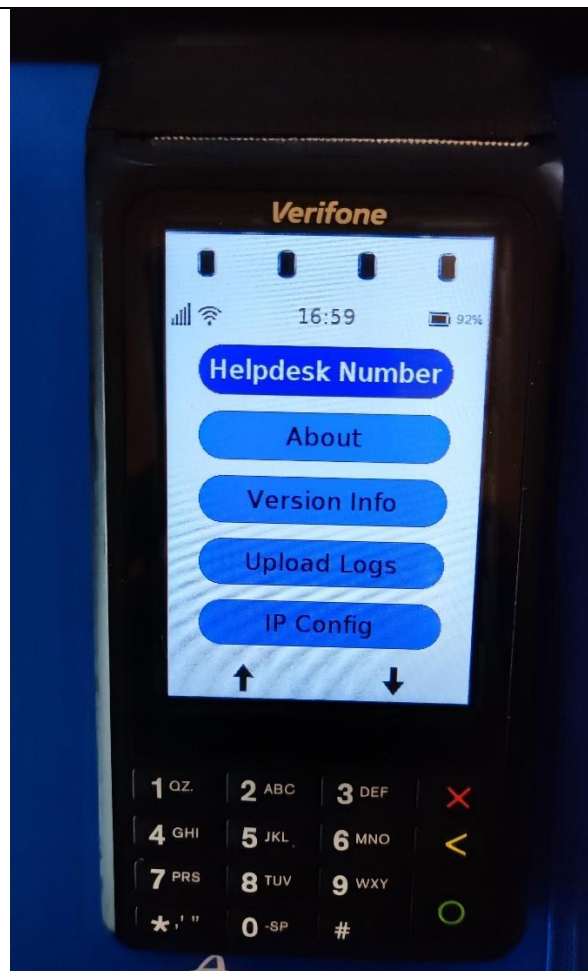


Company	Approval Number 
Verifone, Inc.	
V240m, V240m Plus 3GBWC, V240m Plus 3GBWCU	
Hardware #: H474-07- xxx-xxx-xxx -B0, H474-07- xxx-xxx-xxx -B1, H474-07- xxx-xxx-xxx -B2, H474-07- xxx-xxx-xxx -B3, H474-07- xxx-xxx-xxx -B4, H474-07- xxx-xxx-xxx -B5, H474-07- xxx-xxx-xxx -B6, H474-07- xxx-xxx-xxx -B7, H474-07- xxx-xxx-xxx -B8 (V240m Plus 3GBWCU), H474-07- xxx-xxx-xxx -B8 (v240m, v240m Plus 3GBWC), H474-07- xxx-xxx-xxx -B9 (V240m Plus 3GBWCU)	4-80023
Firmware #: 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, AppM 16.x.x, VFOP: 3.x.x, VFSRED: 13.x.x, Vault: 12.x.x, AppM: 17.x.x, VFOP: 4.x.x, VFSRED: 14.x.x, Vault: 13.x.x	
Applic #: Approved Components  :	

3. Go to main menu and select 'help'

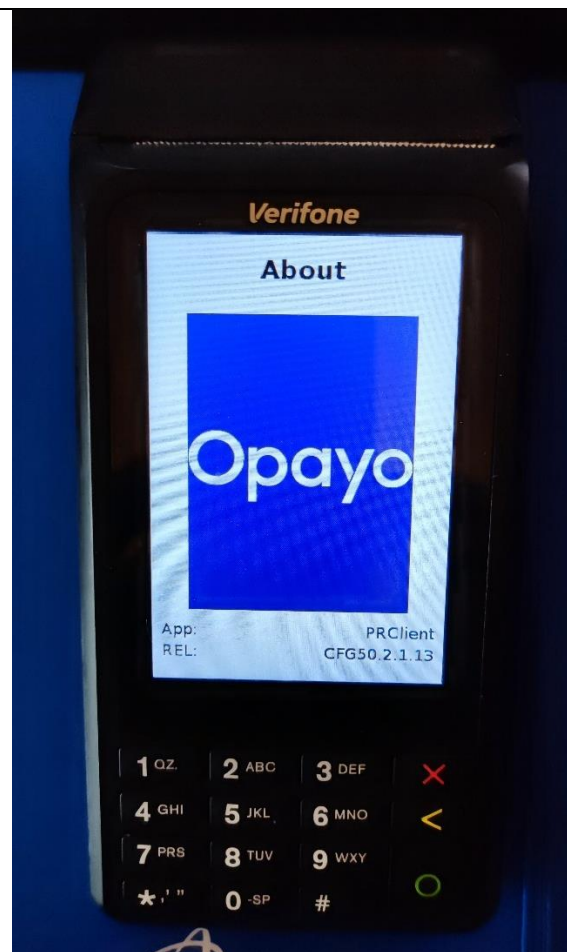


4. From the help menu, select 'about'



5. The about screen will display the P2PE Application name. This will correspond to information on the PCI SSC listing and section 2.1 of this manual.

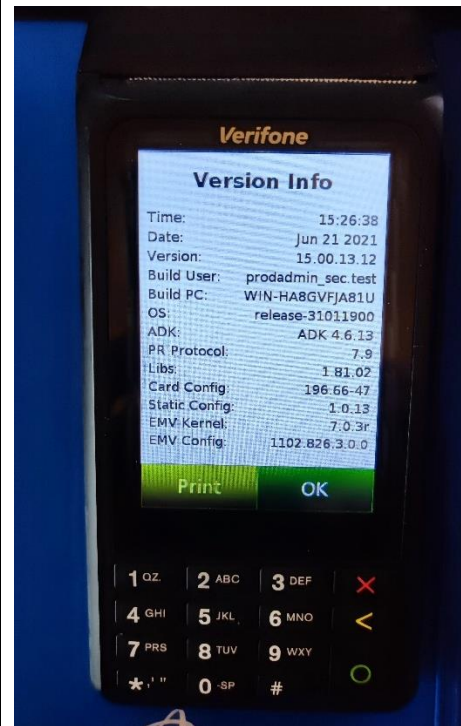
Please ensure the device type and versioning match as there may be multiple PCI PTS listings.



	<p data-bbox="936 215 1310 338">Application Name: PRClient Application Version #: 15.00.x.x Reference #: 2022-00240.011 Close Application Details</p> <p data-bbox="1675 220 1783 242">P2PE v3.1</p> <p data-bbox="996 376 1348 402">Open details in a new window</p> <div data-bbox="996 432 1861 647"><p data-bbox="1025 451 1491 477">PCI-Approved PTS POI Devices Supported</p><p data-bbox="1025 534 1854 560">Verifone, Inc., V240m, V240m Plus 3GBWC, V240m Plus 3GBWCU (4-80023)</p><p data-bbox="1025 611 1491 636">Verifone, Inc., V400c, V400c Plus (4-30306)</p></div>
--	---

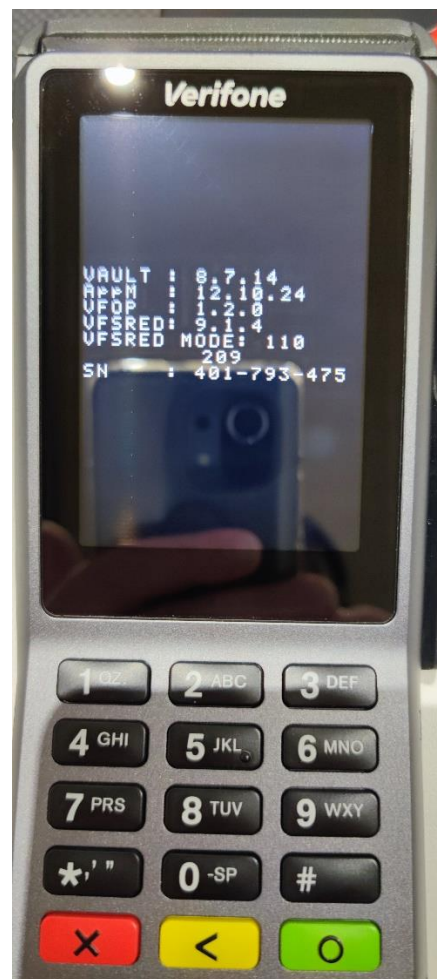
6. Go back to the help menu (step 4) and select 'version info'. This will correspond to information on the PCI SSC listing and section 2.1 of this manual.

Please ensure the device type and versioning match as there may be multiple PCI PTS listings.



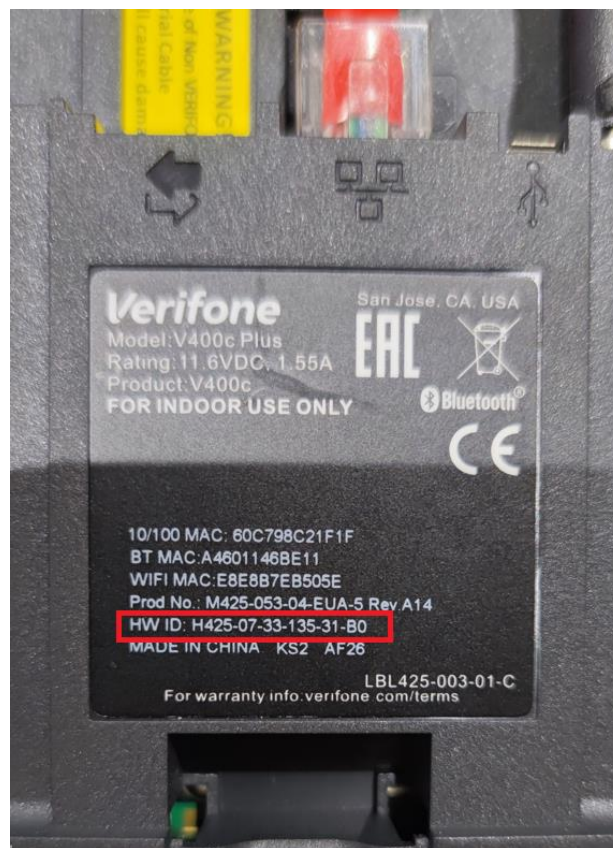
	<p data-bbox="936 215 1326 352">Application Name: PRClient Application Version #: 15.00.x.x Reference #: 2022-00240.011 Close Application Details</p> <p data-bbox="1675 220 1783 242">P2PE v3.1</p> <p data-bbox="996 376 1348 402">Open details in a new window</p> <div data-bbox="999 432 1863 497"><p>PCI-Approved PTS POI Devices Supported</p></div> <div data-bbox="1016 517 1859 584"><p>Verifone, Inc., V240m, V240m Plus 3GBWC, V240m Plus 3GBWCU (4-80023)</p></div> <div data-bbox="1016 608 1859 647"><p>Verifone, Inc., V400c, V400c Plus (4-30306)</p></div>
<p data-bbox="757 738 1435 770">V400c / V400c Plus (PCI PTS Approval # 4-30306)</p>	

1. The boot screen should correspond to information on the PCI SSC listing and section 2.1 of this manual.




Company	Approval Number ⓘ
Verifone, Inc.	
V400c, V400c Plus	
Hardware #: H425-07-03-xxx-xx-B0, H425-07-03-xxx-xx-B1 (V400c), H425-07-33-xxx-xx-B0, H425-07-33-xxx-xx-B1 (V400c Plus)	4-30306
Firmware #: VAULT: 7.x.x, AppM: 11.x.x, VFSRED: 7.x.x, VFOP: 1.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, AppM: 16.x.x, VFSRED: 13.x.x, Vault: 12.x.x, VFOP: 3.x.x, AppM: 17.x.x, VFSRED: 14.x.x, Vault: 13.x.x, VFOP: 4.x.x Applic #: Approved Components ⓘ:	

2. The back of the device should show the hardware ID (HW ID) and correspond to information on the PCI SSC listing and section 2.1 of this manual.



Company

Approval Number 


Verifone, Inc.

V400c, V400c Plus

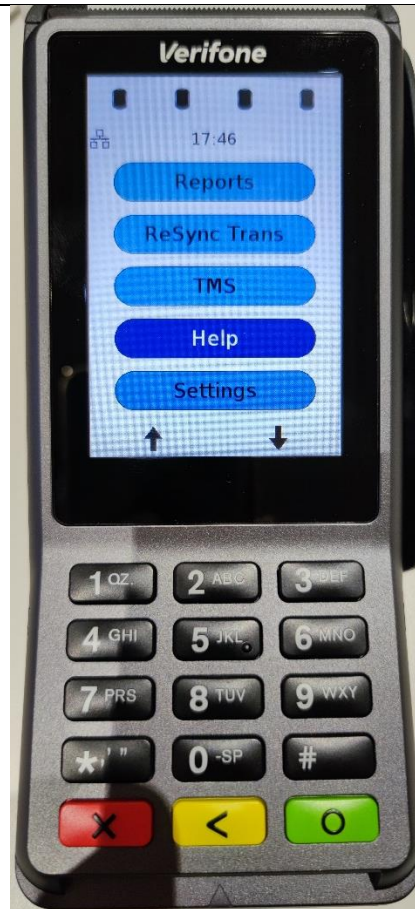
Hardware #: H425-07-03-xxx-xx-B0, H425-07-03-xxx-xx-B1 (V400c) **H425-07-33-xxx-xx-B0**, H425-07-33-xxx-xx-B1 (V400c Plus) 4-30306

Firmware #: VAULT: 7.x.x, AppM: 11.x.x,
VFSRED: 7.x.x, VFOP: 1.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, AppM:
16.x.x, VFSRED: 13.x.x, Vault: 12.x.x, VFOP:
3.x.x, AppM: 17.x.x, VFSRED: 14.x.x, Vault: 13.x.x,
VFOP: 4.x.x

Applic #:

Approved Components 

3. Go to main menu and select 'help'



4. From the help menu, select 'about'



5. The about screen will display the P2PE Application name. This will correspond to information on the PCI SSC listing and section 2.1 of this manual.

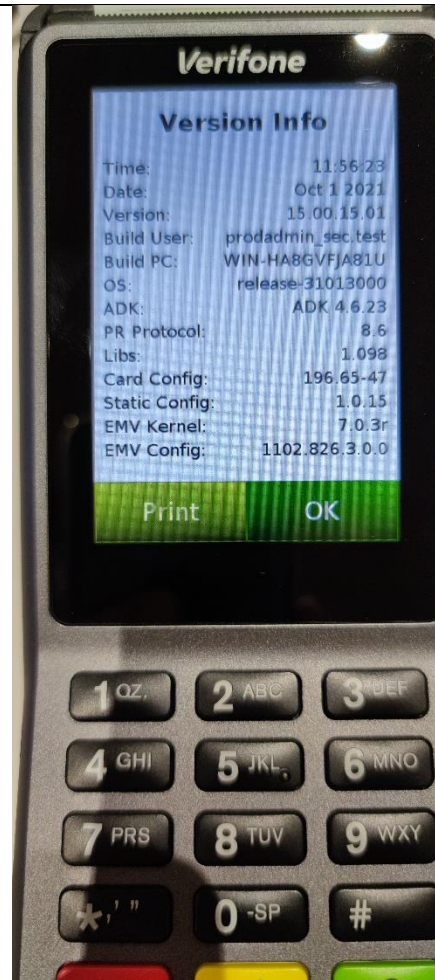
Please ensure the device type and versioning match as there may be multiple PCI PTS listings.



	<p data-bbox="1682 204 1792 228">P2PE v3.1</p> <div data-bbox="943 204 1328 331"><p>Application Name: PRClient Application Version #: 15.00.x.x Reference #: 2022-00240.011 Close Application Details</p></div> <p data-bbox="1005 360 1359 384">Open details in a new window</p> <div data-bbox="1010 416 1872 480"><p>PCI-Approved PTS POI Devices Supported</p></div> <p data-bbox="1037 517 1859 544">Verifone, Inc., V240m, V240m Plus 3GBWC, V240m Plus 3GBWCU (4-80023)</p> <div data-bbox="1001 576 1541 628"><p>Verifone, Inc., V400c, V400c Plus (4-30306)</p></div>
--	---

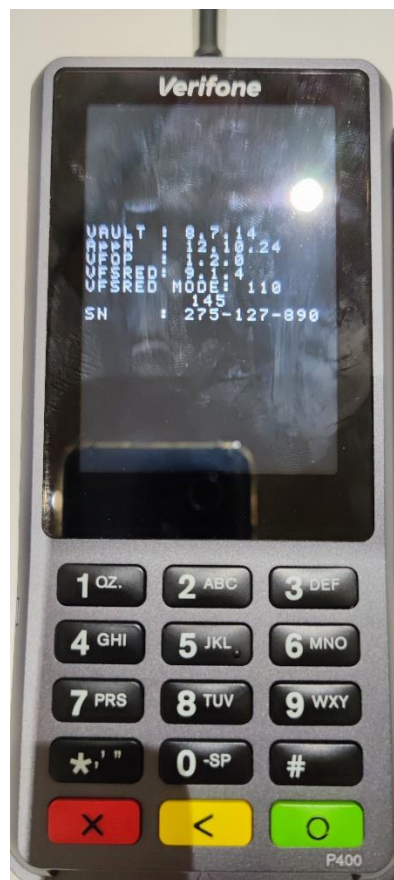
6. Go back to the help menu (step 4) and select 'version info'. This will correspond to information on the PCI SSC listing and section 2.1 of this manual.



Please ensure the device type and versioning match as there may be multiple PCI PTS listings.



	<p>Application Name: PRClient P2PE v3.1 Application Version #: 15.00.x.x Reference #: 2022-00240.011 Close Application Details</p> <p>Open details in a new window</p> <p>PCI-Approved PTS POI Devices Supported</p> <p>Verifone, Inc., V240m, V240m Plus 3GBWC, V240m Plus 3GBWCU (4-80023)</p> <p>Verifone, Inc., V400c, V400c Plus (4-30306)</p>
<p>P400/P400 Plus/P400 DMSR (PCI PTS Approval # 4-10239)</p>	



1. The boot screen should correspond to information on the PCI SSC listing and section 2.1 of this manual.



Company	Approval Number 
Verifone, Inc.	
P400/P400 Plus/P400 DMSR	
<p>Hardware #: H435-07-02-xxx-x0-B0, H435-07-32-xxx-x0-B0, H435-07-02-xxx0-x0-A0, H435-07-02-xxx0-x0-A1 (P400), H435-07-32-xxx0-x0-A0, H435-07-32-xxx0-x0-A1 (P400 Plus), H435-07-02-xxx-x0-B0 (P400), H435-07-32-xxx-x0-B0 (P400 Plus), H435-07-02-xxx0-x0-A0 (P400), H435-07-32-xxx0-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), H435-07-02-xxx-x0-B3 (P400), H435-07-32-xxx-x0-B3 (P400 Plus), H435-17-02-xxx-x0-B3 (P400 DMSR), H435-07-02-xxx-x0-B4 (P400), H435-07-32-xxx-x0-B4 (P400 Plus), H435-17-02-xxx-x0-B4 (P400 DMSR)</p> <p>Firmware #: 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, Vault: 12.x.x, AppM: 16.x.x, SRED: 13.x.x, OP: 3.x.x, Vault: 13.x.x, AppM: 17.x.x, SRED: 14.x.x, OP: 4.x.x</p> <p>Applic #:</p> <p>Approved Components :</p>	<p>4-10239</p>

2. The back of the device should show the hardware ID (HW ID) and correspond to information on the PCI SSC listing and section 2.1 of this manual.



Company	Approval Number 
Verifone, Inc.	
P400/P400 Plus/P400 DMSR	
<p>Hardware #: H435-07-02-xxx-x0-B0, H435-07-32-xxx-x0-B0, H435-07-02-xxx0-x0-A0, H435-07-02-xxx0-x0-A1 (P400), H435-07-32-xxx0-x0-A0, H435-07-32-xxx0-x0-A1 (P400 Plus), H435-07-02-xxx-x0-B0 (P400), H435-07-32-xxx-x0-B0 (P400 Plus), H435-07-02-xxx0-x0-A0 (P400), H435-07-32-xxx0-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), H435-07-02-xxx-x0-B3 (P400), H435-07-32-xxx-x0-B3 (P400 Plus), H435-17-02-xxx-x0-B3 (P400 DMSR), H435-07-02-xxx-x0-B4 (P400), H435-07-32-xxx-x0-B4 (P400 Plus), H435-17-02-xxx-x0-B4 (P400 DMSR)</p> <p>Firmware #: 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, Vault: 12.x.x, AppM: 16.x.x, SRED: 13.x.x, OP: 3.x.x, Vault: 13.x.x, AppM: 17.x.x, SRED: 14.x.x, OP: 4.x.x</p> <p>Applic #:</p> <p>Approved Components :</p>	<p>4-10239</p>

3. Go to main menu and select 'help'. Then select 'about'. The about screen will display the P2PE Application name. This will correspond to information on the PCI SSC listing and section 2.1 of this manual.

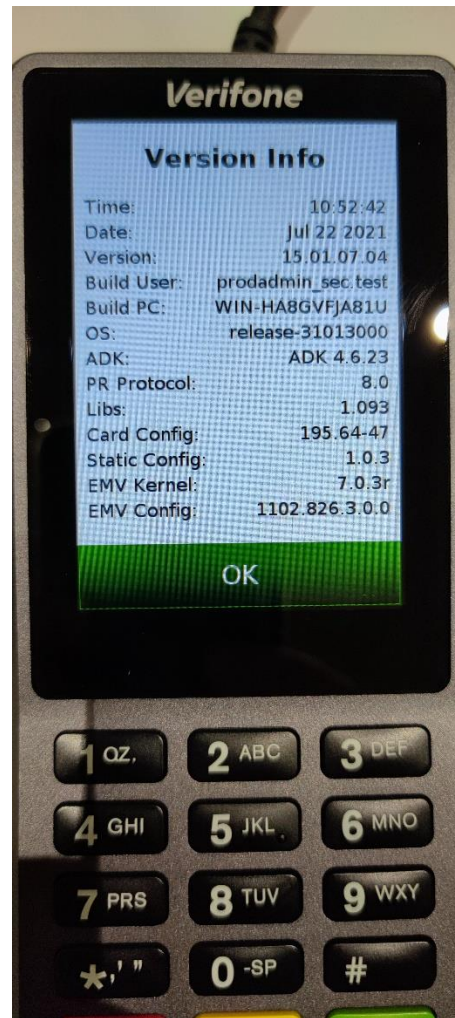
Please ensure the device type and versioning match as there may be multiple PCI PTS listings.



	<div data-bbox="929 199 1406 338" style="border: 2px solid red; padding: 5px;"> <p>Application Name: SmartManager P2PE Application Version #: 15.00.x.x Reference #: 2022-00240.012 Close Application Details</p> </div> <div data-bbox="1653 209 1765 233" style="text-align: right;">P2PE v3.1</div> <p data-bbox="994 360 1339 384" style="text-align: center;">Open details in a new window</p> <div data-bbox="999 416 1827 480" style="background-color: #006666; color: white; padding: 5px; text-align: center;">PCI-Approved PTS POI Devices Supported</div> <div data-bbox="1016 499 1610 555" style="border: 2px solid red; padding: 2px;">Verifone, Inc., P400/P400 Plus/P400 DMSR (4-10239)</div> <hr/> <div data-bbox="929 608 1438 746" style="border: 2px solid red; padding: 5px;"> <p>Application Name: SmartManager P2PE Application Version #: 15.01.x.x Reference #: 2022-00240.013 Close Application Details</p> </div> <div data-bbox="1653 617 1765 641" style="text-align: right;">P2PE v3.1</div> <p data-bbox="994 767 1339 791" style="text-align: center;">Open details in a new window</p> <div data-bbox="999 823 1827 887" style="background-color: #006666; color: white; padding: 5px; text-align: center;">PCI-Approved PTS POI Devices Supported</div> <div data-bbox="1016 906 1610 962" style="border: 2px solid red; padding: 2px;">Verifone, Inc., P400/P400 Plus/P400 DMSR (4-10239)</div>
--	---

4. Go back to the help menu and select 'version info'. This will correspond to information on the PCI SSC listing and section 2.1 of this manual.

Please ensure the device type and versioning match as there may be multiple PCI PTS listings.



	<div data-bbox="929 199 1391 331" style="border: 2px solid red; padding: 5px;"> <p>Application Name: SmartManager P2PE Application Version #: 15.00.x.x Reference #: 2022-00240.012 Close Application Details</p> </div> <div data-bbox="1630 209 1738 233" style="text-align: right;">P2PE v3.1</div> <p data-bbox="992 357 1328 381" style="text-align: center;">Open details in a new window</p> <div data-bbox="996 411 1803 472" style="background-color: #006666; color: white; padding: 5px; text-align: center;">PCI-Approved PTS POI Devices Supported</div> <div data-bbox="996 491 1592 549" style="border: 2px solid red; padding: 5px; text-align: center;">Verifone, Inc., P400/P400 Plus/P400 DMSR (4-10239)</div> <hr/> <div data-bbox="929 595 1422 727" style="border: 2px solid red; padding: 5px;"> <p>Application Name: SmartManager P2PE Application Version #: 15.01.x.x Reference #: 2022-00240.013 Close Application Details</p> </div> <div data-bbox="1630 604 1738 628" style="text-align: right;">P2PE v3.1</div> <p data-bbox="992 750 1328 774" style="text-align: center;">Open details in a new window</p> <div data-bbox="996 804 1803 865" style="background-color: #006666; color: white; padding: 5px; text-align: center;">PCI-Approved PTS POI Devices Supported</div> <div data-bbox="996 884 1592 941" style="border: 2px solid red; padding: 5px; text-align: center;">Verifone, Inc., P400/P400 Plus/P400 DMSR (4-10239)</div>
--	---

2.5 PTS POI Device Inventory & Monitoring

- All PTS POI devices must be documented via inventory control and monitoring procedures, including device status (e.g., 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 PTS POI devices, must be reported to the P2PE Solution Provider via the contact information and instructions in Section 1 above.

- A sample inventory table below is for illustrative purposes only. The actual inventory should be captured and maintained by the merchant in an external document.

Instructions on documenting and maintaining an inventory of the PTS POI Devices.

All devices must be documented in a format similar to the sample inventory table below. The inventory table should be updated when any changes to the POIs locations are made. The maintenance of a PTS POI inventory is the merchant’s responsibility. Asset management is not the responsibility of Opayo. In the scenario where tampering and / or skimming is suspected, account data encryption failures or any other security incident has occurred it is the responsibility of the merchant to make Opayo aware immediately.

Sample Inventory Table

PTS POI Device Vendor	PTS POI Device Model Name(s) and Number(s)	Device Location	Device Status	Serial Number or Other Unique Identifier	Date of Inventory	Additional Notes (as needed)

3. Receipt of PTS POI Devices

3.1 Instructions for ensuring PTS POI devices originate from trusted sources/sites/locations

To ensure the integrity of the P2PE solution when devices are in transit; devices should only be moved between trusted sites listed here. A trusted site could be another site that is part of the Merchant’s trading group, the PED manufacturer, Trusted Deployment Partner, or Opayo as the solution provider. No other location can be deemed as a trusted site. If the PED device forms part of a direct delivery arrangement with the manufacturer, please refer to the contractual arrangements with Opayo to confirm the original trusted site. If there is any doubt over whether a device came from one of these trusted sites, contact the Opayo Helpdesk or Integrator to check before allowing it to be connected.

The following are the Opayo **currently approved** Trusted Sites & Deployment Partners.

Opayo by U.S. Bank Europe DAC
 Building F1
 Cherrywood Business Park
 Loughlinstown

Dublin 18
D18 W2X7
Ireland

Opayo Helpdesk

Second Floor
Q16 Quorum Business Park
Benton Lane
Newcastle Upon Tyne
NE12 8BX
United Kingdom
Phone: +353 12408779 (Ireland) / +44 191 3130296 (UK)

Verifone Inc

VAT No: NL 825816270B01
c/o Teleplan Communications B.V.
Coenecoop 103-105, Waddinxveen, 2741
PH
Netherlands.

SafeNet (Thales), Inc

4690 Milenium Drive,
Belcamp, MD 21017

CBE

IDA Business Park
Claremorris
Co Mayo
Ireland
F12 PE13
Phone: 094 9373000 / Email: retailsupport@cbe.ie

CXM Ireland

Unit C North Dublin Corporate Business Park
Swords

Co Dublin
Phone: 01 8971265

CXM UK

Unit 10 Lovett Way
Woodside
Dunstable
LU5 4TU
Phone: 01582-501939.

Secure Retail Ltd

Walker Road
Bardon Hill
Coalville
Leicestershire
LE67 1TU
Telephone: +44 (0)1530 511150

Vista Retail Support

Vista House
Wharfedale Road
Pentwyn
Cardiff
CF23 7HB
Support: 0345 070 0393
info@vistasupport.com

Aspen Payments Ltd

72a Green End Road
Sawtry
Huntingdon
Cambridgeshire
PE28 5UY
Email: Support@aspenspayments.co.uk
Phone: 01487 832 672

Henderson Technology Ltd

745 Antrim Road
Templepatrick
Co Antrim
BT39 0AP
Phone (support): 028 9094 1911

Store Computer Technology (SCT)

1 – 3 Oak Road Business Park
Nangor Road
Dublin
D12 DC95
Phone: +353 1 5241389

3.2 Instructions for confirming PTS POI device and packaging were not tampered with

Prior to the engineer or courier arriving at the Merchant site to install or deliver the PED(s), the Merchant must ensure that a nominated authorised person is:

- Available to accept a call from the service desk
- Confirm that the site is ready for the install and expecting the install
- Able to record the PED serial number to be delivered.

When the engineer has arrived onsite, there must be a Merchant nominated authorised person available on site to:

- Authorise the receipt,
- Confirm that the serial number(s) match those advised by *Deployment Partner's* service desk,
- Confirm that the devices delivered are still in tamper evident bags
- Confirm the installation of the PED(s).

Where a nominated person is not available, the engineer or courier will not proceed to deliver and install the device(s) and a charge for an aborted visit may apply.

Where the serial numbers tally, the terminal is now ready to use. This information should also be included in the Merchant's inventory list. Prior to install, the engineer will ensure in conjunction with the Merchant's authorised personnel that the tamper evident package shows no evidence of

tampering and will remove the device from the box. [See section on Tamper Evident Package below]. If there is evidence that the tamper evident package has been compromised, the device must be viewed as compromised and made ready for return.

The engineer with the Merchant's authorised member of staff will ensure that the serial number of the device the engineer delivers is identical to the serial number that the Merchant's authorised member of staff has received from Opayo. If the two serial numbers do not tally, the install cannot proceed and arrangements will need to be made for a future attempt at install. Assuming the serial numbers do tally, the install can then proceed.

When the device is removed from the packaging, the engineer will physically check the device to ensure that the device has not been tampered ensuring that there is no evidence of a wire or tapping device evident in the card reader. If the device shows no evidence of tamper, the install can continue. The engineer will then proceed to connect and power up the device(s), load the software and keys and complete a transaction before finalising the installation. When the installation is complete; the engineer scans the serial number of the device installed into the relevant job sheet on their handheld PDA, and requests that the customer signs for completion of the job.

If an engineer model is used there should be no reason for not installing devices directly, as the engineer is on site for that purpose. If a reason does transpire whereby the device(s) cannot be installed immediately, the device(s) should be stored securely immediately. Securely means as a minimum that the device(s) is stored in a lockable cabinet whose access is restricted to authorised personnel only. If a Merchant's authorised member of staff is to install the device(s), the above steps of this section should be adhered to at all times.

3.3 Instructions to confirm the business need for, and identities of, any third-party personnel claiming to be delivery, support, and/or repair personnel, prior to granting those personnel access to PTS POI devices.

Before Opayo or a Delivery Partner sends an engineer to site for repair or support purposes, they will provide a notification to the merchant's primary contact of the designated engineer name.

Prior to allowing the engineer access to the POI device, ensure that the engineer's identity document has been verified and that the name on the identity document matches the name on the notification sent prior.

In the event of failures requiring engineering support Opayo's preferred mechanism is for our Deployment Partner to be contacted and have the POI device replaced through the usual RMA process.

In the event of an engineer arriving to site without any formal notification from Opayo, please treat the activity as suspicious and do not permit them to have access to a POI device.

Physically secure POI devices in your possession, including devices:

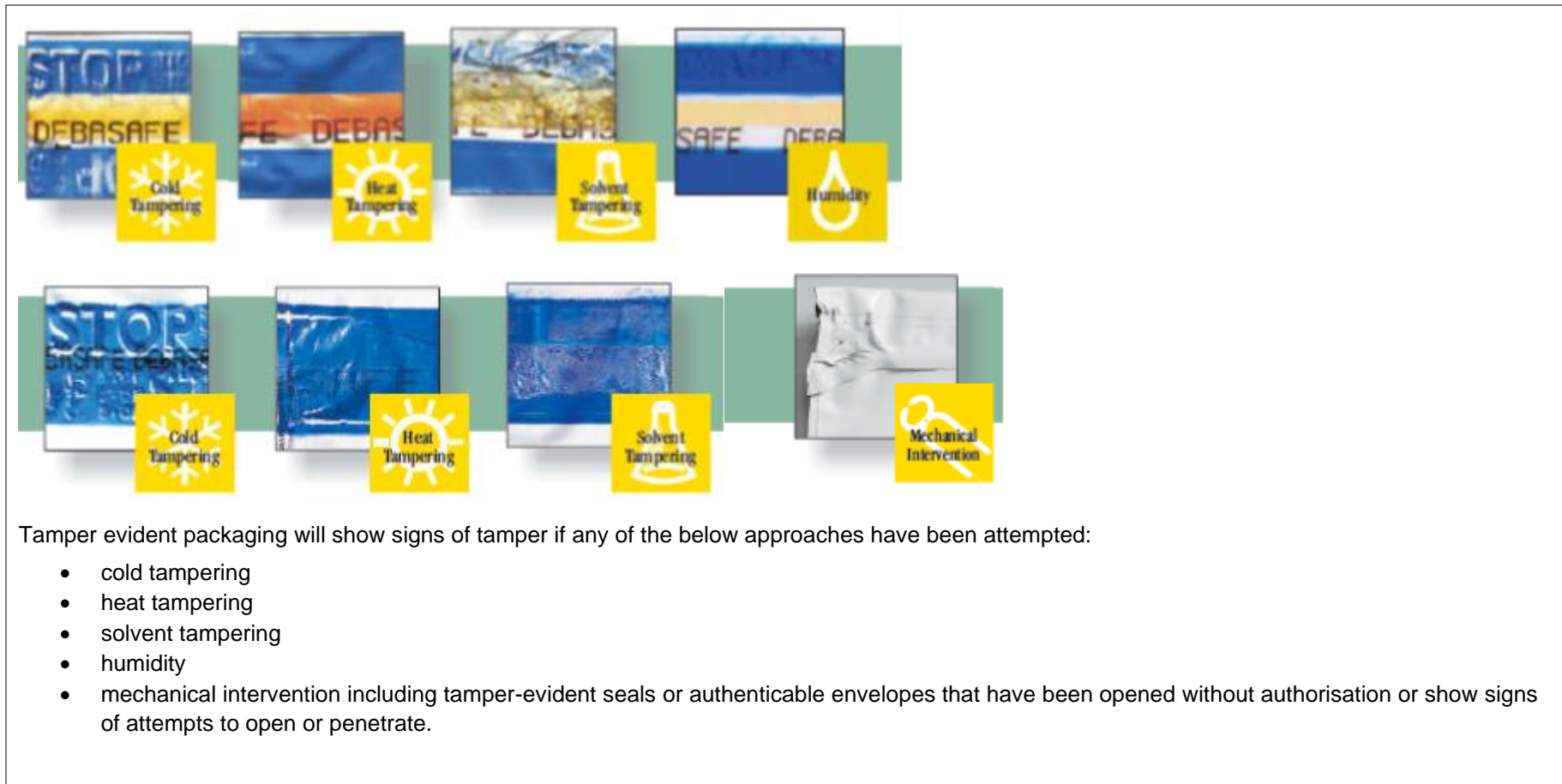
- Awaiting deployment
- Undergoing repair or otherwise not in use
- Waiting for transport between sites/locations

Example of Tamper Evident Package

TEE Bag:



What does a tampered package look like?



4. Deployment and Installation of PTS POI Devices

Do not connect or otherwise use non-approved payment account data capture devices.

The P2PE Solution is approved to use specific PTS POI devices, as detailed above in Table 2.1, which must be denoted on the P2PE Solution Listing.

If any devices that are not in Table 2.1 are used to accept [payment account data](#), it could affect the merchant eligibility to use SAQ P2PE – contact your acquirer or payment brands.

Do not change or attempt to change PTS POI device secure configurations or settings.

Changing secure PTS POI device configurations or settings may invalidate the P2PE Solution implementation and it could affect the merchant eligibility to use SAQ P2PE – contact your acquirer or payment brands.

Examples include, but are not limited to attempting to perform the following on the PTS POI devices:

- Enabling any device interfaces or data-capture mechanisms that are disabled
- Altering security configurations or authentication controls
- Physically opening the device
- Attempting to install unauthorized applications/software

4.1 Installation and connection instructions for the PTS POI devices

There are two main installation service offerings for installation of the P2P Solution:

1. Engineer Installation: Where a selected member of staff will attend the merchant site and install the device as appropriate.
2. Courier Installation: Where the device is delivered in a secure manner and must be installed by a nominated, trained member of staff.

In both cases the device must be connected to the appropriate port on the till if it is integrated. This port will be nominated by the till provider. The location and how the device is secured is detailed in sections 3.2 and 3.3 respectively.

The device may be preloaded with the relevant application and configuration. If it is then it is ready to use. If not, the device will download the appropriate package when communication is available.

4.2 Guidance for selecting appropriate locations to deploy PTS POI devices

Location of devices is extremely important to ensure security. All devices must be located where it is possible for members of staff to view them and to ensure that daily checks can be easily conducted. Devices should always be in locations that allow deterrent of compromise and where visible security measures are evident.

4.3 Guidance for physically securing deployed PTS POI devices to prevent unauthorized removal and/or substitution

Devices can be physically secured by using a mounting pole or other method of protection.

When PEDs are not in use, they should be secured in an area that is lockable and has restricted access such as a safe or lockable cabinet. The devices should be serialised and recorded using the inventory template featured in section 2.3 or similar listing.

Portable terminals should be secured when unattended or left overnight.

Items that are in use should be located so that they can be seen at all times by merchant staff.

5. Continual Monitoring and Inspection of Deployed PTS POI Devices

5.1 Instructions for inspecting PTS POI devices for signs of tampering and responding to suspected tamper incidents

When a device has been deployed into the merchant environment, you must conduct periodic reviews of the device(s) to ensure that any tampering, alteration or substitution has not occurred. Typically checks should be of the original commissioning such as security screws and seals, labelling and physical connections. The location of these items on the device can be referenced in the accompanying device manufacturer user manual and in the 'Tamper Evidence Checking of the Devices' section and photos below.

Additionally, the device should be checked to ensure that no extraneous labelling has been applied and that no holes are visible other than those pictured in the user manual. It is highly recommended that these checks are undertaken at the start and end of each shift, and that a list of these checks are recorded itemising as a minimum for each of your devices (see Inventory Table in Section 2.5):

- Device Vendor (Manufacturer)
- Device Model Name(s) and Number
- Device Location
- Device Status
- Device Serial Number
- Date & Time of Inventory when device was checked

The minimum recommended visual inspection of the device(s) is weekly. This will maintain your compliance.

If at any point any dissonance between how the device was delivered and how it has been found is apparent, the unit should be considered tampered, and the instructions below should be strictly adhered to.

Where units are installed in remote or unattended scenarios, increased rigour should be used to monitor the status of the PED. For instance, monitoring and/or physical mechanisms should be implemented to safeguard the security of the device such as the installation of security cameras or alarm systems in unattended scenarios. Where units are deployed in remote sites, surveillance equipment and periodic reviews should be implemented to ensure the device has neither been tampered with nor removed or substituted. In addition, attention should be employed to the frequency of PED inspection and those inspections should be logged on each occasion. Details to be logged should include the PED serial number, reviewer, date and time and outcome i.e. satisfactory or issue detected as a minimum. Where a tamper or other suspicious activity is believed to have occurred, PEDs should not be used and the Service desk should be contacted.

Tamper Evidence Checking of the Devices

Please ensure the rear of your device looks as in the photos below, which are shown with & without the rear covers in place where possible.

Where visible, Tamper seals are highlighted by a red arrow in the photos, please ensure these are intact and show no signs of damage.

Also ensure that there are no unusual markings, scratches or evidence of damage.

If there are any signs of unusual wires, damage, or tampering with the unit please call Opayo immediately.

Verifone – V240m Plus (cover on)



Verifone – V240m Plus (cover off)



5.2 Instructions for inspecting PTS POI devices for skimming devices and responding to suspected skimming detection

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

Following the below steps will help maintain the integrity of your PEDs. If you feel that your terminal has been tampered with in any way, stop processing transactions and immediately contact the Opayo helpdesk.

- Inspect the terminal regularly and make sure that there are no unusual scratches, marks, or damage.
- 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 the card reader is clean and 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.
- Inspect all wires and cables to ensure that they are securely connected and are in good condition with no tears or ripping.
- Verify that the terminal cable is securely attached to the device and there is nothing in-between it and the device.

5.3 Instructions for detecting and responding to PTS POI device account data encryption failures

In the scenario where there is an account data encryption failure, the transaction/s will end in an error and will be communicated to the merchant as the following:

- SRED encryption error

Note that the error code may show on the till logs or on the device itself. Please contact the Opayo Helpdesk (contact details provided in section 1.2) as soon as possible, who will be able to assist. Depending on the advice provided by the helpdesk the device/s may need to be immediately shut down and taken offline.

5.4 Instructions for troubleshooting a PTS POI device

Where you the retailer believe that there is a problem with the operation of a PED or PEDs, you should call the Opayo Helpdesk for further information in the first instance.

6. Transporting / Shipping PTS POI Devices

6.1 Instructions for ensuring PTS POI devices are shipped to trusted sites/locations only, as needed (e.g., for repair)

To ensure the integrity of the P2PE solution when devices are in transit; devices should only be moved between trusted sites listed in Section 2.1. A trusted site could be another site that is part of the Merchant's trading group, the PED manufacturer, Trusted Deployment Partner, or Opayo as the solution provider. No other location can be deemed as a trusted site. If the PED device forms part of a direct delivery arrangement with the manufacturer, please refer to the contractual arrangements with Opayo to confirm the original trusted site (Section 2.1 lists the Opayo **currently approved** trusted sites).

6.2 Instructions for securing PTS POI devices intended for, and during, transit to other locations (e.g., to a repair facility)

As a Merchant, should you need to move a device from one location to another, the following steps should be followed.

Each device to be moved should be annotated on the inventory list and the *Deployment Partner's* service desk must be advised of this transfer in writing.

Prior to placing the device and box in a tamper evident package which can be found inside the box [supplied by Opayo]. The device should be removed and checked to ensure that the device has not been tampered with nor substituted. If satisfactory, the device should then be placed in the box and the box and device placed within a tamper evident package. If the device is to be in transit under the control of your organisation immediately then the device should be loaded to the vehicle and the journey to the location that the device is to be used in undertaken. If a courier is to be used, the package will be scanned / serial number recorded prior to leaving your premises. When the device is delivered at the new location, the package will again be scanned / serial number recorded prior to being signed for.

Upon arrival, if the tamper evident package shows evidence of a tamper, then the unit should be stored securely, for instance in a safe or lockable cabinet, the *Deployment Partner's* service desk should be called for advice on next steps to be taken. Opayo will replace the suspect device and dispose of the unit in a secure manner.

Where transferring devices from one Merchant site to another by a 3rd party, the 3rd party should be a secure or bonded courier. [The courier used must accept responsibility for the Tamper Evident package].

7.1 Additional guidance for merchants regarding the P2PE Solution (as needed).

Glossary of terms and acronyms used in this manual:

- P2PE = Point To Point Encryption. A method of securing sensitive card details by encrypting them as soon as the card is entered, so the full card details are never available to the merchant.
- PED = Pin Entry Device. This is the terminal or pinpad where a cardholder keys in their PIN number when carrying out a card transaction. See also POI below.
- POI = Point Of Interaction. These are the card-reading devices such as a terminal or pinpad where cards are keyed, swiped, dipped, or tapped. Depending on the implementation, the PED & POI are often the same device with the card entry & PIN number being handled on the same terminal.

7. Additional Guidance / Instructions

INTENTIONALLY LEFT BLANK