Payment Card Industry (PCI)

Point-to-Point Encryption

P2PE Instruction Manual (PIM)

P2PE Version 3.0

November 22, 2022

Version	Release Date	Changes
1.00	12/8/2021	Initial document released
1.01	12/17/2021	Updated CSG Forte logo with higher resolution image.
1.02	3/31/2022	Corrected table "3.2 POI Software/Application Details" with No in the "Does Application Have Access to Clear-text Account Data (Y/N)" column for the Forte Application.
1.03	3/31/2022	Added this table to the PIM.
1.04	5/9/2022	Inserted XPI version information.
1.05	8/11/2022	Updated CSG Forte logo with latest logo.
1.06	11/21/2022	Updated solution reference number and Company address.

1. P2PE Solution Information and Solution Provider Contact Details

1.1 P2PE Solution Information	
Solution name:	Forte Protect
Solution reference number per PCI SSC website:	2022-01415.001

1.2 Solution Provider Contact Information	
Company name:	CSG Forte Payments, Inc.
Company address:	CSG Forte Payments, INC. P.O. BOX 208655 Dallas, TX 75320-8655
Company URL:	www.forte.net
Contact name:	Praveen Balireddy
Contact phone number:	+14693936593
Contact e-mail address:	customerservice@forte.net

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.

Validating device shipments from CSG Forte to the merchant

The CSG Forte P2PE solution helps to manage and validate all POI device shipments from Forte's key injection facilities (KIF) to the merchant's location.

Device orders for merchants are initiated with a Forte Payment Systems representative who then works to fulfill the order utilizing CDE and Bluefin.

Utilizing the Bluefin P2PE Manager, the Forte employee sets up the merchant profile in the system, the individual merchant user accounts, and then creates the merchant locations that are eligible for devices. Each location profile contains an address, contact information, and a recipient's name. All shipments from the KIF to that location will be addressed to the recipient listed in the location profile.

Before leaving the KIF, the POI device is placed in a tamper evident bag, and then sealed with a serialized tamper sticker. The KIF then records the serial number from the tamper bag, and the serial number of the device into P2PE Manager.

When the POI devices arrive at the customer location, the employee listed as the contact for the location logs into the Bluefin P2PE Manager and confirms receipt of the device. The merchant employee manually keys (or scans) in the serial number of the device, and the serial number from the tamper seal into the Bluefin P2PE Manager. If the Bluefin P2PE Manager confirms that the two serial numbers both match the injection and shipment records recorded by the KIF, then the device is eligible for use.

If the serial number of the device or the serial number on the tamper bag do not match, the device is programmatically barred from use. Without the validation of both authenticating serial numbers, a device cannot be put into use.

If a merchant receives a device that they are unable to activate with the serial number on the device and the serial number on the bag, CSG Forte should be contacted via the contact information found in Section 1.2 of this document to report the issue. Devices should be held on to by the merchant until further instructions are provided by CSG Forte.

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

Once a merchant receives confirmation that the order for their units has been submitted, within a few business days (once the order is prepared for shipment) the merchant will be able to log into the Bluefin P2PE Manager and review the status of their pending shipment. The merchant can review the serial numbers of the devices contained in the shipment and confirm the carrier and tracking number for the shipment, the destination location information, as well as the merchant representative to whom the order is being shipped to.

When the responsible party at the merchant location takes possession of the shipment of POI devices, they must log the confirmation of the receipt of those devices into Bluefin's P2PE Manager.

Immediately upon receipt, the merchant should inspect the shipment box for major damage such as tears, or holes and they must visually inspect that the packaging has not been re-taped or resealed.

The merchant representative should also visually inspect the contents of the shipment box which should contain the expected number of cardboard boxes which contain an outer sticker that indicates the serial number of each POI device.

The POI device should be contained within two packaging elements

The outer element is a tamper-evident bag. This bag will be sealed with serialized sticker/tape. This sticker is a tamper-evident sticker. If the sticker/tape has not been tampered with, it should look like Figure 1. Minor evidence of potential tampering with the sticker (rumpling or minor stretching) may occur while the box is in transit.

Figure 1: POI Device in tamper evident bag with a tamper evident sticker on it

If the sticker/tape has been removed or tampered with, the sticker may look like **Figure 2.**

Figure 2: Device with potential tampering

If you see a sticker on the tamper-evident bag near this level of evidence, you should consider the device as having been tampered with.

Confirming receipt of your shipment and preparing the device for activation

After receipt of the shipment, the merchant is required to confirm their shipment order in the P2PE Manager by navigating to the receipt of shipment screen. Once on this screen, the merchant representative will be required to attest to the receipt of each POI device. Proper attestation requires confirming the serial number of the device (found on a sticker on the cardboard packaging of the device box, and on a sticker on the device itself) and then opening the cardboard box and verifying the serial number from the tamper-evident bag.

Specific steps for activating a device within P2PE Manager can be found in your Bluefin P2PE Manager User Guide or via the following video link: https://vimeo.com/182772442/30b87f999e

Note: The tamper-evident bag SHOULD NOT BE OPENED UNTIL THE DEVICE IS IN THE FIELD LOCATION WHERE IT WILL BE DEPLOYED.

This is important to preserve the tracking, device activation and chain of custody. Additionally, the merchant should keep the cardboard box that the device was shipped in as it will be the primary way in which a merchant can identify the serial number of the device without having to remove the device from the tamper-evident bag.

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.

Access to POI devices by third-party personnel for repair and/or maintenance must be monitored. This monitoring is required to ensure that there is no unauthorized access to the device that could result in tampering, theft, or substitution of the device. To ensure proper third-party access monitoring, you should have a policy in place that requires the following steps:

1) Maintenance or repair of the device must be pre-arranged with date and timeframe of third-party personnel defined. Unexpected visits for repair or maintenance must be verified. If they cannot be verified, access to the device must be denied.
2) Prior to granting access to a device, personnel must be identified and authorized to access the device.
3) Third-party personnel access must be recorded and include personnel name, company, time of access, and purpose of access. Log must be maintained for no less than one year.
4) Personnel must be escorted and always observed.
5) Personnel may not remove or replace a device without prior authorization. If authorized, new devices must be properly inspected and inventoried.

Logging activity

The merchant should keep a log of any onsite visits by a Forte representative or one of its contracting representatives. The log should contain the name of the representative who visits, their contact phone number, contact email address, their company name, the date of their visit, the time

they arrived, the time they departed, and the purpose of their visit. These logs should be saved for up to one year.

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

3.1 POI Device Details

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

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

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

PCI PTS approval #:	POI device vendor:	POI device model name and number:	Hardware version #(s):	Firmware version #(s):
4-30306	Verifone, Inc	V400c Plus	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

3.2 POI Software/Application Details

The following information lists the details of all software/applications (both P2PE applications and P2PE non-payment software) on POI devices used in this P2PE solution.

All applications with access to clear-text account data must be reviewed according to Domain 2 and are included in the P2PE solution listing. These applications may also be optionally included in the PCI P2PE list of Validated P2PE Applications list at vendor or solution provider discretion.

Application Vendor, Name, and Version #	POI Device Vendor	POI Device Model Name(s) and Number:	POI Device Hardware & Firmware Version #	Is Application PCI Listed? (Y/N)	Does Application Have Access to Clear-text Account Data (Y/N)
Verifone, XPI, 20.04.00.00-354	Verifone, Inc	V400c Plus	Hardware: **V400c Plus:** H425-07-33-xxx-xx-B0, H425-07-33-xxx-xx-B1	YES	YES
Verifone, VHQ 3.2.3	Verifone, Inc	V400c Plus		NO	NO
Forte, Forte Application, 103F	Verifone, Inc	V400c Plus		NO	NO
Verifone, ADK, 4.7.8.1	Verifone, Inc	V400c Plus	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	YES	YES

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 CSG Forte Payments 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.

All devices that are issued to a merchant are tracked by CSG Forte within the Bluefin P2PE Manager®.

Merchants can review an inventory of all devices that have been in their possession. This includes units that have been temporarily removed from service, awaiting deployment, actively processing, or devices that are retired and no longer eligible to run transactions. Merchants can update devices on their own in real time to ensure that when annual inventories are performed, all records are up to date.

Specific operational instructions on how to perform an inventory are provided below.

Inventory Reporting

Bluefin P2PE Manager

The Bluefin P2PE Manager can be accessed at the following link: https://bluefin.p2pemanager.com/

Inventory Report

To generate a report of all POI devices, please go to the REPORTS link in the top global navigation bar. From there you can select the date range for your device inventory report.

By selecting ALL POIs, ALL CUSTODIANS, and ALL LOCATIONS, any POI devices in the custody of the merchant during the time frame selected will be displayed.

Those results can then be exported by hitting either the CSV or PDF button. When viewing the report, you can reference this glossary to understand the different columns of information that are provided.

• POI MODEL: This is the manufacturer name for the device.

• POI SERIAL NUMBER: This is the unique serial number for the device. This should match the serial number sticker on the device. It should also match the serial number on the box that the device was shipped in originally.

• LOCATION: This is the last confirmed location of the device.

• ADDRESS: This is the address detail that matches the LOCATION name.

• CITY: This is the city that matches the LOCATION name.

• STATE/PROVIENCE: This is the state or province that matches the LOCATION name.

• POSTAL CODE: This is the zip code that matches the LOCATION name.

• COUNTRY: This is the country that matches the LOCATION name.

• CUSTODIAN: This is the individual person who is associated as the primary person responsible for the receipt and stewardship of the device for the LOCATION.

• STATUS: This is the current operational STATUS of the device.

State Changes

Before creating an annual inventory report, or at any other time, the merchant can update the state of their device to reflect its current condition.

This can be done by going to the DEVICES link in the top global navigation bar. From there the merchant can click on a specific device and click the EDIT link. This will provide the ability to view and potentially change the device state.

Merchants can change devices to the following temporary states that leave the device unable to process transactions:

- Damaged
- Malfunctioning
- Lost
- In Repair
- Stored

Merchant can change devices to the following permanent states that leave the device unable to process transactions:

- Retired
- Destroyed
- Tampered

Note: If this state is accidently selected there may be remediation options available by contacting the Forte P2PE contact found in Section 1.2 of this document.

Additionally, as a safeguard, devices that exhibit TAMPERED behaviours such as passing credit card data in the clear or repeatedly failed decryptions will be automatically disabled and marked as TAMPERED. In such events, a Forte representative will follow up from those automated events to coordinate an inspection/review of the device with the merchant.

Additional device states that may be displayed but are not eligible to be modified by the merchant are:

- Quarantined (by KIF)
- DOA (by KIF)
- Injected
- Authorizing

Dealing with missing devices

The P2PE Manager is a reporting tool and reviewing devices in the field is still needed to validate against missing devices. If a device has been lost or stolen, the merchant should log into the P2PE Manager, find the serial number of the device that can't be inventoried, and change the state of the device to LOST. This will ensure that the device won't be able to process P2PE transactions in Forte's P2PE environment. After the device state has been changed, contact CSGForte via the contact information in Section 1.2 to report the device as missing. At the merchant's discretion, a replacement device can be ordered.

If a missing device is found, the merchant should conduct a full visual inspection. If the device appears to be untampered, the merchant at their own discretion can choose to activate the device again. If the merchant is unable to ascertain the integrity of the device, at the merchant's own discretion they may choose to order a replacement device and have the now found device sent to Forte for destruction.

All device destructions will include formal attestation for the destruction of the device.

Dealing with substituted devices

The P2PE Manager is a reporting tool and reviewing devices in the field is still needed to validate against substituted devices. Substituted devices may be found when the merchant completes their annual attestation, or during periodic inspection.

A substituted device may appear to be identical to the merchant's equipment, which is why it's important to follow the inspection guidance in Section 6.1. If the merchant believes that there may be a device substitution, the merchant should immediately discontinue use of the device. Most likely a substituted device will not match the printed serial number of the device.

If a device has been substituted, and the merchant believes the substituted device has a forged serial number that matches the serial number that should be in the P2PE Manager, the merchant should log into the P2PE Manager, find the serial number of the device, and change the state of the device to TAMPERED.

If the suspected substituted device has replaced the merchant's working device, then the working device that was stolen in the swap will not be able to process P2PE transactions in Forte's P2PE solution. If the substituted device turns out to be a modified and/or tampered version of the actual device owned by the merchant, then this will ensure that the device will not be able to process P2PE transactions in Forte's P2PE solution. If a device is marked to TAMPERED, a Forte representative will contact the merchant, but the merchant may still initiate the contact via the contact information found in Section 1.2.

Substituted devices should never be returned to service. At the discretion of the merchant, the device should either be sent to Forte to coordinate a validated destruction of the device, or the device can be sent to a PCI forensic auditor for inspection. For either destruction or PCI forensic inspection, please coordinate via the contact information found in Section 1.2. In either shipping scenario, the devices should be shipped in accordance with the guidance in Section 5.1.

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

Please make sure that device receiving instructions in Section 5 were properly followed before installing a device. Devices that do not follow the tamper inspection, logging and activation process detailed in Section 5 will not work properly when deployed in the field.

Specific steps for activating a device within P2PE Manager can be found in your Bluefin P2PE Manager User Guide or via the following video link: https://vimeo.com/182772442/30b87f999e

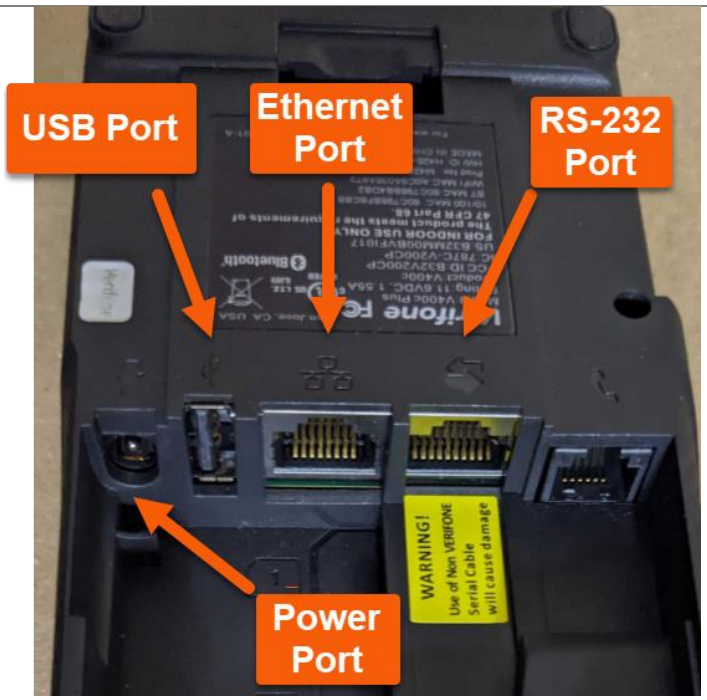
Device Configurations

Devices come preconfigured to specific hardened security guidelines that meet P2PE governance requirements. These configuration parameters are digitally signed to confirm authenticity and ensure that security risks are minimized. As part of the secure terminal configuration, SRED (secure reading and exchange of data) is enabled and enforced for all payment card capture mechanisms prior to being serviced at the secure key injection facility and before deployment to the merchant and may not be disabled at any time.

Before you can start testing with the V400C Plus, ensure you've completed the following steps:

NOTE: All accessories except for the Ethernet cable should be ordered from Forte's Equipment page.

The following image displays the ports for each cable and connector.



Connect to the Internet

The V400C Plus can connect to the internet via the following methods.

Ethernet Cable

1. Plug in the terminal's power cable.
2. Plug in the Ethernet cable to the Ethernet port on the device. NOTE: Do not use a phone cord.
3. Press 1-5-9 at the same time.
4. Select Control Panel > Sysmode.
5. Select the Supervisor option.
6. Enter the 7-digit password and hit the green O key. NOTE: Please reach out to our integration team at EquipmentQuestions@forte.net or 866-290-5400 (select option 5 for the Tech Support Queue then option 4 for the Equipment Queue) if you require assistance with the password.
7. Select Administration and from the next set of options, select Communications.
8. From the next set of options, select Communications.
9. Select Ethernet > eth0.
10. Switch between DHCP or Static using the Mode option, if required. NOTE: In Static mode, while entering IP addresses, use the # key to enter dots in the IP.
11. Change AutoStart to On.
12. Tap the red -{ }- in the upper right corner to change to a yellow/green -{ }-, if it is not already displaying a yellow/green -{ }-.
13. Once you have made the changes use the << button on the top left corner and hit No for the “Configure another interface?” popup.
14. Hit << until you get to the Main (Prod) menu and choose Exit and Reboot

Wi-Fi

1. Plug in the terminal's power cord.
2. Press **1**-**5**-**9** at the same time
3. Select **Control Panel** > **Sysmode**.

4. Select the **Supervisor** option.
5. Enter the 7-digit password and hit the green **O** key. **NOTE:** Please reach out to our integration team at EquipmentQuestions@forte.net or 866-290-5400 (select option 5 for the Tech Support Queue then option 4 for the Equipment Queue), if you require assistance with the password.
6. Select **Administration** and from the next set of options, select **Communications**.
7. Choose **Wi-Fi** > **Wi-Fi Scan**. If you get a prompt to turn on Wi-Fi, hit **OK**.
8. The device will scan and display available Wi-Fi networks.
9. Choose your network and hit **OK** on the "Network Saved" popup.
10. Press **<<** in upper left corner.
11. Tap **Wi-Fi Configuration** and enter the Wi-Fi password in the box labelled **PSK**. Use the # key to switch between lowercase, uppercase, and numbers. Use the ***** key for comma (,) and quotes (' "). Use the **0** key for all other special characters.
12. Press the green **O** key to ensure the submitted password is correctly stored on the same screen.
13. Press **<<** in the upper left corner.
14. Tap on **Wi-Fi Interface Ipv4**.
15. Switch between **DHCP** or **Static** using the **Mode** option (if required).
16. Change **AutoStart** to **On**.
17. Tap the red **-{ }-** in the upper right corner from the **Status** field and tap **OK** when asked "Do you want to save changes?"
18. It should change to a yellow/green **-{ }-**.
19. Tap **<<** in the upper left corner four times.
20. Tap **Exit** and **Reboot**.

Support

For assistance with your V400C Plus integration, reach out to our Integration Team at EquipmentQuestions@forte.net or 866-290-5400 (select option 5 for the Tech Support Queue then option 4 for the Equipment Queue)

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

The following guidance in this section represents best practices that merchants can follow. Merchants may utilize comparable measures adapted to their deployment environments to ensure safe storage and usage of their POI devices

Guidance for countertop/cabled devices

Devices should be placed in a low access yet high visibility area. For example, in a retail environment, the unit should be placed on the counter where it can be observed, but not so close to the customers where the customer could gain easy access to manipulate the device without supervision. For a call center type environment, the device should be placed on a desk where it is not obstructed by desktop clutter and should not be placed in such a manner where people other than the individual responsible for the device can get convenient access to the POI device.

Merchants should take steps to ensure a level of protection with their devices when left unattended for long periods of time. Methods could include, but are not limited to, securing corded devices via their cords, securing devices via mounting guidelines provided by the manufacturer, locking up the POI separately in the evenings, or ensuring the devices remain under video monitoring.

Select an installation location appropriate to the device and with protection measures in mind:

- Control public access to devices such that device access is limited to only parts of the device a person is expected to use to complete a transaction (for example, PIN pad and card reader).
- Locate devices so they can be observed/monitored by authorized personnel—for example, during daily store checks of the devices performed by store/security staff.
- Locate devices in an environment that deters compromise attempts—for example, through lighting, access paths, visible security measures, etc.
- Position the terminal on the check-stand in such a way as to make visual observation of the PIN-entry process infeasible. Examples include:
    1. Visual shields designed into the check-stand. The shields may be solely for shielding purposes or may be part of the general check-stand design.
    2. Position the PIN Entry Device (device) so that it is angled in such a way that PIN spying is difficult. Installing device on an adjustable stand that allows consumers to swivel the terminal sideways and/or tilt it forwards/backwards to a position that makes visual observation of the PIN-entry process difficult.
- Position in-store security cameras so that the PIN-entry keypad is not visible.
- Devices should be placed such that they allow handling only by authorized personnel who initiate transactions. For example, in a retail environment the unit should be placed on the counter where it can be observed, but not so close to the customers where the customer could gain easy access to manipulate the device without supervision.
- Authorized personnel should complete daily checks of the device to look for indications of tampering to restrict access to any part of the device that is not required for public use such as
- cables, power cords or access panels.

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

The following guidance in this section represents best practices that merchants can follow. Merchants may utilize comparable measures adapted to their deployment environments to ensure safe storage and usage of their POI devices.

Guidance for countertop/cabled devices

Please note that modification to the device such as attachment of adhesives, cable locks, or other add-on hardware, while not banned by the P2PE specifications, can have negative impacts when conducting tamper evidence inspections. Merchants should be cognizant of the impact of anything attached to the main unit of their POI device when performing a visual inspection.

Merchants can explore using cable lock systems, or even cable staples/fasteners to ensure that the device is not easily pulled free. Many POI device manufacturers provide mounting instructions or even mounting hardware to secure the device to a stationary object such as a counter or desk. The use of a system like this does not modify the device or in any way impede visual inspection.

Merchants should physically secure devices when not deployed or being used. Including devices:

- Undergoing repair or maintenance while in the merchant's possession.
- Awaiting deployment.
- Awaiting transport between sites/locations.

Merchants should prevent unauthorized physical access to devices undergoing repair or maintenance while in their possession, to include the following:

- Verify the identity and authorization of repair personnel.
- All repair personnel must be verified and authorized prior to granting access.
- Unexpected personnel must be denied access unless fully validated and authorized.

5. POI Device Transit

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

After receipt of the device, if the merchant is shipping the devices between multiple locations, the following practices should be followed.

If the POI device is still in the original packaging and the device is still in the unopened tamper evident bag, then the merchant may place that device in its original packaging into another shipment box and ship it to another location under the control of the merchant.

The P2PE Manager should be updated by the merchant to show the new intended location of the device. The device should only be addressed to the person associated as the contact for the merchant location as found in the P2PE Manager.

If the device has been logged into the P2PE Manager already, the status of the device should be set to STORED. This will ensure that during transit and subsequent storage at the new merchant location, the device will be ineligible to run transactions. If the device has not been logged in and activated in the P2PE Manager, the device can be logged as received at the new location by the authorized contact at the new merchant location.

Merchants, for their own validation processes, should use only trusted couriers (such as FedEx, UPS, etc.) and document the tracking number for the shipment. That tracking number should be conveyed to the specific recipient at the new merchant location via a separate communication method such as email or phone.

If the POI device has been removed from the tamper evident packaging, then the merchant should obtain new tamper evident packaging. New tamper evident packaging can either be independently obtained by the merchant or tamper evident packing can be requested from CSG Forte.

The merchant should place the device in the tamper evident packaging and record the serial number of the tamper evident packaging.

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

Validating device shipments from merchants back to Forte

If a merchant needs to return a device back to Forte, the merchant will need to contact CSG Forte via the contact information found in Section 1.2 of this document.

The CSG Forte representative will then coordinate the shipment of the device back to the appropriate location.

6. POI Device Tamper & Modification Guidance

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

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

Inspection Frequency

Devices deployed in retail or customer service environments should be inspected periodically, but no less then annually. The merchant should keep their own logs that detail the inspection date and the individual responsible for the inspection. These logs are for the merchant's own record keeping which will help in determining whether a device has been tampered with.

Inspection procedures for un-deployed devices

Devices should be logged into the P2PE Manager upon receipt. However, if a device will be stored upon receipt, best practice would be to leave the device in the tamper evident bag. The tamper evident packaging should be checked for signs of forced entry before deployment in the field.

Inspection procedures for deployed devices

Devices should be visually inspected for evidence of tampering or substitution. When inspecting a device, a merchant should confirm the serial number of the device and make sure it's logged in the P2PE Manager appropriately.

Check for missing or altered seals or screws, extraneous wiring, holes in the device, or the addition of labels or other covering materials that could be used to mask damage from device tampering.

Monitor devices in remote or unattended locations (for example, via the use of video surveillance or other physical mechanisms to alert personnel).

If anything, suspicious is detected, the device should not be used.

The PCI provided document entitled Skimming Prevention: Best Practices for Merchants, available at www.pcisecuritystandards.org, is a good document to reference in every inspection.

6.2 Instructions for responding to evidence of POI device tampering

Evaluating a device for evidence of tampering upon receipt of shipment

For all devices that are received from Forte's KIF, please see the information in Section 2.2 for detailed inspection guidance when reviewing the shipment at the merchant location.

If the devices come in any packaging other than described in Section 2.2, if the tamper evident packaging appears to have been opened, if the device does not match the photos in the inspection guide, the devices appear to have been damaged or altered, and/or if the serial numbers do not match when entered into P2PE Manager, do not deploy the device. See the detailed instructions on removing the device and notifying Bluefin at the bottom of this section.

Revisit Section 6.1 for more detailed inspection instructions.

Evaluating a device in the field for evidence of tampering

If during a scheduled inspection or observed during use of the product the device appears to be physically tampered with or substituted, the device should immediately be pulled from use. Please see the detailed instructions on removing the device and notifying Bluefin at the bottom of this section.

Dealing with a tampered device

If the merchant feels that they have observed visual signs or device activity that they believe may indicate tampering with the device, the merchant can log into the P2PE Manager, identify the device in inventory by the device serial number and change the status of the device to TAMPERED.

This status change will do two things. First, it will send a notification email to CSG Forte that a device and its output needs to be reviewed. Second, it will disable the device from processing through CSG Forte. A CSG Forte representative will contact the merchant to follow up regarding the device.

Merchants may also contact CSG Forte via the contact information provided in Section 1.2 of this document.

Please note that if the device has not been logged into P2PE Manager, contact CSG Forte as soon as possible.

7. Device Encryption Issues

7.1 Instructions for responding to POI device encryption failures

If the merchant is getting an encryption failure reported by the device, it must be reported to CSG Forte technical support. No further transactions will be authorized from the affected device, and it must be removed from service. The terminal must be updated in P2PE Manager with a status of 'Repair'. If CSG Forte technical support can resolve the encryption issue, the device can be re-enabled in P2PE Manager. Otherwise, a replacement device will be ordered by CSG Forte technical support.

8. POI Device Troubleshooting

8.1 Instructions for troubleshooting a POI device

If your V400c Plus malfunctions in any way, including:

- Can't process transactions (regardless of actual error)
- Receipt issues
- Reporting issues

Please contact CSG Forte technical support at 866-290-5400, option 5, then option 3.

9. Additional Guidance

9.1 Instructions for troubleshooting a POI device

For assistance with your V400C Plus integration, reach out to our Integration Team at EquipmentQuestions@forte.net or 866-290-5400 (select option 5 for the Tech Support Queue then option 4 for the Equipment Queue)

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

Hardware version

The product hardware version (HW ID) is printed on the label at the back side of the device; see Figure 4. The label should not be torn off, covered, or manipulated in any way.

Figure 4: Hardware identification

Firmware version

The firmware versions can be retrieved from the boot splash screen. Shortly after powering up, a splash screen displays the version number for the four security kernels; see Figure 5 and Figure 6. You must be able to find these numbers on the list of Approved PIN Transaction Security (PTS) Devices. If these numbers do not match, notify your service provider immediately.

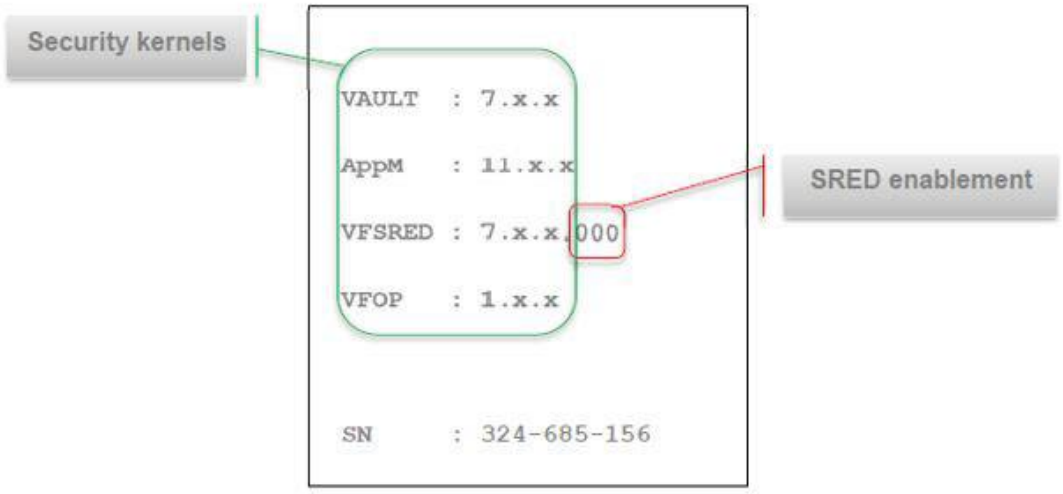


Figure 5: A boot splash screen displays the version number for the four security kernels

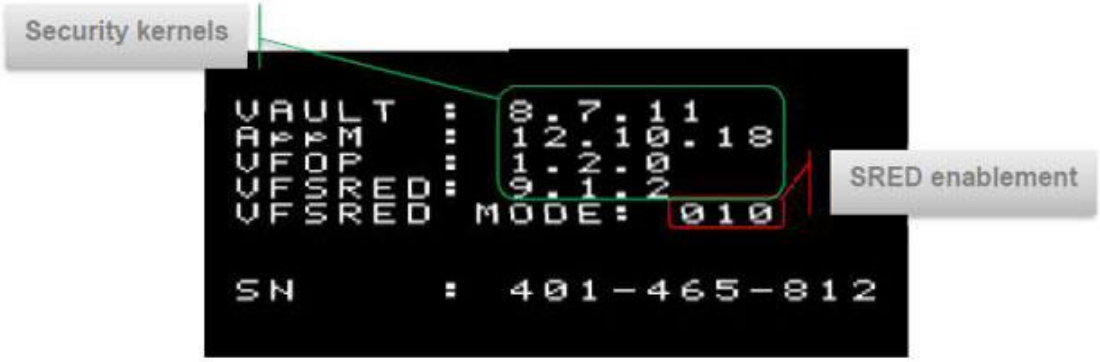


Figure 6: A boot splash screen displays the version number for the four security kernels

Application version

Application Version can be retrieved by clicking the **?** symbol on home screen it opens new screen where you can see the application version.

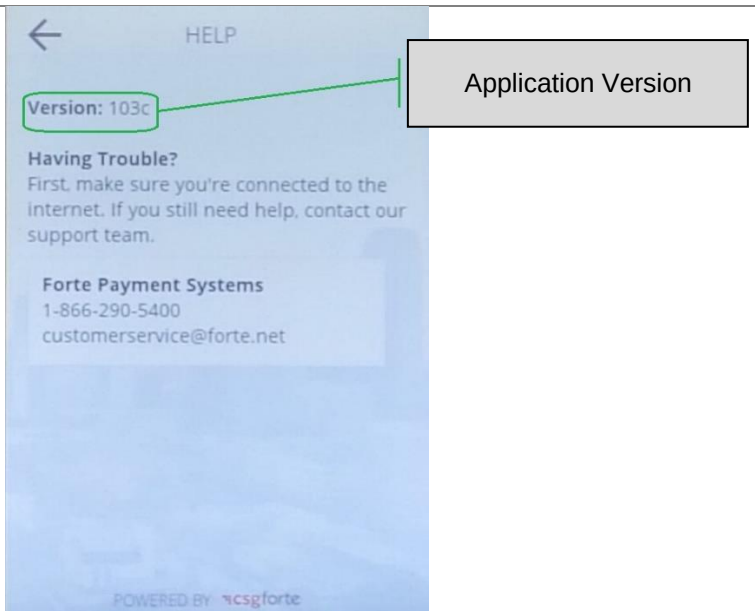


Figure 7: The application version

XPI Version

When the terminal is booting it will come to a screen that says “Initializing Please Wait ##.##.##.##-### “. The ##.##.##.##-### is the XPI version.

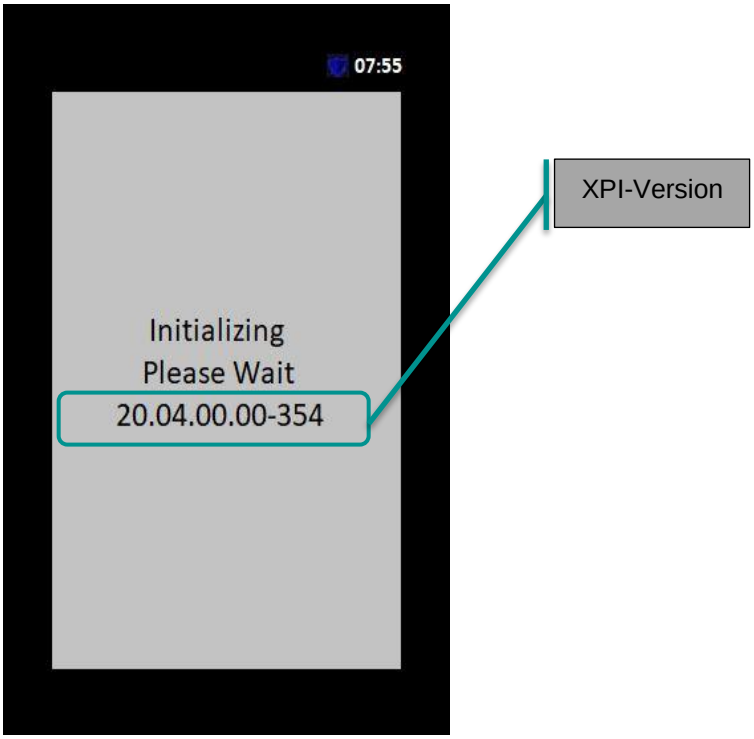


Figure 8: The XPI version