

Verifone Confidential



Suite – Bypass 3.06.XX



Verifone®, Inc.

88 West Plumeria Drive

San Jose, CA 95134

Telephone: 408-232-7800

<http://www.Verifone.com>

Printed in the United States of America.

© 2018 Verifone, Inc. All rights reserved.

This document is confidential to Verifone and may not be disclosed to any party without the express prior written consent of Verifone. No part of this document may be reproduced, copied or distributed in any form or by any means - graphic, electronic, or mechanical, including photocopying, taping, or information storage and retrieval systems - without the express prior written consent of Verifone.

The contents of this document are subject to change without notice.

Verifone is a registered trademark of Verifone, Inc. Commander Site Controller is a trademark of Verifone. All other brand names and trademarks mentioned in this document are the properties of their respective holders.

NOTICE

THE INFORMATION IN THIS DOCUMENT IS FOR INFORMATIONAL PURPOSES ONLY. VERIFONE MAKES NO REPRESENTATION OR WARRANTY OF ANY KIND AS TO THE ACCURACY OR THE COMPLETENESS OF THE INFORMATION CONTAINED HEREIN. THIS DOCUMENT IS SUPPLIED "AS-IS," WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OF THIRD PARTY RIGHTS. YOU ACKNOWLEDGE AND AGREE THAT THIS INFORMATION IS PROVIDED TO YOU ON THE CONDITION THAT NEITHER VERIFONE NOR ANY OF ITS AFFILIATES OR REPRESENTATIVES WILL HAVE ANY LIABILITY IN RESPECT OF, OR AS A RESULT OF, THE USE OF THIS INFORMATION. IN ADDITION, YOU ACKNOWLEDGE AND AGREE THAT YOU ARE SOLELY RESPONSIBLE FOR MAKING YOUR OWN DECISIONS BASED ON THE INFORMATION HEREIN. WITHOUT LIMITING THE GENERALITY OF THE FOREGOING, IN NO EVENT SHALL VERIFONE BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, INCLUDING DAMAGES FOR LOSS OF BUSINESS, PROFITS, TRANSACTIONS, OR THE LIKE, EVEN IF VERIFONE OR ITS REPRESENTATIVES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Nothing herein shall be construed as limiting or reducing your obligations to comply with any applicable laws, regulations or industry standards relating to security or otherwise including, but not limited to, PA-DSS and PCI DSS.

The retailer may undertake activities that may affect compliance. For this reason, Verifone is required to be specific to only the standard software provided by it.

Table of Contents

About this Document	4
Revision Information	5
Executive Summary	8
Application Summary	9
Typical Commander Network Implementation	12
Dataflow Diagram	15
Difference between PCI Compliance and PA-DSS Validation	19
Considerations for the Implementation of Payment Applications in a PCI-Compliant Environment.....	21
Remove Historical Sensitive Authentication Data (PA-DSS 1.1.4)	21
Handling of Sensitive Authentication Data (PA-DSS 1.1.5).....	21
Secure Deletion of Cardholder Data (PA-DSS 2.1).....	22
All PAN is Masked by Default (PA-DSS 2.2)	22
Cardholder Data Encryption Key Management (PA-DSS 2.3, 2.4, and 2.5).....	22
Removal of Historical Cryptographic material (PA-DSS 2.6).....	25
Set up Strong Access Controls (PA-DSS 3.1 and 3.2)	25
Properly Train and Monitor Admin Personnel (PA-DSS 3.4)	26
Log settings must be compliant (PA-DSS 4.1, 4.4).....	26
PCI-Compliant Wireless settings (PA-DSS 6.1, 6.2 and 6.3).....	27
Services and Protocols (PA-DSS 8.2).....	28
Never store cardholder data on internet-accessible systems (PA-DSS 9.1)	28
PCI-Compliant Remote Access (10.1)	28
PCI-Compliant Delivery of Updates (PA-DSS 10.2.1)	29
PCI-Compliant Remote Access (10.2.3)	30
Data Transport Encryption (PA-DSS 11.1)	31
PCI-Compliant Use of End User Messaging Technologies (PA-DSS 11.2)	31
Non-console administration and Multi-Factor Authentication (PA-DSS 12.1, 12.2)	31
Network Segmentation	34
Maintain an Information Security Program	34
Application System Configuration.....	34
Payment Application Initial Setup & Configuration	35

About this Document

This document describes the steps that must be followed in order for your installations to comply with Payment Application – Data Security Standards (PA-DSS). The information in this document is based on PCI Security Standards Council Payment Application Data Security Standards program (version 3.2 dated May, 2016)¹.

Verifone instructs and advises its customers to deploy Verifone applications in a manner that adheres to the PCI Data Security Standard (v3.2). Subsequent to this, best practices and hardening methods, such as those referenced by the Center for Internet Security (CIS) and their various “Benchmarks”, should be followed in order to enhance system logging, reduce the chance of intrusion and increase the ability to detect intrusion, as well as other general recommendations to secure networking environments. Such methods include, but are not limited to, enabling operating system auditing subsystems, system logging of individual servers to a centralized logging server, the disabling of infrequently-used or frequently vulnerable networking protocols and the implementation of certificate-based protocols for access to servers by users and vendors.

While you must follow the steps outlined in this *Implementation Guide* in order for your installation to support your PCI DSS compliance efforts, following these steps does not result in PCI-DSS certification. That must be performed by an authorized PCI-DSS QSA.

¹ PCI [PA-DSS 3.2](#) can be downloaded from the PCI SSC Document Library.

Revision Information

Rev	Date	Description	Changed By
1.0	11/28/12	Initial version.	David C. Brown
1.1	02/28/14	Revised for Application Independence Applications Reviewed: BUYPASS 2.00 BUYPASS Valero 2.00 BUYPASS Exxon Mobil 1.00 BUYPASS Sunoco 1.00	Steven K. Shapiro
1.2	5/02/14	Revised for Application Independence Applications Reviewed: BUYPASS 2.01 BUYPASS Valero 2.01 BUYPASS Exxon Mobil 1.01 BUYPASS Sunoco 1.00	Steven K. Shapiro
1.3	7/8/14	ASA Routed Network Diagram duplicated. Replaced duplicate with the Franchised Network Diagram Additional descriptive text for network diagrams Replaced "Payment Controller (PMC)" with "Payment Controller (Viper)"	Steven K. Shapiro
1.4	10/16/14	Integrated both the Viper/EPS and Commander implementation documents into a single document	Steven K. Shapiro
1.5	11/21/14	Updates from reviewers List additional applicable application names	Steven K. Shapiro
3.0	01/14/15	Revisions for PA-DSS 3.0	Steven K. Shapiro
3.1	08/13/15	Ongoing Revisions for PA-DSS 3.1	Edward J Kelb
3.2	12/08/15	Applications Submitted for Dec 2015 Review: Suite - BP 1.06 Suite - BUYPASS 2.08 Suite - CITGO 1.03 Suite - Heartland 1.02 Suite - Marathon 1.02 Suite - NBS 1.03 Suite - Worldpay 1.03	Edward J Kelb
3.3	04/30/16	Applications Submitted for Apr 2016 Validations: Suite - BP 1.09 Suite - BUYPASS 3.02 Suite - Heartland 1.05 Suite - NTS-VAPS 1.02 Suite - Shell 2.01 FDCPAK 8.01 HPSPAK 5.00 MARPAK8.00	Edward J Kelb

3.4	07/06/16	Legal Banner Updates, miscellaneous cleanup	Edward J Kelb
3.5	07/18.16	Applications Submitted for Apr 2016 Validations: Suite – Chevron 1.06 Suite – Phillips66 1.07 NBSPAK 5.00 WPYPAK 6.02	Edward J Kelb
3.6	07/30/16	Commander and Sapphire Documentation Split	Edward J Kelb
3.7	08/10/16	ToC and Properties Corrections	Edward J Kelb
3.8	02/23/17	Applications Submitted for Feb 2017 Validations: NBS 2.00	Edward J Kelb
3.9	08/06/17	Application Submitted for July PA-DSS Validation	Edward J Kelb
3.10	8/11/17	Versioning Information Added	Edward J Kelb
4.0	11/29/17	PA-DSS 3.2 IG Updates	Edward J Kelb


Note: This PA-DSS Implementation Guide must be reviewed on a yearly basis, whenever the underlying application changes or whenever the PA-DSS requirements change. Updates should be tracked and reasonable accommodations should be made to distribute or make the updated guide available to users. Verifone will distribute this Implementation Guide to customer and Verifone Authorized Service Contractors (VASC) via the Verifone internet portal. VASCs must provide a copy of this document to the merchant for whom the payment system was installed.

Glossary of Terms

Viper	Payment Controller
Ruby, Ruby 2	POS Terminal
Ruby CI	Integrated POS Terminal and Payment Controller
Sapphire	Hardware platform to support the Store, Payment and Forecourt controller applications
Topaz	POS Terminal
Commander Site Controller	Hardware platform to support the Store, Payment, and Forecourt controller applications
Forecourt Controller	Software application to control / interface to the DCRs, Carwash, Price Sign, and other devices outside of the store.
Core Services	Application to control store-wide services as well as in-store devices.
Payment Controller	Software application to interface payments between the site and the financial host

Executive Summary

The identified Payment Applications have been Payment Application - Data Security Standard (PA-DSS) validated, in accordance with PA-DSS Version 3.2. For the PA-DSS assessment, we worked with the following PCI SSC approved Payment Application Qualified Security Assessor (PA-QSA):

	Coalfire Systems, Inc. 11000 Westmoor Circle, Suite 450 Westminster, CO 80021	Coalfire Systems, Inc. 1633 Westlake Ave N #100 Seattle, WA 98109
---	---	---

This document also explains the Payment Card Industry (PCI) initiative and the Payment Application Data Security Standard (PA-DSS) guidelines. The document then provides specific installation, configuration, and ongoing management best practices for using the Verifone Payment Application as a PA-DSS validated Application operating in a PCI DSS Compliant environment.

PCI Security Standards Council Reference Documents

The following documents provide additional detail surrounding the PCI SSC and related security programs (PA-DSS, PCI DSS, etc.):

- Payment Card Industry Payment Applications - Data Security Standard (PCI PA-DSS)
https://www.pcisecuritystandards.org/security_standards/index.php
- Payment Card Industry Data Security Standard (PCI DSS)
https://www.pcisecuritystandards.org/security_standards/index.php
- Open Web Application Security Project (OWASP)
<http://www.owasp.org>
- Center for Internet Security (CIS) Benchmarks (used for OS Hardening)
<https://benchmarks.cisecurity.org/downloads/multiform/>

Application Summary

Payment Application Name:	Verifone Payment Controller with POS Application																													
Payment Application Version:	Suite – Buypass 3.06.XX																													
Application Description:	The Verifone Payment Controller with POS Application manages the card swipe and PIN data from both the Forecourt and free-standing PIN-pad devices associated with fueling positions and POS devices, respectively. The Payment Controller (aka Viper) is the sole custodian of cardholder data. In addition, the Verifone Payment Controller with POS Application supports the Topaz, Ruby2, Ruby CI, and Smart Fuel Controller; provides reporting of sales totals, configuration of peripheral devices, price book, POS users and application users. It provides logging to a secured log server and utilizes an associated Verifone Zone Router to segment and secure Verifone Payment Application components.																													
Target Market for Payment Application:	<div>The Verifone Payment Controller with POS Application is designed to support the retail convenience store and petroleum market.</div> <table><tr><th colspan="6">Target Market for Payment Application (check all that apply):</th></tr><tr><td>X</td><td>Retail</td><td></td><td>Processors</td><td>X</td><td>Gas/Oil</td></tr><tr><td></td><td>e-Commerce</td><td>X</td><td>Small/medium merchants</td><td></td><td></td></tr><tr><td>X</td><td colspan="5">Others (please specify): Petroleum Industry</td></tr></table>						Target Market for Payment Application (check all that apply):						X	Retail		Processors	X	Gas/Oil		e-Commerce	X	Small/medium merchants			X	Others (please specify): Petroleum Industry				
Target Market for Payment Application (check all that apply):																														
X	Retail		Processors	X	Gas/Oil																									
	e-Commerce	X	Small/medium merchants																											
X	Others (please specify): Petroleum Industry																													
Stored Cardholder Data:	<div>The only files containing CHD are the STAN files.</div> <div>The system will store both the Track1 and Track2 data until we can send it to the host. Once we know that the host has received the track data the system will delete the track data. The PAN and the expiration date are kept in the encrypted STAN files on the system, for reporting purposes, for a configurable number of days and defaults to 15 days. While there is no specific limit for this value, the amount of log data retained is limited to the available space on the compact flash. Any access to STAN files requires Secure User privileges and is logged to SYSLOG files.</div>																													
Components of Application Suite (i.e. POS, Back Office, etc.)	<div>The Commander Suite consists of controller applications (Payment Controller, Forecourt Controller, Store Controller and Core Services) that get deployed on Commander / Ruby CI, the POS application that gets deployed on Topaz / Ruby 2 terminals, and Site Management Suite tools that get deployed on customer provided PCs.</div> <div>The Site Management Suite is an application that is installed on a customer-supplied PC and provides configuration for Topaz and Ruby2 POS. (PAN and similar data is unavailable by default from the exported data.)</div> <div>Configuration for the Viper Payment Controller is available over a secure HTTP connection to properly credentialed users via web browser.</div>																													

	Verifone also has a list of certified back office partners to manage reporting, inventory forecasting, etc. These data are managed via secure http requests from the back office software installed on a customer-supplied computer.
Required Third Party Payment Application Software:	The Verifone Payment Controller with POS Application is a complete integrated solution. When Viper is released as a stand-alone entity, the site would be responsible for providing a compatible POS system (which would itself need to be PA-DSS validated by the vendor).
Database Software Supported:	Non-payment applications use an embedded database that is not accessible or available outside of the application. The payment controller itself does not use a database.
Other Required Third Party Software:	A web browser is highly desirable but not required.
Operating System(s) Supported:	The operating system is integrated as part of the application suite and root file system. The application uses Linux version 3.2, compiled with GRSecurity enabled. Site Management Suite (SMS) installs on a PC with Windows 7, Windows 8 or Windows 10.
Application Authentication	For the payment application itself, there is only one means to access sensitive data and that is with the secured user's credentials. Strong passwords are required for all application user access. All default passwords are inactive upon installation and must be changed with the first log in. Password expiration is enforced. Passwords are never retained as clear text. POS application users have a separate set of passwords as they have no access to the secured data. POS application users have a different (and smaller) set of privileges. Lastly, administrative access for the purpose of field support is controlled by two factor authentication involving a temporary access token generated by the site controller in conjunction with a password entered over a secured shell session. A remote user cannot initiate administrative access without intervention from someone at the site. The temporary access token is generated when someone at the site either enables login through the web interface or flips the mechanical login switch on the site controller. This administrative access has no means to decrypt sensitive data and all activity is forwarded to a security log server.
Application Encryption	The Payment Controller (Viper) maintains the encryption information for any sensitive data that needs to be saved in the course of processing the request. Data is expired and deleted after a maximum time period is reached, unless a lower expiration time is configured by the merchant. Payment from the forecourt is handled in a similar manner with card and PIN data obtained from the forecourt devices via the Forecourt Controller (FCC.)

Application Functionality Supported	<input type="checkbox"/>	POS Suite	<input type="checkbox"/>	POS Admin	<input type="checkbox"/>	Shopping Cart & Store Front
	<input type="checkbox"/>	POS Face-To-Face	<input type="checkbox"/>	Payment Middleware	<input checked="" type="checkbox"/>	Automated Fuel Dispenser
	<input type="checkbox"/>	POS Kiosk	<input type="checkbox"/>	Payment Back Office	<input type="checkbox"/>	Other: Forecourt payment and controller
	<input type="checkbox"/>	POS Specialized	<input type="checkbox"/>	Payment Gateway/Switch		
Payment Processing Connections:	<p>Payment card processing conforms to the IFSF standard. For a POS transaction all card processing is handled by the customer-facing PIN-pad (POP). The POS places a card request with the Payment Controller (Viper) application. (The Magnetic Stripe Reader (MSR) on the PIN pad is NEVER sampled for card data.) The Payment Controller (Viper) obtains the card information from the Point of Purchase (POP) device associated with the requesting POS. The Payment Controller (Viper) then utilizes a dedicated network interface (NIC) to communicate with the payment network host. The Payment Controller (Viper) drives prompts to both the POP and the POS indicating the status of the transaction.</p>					
Description of Versioning Methodology:	<p>Versioning is based off an application suite. Suites are further assembled from versioned software components.</p> <ol style="list-style-type: none"> 1. Verifone uses a three-tiered versioning methodology for its applications. 2. Version numbers contain three numbers, separated by periods. 3. The Verifone Payment Controller with POS Application versioning has three levels: <Major>.<Minor>.<Maintenance> 4. Major changes include a new product or a significant enhancement has been implemented for an existing product. These changes may also include defect corrections. These changes may or may not have an impact on PA-DSS requirements. 5. Minor changes include small changes such as minor enhancements or defect corrections. These changes may or may not have an impact on PA-DSS requirements. 6. Maintenance changes include defect corrections or roll ups and would have no negative impact on PA-DSS requirements and are indicated by the WILDCARD (XX). 7. Based on the above versioning methodology the application version being listed with the PCI SSC is: 3.06.XX 					
List of Resellers/Integrators:	All Verifone products are available from Verifone authorized service contractors as listed on the Verifone web site.					

Typical Commander Network Implementation

With a Commander Site Controller, the Core Services, Forecourt Controller, and the Payment Controller (Viper) all reside on the hardware within the Commander box

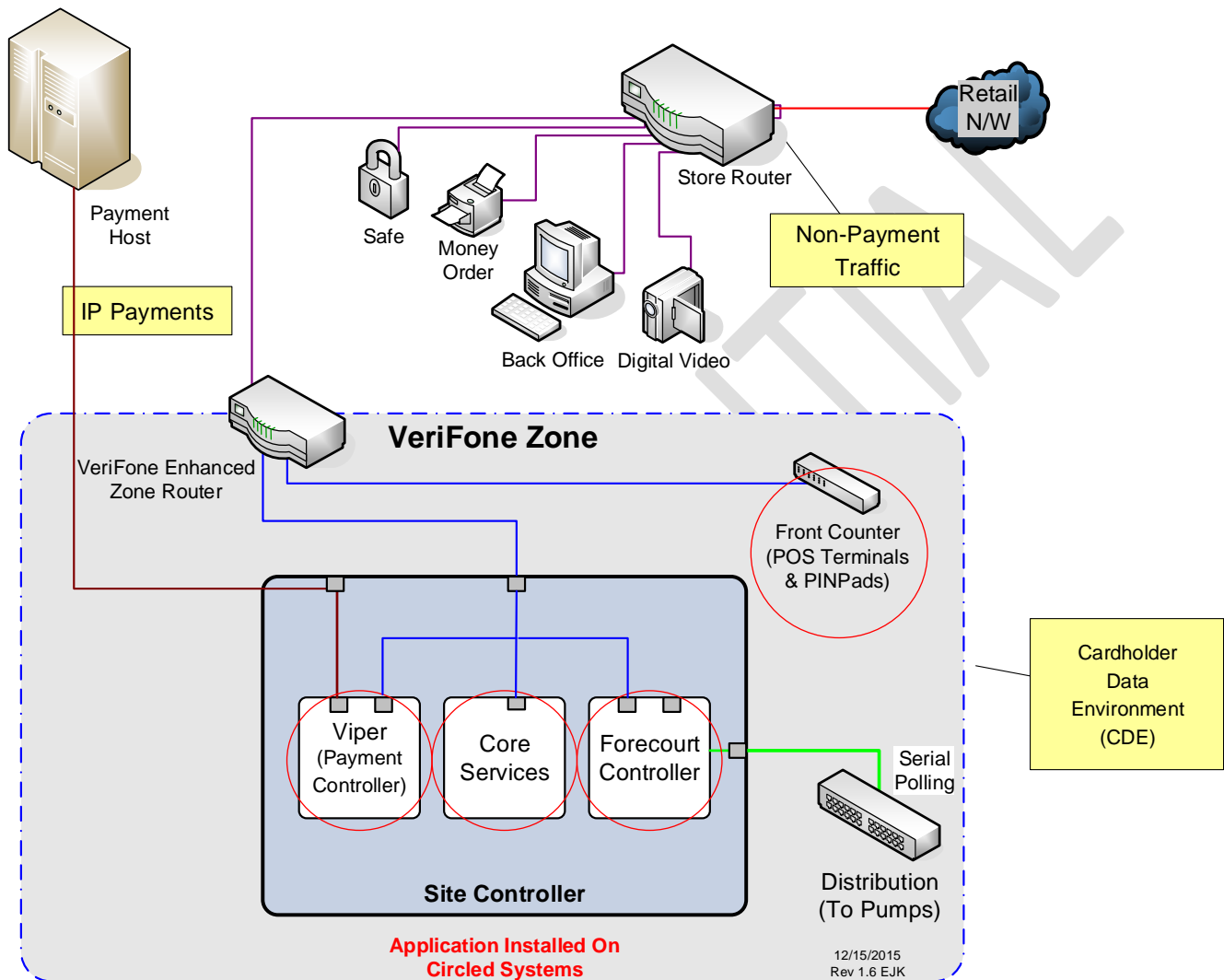
The following diagrams illustrate typical network implementations of the *Verifone Payment Controller with POS Application*. Topaz or Ruby POS terminals and PIN Pads are located at the Front Counter as depicted in the diagrams. The application is installed on the circled systems.

CONFIDENTIAL

Commander Network Diagrams

The following diagrams depict typical Commander network implementations.

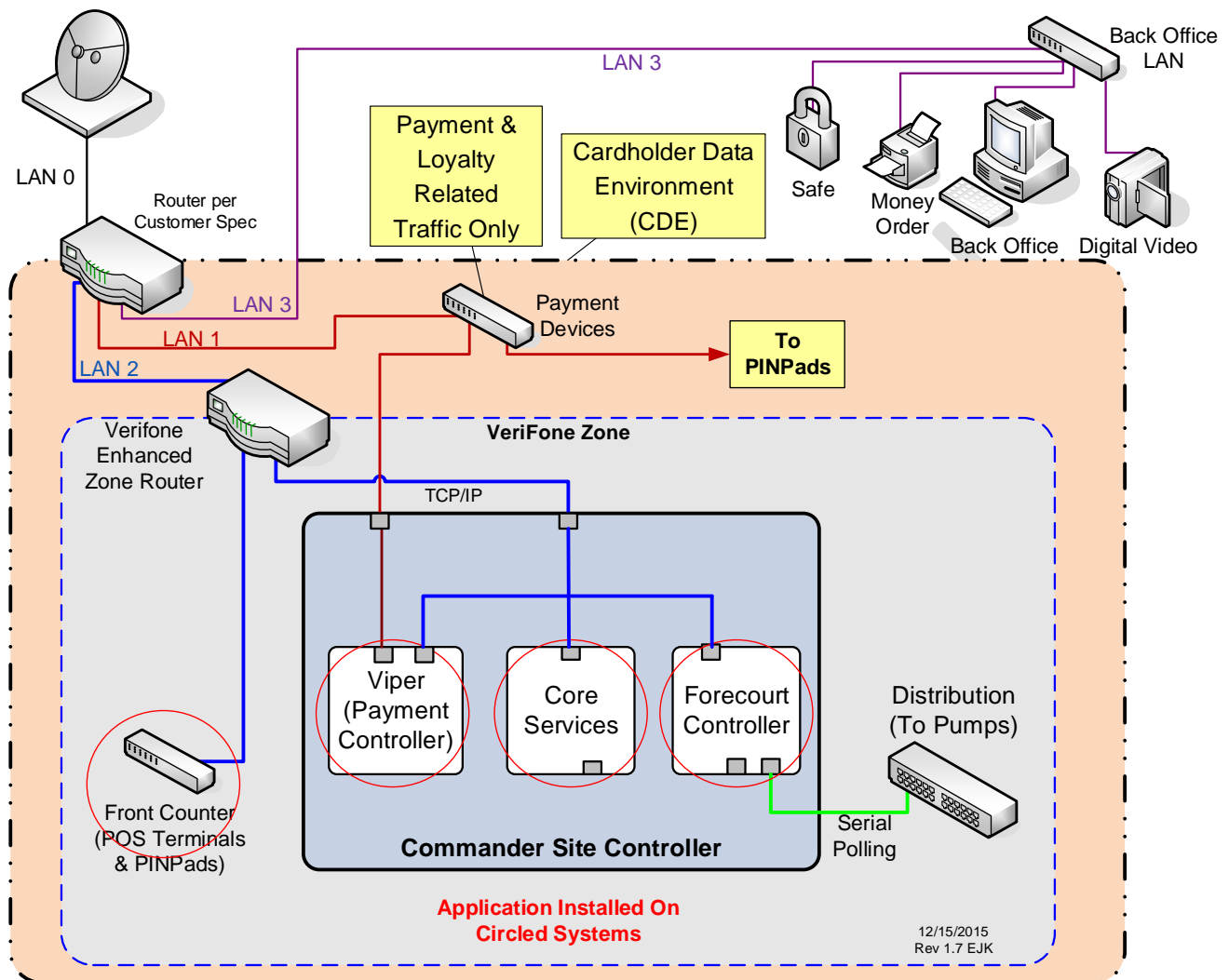
Commander Verifone Zone Routed Payments



From the text of the document:

- Front Counter: Topaz or Ruby POS Terminals and PINPads
- Payment Controller: Payment Processing and Cardholder Data Storage
- Core Services: Application to control store-wide services as well as in-store devices.
- Forecourt Controller: Manages the communications between the outdoor payment device and the customer

Commander Customer Routed Payments

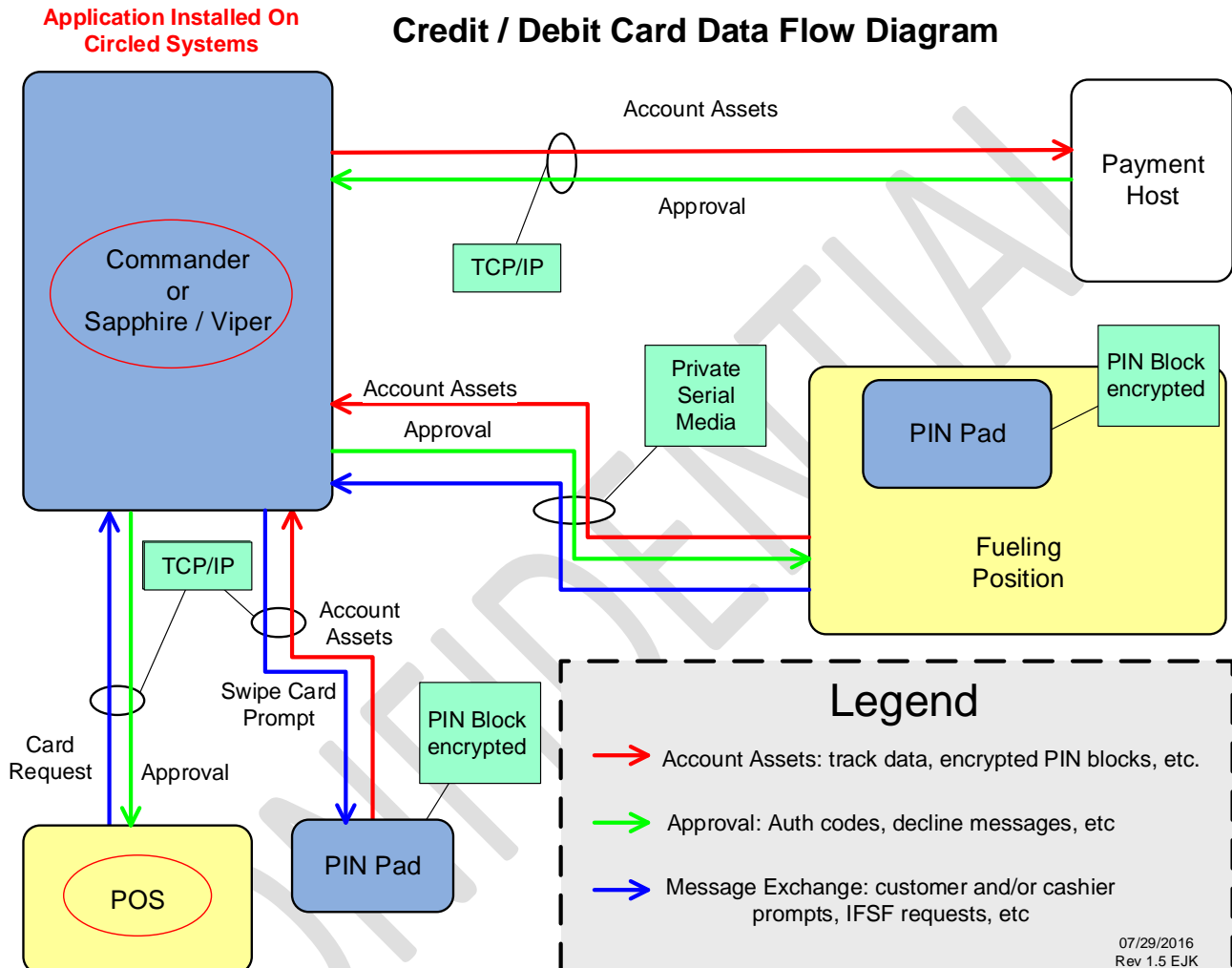


From the text of the document:

- Front Counter: Topaz or Ruby POS Terminals and PINPads
- Payment Controller: Payment Processing and Cardholder Data Storage
- Core Services: Application to control store-wide services as well as in-store devices.
- Forecourt Controller: Manages the communications between the outdoor payment device and the customer

Dataflow Diagram

The diagram below illustrates the data flow of a credit or debit card transaction as it occurs in the payment application. The application is installed on the circled systems.



From the text of the document:

- POS: Topaz or Ruby POS Terminals
- Commander or Sapphire / Viper: Contains the Viper Payment Controller, Core Services and Forecourt controller to manage the communications between the indoor and outdoor payment devices and the customer

The Data Flow Diagram above depicts an indoor payment scenario and an outdoor payment scenario.

In the following text, the term “Card Table Rules” indicate a set of parameters used by the Payment Controller (Viper) to process card payments for a particular host and card ISO, card type, card circuit, etc. These rules can be updated by the host, via Parameter Download (PDL) or similar mechanisms.

Indoor Payment:

- 1) The PINPad indicates the customer may swipe the credit card at any time by flashing LEDs along the swipe track (lane lights) or with instructions on the LCD display
- 2) When the cashier totals the sale and selects a credit or debit MOP the POS will make an IFSF Card Request to the Payment Controller (Viper).
- 3) The Payment Controller (Viper) will make an IFSF request to the PINPad for the card track data.
 - a. If the customer has already swiped the card the PINPad will send the data
 - b. Otherwise as soon as the customer swipes the data the PINPad will respond to the request.
 - c. The Payment Controller (Viper) will expire the request if no response is received according to a timeout value set in the card table rules.
 - d. The request will be retried if there is a card read error or timeout according to the number of retries set in the card table rules.
- 4) The PINPad supplies the card data to the Payment Controller (Viper).
 - a. If the card is determined to be debit, another request is issued to the PINPad for the encrypted PIN block.
 - b. If the card could be either debit or credit a request to prompt the customer for debit or credit is sent to the PINPad.
 - c. Depending on the customer response the Payment Controller (Viper) will prompt for the PIN as in 4.a above or it will proceed as a credit sale.
- 5) In the event repeated card reads fail the Payment Controller (Viper) will prompt the POS for manual account number entry. The manual prompt and number of card read failures are determined by the card table rules.
 - a. The Payment Controller (Viper) sends an IFSF device request to prompt the cashier for the account number and expiration date.
 - b. The cashier enters the data and presses an “OK” button on the POS dialog box.
 - c. The POS responds to the device request with the data for the Payment Controller (Viper) but does not in any case save that response to the file system, a database or any other persistent storage.
- 6) The Payment Controller (Viper) will then communicate with the payment host according to the protocols established by the payment network and the card table rules.
- 7) The status of the payment request is received from the payment network by the Payment Controller (Viper).
 - a. The transaction information is saved in an encrypted STAN file as described elsewhere in this document.
 - b. The Payment Controller (Viper) sends an IFSF message to the POS indicating success or failure of the request.
 - c. The Payment Controller (Viper) may provide further messaging to the customer via the PINPad if loyalty / rewards programs are active, etc.

- d. The POS will apply approval information, masked account numbers and other details in the “network body” portion of the receipt. (Masking is done within the Payment Controller (Viper) as part of the message to the POS.)
- 8) If the customer was approved for the full amount the POS will complete the sale and send the transaction information to the Core Services for archiving and updating report totals. This data does not contain any cardholder data.
- 9) If the card was declined or a balance remains due in the sale the POS will collect additional MOPs until the balance is satisfied and the completed sale is sent to the Core Services as in step 8 above.

Outdoor Payment:

- 1) Customer initiates an outdoor transaction either with a “card dip” event or by pressing a key according to prompts on the payment device.
- 2) The Forecourt Controller and the Payment Controller (Viper) then broker the exchanges between the outdoor payment device and the customer.
- 3) Communication to the outdoor payment devices is over a serial communications link conforming to the standards of the outdoor payment device vendor. Verifone Secure Pump Pay, Wayne, Gilbarco, Tokheim and Schlumberger devices are supported.
- 4) As with the PINPad transactions, the Payment Controller (Viper) will obtain the card track data and either prompt whether the customer desires a debit sale, prompt for the PIN information or process the card as a credit sale.
- 5) The Payment Controller (Viper) then communicates with the payment host.
 - a. If the sale was declined the Payment Controller (Viper) presents a message to the device via the FCC.
 - b. If the sale was approved the Payment Controller (Viper) presents the FCC with the authorization information and the FCC will arm the pump for the appropriate amount.
- 6) Once the sale is complete the FCC will print a receipt with the masked account numbers and other details in the “network body” of the receipt.
- 7) The FCC will send the completed transaction to the Core Services to archive the data and update the reporting. Only masked account numbers are archived.

NOTES:

Once the card data is obtained and validated the card type, circuit name, etc. are returned to the POS. Though the IFSF spec allows the PAN to be present in the response to the POS, the POS software ignores it. No PAN data is utilized by the POS. No application log messages contain the PAN data.

There may be several intermediate exchanges between the Payment Controller (Viper) and POS to process discounting programs keyed off the card type, card circuit name, or merchandise product code. Further, there may be partial payment responses and multiple cards tendering the transaction. Once these steps have been completed and the transaction is settled the Payment Controller (Viper) saves the authorization information, any required PAN data, etc. in an encrypted file (STAN file), one file per transaction. Each encryption key is unique.

Card data to the payment host includes all information required per their functional specifications –such as track data. The Front-End-Processing modules (FEP’s) are the same for both the Commander and Sapphire / Viper platforms. In particular, payment hosts that have certified the Viper Payment Controller with a device that provides the secure transmission to their systems but use RS-232 serial data connection to said device are

supported the same way with the Commander and Sapphire / Viper platforms. Traffic over this serial connection is clear text and the merchant must provide a secure location for those devices. Examples of such devices with the payment network are provided by Datawire (which provides a VPN connection from the device to the payment host) and Prysm (which uses secured sockets.)

If the merchant should require account numbers for network settlement purposes the Payment Controller (Viper) provides a report with that information. A connection is initiated to the Payment Controller (Viper) from a menu on the POS. A secure user ID with a complex password is required to be able to access that report.

SENSITIVE DATA WARNING

WARNING: Merchant is liable for these printed contents.

You must make every effort to secure the contents disclosed.

[OK]

[CANCEL]

If a report is requested that contains PAN data it will be printed by the POS printer but in no way retained by the POS. The information is received by a device request from the Payment Controller (Viper) to the POS printer device and is not saved in either a temporary or persistent file or database.

All printed reports have headings stating the document must be destroyed and not simply discarded.

Difference between PCI Compliance and PA-DSS Validation

As a software vendor who develops payment applications, our responsibility is to be “PA-DSS Validated.” We have performed an assessment and payment application validation review with our independent assessment firm (PAQSA), to ensure that our platform does conform to industry best practices when handling, managing and storing payment related information.

PA-DSS Version 3.1 is the standard against which the Verifone Payment Controller with POS Application has been tested, assessed, and validated.

PCI Compliance is then later obtained by the merchant, and is an assessment of your actual server (or hosting) environment called the Cardholder Data Environment (CDE).

Obtaining “PCI Compliance” is the responsibility of you the merchant and your hosting provider, working together, using PCI compliant architecture with proper hardware & software configurations and access control procedures.

The PA-DSS Validation is intended to ensure that the Verifone Payment Controller with POS Application will help you facilitate and maintain PCI Compliance with respect to how the payment application handles user accounts, passwords, encryption, and other payment data related information.

The Payment Card Industry (PCI) has developed security standards for handling cardholder information in a published standard called the PCI Data Security Standard (DSS). The security requirements defined in the DSS apply to all members, merchants, and service providers that store, process, or transmit cardholder data.

The PCI DSS requirements apply to all system components within the payment application environment which is defined as any network device, host, or application included in, or connected to, a network segment where cardholder data is stored, processed or transmitted.

The 12 Requirements of the PCI DSS:

Build and Maintain a Secure Network

- 1. Install and maintain a firewall configuration to protect data*
- 2. Do not use vendor-supplied defaults for system passwords and other security parameters*

Protect Cardholder Data

- 3. Protect Stored Cardholder Data*
- 4. Encrypt transmission of cardholder data across open, public networks*

Maintain a Vulnerability Management Program

- 5. Protect all systems against malware and regularly update anti-virus software or programs*
- 6. Develop and maintain secure systems and applications*

Implement Strong Access Control Measures

- 7. Restrict access to cardholder data by business need-to-know*
- 8. Identify and authenticate access to system components*
- 9. Restrict physical access to cardholder data*

Regularly Monitor and Test Networks

- 10. Track and monitor all access to network resources and cardholder data*
- 11. Regularly test security systems and processes*

Maintain an Information Security Policy

- 12. Maintain a policy that addresses information security for all personnel*

Considerations for the Implementation of Payment Applications in a PCI-Compliant Environment

The following areas must be considered for proper implementation in a PCI-Compliant environment.

- Remove Historical Sensitive Authentication Data
- Handling of Sensitive Authentication Data
- Secure Deletion of Cardholder Data
- All PAN is masked by default
- Cardholder Data Encryption & Key Management
- Removal of Historical Cryptographic Material
- Set up Good Access Controls
- Properly Train and Monitor Admin Personnel
- Key Management Roles & Responsibilities
- PCI-Compliant Remote Access
- Use SSH, VPN, or TLS 1.1 or higher for encryption of administrative access
- Log settings must be compliant
- PCI-Compliant Wireless settings
- Data Transport Encryption
- PCI-Compliant Use of Email
- Network Segmentation
- Never store cardholder data on internet-accessible systems
- Use TLS 1.1 or higher for Secure Data Transmission
- Delivery of Updates in a PCI Compliant Fashion

Remove Historical Sensitive Authentication Data (PA-DSS 1.1.4)

Previous versions of the Verifone Payment Controller with POS Application did not store sensitive authentication data (track 1, track 2, card validation values or codes, PIN or PIN block data). Therefore, there is no need for secure removal of this historical data by the application as required by PA-DSS v3.1.

Handling of Sensitive Authentication Data (PA-DSS 1.1.5)

The Verifone Payment Controller with POS Application does not store Sensitive Authentication Data for any reason once authorization has been completed. We strongly recommend that you do not do this either. However, if for any reason you should do so, the following guidelines must be followed when dealing with sensitive authentication data used for pre-authorization (track 1, track 2, card validation values or codes, PIN or PIN block data):

- Collect sensitive authentication data only when needed to solve a specific problem
- Store such data only in specific, known locations with limited access
- Collect only the limited amount of data needed to solve a specific problem
- Encrypt sensitive authentication data while stored
- Securely delete such data immediately after use

Secure Deletion of Cardholder Data (PA-DSS 2.1)

The following guidelines must be followed when dealing with Cardholder Data (Primary Account Number (PAN); Cardholder Name; Expiration Date; or Service Code):

- A customer defined retention period must be defined with a business justification.
- Cardholder data exceeding the customer-defined retention period or when no longer required for legal, regulatory, or business purposes must be purged.
- The Payment Controller (Viper) is the sole custodian of cardholder data, which is saved within encrypted STAN files. Operating system permissions allow only the Payment Controller (Viper) to manipulate these files. These files are deleted when the expiration period not to exceed 90 days is reached. This data is not stored in a database.

Any cardholder data you store outside of the application must be documented and you must define a retention period at which time you will purge (render irretrievable) the stored cardholder data. When defining a retention period you must take into account legal, regulatory, or business purpose.

Encrypted account data is not backed up to any external device by the Payment Controller (Viper) to be restored after an upgrade.

All PAN is Masked by Default (PA-DSS 2.2)

The Verifone Payment Controller with POS Application masks all PAN by default in all locations that display PAN (screens, paper receipts, printouts, reports, etc.). It is masked except the last four digits when displayed on receipts and reports.

The Verifone Payment Controller with POS Application does have the ability to display full PAN for users with legitimate business need. In order to configure the application to display full PAN for only personnel with a legitimate business need you must use the following process.

A user that is configured as a Secure User requiring complex passwords that comply with PCI password requirements can print a report that has full account numbers in the clear. A non-secure user does not get the full account numbers in the clear in any report.

On the Commander Site Controller platform, a random complex password is generated and displayed as part of the installation process. The system then requires that the generated password is changed after installation.

The PAN is strongly encrypted using AES 128 encryption and is stored in the STAN files for the configured number of days as described above. The key varies by STAN file and contains a random number stored within the file and a hardware based value.

Cardholder Data Encryption Key Management (PA-DSS 2.3, 2.4, and 2.5)

The Verifone Payment Controller with POS Application automatically generates and manages its encryption keys. If a key change is required it is handled by a payment application update.

The encryption method used in the Verifone Payment Controller with POS Application uses AES 128 bit encryption.

The Verifone Payment Controller with POS Application does not provide users any ability to output files containing CHD (STAN files).

As noted on page 18, the SECURE user does have the ability to print a report from data contained within the STAN files. Upon selecting this report, the SECURE user is informed to destroy the report when finished.

Encryption Software

The Verifone Payment Controller with POS Application takes advantage of the Java Cryptography Extension built into Java SDK 2.0 and above. It uses “unlimited strength” policy files resident in Java.

Encryption Key Processing

The EPS payment application uses “AES” for key generation. “AES key size must be a multiple of 8, and can only range from 32 to 448, inclusive. The AES Key size must be 128, 192, or 256 bits. As stated above, we use a 128 bit key size.

Key Construction

The key construction is done entirely within the payment application. There are two entities that make up the key. Each entity adds up to provide a 128 bit key. The entities are derived from a value that is unique with each hardware device the application runs on and a value randomly generated by the application that is unique with each transaction being encrypted. These two entities are assembled using the following algorithm;

Example:

Key = Dynamic key part + Static key part

or

Key = Random value + Hardware unique value.

Key Part Embedding

When a transaction record is successfully encrypted, given the correct key calculation, it is placed in the file and not viewable by any means unless properly decoded. One part of the key is then saved in this file, obfuscated from view, and is referred to as the dynamic key part.

Key Change / Update Procedure

In response to any business request or in the event of a potential or actual compromise of the encryption used within the Payment Controller Application (Viper), the following describes those steps and actions taken to change or update the key used for encryption.

1. Depending on the nature of the request, the change of the key would involve a Payment Controller Application (Viper) change where that change would utilize different values for each or one of the key parts used as part of the encryption process. This means the application would utilize:
 - a. A different/unique hardware value

- b. A different method to obfuscate the dynamic key part
- 2. If the business requirement or a compromise was made, and the needed change was to no longer use the AES encryption engine of the operating system, the OS update and new Payment Controller (Viper) application would be generated. This update would remove the AES engine and replace it with the newer or update for the encryption engine.
- 3. Once the payment application and/or the OS update was made, tested and certified, these updates would then be provided to each customer, where they would be responsible to deploy these updates to their locations.

CONFIDENTIAL

Removal of Historical Cryptographic material (PA-DSS 2.6)

The Verifone Payment Controller stores encrypted account number data in the normal course of operation.

To render all cryptographic material (encryption keys and encrypted cardholder data) irretrievable it is necessary to remove the compact flash and either reflash or securely destroy the compact flash.

Set up Strong Access Controls (PA-DSS 3.1 and 3.2)

The PCI DSS requires that access to all systems in the payment processing environment be protected through use of unique users and complex passwords. Unique user accounts indicate that every account used is associated with an individual user and/or process with no use of generic group accounts used by more than one user or process.

3.1: You must assign strong passwords to any default accounts (even if they won't be used), and then disable or do not use the accounts. The following are true with the Verifone Payment Controller with POS Application.

1. During installation
On the Viper platform, a default secure password is provided.

On the Commander Site Controller platform, a random complex password is generated and displayed as part of the installation process.
2. System vs. Application (user) accounts (PCI DSS 2.1 and PCI DSS 8.3 / PA-DSS 3.1.1 and 3.1.2)
 - a. Application User Account "manager" is the only account generated during installation. Password is randomly generated and must be changed at first login.
 - i. Note: If any application account is attempting to update a field that impacts the security of the CDE (e.g. Payment Processor IP Address) or the security of another user, then the user is challenged for a secondary authentication credential (One Time Passcode or OTP). The OTP is generated via software on the Topaz or Ruby 2 by accessing CSR FUNC -> MAINTENANCE -> GENERATE CONFIG OTP.
 - a. Access to a system account (with limited privileges) for the purpose of helpdesk support requires Multifactor Authentication. In addition to account and password, a software or hardware switch must be toggled to generate a four digit One Time Passcode (OTP) entered by the Helpdesk agent. The mechanical switch resides inside an access panel on the Commander Site Controller or Sapphire hardware. The OTP can also be generated via software on the Topaz or Ruby 2 by accessing CSR FUNC -> MAINTENANCE -> ENABLE HELPDESK LOGIN. There is a time limit to enter the password before the entire log in process must be reattempted. Invalid entry of either password or OTP requires both to be reentered. The system does not indicate which factor was entered incorrectly.
3. Each application user has their own password per section PCI DSS 8.1.1 / PA-DSS 3.1.3.
4. The application requires passwords to be changed at least every 90 days (PCI DSS 8.2.4 / PA-DSS 3.1.7) shorter retention periods can be specified.
5. The application requires passwords to be at least 7 characters (PCI DSS 8.2.3 / PA-DSS 3.1.6) longer restrictions can be specified.
6. The application requires passwords to include both numeric and alphabetic characters (PCI DSS 8.2.3 / PA-DSS 3.1.6)

7. The application keeps password history and requires that a new password is different than any of the last four passwords used. (PCI DSS 8.2.5 / PA-DSS 3.1.8)
8. The application limits repeated access attempts by locking out the user account after not more than six failed logon attempts. (PCI DSS 8.16 / PA-DSS 3.1.9)
9. The application requires an administrator enable any locked out user ID. (PCI DSS 8.1.7 / PA-DSS 3.1.10) Note the administrator in this case is not a system account, only an application account that has been given the privilege level of creating or deleting application users.
10. The application requires the user to re-authenticate to re-activate the session if the application session has been idle for more than 15 minutes (PCI DSS 8.1.8 / PA-DSS 3.1.11).

No database applications are involved in handling PANs, sensitive account data, etc. [Note: These password controls are not intended to apply to employees who only have access to one card number at a time to facilitate a single transaction. These controls are applicable for access by employees with administrative capabilities, for access to servers with cardholder data, and for access controlled by the application.]

3.2: Control access, via unique username and PCI DSS-compliant complex passwords, to any PCs or servers with payment applications and to databases storing cardholder data. (Any such devices are not part of the Verifone system and would be the result of the merchant's own policies.)

Properly Train and Monitor Admin Personnel (PA-DSS 3.4)

It is your responsibility to institute proper personnel management techniques for allowing admin user access to cardholder data, site data, etc. You can control whether each individual admin user can see credit card PAN (or only last 4).

In most systems, a security breach is the result of unethical personnel. So pay special attention to whom you trust into your admin site and who you allow to view full decrypted and unmasked payment information.

Log settings must be compliant (PA-DSS 4.1, 4.4)

By default all application logs are set to comply with the PA-DSS requirements (PA-DSS 4.1.b, PCI-DSS 10.2 & 10.3). These settings cannot be changed by the merchant; however the merchant must understand that disabling or subverting the logs in any way will result in non-compliance with PCI DSS.

During installation the servicer will be prompted to enter the IP address of a security log server that uses the syslog protocol. If at some point the IP address is changed the servicer or Verifone helpdesk can update the IP address settings. Syslog server configuration is restricted to secure administrators. Any modifications will be logged both to the internal data log, and to the old IP address for the log server, in the event it is still functioning during a transition period.

Implement automated assessment trails for all system components to reconstruct the following events:

- 10.2.1 All individual user accesses to cardholder data from the application*
- 10.2.2 All actions taken by any individual with administrative privileges in the application*
- 10.2.3 Access to application audit trails managed by or within the application*
- 10.2.4 Invalid logical access attempts*

- 10.2.5 Use of the application's identification and authentication mechanisms (including but not limited to creation of new accounts, elevation of privileges, etc.) and all changes, additions, deletions to application accounts with root or administrative privileges*
- 10.2.6 Initialization, stopping, or pausing of the application audit logs*
- 10.2.7 Creation and deletion of system-level objects within or by the application*

Record at least the following assessment trail entries for all system components for each event from 10.2.x above:

- 10.3.1 User identification*
- 10.3.2 Type of event*
- 10.3.3 Date and time*
- 10.3.4 Success or failure indication*
- 10.3.5 Origination of event*
- 10.3.6 Identity or name of affected data, system component, or resource.*

Disabling or subverting the logging function of the Verifone Payment Controller with POS Application in any way will result in non-compliance with PCI DSS.

4.4.b: Verifone Payment Controller with POS Application facilitates centralized logging.

The install option "logserver" can be used to assign the IP address of a third-party provided server that will receive system log messages from the Verifone Payment Controller with POS Application and the POS. The log messages are sent one line per packet using UDP on port 514 per common UNIX usage. Each message is prefixed with the application name (pmc, topaz101, topaz102...) so that they can be filtered out later if needed.

The log messages capture information about individual access to cardholder data. The routers at different merchant locations will have a different forward looking IP address in a broader network topology. A central log server provided, installed, and configured by a third party should be set up to capture this outbound forward looking address of the Verifone Payment Controller with POS Application, which can help determine which *syslog* message came from which location.

It is the merchant's responsibility to promptly backup and preserve the logs per PCI DSS requirements (PCI-DSS 10.5.3, PCI-DSS 10.5.4, and PCI-DSS 10.7)

PCI-Compliant Wireless settings (PA-DSS 6.1, 6.2 and 6.3)

Verifone Payment Controller with POS Application does not support wireless technologies. However, should the merchant implement wireless access within the cardholder data environment, the following guidelines for secure wireless settings must be followed per PCI Data Security Standard 1.2.3, 2.1.1 and 4.1.1:

2.1.1: Change wireless vendor defaults per the following 5 points:

1. Encryption keys must be changed from default at installation, and must be changed anytime anyone with knowledge of the keys leaves the company or changes positions
2. Default SNMP community strings on wireless devices must be changed

3. Default passwords/passphrases on access points must be changed
4. Firmware on wireless devices must be updated to support strong encryption for authentication and transmission over wireless networks
5. Other security-related wireless vendor defaults, if applicable, must be changed

1.2.3: Perimeter firewalls must be installed between any wireless networks and systems that store cardholder data, and these firewalls must deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.

4.1.1: Industry best practices (for example, IEEE 802.11.i) must be used to implement strong encryption for authentication and transmission of cardholder data.

Note: The use of WEP as a security control was prohibited as of June 30, 2010.

Services and Protocols (PA-DSS 8.2)

The following are the services and protocols that are required by the Verifone Payment Controller with POS Application:

TLS1.1, TLS1.2

SSH

SFTP

HTTPS

However, IFSF message exchanges *within* the payment processing environment are not secured and require isolation within a firewall. In particular, traffic between the Payment Controller (Viper) and the POP must be on an isolated subnet.

Never store cardholder data on internet-accessible systems (PA-DSS 9.1)

Never store cardholder data on Internet-accessible systems (e.g., web server and database server must not be on same server.)

PCI-Compliant Remote Access (10.1)

The PCI standard requires that if employees, administrators, or vendors are granted remote access to the payment processing environment; access should be authenticated using a two-factor authentication mechanism. This means two of the following three authentication methods must be used:

1. Something you know, such as a password or passphrase
2. Something you have, such as a token device or smart card
3. Something you are, such as a biometric

Verifone Payment Controller with POS Application requires the following two authentication factors for access (remote or local) to the Commander Shell:

1. Something you know (password or passphrase)
2. Something you have (random token generated by the Verifone Payment Controller)

A remote user cannot initiate administrative access without intervention from someone at the site. A temporary access token is generated when someone at the site either enables remote login through the web interface or flips the mechanical remote login switch on the site controller. A remote user's password and the temporary access token are required to successfully authenticate and obtain shell access.

PCI-Compliant Delivery of Updates (PA-DSS 10.2.1)

The Verifone Payment Controller with POS Application delivers patches and updates in a secure manner that maintains a secure chain of trust per requirement PA-DSS 7.2.a, including:

- Timely development and deployment of patches and updates.

Patches deployment depends on the urgency required. All released software is available to properly credentialed servicers via a web portal. Customers with a satellite distribution network can deploy software updates via a broadcast mechanism. Customer with no remote connectivity will be visited on site by a servicer.

- Delivery in a secure manner with a known chain-of-trust.

Only properly credentialed Verifone Authorized Service Contractors can download software from the Verifone portal.

- Delivery in a manner that maintains the integrity of the deliverable.

The installation utility is based on the Verifone proprietary Netloader installation package. Any transfers that are not production signed are deleted. Patches applied by field support are installed via SCP or SFTP.

- Integrity testing of patches or updates prior to installation.

All Verifone distributed software is signed with a production certificate. The Verifone Payment Controller with POS Application will delete any software transferred that fails signature checks.

Software updates performed via the Viper Remote Configuration Interface are not signed. These updates must be performed via customer implemented secure network such as VPN, dedicated lines, etc.

As a development company, we keep abreast of the relevant security concerns and vulnerabilities in our area of development and expertise.

We do this by:

- Monitoring of security alerts concerning O/S and middleware components
- Continual review of development builds with software tools such as vulnerability and exploit scanners

Once we identify a relevant vulnerability, we work to develop & test a patch that helps protect the Verifone Payment Controller with POS Application against the specific, new vulnerability. Depending on the severity, we attempt to publish a patch within 15 days of the identification of the vulnerability. (Vulnerabilities within 3rd party software integrated into the system may take more than 30 days to resolve.) We will then contact vendors and dealers to encourage them to install the patch. Typically, merchants are expected to respond quickly to and install available patches within 30 days.

Software and updates are available by utilizing the upgrade features of the Verifone Payment Controller with POS Application. The software upgrade can be supplied by Verifone Authorized Service Contractors visiting the sites or if the customer has a means to distribute the software upgrade they can assume responsibility making the same available to each installation. Additionally, customers can elect to use Verifone Remote Software Delivery (VRSD), a feature provided by Verifone where remote customer sites can access Verifone servers for available signed updates.

PCI-Compliant Remote Access (10.2.3)

The PCI standard requires that if employees, administrators, or vendors are granted remote access to the payment processing environment; access should be authenticated using a two-factor authentication mechanism (username/ password and an additional authentication item such as a token or certificate).

In the case of vendor remote access accounts, in addition to the standard access controls, vendor accounts should only be active while access is required to provide service. Access rights should include only the access rights required for the service rendered, and should be robustly audited.

The Verifone Payment Controller with POS Application does not host third party remote access software. However, other devices may be installed on the same network segment which do.

If users and hosts within the payment application environment need to use third-party remote access software such as secured shell access etc. to access other hosts within the payment processing environment, special care must be taken.

In order to be compliant, every such session must be encrypted with at least 128-bit encryption (in addition to satisfying the requirement for two-factor authentication required for users connecting from outside the payment processing environment). There is no desktop application mechanism (such as RDP or PCAnywhere) to the payment environment. Additionally, (for any customer-supplied equipment within the payment processing environment) the PCI user account and password requirements will apply to these access methods as well.

When requesting support from a vendor, reseller, or integrator, customers are advised to take the following precautions:

- Change default settings (such as usernames and passwords) on remote access software (e.g. VNC)
- Allow connections only from specific IP and/or MAC addresses
- Use strong authentication and complex passwords for logins according to PA-DSS 3.1.1 – 3.1.10 and PCI DSS 8.1, 8.3, and 8.5.8-8.5.15
- Enable encrypted data transmission according to PA-DSS 12.1 and PCI DSS 4.1
- Enable account lockouts after a certain number of failed login attempts according to PA-DSS 3.1.8 and PCI DSS 8.5.13

- Require that remote access take place over a VPN via a firewall as opposed to allowing connections directly from the internet
- Enable logging for auditing purposes
- Restrict access to customer passwords to authorized reseller/integrator personnel.
- Establish customer passwords according to PA-DSS 3.1.1 – 3.1.10 and PCI DSS Requirements 8.1, 8.2, 8.4, and 8.5.

Data Transport Encryption (PA-DSS 11.1)

The PCI DSS requires the use of strong cryptography and encryption techniques with at least a 128 bit encryption strength (either at the transport layer with TLS 1.1, TLS 1.2 or IPsec); or at the data layer with algorithms such as RSA or Triple-DES) to safeguard cardholder data during transmission over public networks (this includes the Internet and Internet accessible DMZ network segments).

PCI DSS requirement 4.1: Use strong cryptography and security protocols such as transport layer security (TLS 1.1 or higher) and Internet protocol security (IPSEC) to safeguard sensitive cardholder data during transmission over open, public networks.

Examples of open, public networks that are in scope of the PCI DSS are:

- The Internet
- Wireless technologies
- Global System for Mobile Communications (GSM)
- General Packet Radio Service (GPRS)

Refer to the Dataflow diagram for an understanding of the flow of encrypted data associated with the Verifone Payment Controller with POS Application.

PCI-Compliant Use of End User Messaging Technologies (PA-DSS 11.2)

The Verifone Payment Controller with POS Application does not allow or facilitate the sending of PANs via any end user messaging technology (for example, e-mail, instant messaging, and chat).

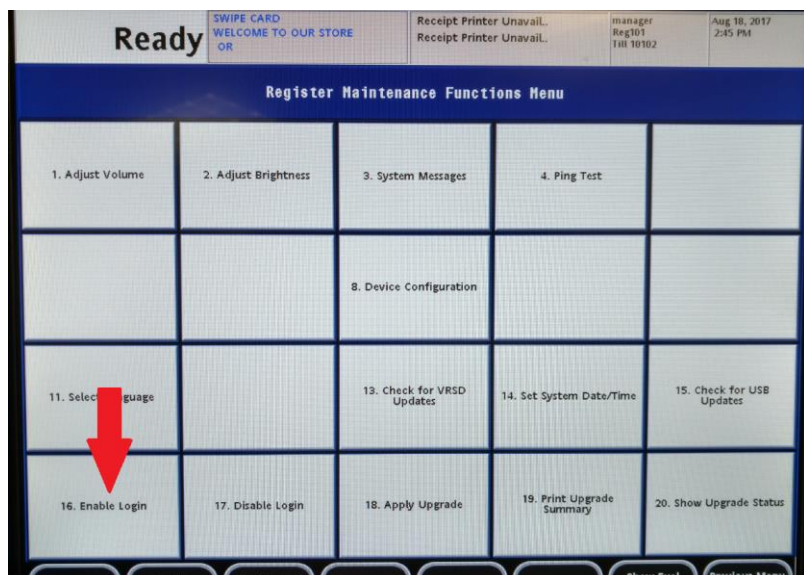
Non-console administration and Multi-Factor Authentication (PA-DSS 12.1, 12.2)

The Verifone Payment Controller with POS Application requires that non-console administration utilize strong encryption using technologies such as SSH, VPN or TLS 1.1 or higher. Because the Verifone Payment Controller allows such access, multi-factor authentication (at least 2 of something you know, something you have, something you are) must be utilized when accessing over these technologies.

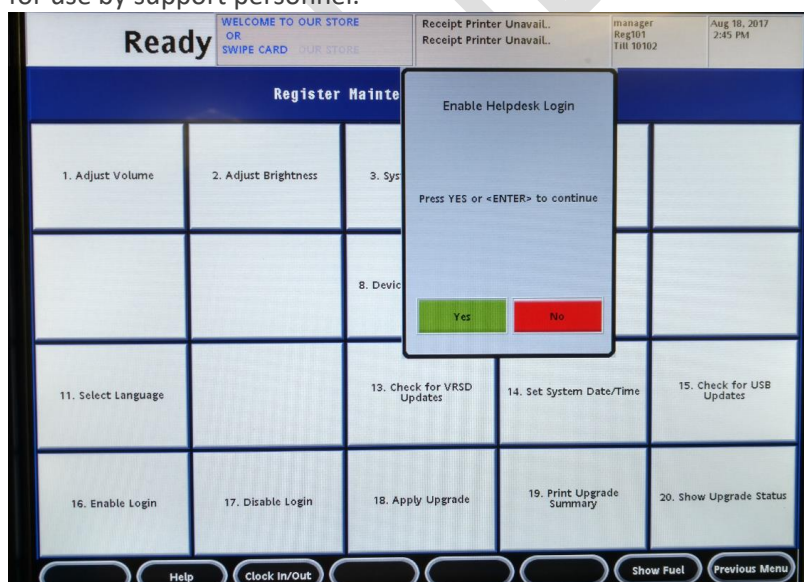
The Verifone Payment Controller utilizes something you know (account and password) and something you have (Commander generated One Time Passcode (OTP)) to provide MFA control over such access. In order to properly utilize the MFA solution:

1. Enable Remote Login via the Topaz or Ruby POS terminal. In the event the POS terminal is offline and cannot perform this function, dipswitch one on the side of the Commander Payment Controller hardware can be toggled.

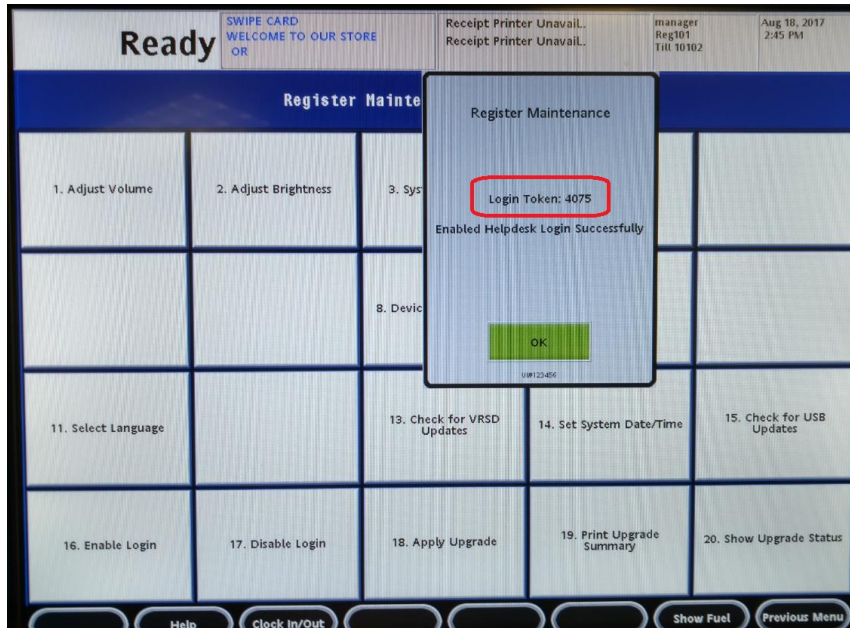
Note: The Payment Controller must always be housed in a location that is accessible only to store employees.



2. Upon Enabling Login, store personnel will be instructed to generate a One Time Password (OTP) token for use by support personnel.



From time of creation, the OTP token must be used within 15 minutes. After 15 minutes the token expires and a new token will need to be generated. After a token is used for authentication it cannot be reused.



3. The Commander generated OTP is not transmitted across a network. Store personnel must read the token to support personnel over the phone. Support personnel utilize two factor authentication (account with password and CMDR OTP token) to access Commander.



All data transmission, including authentication, is encrypted via TLS 1.2 across a TLS VPN tunnel to the site.

4. Once a support session is completed, site personnel should select DISABLE LOGIN to disable remote support connectivity.

Network Segmentation

The PCI DSS requires that firewall services be used (with NAT or PAT) to segment network segments into logical security domains based on the environmental needs for internet access. Traditionally, this corresponds to the creation of at least a DMZ and a trusted network segment where only authorized, business-justified traffic from the DMZ is allowed to connect to the trusted segment. No direct incoming internet traffic to the trusted application environment can be allowed. Additionally, outbound internet access from the trusted segment must be limited to required and justified ports and services.

- Refer to the typical Network diagram (above) for an understanding of the flow of encrypted data associated with the Verifone Payment Controller with POS Application.

Maintain an Information Security Program

In addition to the preceding security recommendations, a comprehensive approach to assessing and maintaining the security compliance of the payment application environment is necessary to protect the organization and sensitive cardholder data.

The following is a very basic plan every merchant/service provider should adopt in developing and implementing a security policy and program:

- Read the PCI DSS in full and perform a security gap analysis. Identify any gaps between existing practices in your organization and those outlined by the PCI requirements.
- Once the gaps are identified, determine the steps to close the gaps and protect cardholder data. Changes could mean adding new technologies to shore up firewall and perimeter controls, or increasing the logging and archiving procedures associated with transaction data.
- Create an action plan for on-going compliance and assessment.
- Implement, monitor and maintain the plan. Compliance is not a one-time event. Regardless of merchant or service provider level, all entities should complete annual self-assessments using the PCI Self-Assessment Questionnaire.
- Call in outside experts as needed.

Application System Configuration

Below are the operating systems and dependent application patch levels and configurations supported and tested for continued PCI DSS compliance.

- The Verifone Payment Controller with POS Application as listed in the “Payment Application Version” section of the Application Summary table above.
- One of the two Verifone Hardware Systems
 - Commander Site Controller hardware system

- Sapphire / Viper hardware system
- TCP/IP network connectivity

Payment Application Initial Setup & Configuration

Refer to the specific setup and configuration instructions for the specific Verifone Payment Controller with POS Application as listed in the “Payment Application Version” section of the Application Summary table above. These documents are located on the Verifone internet portal.

CONFIDENTIAL