UnifyPOS PA-DSS Implementation Guide

UPDATED for new Version 11.1.95, Out of Scope (OOS) of PA-DSS* *using Datacap NETePay as the Payment Application

The Payment Card Industry's (PCI) Payment Application Data Security Standard (PA-DSS) requires the Payment Application Software Manufacturer to produce a document for customers, with instructions, notes and pointers on how to properly implement the Payment Application in a secure manner.

UnifyPOS version 11.1.95 no longer has access to any sensitive cardholder data, so it is no longer considered a "payment application". To achieve this, UnifyPOS no longer controls any secure device that has access to sensitive cardholder data, such as a Magnetic Stripe Reader or Pin Pad. Osprey Retail Systems (ORS) has integrated version 11.1.95 solely to **3rd party controls*,** that not only handle the integrated payment application, but also all interaction with the secure devices.

***The pertinent Datacap NETePay v5 Implementation Guide is attached, followed by the ORS UnifyPOS v11.1.95 "PCI Out of Scope" Guide.**

Although ORS, Datacap, or DCRS Solutions are not required to educate our customers on cardholder security requirements (your Credit Processor or Acquirer is responsible), **as responsible vendors, we want to make our customers aware that the cardholder industry has published security related standards *that all Merchants are required to follow, per the Merchant Agreements you signed with your Credit Processor or Acquirer.*** If compromised and found to be non-compliant, Merchants can and will incur significant fines and/or penalties, etc.

In addition to reviewing the Datacap NETePay & UnifyPOS v11 PA-DSS Implementation Guides included here, our customers should also visit the Payment Card Industry Security Standards Council (PCI-SSC) web site, and become familiar with these standards and requirements, available at:

PCI-SSC: https://www.pcisecuritystandards.org/index.shtml

Please let us know if you have any questions or need any assistance.

IMPLEMENTATION GUIDE
FOR SYSTEMS USING NETEPAY 5.0

Introduction

Systems which process payment transactions necessarily handle sensitive cardholder account information. The card associations (VISA, MasterCard) have developed security standards for handling cardholder information in a published document named ***Payment Card Industry (PCI) Data Security Standard (DSS)***.

The security requirements defined in the standard apply to all members, merchants, and service providers that store, process or transmit cardholder data.

The PCI Data Security Requirements apply to all **system components** which is defined as any **network component**, **server**, or **application** included in, or connected to, the cardholder data environment. Network components, include, but are not limited to, firewalls, switches, routers, wireless access points, network appliances, and other security appliances. Servers include, but are not limited to, Web, database, authentication, Domain Name Service (DNS), mail, proxy, and Network Time Protocol (NTP). Applications include all purchased and custom applications, including internal and external (Web) applications.

The following **12 Requirements** comprise the Payment Card Industry Data Security Standard.

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 Data
4. Encrypt transmission of cardholder data and sensitive information across public networks

Maintain a Vulnerability Management Program
5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications

Implement Strong Access Control Measures
7. Restrict access to data by business need-to-know
8. Assign a unique ID to each person with computer access
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

Access Control

The PCI standard 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. Additionally any default accounts provided with operating systems, databases and/or devices should be removed/disabled/renamed if possible, or at least should have complex passwords and should not be used. Examples of such default administrator accounts include administrator (Windows systems), sa (SQL/MSDE), and root (UNIX/Linux).

The PCI standard requires the following password complexity for compliance:

- Passwords must be at least 7 characters
- Passwords must be include both numeric and alphabetic characters
- Passwords must be changed at least every 90 days
- New passwords can not be the same as the last 4 passwords

Below are the other PCI account requirements beyond uniqueness and password complexity:

- If an incorrect password is provided 6 times the account should be locked out
- Account lock out duration should be at least 30 min. (or until an administrator resets it)
- Sessions idle for more than 15 minutes should require re-entry of username and password to reactivate the session.

These same account and password criteria must also be applied to any applications or databases included in payment processing to be PCI compliant.

Remote Access Control

The PCI standard requires that if employees, administrators, or vendors can access the payment processing environment remotely; access should be authenticated using a 2-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, should include only the access rights required for the service rendered, and should be robustly audited.

Access to hosts within the payment processing environment via 3 rd party remote access software such as Remote Desktop (RDP)/Terminal Server, PCAnywhere, etc. requires that when such programs are used that there sessions are encrypted with at least 128 bit encryption (this requirement is in addition to the requirement for 2-factor authentication required for users connecting from outside the payment processing environment). For RDP/Terminal Services this means using the high encryption setting on the server, and for PCAnywhere it means using symmetric or public key options for encryption.

NETePay 5.0 does not directly support remote access for maintenance, monitoring, operation, troubleshooting or updates. Datacap Systems does not use remote access software to deliver any services, software, or support to users of NETePay 5.0. If merchants, integrators or resellers elect to use third party remote access independent of NETePay 5.0, they should observe the following remote access procedures:

- *Change default settings in the remote access software (for example, change default passwords and use unique passwords for each customer).*
- *Allow connections only from specific (known) IP/MAC addresses.*
- *Use strong authentication and complex passwords for logins according to PCI DSS Requirements 8.1, 8.3, and 8.5.8–8.5.15*
- *Enable encrypted data transmission according to PCI DSS Requirement 4.1*
- *Enable account lockout after a certain number of failed login attempts according to PCI DSS Requirement 8.5.13*
- *Configure the system so a remote user must establish a Virtual Private Network "VPN") connection via a firewall before access is allowed.*
- *Enable the logging function.*
- *Restrict access to customer passwords to authorized reseller/integrator personnel.*
- *Establish customer passwords according to PCI DSS Requirements 8.1, 8.2, 8.4, and 8.5.*

Wireless Access Control

The PCI standard requires the encryption of cardholder data transmitted over wireless connections. The following items identify the PCI standard requirements for wireless connectivity to the payment environment:

- Firewall/port filtering services should be placed between wireless access points and the payment processing environment with rules restricting access
- Use of appropriate encryption mechanisms such as **VPN, SSL/TPS at 128** bit, WEP at 128 bit, and/or WPA
- If WEP is used the following additional requirements must be met:
  - Another encryption methodology must be used to protect cardholder data
  - If automated WEP key rotation is implemented key change should occur every 10-30 minutes
  - If automated key change is not used, keys should be manually changed at least quarterly and when key personnel leave the organization
- Vendor supplied defaults (administrator username/password, SSID, and SNMP community values) should be changed
- Access point should restrict access to known authorized devices (using MAC Address filtering)

Network Encryption

The PCI standard requires the use of strong cryptography and encryption techniques (at least 128 bit); such as Secure Sockets Layer (SSL) and Internet Protocol Security (IPSEC) to safeguard sensitive cardholder data during transmission over public networks (like the Internet).

Additionally PCI requires that cardholder information never be sent via e-mail without strong encryption of the data.

Network Security

ePay Administrator and ePay Administrator for NETePay may be installed on other computers on the network rather than on the computer on which the NETePay server is installed. ***If either of these ePay Administrators is installed remotely in this manner, you should enable SSL encryption for the instance of MSD or SQL Express by using Microsoft Management Console.***

NETePay Compliance

All versions of **NETePay** at or above Version 5.00 implement all of the PCI Data Security Standard requirements that are applicable to a payment processing application.

- **NETePay** does not store any magnetic stripe (Track 1 or 2), card verification (CVV, CVV2, etc.) or PIN data, ever.
- **NETePay** truncates all account and expiration date information for transactions which have been settled in every area where it is either stored or displayed.
- **NETePay** encrypts account numbers and expiration dates for transactions which have not yet been settled.
- **NETePay** logs only record truncated account number and expiration date information and never record any magnetic stripe (Track 1 or 2), card verification (CVV, CVV2, etc) or PIN data, ever. NETePay 5.0 logs are fixed in function, format and contents and cannot be disabled or configured by any user.
- **NETePay** utilities which present data in a user interface (display or print) always truncate account number and expiration date data and never display magnetic stripe (Track 1 or 2), card verification (CVV, CVV2, etc) or PIN data, ever.
- **NETePay** encrypts all IP transmissions that contain cardholder data using current SSL/TLS standards.
- **NETePay** does not allow or facilitate sending of PANs (Primary Account Numbers) by end user messaging technologies; however if a merchant, integrator or reseller transmits information of this type, a solution that implements strong cryptography should be employed.

Baseline System Configuration

To realize the maximum security from *NETePay*, the server on which it is installed should meet or exceed the following system requirements:

- Microsoft Windows 2000 Professional with Service Pack 4, Windows XP Pro with Service Pack 2, Windows Vista Business Edition, Windows 7, Windows Server 2003 or 2008. All latest updates and hotfixes should be applied.
- 1 GB of RAM minimum, 2 GB or higher recommended
- 10 GB of available hard-disk space
- Microsoft Internet Explorer with 128-bit encryption, Microsoft Internet Explorer 6.0 or higher recommended
- TCP/IP network connectivity.
- Microsoft Internet Explorer with 128-bit encryption, Microsoft Internet Explorer 6.0 or higher recommended
- TCP/IP network connectivity.
- Available COM port (if using dial backup or dial primary communications)
- Datacap DialLink modem (if using dial backup or dial primary communications)
- Persistent Internet Connection (DSL, cable, frame relay, etc.)

Additional System Security Recommendations

Although NETePay 5.0 implements all of the PCI Data Security Standard requirements which are applicable to a payment processing application, additional overall security can be realized by implementing the following:

- Use a router which implements NAT (Network Address Translation).
- Use antivirus software with auto update capability, from vendors such as McAfee, Norton, Panda, Kaspersky, Trend Micro, etc.
- Enable firewall services (either software based like Windows Firewall or hardware based) between the payment processing environment and the internet access device (typically an ISP provided router/modem).
- Define and use strong passwords to restrict access to authorized personnel.
- Test and install security related Windows and SQL/MSDE updates, service packs and hotfixes promptly. Consider using automatic updating.

POS System Considerations

Although NETePay 5.0 implements all of the PCI Data Security Standard (DSS) requirements that are applicable to a payment processing application, your POS application may not handle cardholder information in such a secure fashion.

PCI Data Security requirements must be implemented in all the components of a system which handle cardholder data in order to provide comprehensive security. The PCI Data Security requirements ***must*** be implemented in your POS system and any other applications which handle cardholder data. You should verify with your POS system provider that the version of the POS software you are using is compliant.

Removal of Historical Data

If you are upgrading to NETePay 5.0 from a previous version, you should securely delete the previous NETePay database and logs before upgrade installation. NETePay normally truncates and deletes any sensitive information for all settled transactions but to assure there are no residual unsettled transactions; the following procedure should be followed to delete the previous NETePay database, any backups and all logs:

1. Shut down **NETePay**
2. Using Windows Control Panel, select Add/Remove Programs
3. Select **NETePay** and remove it
4. Locate the **NETePay** folder in **<bootdrive>:/Program Files/Datacap Systems** and use a secure file deletion utility to remove it
5. Install **NETePay 5.0**
6. From the **Programs/Software from Datacap** group, run the **NETePay Database Manager**
7. Select Connect
8. Select Crate New Database
9. Shut down **NETePay Database Manager**
10. Start **NETePay 5.0**

Information Handling and Collection Criteria

NETePay 5.0 and all of its components handle sensitive cardholder data in accordance with the PA-DSS 1.2 standard of the PCI Data Security Council. However, NETePay 5.0 does not monitor the activities of users or other software to assure that they accord sensitive data the same standards. Merchant, and reseller/integrators should adhere to the following guidelines if they handle cardholder information:

- Collect sensitive authentication 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.

NETePay 5.0 only stores cardholder information only for unsettled transactions. Once NETePay 5.0 settles transactions, all cardholder information is either deleted or truncated. The merchant, integrator or reseller does not need to manage retention of cardholder data in NETePay 5.0 beyond assuring that transactions are settled in a timely manner.

NETePay 5.0 logs are fixed in function, format and contents and cannot be disabled or configured by any user. NETePay 5.0 logs only record truncated account number and expiration date information and never record any magnetic stripe (Track 1 or 2), card verification (CVV, CVV2, etc) or PIN data.

NETePay 5.0 does not allow or facilitate sending of PANs (Primary Account Numbers) by end user messaging technologies; however if a merchant, integrator or reseller transmits information of this type, a solution that implements strong cryptography should be employed.

Security Action Plan

In addition to the preceding security recommendations, a comprehensive approach to assessing the security compliance of your entire system is necessary to protect you and your data. The following is a basic plan every merchant should adopt.

1. Read the PCI Standard in full and perform a security gap analysis. Identify any gaps between existing practices in your organization and those outlined by the PCI requirements.
2. Create an action plan for on-going compliance and assessment. Once the gaps are identified, companies must determine the steps needed to close the gaps and protect cardholder data. It could mean adding new technologies to shore up firewall and perimeter controls, or increasing the logging and archiving procedures associated with transaction data.
3. Implement, monitor and maintain the plan. Compliance is not a one-time event. Regardless of merchant or service provider level, all entities must complete annual self-assessments using the PCI Self Assessment Questionnaire.
4. Call in outside experts as needed. Visa has published a Qualified Security Assessor List of companies that can conduct on-site CISP compliance audits for Level 1 Merchants, and Level 1 and 2 Service Providers. MasterCard has a Compliant Security Vendor List of SDP-approved scanning vendors.

Implementation Guide Reviews and Updates

Datacap Systems reviews the NETePay 5.0 Implementation Guide and issues updates to maintain compliance at least once per year or whenever a software change warrants. This implementation guide is also incorporated as part of every NETePay Installation and User Guide. The latest version, which is supplied on the distribution CD, may also be downloaded from Datacap's site at www.datacapepay.com in the NETePay section separately at any time.

Development and Deployment of Security Updates

Datacap is committed to timely development and deployment of security patches. When a vulnerability is detected, we will develop and deploy an updated NETePay executable within 30 days of discovery. These update will be delivered using a known chain of trust. A technical notice will be sent out via email and the update will be made available on our web site. The update file can then be downloaded directly. The update files are digitally signed to verify their authenticity.

More Information

You may download a copy of the ***Payment Card Industry (PCI) Data Security Standard*** from the PCI Security Standards Council website at the following Internet address:

https://www.pcisecuritystandards.org/security_standards/pci_dss_download_agreement.html

Additional information for merchants from the PCI Security Standards Council is available at the following Internet address:

http://www.pcisecuritystandards.org/education/fact_sheets.shtml

A listing in PDF format of qualified security assessors from the PCI Security Standards Council is available at the following Internet address:

http://www.pcisecuritystandards.org/pdfs/pci_qsa_list.pdf

404 County St.
New Bedford, MA 02740-4936
Phone 508.992.1097
Fax 508.992.2716
www.ospreyretailsystems.com

Osprey Retail Systems

OOS Implementation Guide

Owner:	Roger Blanchard	
Audience:	UnifyPOS Resellers and UnifyPOS Merchants	
Version / Status:	3.0	
Location:	New Bedford, MA	
Updated:	10/31/2012	Updated for 11.1.95 OOS Payment Interface by converting PA-DSS Implementation Guide into OOS Implementation Guide.

1. Executive Summary

1.1. Objective

The purpose of this document is to provide guidance for Osprey resellers when implementing UnifyPOS to be out of scope for PCI DSS. Prior to 11.1.95 UnifyPOS was considered a “payment application” even though UnifyPOS did not store, process or transmit sensitive cardholder data. Since UnifyPOS did have access to this sensitive cardholder data it was deemed a “payment application”. In 11.1.95 UnifyPOS no longer has access to any sensitive cardholder data and therefore is no longer considered a “payment application”.

1.2. Intended Audience

This document is intended for Osprey resellers that are configuring UnifyPOS to accept integrated payments and are seeking guidance on how implementing UnifyPOS may impact the scope of their merchant’s compliance efforts with the PCI DSS. UnifyPOS end users may also find the information in this document useful.

1.3. Introduction to OOS

In order for UnifyPOS to be considered out of scope for PCI DSS the application cannot store, process, transmit or have access to any sensitive cardholder data. To achieve this UnifyPOS can no longer control any secure device that has access to this sensitive cardholder data such as a Pin Pad or MSR. Instead of UnifyPOS controlling these secure devices ORS has integrated to 3rd party controls that not only handle the integrated payment but also all interaction with the secure devices.

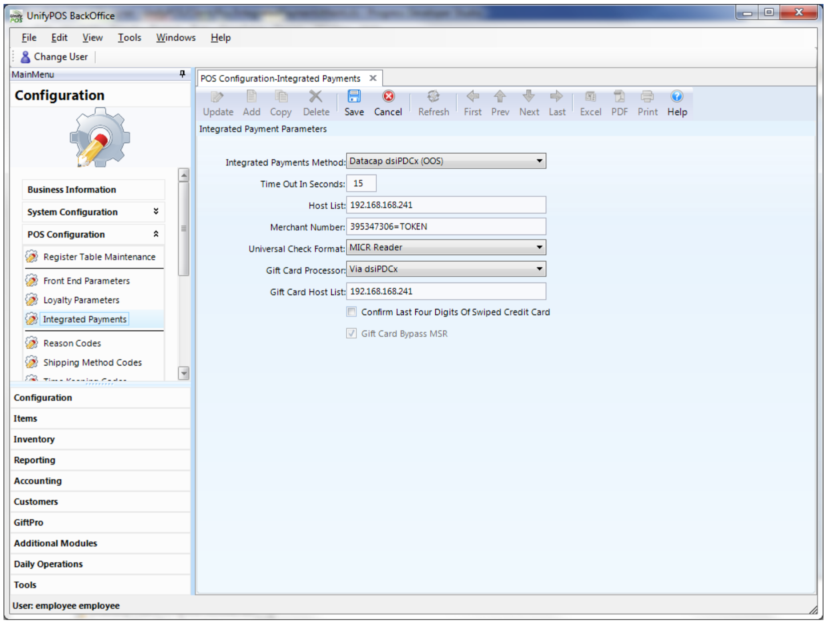
2. OOS Overview

UnifyPOS supports two different OOS solutions both of which shield UnifyPOS from sensitive cardholder data. At no time does UnifyPOS have access to this sensitive data such as full track data, PAN, expiration date or PIN block. The following two sections will give specific details about each solution.

2.1. Datacap Systems dsiPDCx

To configure UnifyPOS to use the dsiPDCx OOS control you would select "Datacap dsiPDCx (OOS)" from the Integrated Payments Method drop down box. The following parameters also need to be setup correctly:

- Host List – this is the host box the OOS control will be sending/receiving requests/responses to/from. If you are using Mercury Payments Systems this will be setup exactly the same as it was prior to 11.1.95. If you are using NET ePay then this will be the IP address of the NET ePay server.
- Merchant Number – this is the merchant number assigned to the merchant. The value entered here is sent with each request to the processor so it must be entered correctly.
- Universal Check Format – if you are using Check Authorization this will determine what format is used. Currently there are two supported formats:
    - MICR Reader – this REQUIRES an OPOS MICR that will read the MICR from the check and send a request to the processor for authorization. Please Note: manual MICR information is NOT allowed.
    - DL Manual – this is the manual input method where the cashier would manually enter information from the customer drivers license.
- Gift Card Processor – this drop down box is used to let UnifyPOS know how to authorized Gift Cards. There are only two options:
    - Via dsiPDCx – Gift Cards will be authorized using the OOS control.
    - Internal Unify GiftPro – UnifyPOS is handling all Gift Card requests.
- Gift Card Host List – this is only used if using the dsiPDCx control for Gift Card processing. This is the host box the OOS control will be sending/receiving requests/responses to/from. If you are using Mercury Payments Systems this will be setup exactly the same as it was prior to 11.1.95. If you are using NET ePay then this will be the IP address of the NET ePay server.



Integrated Payment Parameters

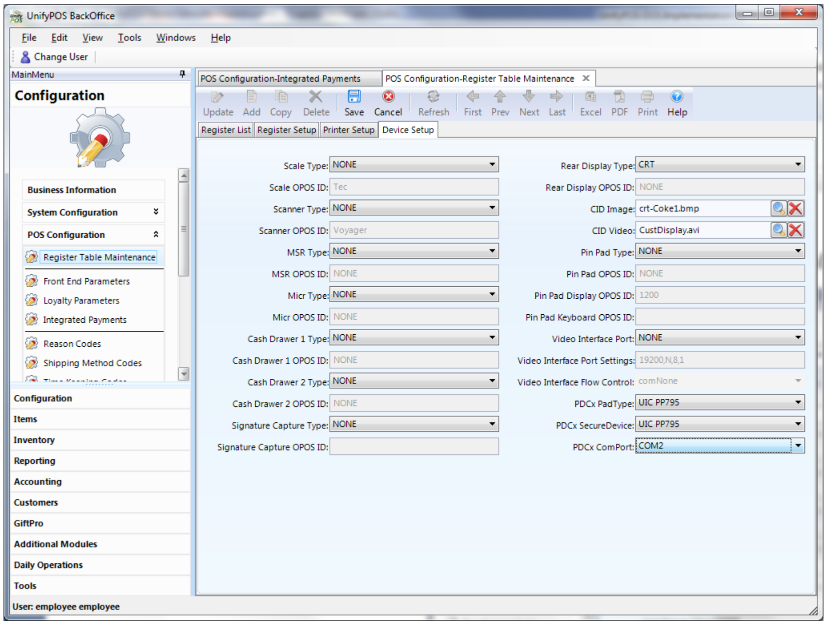
Integrated Payments Method: Datacap dsiPDCx (OOS)
Time Out In Seconds: 15
Host List: 192.168.168.241
Merchant Number: 395347306=TOKEN
Universal Check Format: MICR Reader
Gift Card Processor: Via dsiPDCx
Gift Card Host List: 192.168.168.241
☐ Confirm Last Four Digits Of Swiped Credit Card
☑ Gift Card Bypass MSR

After enabling “Datacap dsiPDCx (OOS)” you also need to select the PadType, SecureDevice and ComPort for each register. As noted in Section 1 UnifyPOS can no longer have access to any sensitive cardholder data so these settings will be used by the OOS control to communicate to the hardware.

- PDCx PadType – this is the Pin Pad type being used to enter a PIN. Please Note: Some of the devices support Signature Capture as well such as UIC PP795 and Equinox L5300. As of this writing the following PadTypes are supported:
  - Verifone 1000SE
  - Verifone Vx810
  - UIC PP795
  - Magtek IPAD
  - Equinox L5300
- PDCx SecureDevice – this is the secure MSR being used to swipe the payment cards. As of this writing the following SecureDevices are supported:
  - Legacy PDC (ordered through Datacap)
  - PDC with Blowfish Encryption (ordered through Datacap)
  - Verifone Vx810
  - UIC PP795
  - IDTech MSR
  - IDTech SecureMag MSR
  - Magtek MINI MSR – HID
  - Magtek SecureSwipe MSR – HID
  - Magtek IPAD Pin Pad

- Magtek MINI MSR – RS232
- Magtek MINI MSR – USB
- Magtek SecureSwipe MSR – USB
- VivoPay 4500m contactless with MSR
- J2 650 POS Internal MSR
- Equinox L5300

- PDCx ComPort – this is the COM PORT the OOS control uses to communicate with the secure device. This could be a Virtual ComPort if using a USB device.



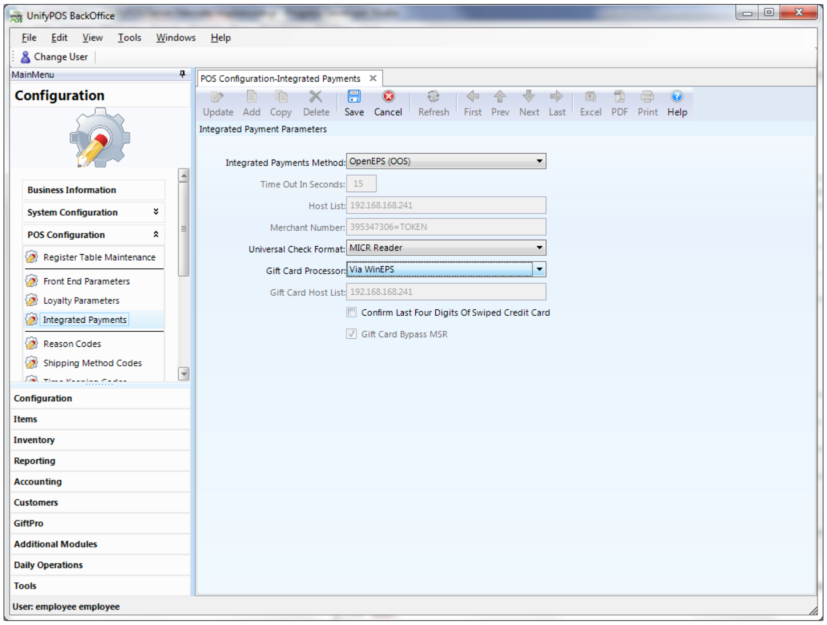
Scale Type:	NONE	Rear Display Type:	CRT
Scale OPOS ID:	Tec	Rear Display OPOS ID:	NONE
Scanner Type:	NONE	CID Image:	crt-Coke1.bmp
Scanner OPOS ID:	Voyager	CID Video:	CustDisplay.avi
MSR Type:	NONE	Pin Pad Type:	NONE
MSR OPOS ID:	NONE	Pin Pad OPOS ID:	NONE
Micr Type:	NONE	Pin Pad Display OPOS ID:	1200
Micr OPOS ID:	NONE	Pin Pad Keyboard OPOS ID:	
Cash Drawer 1 Type:	NONE	Video Interface Port:	NONE
Cash Drawer 1 OPOS ID:	NONE	Video Interface Port Settings:	19200,N,8,1
Cash Drawer 2 Type:	NONE	Video Interface Flow Control:	comNone
Cash Drawer 2 OPOS ID:	NONE	PDCx PadType:	UIC PP795
Signature Capture Type:	NONE	PDCx SecureDevice:	UIC PP795
Signature Capture OPOS ID:		PDCx ComPort:	COM2

2.2. Retalix Payments OpenEPS

To configure UnifyPOS to use the OpenEPS OOS control you would select “OpenEPS (OOS)” from the Integrated Payments Method drop down box. The following parameters also need to be setup correctly:

- Universal Check Format – if you are using Check Authorization this will determine what format is used. Currently there are two supported formats:
  - MICR Reader – this REQUIRES an OPOS MICR that will read the MICR from the check and assign the appropriate OpenEPS bits.
  - DL Manual – this is the manual input method where the cashier would manually enter information from the customer drivers license. Unlike the dsiPDCx control where UnifyPOS prompts the cashier to enter this information in a dialog box the OpenEPS control will prompt UnifyPOS for the required data elements.

- Gift Card Processor – this drop down box is used to let UnifyPOS know how to authorized Gift Cards. There are only two options:
    - Via OpenEPS – Gift Cards will be authorized using the OpenEPS control.
    - Internal Unify GiftPro – This is currently NOT supported as the OpenEPS control does not allow UnifyPOS access to the Gift Card track data in a secure manner. While UnifyPOS does have access to the track data the OpenEPS control does NOT prevent credit/debit card track data from being returned to UnifyPOS. Until the OpenEPS control prevents sensitive card holder data from being returned to UnifyPOS this will not be supported.



Integrated Payment Parameters

Integrated Payments Method: OpenEPS (OOS)

Time Out In Seconds: 15

Host List: 192.168.168.241

Merchant Number: 395347306=TOKEN

Universal Check Format: MICR Reader

Gift Card Processor: Via WinEPS

Gift Card Host List: 192.168.168.241

☐ Confirm Last Four Digits Of Swiped Credit Card

☑ Gift Card Bypass MSR

2.3. Additional OOS Considerations

The following recommendations should be met to guarantee UnifyPOS to be out of scope:

- Do not install an additional MSR on the POS terminal on top of the Secure Device being used for payments unless using the MSR to swipe an employee's badge.
- If UnifyPOS is setup to swipe employee badges **NEVER** install a "keyboard wedge" MSR. UnifyPOS has NO control over this type of MSR as the data is sent just as if it was keyed by the cashier. If a cashier were to swipe a credit card by mistake it is possible sensitive card holder data could be displayed/logged within UnifyPOS.
- Instead of a "keyboard wedge" MSR use an OPOS MSR as UnifyPOS will ONLY enable this device when prompting the cashier to swipe their badge.

3. Security Implementation Guideline

3.1. Introduction

Systems which process payment transactions necessarily handle sensitive cardholder account 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.

In April 2000, Visa began a proactive approach to payment security by announcing the Cardholder Information Security Program (CISP) as a standard for securing Visa cardholder data. Effective since June 2001, CISP compliance has been required for all entities that store, process or transmit Visa cardholder data. Starting September 30, 2008 this program advances to the Payment Application Data Security Standard (PA-DSS).

3.2. Visa CISP Overview

When customers offer their bankcard at the point of sale, over the Internet, on the phone, or through the mail, they want assurance that their account information is safe. That is why USA Visa has instituted the **Cardholder Information Security Program (CISP)**. Mandated since June 2001, the program is intended to protect Visa cardholder data—wherever it resides—ensuring that members, merchants and service providers maintain the highest information security standard.

3.3. The PCI Industry Standard

To achieve compliance with CISP, merchants and service providers must adhere to the Payment Card Industry (PCI) Data Security Standard, which offers a single approach to safeguarding sensitive data for all card brands. This Standard is a result of collaboration between Visa and MasterCard and is designed to create common industry security requirements, incorporating the CISP requirements. Other card companies operating in the U.S. have also endorsed the PCI Data Security Standard within their respective programs.

3.4. Payment Application Data Security Standard (PA-DSS)

PA-DSS is the Council-managed program (Payment Card Industry Security Standards Council or PCI SSC) formerly under the supervision of the Visa Inc. program known as the Payment Application Best Practices (PABP). The goal of PA-DSS is to help software vendors and others develop secure payment applications that do not store prohibited data, such as full magnetic stripe, CVV2 or PIN data, and ensure their payment applications support compliance with the PCI DSS. Payment applications that are sold, distributed or licensed to third parties are subject to the PA-DSS requirements. In-house payment applications developed by merchants or service providers that are not sold to a third party are not subject to the PA-DSS requirements, but must still be secured in accordance with the PCI DSS.

3.5. Understanding “PA-DSS” vs. “PCI Compliance”.

A software vendor has a responsibility to be “PA-DSS Compliant” if they store, process, transmit or have access to sensitive cardholder data. Since UnifyPOS does not meet any of these criteria it is no longer required to be “PA-DSS Compliant”. This falls on Datacap Systems and Retalix Payments as their applications are handling all aspects of the payment process. Please review the appropriate documentation as to how to implement their payment solution correctly.

Note: We want to reiterate that obtaining “PCI Compliance” falls on you (the merchant) and your UnifyPOS reseller, working together, using PCI compliant server architecture with proper hardware & software configurations and access control procedures.

After installation and initial certification to PCI standards, you should then follow our recommended operational guidelines, defined in this document, to ensure continued best practices for management of your storefront.

Visa U.S.A. specifies different levels of compliance requirements, driven mostly by the annual transaction volume of your storefront. You should read the documentation provided by Visa to determine the level of PCI Compliance required for your business.
Depending on annual transaction volume, CISP requirements range from completing a self-assessment questionnaire to engaging an independent security assessor for conducting annual on-site security audits. See www.visa.com/cisp and contact your bank, processor, or acquirer for more information.

Notes on fines: As quoted from Visa's website “If a merchant or service provider does not comply with the security requirements or fails to rectify a security issue, Visa may:

- Fine the acquiring member
- Impose restrictions on the merchant or its agent
- Permanently prohibit the merchant or its agent from participating in Visa programs

Members receive protection from fines for merchants or service providers that have been compromised but found to be CISP-compliant at the time of the security breach. Members are subject to fines up to **$500,000 per incident** for any merchant or service provider that is compromised and not CISP-compliant at the time of the incident.”

Note: The CISP requirements for your systems do not change, and must be validated, no matter if you use an in-house product like Datacaps NET ePay, Retalix Payments Connected Payments or a Visa approved online service provider such as VeriSign®.

For example, the requirement for unique usernames and strong passwords does not change and is even a missing feature on some of the CISP listed Internet gateways. Before being validated, you must ask your staff if the entire system is conforming to the requirements or just the service provider themselves.

3.6. PCI-DSS Requirements.

The following **12 Requirements** comprise the Payment Card Industry Data Security Standard:

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 Data
4. Encrypt transmission of cardholder data and sensitive information across public networks

Maintain a Vulnerability Management Program

5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications

Implement Strong Access Control Measures

7. Restrict access to data by business need-to-know
8. Assign a unique ID to each person with computer access
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

3.7. Access Control

The PCI standard 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. Additionally any default accounts provided with operating systems, databases and/or devices should be removed/disabled/renamed if possible, or at least should have complex passwords and should not be used. Examples of such default administrator accounts include administrator (Windows systems), as (SQL/MSDE), and root (UNIX/Linux).

The PCI standard requires the following password complexity for compliance:

- Passwords must be at least 7 characters
- Passwords must be include both numeric and alphabetic characters
- Passwords must be changed at least every 90 days

- New passwords cannot be the same as the last 4 passwords

Below are the other PCI account requirements beyond uniqueness and password complexity:

- If an incorrect password is provided 6 times the account should be locked out
- Account lock out duration should be at least 30 min. (or until an administrator resets it)
- Sessions idle for more than 15 minutes should require re-entry of username and password to reactivate the session.

These same account and password criteria must also be applied to any applications or databases included in payment processing to be PCI compliant.

3.8. Remote Access Control

The PCI standard requires that if employees, administrators, or vendors can access the payment processing environment remotely; access should be authenticated using a 2-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, should include only the access rights required for the service rendered, and should be robustly audited.

Access to hosts within the payment processing environment via 3rd party remote access software such as Remote Desktop (RDP)/Terminal Server, PCAnywhere, etc. requires that when such programs are used that there sessions are encrypted with at least 128 bit encryption (this requirement is in addition to the requirement for 2-factor authentication required for users connecting from outside the payment processing environment). For RDP/Terminal Services this means using the high encryption setting on the server, and for PCAnywhere it means using symmetric or public key options for encryption.

UnifyPOS does not directly support remote access for maintenance, monitoring, operation, troubleshooting or updates. Osprey Retail Systems does not use remote access software to deliver any services, software, or support to users of UnifyPOS. If merchants, integrators or resellers elect to use third party remote access independent of UnifyPOS, they should observe the following remote access procedures:

- Change default settings in the remote access software (for example, change default passwords and use unique passwords for each customer).
- Allow connections only from specific (known) IP/MAC addresses.
- Use strong authentication and complex passwords for logins according to PCI DSS Requirements 8.1, 8.3, and 8.5.8–8.5.15
- Enable encrypted data transmission according to PCI DSS Requirement 4.1
- Enable account lockout after a certain number of failed login attempts according to PCI DSS Requirement 8.5.1
- Configure the system so a remote user must establish a Virtual Private Network “VPN”) connection via a firewall before access is allowed.
- Enable the logging function.
- Restrict access to customer passwords to authorized reseller/integrator personnel.
- Establish customer passwords according to PCI DSS Requirements 8.1, 8.2, 8.4, and 8.5.

3.9. Wireless Access Control

The PCI standard requires the encryption of cardholder data transmitted over wireless connections. The following items identify the PCI standard requirements for wireless connectivity to the payment environment:

- Firewall/port filtering services should be placed between wireless access points and the payment processing environment with rules restricting access
- Use of appropriate encryption mechanisms such as **VPN, SSL/TPS at 128** bit, WEP at 128 bit, and/or WPA
- If WEP is used the following additional requirements must be met:
    - Another encryption methodology must be used to protect cardholder data
    - If automated WEP key rotation is implemented key change should occur every 10-30 minutes
    - If automated key change is not used, keys should be manually changed at least quarterly and when key personnel leave the organization
- Vendor supplied defaults (administrator username/password, SSID, and SNMP community values) should be changed
- Access point should restrict access to known authorized devices (using MAC Address filtering)

3.10. Network Encryption

The PCI standard requires the use of strong cryptography and encryption techniques (at least 128 bit); such as Secure Sockets Layer (SSL) and Internet Protocol Security (IPSEC) to safeguard sensitive cardholder data during transmission over public networks (like the Internet).

Additionally PCI requires that cardholder information never be sent via e-mail without strong encryption of the data.

3.11. UnifyPOS Compliance

All versions of UnifyPOS 11.1.95 or above implement all of the PCI Data Security Standard requirements that are applicable to UnifyPOS.

- **UnifyPOS** does not store any magnetic stripe (Track 1 or 2), card verification (CVV, CVV2, etc.) or PIN data, ever. In fact **UnifyPOS** has NO access to this sensitive card holder data at all.
- **UnifyPOS** uses the truncated account and expiration date information returned by NET ePay and/or Connected Payments in every area where it is either stored or displayed.

3.12. Additional System Security Recommendations

Additional overall security can be realized by implementing the following:

- Use a router which implements NAT (Network Address Translation).

- Use antivirus software with auto update capability, from vendors such as McAfee, Norton, Panda, Kaspersky, Trend Micro, etc.
- Enable firewall services (either software based like Windows Firewall or hardware based) between the payment processing environment and the internet access device (typically an ISP provided router/modem).
- Define and use strong passwords to restrict access to authorized personnel.
- Test and install security related Windows, SQL/MSDE/OE DB updates, service packs and hot fixes promptly. Consider using automatic updating.

4. References, Acknowledgements

4.1. References

This document references the following publications.

- PCI DSS version 1.2 released October 2008
- PCI PA-DSS version 1.2.1 released July 2009
- UnifyPOS Installation and Configuration Guides
- NET ePay User Guide

4.2. Acknowledgements

Osprey Retail Systems, Inc. software products actively use, support and promote the Progress Software OpenEdge development environment located at www.progress.com