Connected Payments

PCI Implementation Guide

Version 1.08

September 2014

Address correspondence to:

Manager, Information Solutions Group

NCR Corporation

Discovery Centre, 3 Fulton Road

Dundee, DD2 4SW

Scotland

Internet Address:

http://www.info.ncr.com/Feedback

It is the policy of NCR Corporation (NCR) to improve products as new technology, components, software, and firmware become available. NCR, therefore, reserves the right to change specifications without prior notice.

All features, functions, and operations described herein may not be marketed by NCR in all parts of the world. In some instances, photographs are of equipment prototypes. Therefore, before using this document, consult with your NCR representative or NCR office for information that is applicable and current.

To maintain the quality of our publications, we need your comments on the accuracy, clarity, organization, and value of this book.

Revision History

Date	Changed By	Comment	Version
2007 03-08	MJM	▪ Initial Draft	821
2012 03-26	Slava Gomzin, CISSP	▪ Initial Release	1.0
2012 04-02	Slava Gomzin, CISSP	▪ Release 1.01	1.01
2012 07-10	Slava Gomzin, CISSP	▪ Updated firewall guide - added CRL Validation section with information about SSL server certificate revocation validation	1.02
2012 11-19	Slava Gomzin, CISSP	▪ Updated firewall guide - certificate revocation validation addresses	1.03
2013 03-25	MJM	▪ Format change and content revision	1.03
2014 05-28	MJM	▪ Included the updated certificate revocation validation addresses from versions 1.04 and 1.05 of this document as updated by Slava.	1.06
2014 07-03	MJM	▪ Windows XP is not longer supported by Microsoft, so it is no longer listed as a supported OS.	
2014 07-30	MJM	▪ Added crl.ws.symantec.com to the Certificate Validation list.	1.07
2014 08-06	MJM	▪ Updated Certificate Validation list with additional Verisign / Symantec URL & IP information, as well as pointer to the list of full IP addresses.	1.08
2014 09-09	MJM	▪ Updated Format to NCR	

This implementation guide is updated annually along with the PCI-DSS audit. Additional updates are performed as changes to the software necessitate.

The most recent copy of this document can be acquired by contacting Retalix at ConnectedSupport@retalix.com. If you already have an account for Connected Payments, you may download the latest version from the Customer Service page.

Table of Contents

PCI Standards

PCI Introduction

What is PCI?

The Payment Card Industry (PCI) Data Security Standard (DSS) is the latest standard for payment card data security. The PCI standard forms the basis of maintaining a secure environment in order to prevent the unauthorized use of customer payment card data. Originally initiated by the Visa card company to create a set of standards for securing cardholder information under the name CISP (Cardholder Information Security Program), the latest PCI standards are now administrated by an independent PCI Security Standards Council, and embraced and managed by credit issuers such as American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International.

The latest information on PCI standards can be found on the PCI Security Council website: www.pcisecuritystandards.org.

What does PCI mean to me?

The information contained in this document defines the responsibilities of the merchant to create and maintain a PCI compliant environment for the payment software to be deployed in.

The merchant is responsible for maintaining a PCI compliant payments environment.

Failure to maintain a PCI compliant environment may result in fines, penalties, restrictions, and financial responsibility for misused cardholder information.

To meet PCI requirements, the environment in which payments software is deployed must be properly configured. The payments software that Retalix and / or its affiliates produces and its supporting applications have been made compliant with PCI standards, but for the merchant payment environment to properly maintain the required security for cardholder information, specific further setup is required.

This document is designed to provide information to merchants related to the deployment of Retalix payments software products and supporting applications within their network environment in order to allow the merchant to uphold PCI requirements and best practices.

To assist the merchant in their responsibility to maintain a PCI complainant payments environment, this document outlines PCI requirements and provides instructions for deploying Retalix payments software in

compliance with those PCI requirements; the merchant is responsible for knowing an adhering to all additional and current PCI requirements beyond those addressed within this document.

What is a Security Breach?

PCI security precautions are intended to prevent and deter situations that might lead to the release of payments information to unintended parties.

From the PA-DSS version 2.0 document:

Secure payment applications, when implemented in a PCI DSS-compliant environment, will minimize the potential for security breaches leading to compromises of full magnetic stripe data, card verification codes and values (CAV2, CID, CVC2, CVV2), PINs and PIN blocks, and the damaging fraud resulting from these breaches.

Thus a breach can most easily be defined as a compromise of the security surrounding credit card information, which can lead to that information being released to unauthorized parties.

Reporting Security Breaches

Retalix payments software utilizes encryption to keep cardholder information safe. If it is known or suspected that any encryption method utilized by the payments software or any of its components is breached, contact Retalix and / or its affiliates immediately.

Naturally, if a breach is suspected, it is recommended that the encryption keys in use be changed by the merchant immediately. Follow the instructions in the Changing the Encryption Keys section to update your keys.

PCI Merchant Environment

Installation Environment

Retalix provides PCI compliant payments software products, but the merchant environment into which they are installed has an impact on the safety and security of cardholder information that is used to process transactions.

Network and physical security are the responsibility of the merchant; for the production environment to be fully PCI compliant, the below PCI requirements must be followed. In addition to this guide, it is highly recommended that the merchant review the latest PCI DSS requirements themselves, in order to ensure that all aspects of their payments environment meet PCI requirements. The latest PCI DSS standards can be located by contacting the PCI Security Council, or visiting their web site: www.pcisecuritystandards.org.

This chapter covers PCI requirements dealing directly with the merchant network environment.

Network Requirements

PCI requires that the production environment be engineered to protect cardholder information. It is the merchant's responsibility to provide a secure networking environment, including providing security for any needed web based access and properly managing any external network connections such as VPNs and remote software access.

PCI-DSS Requirement	PCI -DSS Testing Procedure
2.2.1 Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.) **Note:** *Where virtualization technologies are in use, implement only one primary function per virtual system component.*	**2.2.1.a** For a sample of system components, verify that only one primary function is implemented per server.
	2.2.1.b If virtualization technologies are used, verify that only one primary function is implemented per virtual system component or device.

As per the PCI-DSS requirements above, payments software must not be installed on servers that provide functions that require different security levels. This means, for example, that OpenEPS can be installed on the same system that runs the POS back office, or other payment applications, but should never be installed on systems that perform network functions such as DHCP, DNS, routing, web services etc.

PCI-DSS Requirement	PCI -DSS Testing Procedure
5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	
5.1.1 Ensure that all anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.	
5.2 Ensure that all anti-virus mechanisms are current, actively running, and generating audit logs.	**5.2.d** For a sample of system components, verify that anti-virus software log generation is enabled and that such logs are retained in accordance with PCI DSS Requirement 10.7.

Make sure that virus scanning software is present within the payments environment. PCI requirements state that virus scanners be up to date, active, and be capable of writing log.

PCI-DSS Requirement	PCI -DSS Testing Procedure
6.1 Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. ***Note:*** *An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*	6.1.a For a sample of system components and related software, compare the list of security patches installed on each system to the most recent vendor security patch list, to verify that current vendor patches are installed.
	6.1.b Examine policies related to security patch installation to verify they require installation of all critical new security patches within one month.

PCI requirements state that all software in the payments environment must have the latest security updates and that all critical security related patches be installed within a month of release.

PCI-DSS Requirement	PCI -DSS Testing Procedure
8.1 Assign all users a unique ID before allowing them to access system components or cardholder data.	**8.1** Verify that all users are assigned a unique ID for access to system components or cardholder data.

PCI-DSS Requirement	PCI -DSS Testing Procedure
8.2 In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users: • Something you know, such as a password or passphrase • Something you have, such as a token device or smart card • Something you are, such as a biometric	**8.2** To verify that users are authenticated using unique ID and additional authentication (for example, a password) for access to the cardholder data environment, perform the following: • Obtain and examine documentation describing the authentication method(s) used. • For each type of authentication method used and for each type of system component, observe an authentication to verify authentication is functioning consistent with documented authentication method(s).

The PCI standard requires that access to all systems in the payment processing environment be protected through use of unique user accounts and complex passwords, a token, device, smart card, or a biometric. Unique user accounts indicate that every account used is associated with an individual user and/or process with no use of group or shared accounts (accounts which are used by more than one user or process), and no use of generic accounts and/or passwords. This ensures that actions taken can be logged and traced back to individual, authorized users.

PCI-DSS Requirement	PCI -DSS Testing Procedure
2.1 Always change vendor-supplied defaults **before** installing a system on the network, including but not limited to passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.	
2.1.1 For wireless environments connected to the cardholder data environment or transmitting cardholder data, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.	

Any default accounts provided with operating systems and/or devices must be changed, and assigned secure authentication, or renamed and disabled before implementation in the payments environment. Likewise, also change any other security related defaults on systems or devices before installing into the payments environment.

PCI-DSS Requirement	PCI -DSS Testing Procedure
8.5.9 Change user passwords at least every 90 days.	**8.5.9.a** For a sample of system components, obtain and inspect system configuration settings to verify that user password parameters are set to require users to change passwords at least every 90 days.

PCI-DSS Requirement	PCI -DSS Testing Procedure
8.5.10 Require a minimum password length of at least seven characters.	**8.5.10.a** For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require passwords to be at least seven characters long.
8.5.11 Use passwords containing both numeric and alphabetic characters.	**8.5.11.a** For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require passwords to contain both numeric and alphabetic characters.
8.5.12 Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.	**8.5.12.a** For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require that new passwords cannot be the same as the four previously used passwords.

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

PCI-DSS Requirement	PCI -DSS Testing Procedure
8.5.13 Limit repeated access attempts by locking out the user ID after not more than six attempts.	**8.5.13.b** For service providers only, review internal processes and customer/user documentation to verify that non-consumer user accounts are temporarily locked-out after not more than six invalid access attempts.
8.5.14 Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.	**8.5.14** For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require that once a user account is locked out, it remains locked for a minimum of 30 minutes or until a system administrator resets the account.
8.5.15 If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.	**8.5.15** For a sample of system components, obtain and inspect system configuration settings to verify that system/session idle time out features have been set to 15 minutes or less.

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

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

PCI-DSS Requirement	PCI -DSS Testing Procedure

PCI-DSS Requirement	PCI -DSS Testing Procedure
11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades). ***Note:*** *It is not required that four passing quarterly scans must be completed for initial PCI DSS compliance if the assessor verifies 1) the most recent scan result was a passing scan, 2) the entity has documented policies and procedures requiring quarterly scanning, and 3) vulnerabilities noted in the scan results have been corrected as shown in a rescan. For subsequent years after the initial PCI DSS review, four passing quarterly scans must have occurred.*	

Networks should be tested for vulnerability on a regular basis. Many systems are required to be tested at least quarterly.

LAN Setup

The Local Area Network requires both physical and electronic security. It is the responsibility of the merchant to provide appropriate physical and electronic security to protect customer card information. This section covers some specific suggestions for LAN network security relating to Retalix payments software.

Merchants must prevent unauthorized access to any directory that contains payment application logs, configuration files and/or program files, and to the Windows Registry on any system processing payments. Only Administrative user accounts and accounts that are required by the payments application itself to run or perform its assigned function should be granted access to these directories or to the registry.

PCI-DSS Requirement	PCI -DSS Testing Procedure
1.1 Establish firewall and router configuration standards that include the following:	**1.1** Obtain and inspect the firewall and router configuration standards and other documentation specified below to verify that standards are complete. Complete the following:
1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations	**1.1.1** Verify that there is a formal process for testing and approval of all network connections and changes to firewall and router configurations.
1.1.3 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone	**1.1.3.a** Verify that firewall configuration standards include requirements for a firewall at each Internet connection and between any DMZ and the internal network zone.

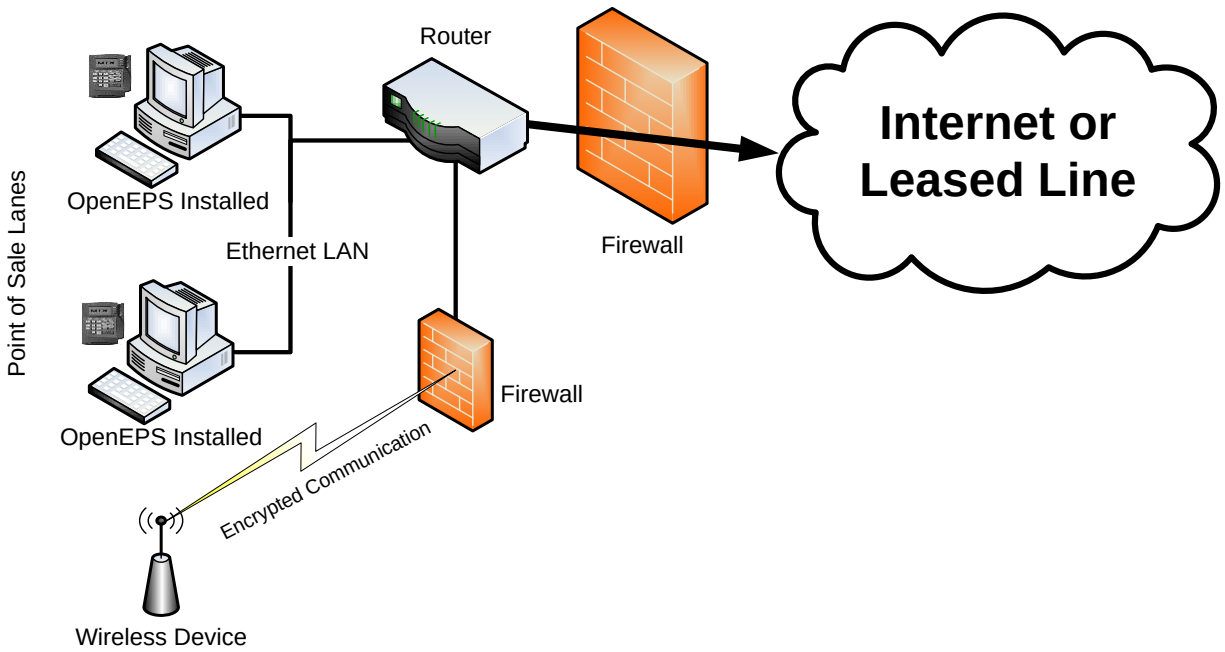
PCI-DSS Requirement	PCI -DSS Testing Procedure
1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment. ***Note:*** *An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.*	**1.2** Examine firewall and router configurations to verify that connections are restricted between untrusted networks and system components in the cardholder data environment, as follows:

Merchants must install and maintain firewalls to prevent unauthorized access to the payments network.

Servers and systems containing customer card information must also be protected physically. Any server where sensitive card data is stored must be placed in a secure server room or otherwise physically secured to prevent unauthorized access to the physical hardware which could compromise security

POS systems at the lane should be made as difficult to gain unauthorized physical access to as feasible.

LAN Network



Wireless Networking

When installing a payments application into a production environment that includes wireless networking, additional requirements must be met. PCI DSS requirements section 1, 2 and 4 (specifically 1.2.3, 2.1.1, & 4.1.1) should be reviewed for complete information on wireless setup. The PA-DSS section 6.1 aligns with PCI DSS Requirements 1.2.3 & 2.1.1. Section 6.1 is listed below:

6.1 For payment applications using wireless technology, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings. The wireless technology must be implemented securely. ***Aligns with PCI DSS Requirements 1.2.3 & 2.1.1***

The following information is provided to assist in wireless setup:

6.1.a Verify encryption keys were changed from default at installation, and are changed anytime anyone with knowledge of the keys leaves the company or changes positions

If anyone with knowledge of any of the encryption keys leaves the company or changes position, keys to which they had access must be changed to maintain PCI compliance.

6.1.b Verify default SNMP community strings on wireless devices were changed

6.1.c Verify default passwords/passphrases on access points were changed

Vendor supplied defaults (administrator username/password, SSID, and SNMP community values) must be changed.

6.1.d Verify firmware on wireless devices is updated to support strong encryption for authentication and transmission over wireless networks

For wireless networks transmitting cardholder data or connected to the cardholder data environment, verify that industry best practices (for example, IEEE 802.11i) are used to implement strong encryption for authentication and transmission.

PCI-DSS Requirement	PCI -DSS Testing Procedure
4.1.1 Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission. **Note:** *The use of WEP as a security control was prohibited as of 30 June 2010.*	**4.1.1** For wireless networks transmitting cardholder data or connected to the cardholder data environment, verify that industry best practices (for example, IEEE 802.11i) are used to implement strong encryption for authentication and transmission

Ensure that each wireless device in use has been updated and properly supports strong encryption.

For wireless networks that transmit cardholder data, encryption must be in use, such as: WPA or WPA2, IPSEC VPN, SSL/TLS at 128 bit.

For wireless implementations, it is prohibited to implement WEP (Wired Equivalency Protocol); the use of WEP as a security control was prohibited as of 30 June.

Messages exchanged between separate portions of the Retalix payment software are encrypted; this encryption satisfies PCI requirements on card holder data transmission across wired LAN networks, but additional encryption and security is necessary for wireless networks, as noted above. “For wireless networks transmitting cardholder data or connected to the cardholder data environment, verify that industry best practices (for example, IEEE 802.11i) are used to implement strong encryption for authentication and transmission” (PCI DSS section 4.1.1)”.

• Install a firewall between any wireless networks and systems that store cardholder data

Wireless connection points must be secured with the appropriate use of firewalls. The firewall must reside between the wireless network and any system that stores card holder data, as show in LAN Network the diagram above.

• Configure firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment

Firewall/port filtering services must be placed between wireless access points and the payment processing environment with rules restricting access. If there is no business need for access, then access must be prohibited to systems containing card holder data.

Access points should restrict access to known authorized devices (using MAC address filtering).

6.1.e Verify other security-related wireless vendor defaults were changed, if applicable

If any wireless device has other default settings related to security that would benefit from changing or making unique (changing the default SSID name and setting the device to not broadcast its SSID, for example), ensure that these settings are changed so as to be unique.

WAN Setup / External Connections

This section covers requirements for WAN setup and external connections, such as VPNs into the LAN, and connections from OpenEPS to the Connected Payments' Data Centers.

PCI-DSS Requirement	PCI -DSS Testing Procedure
1.3.3 Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment.	**1.3.3** Verify direct connections inbound or outbound are not allowed for traffic between the Internet and the cardholder data environment.

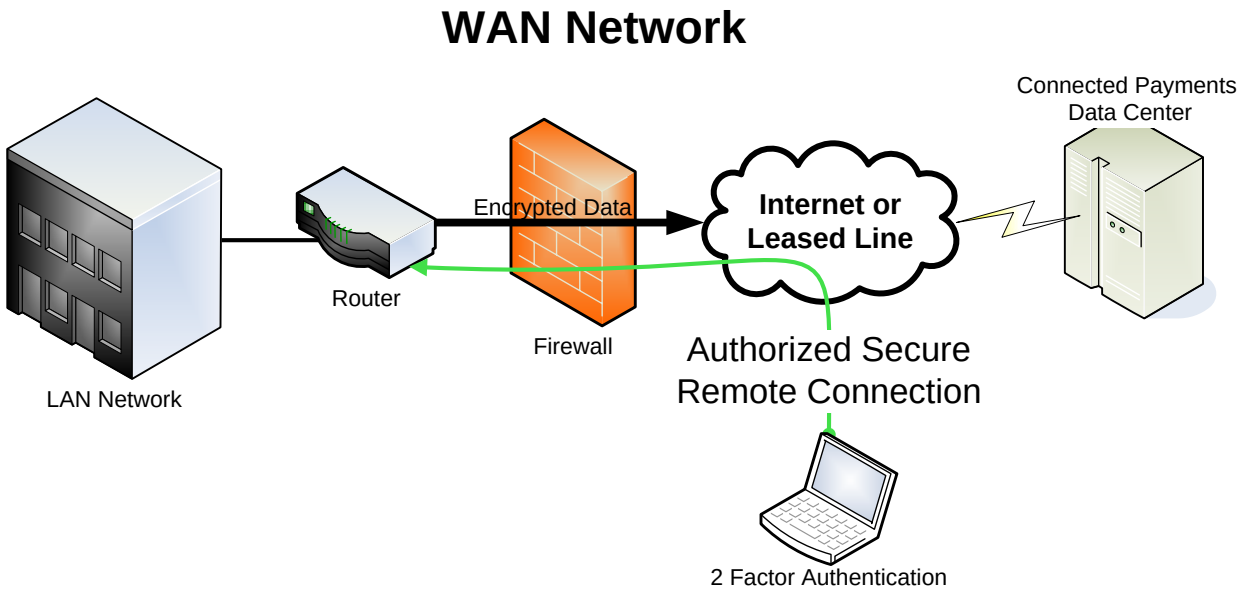
Payments software and components must never be deployed onto systems that allow direct inbound or outbound connections to the Internet. Payments software must be deployed on servers that reside behind firewalls, with communication to any external financial processor secured and allowed through the firewall. The firewalls must be configured to protect cardholder information contained within the payments software by limiting the incoming and outgoing connections to only those which are required.

The computer on which the payments software runs must never allow any incoming connections from the internet. In order to comply with PA-DSS requirement 9.1.b, no incoming internet connections can be allowed to a payment server:

9.1.b If customers could store cardholder data on a server connected to the Internet, examine PA-DSS Implementation Guide prepared by vendor to verify customers and resellers/integrators are instructed not to store cardholder data on Internet-accessible systems (for example, web server and database server must not be on same server).

PCI-DSS Requirement	PCI -DSS Testing Procedure
2.3 Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for webbased management and other nonconsole administrative access.	

PCI Requirements state that it is necessary to use strong encryption technology such as Secure Sockets Layer/Transport Layer Security (SSL/TLS), SSH, or Virtual Private Network (VPN) to secure communications over any public network, such as the internet.



Remote Network Connections

PA-DSS Requirement	PA-DSS Testing Procedure
10.3.2 If vendors, resellers/integrators, or customers can access customers' payment applications remotely, the remote access must be implemented securely.	**10.3.2.a** If the software vendor uses remote access products for remote access to the customers' payment application, verify that vendor personnel implement and use remote access security features.

Note: Examples of remote access security features include: • *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 (See PA-DSS Requirements 3.1.1 through 3.1.10)* • *Enable encrypted data transmission according to PA-DSS Requirement 12.1* • *Enable account lockout after a certain number of failed login attempts (See PADSS Requirement3.1.8)* • *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 PA-DSS Requirements 3.1.1through 3.1.10.* **Aligns with PCI DSS Requirement 8.3**	**10.3.2.b** If resellers/integrators or customers can use remote access software, examine PA-DSS Implementation Guide prepared by the software vendor, and verify that customers and resellers/integrators are instructed to use and implement remote access security features.

As per PCI-DSS, it is required that any type of remote access to the payments network be established through secure methods, whether the remote access come from outside the merchant's company, such as Retalix technical support, or even from inside the merchant's company, such as remote administration.

The above PA-DSS requirements list a section of example security features that must be employed, when available. Be sure to review the above list and incorporate any of the suggested security features that can be incorporated within your network.

It is necessary for the merchant to establish secure methods of determining the identities of users who will be granted access to the local network. Use an access request form that is filled out when any outside party, including Retalix personnel, needs to remotely connect to a production environment system. This form must contain, at minimum, information on who is accessing the network, their contact information and the contact information of their immediate superior, the purpose of the access, and the expected duration of the access.

PCI-DSS Requirement	PCI -DSS Testing Procedure

PCI-DSS Requirement	PCI -DSS Testing Procedure
8.5.6 Enable accounts used by vendors for remote access only during the time period needed. Monitor vendor remote access accounts when in use.	**8.5.6.a** Verify that any accounts used by vendors to access, support and maintain system components are disabled, and enabled only when needed by the vendor.

Vendor access accounts must be disabled while not in use.

For internal access to the payments network, be sure to establish internal guidelines for determining who may access the network, restricting the access to only those who have a legitimate business need to have network access, and periodically reviewing the access list to determine if that business need continues to exist for each individual that has access.

For remote access requests, the identity of the requesting individual must be firmly established. Contact known personnel, such as the account manager or their designate that is assigned to your company. This may also entail contacting the requesting individual or company at a known telephone number or e-mail address.

PCI-DSS Requirement	PCI -DSS Testing Procedure
8.5.8 Do not use group, shared, or generic accounts and passwords, or other authentication methods.	**8.5.8.a** For a sample of system components, examine user ID lists to verify the following: • Generic user IDs and accounts are disabled or removed • Shared user IDs for system administration activities and other critical functions do not exist • Shared and generic user IDs are not used to administer any system components

Remote access accounts must be granted only to individuals; a single access account must not be given to a group of individuals for common use. Remote access must be logged in an auditable format.

Remote access to the payments environment must follow the same requirements for user accounts as normal network logins detailed above in the Network Requirements section, such as a unique account secured with two-factor authorization (username/password and an additional authentication item such as password, device or biometrics) for remote access. Complex, 7 character or longer passwords must be used. Automatically lock out access after a maximum of 6 failed login attempts, for a minimum time period of 30 minutes. Log out a user after 15 minutes of inactivity.

Remote access accounts must be enabled only for the duration of the approved access. After the duration of the remote access, user accounts must be disabled and removed. Any account that is unused for 90 days must be removed.

All remote access accounts should use the highest encryption method possible. Use secure technologies such as SSH, VPN and SSL/TLS (PCI DSS section 2.3).

PCI-DSS Requirement	PCI -DSS Testing Procedure
2.2.2 Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.	2.2.2.a For a sample of system components, inspect enabled system services, daemons, and protocols. Verify that only necessary services or protocols are enabled.

Insecure protocols should not be used, and if a insecure protocol is used, a secured must be used to protect the insecure service. It bears noting again that remote access must never be a permanent feature of a payments server or POS lane, and must only be enabled for the duration such access is required.

PCI-DSS Requirement	PCI -DSS Testing Procedure
4.1 Use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks. *Examples of open, public networks that are in scope of the PCI DSS include but are not limited to:* • The Internet • Wireless technologies, • Global System for Mobile • communications (GSM) • General Packet Radio Service • (GPRS).	**4.1.c** Verify that the protocol is implemented to use only secure configurations, and does not support insecure versions or configurations. **4.1.d** Verify that the proper encryption strength is implemented for the encryption methodology in use. (Check vendor recommendations/best practices.)

Transmission of Cardholder Data over Public Networks

The PCI standard requires the use of strong cryptography and encryption techniques (at least 128 bit) such as Secure Sockets Layer (SSL), Point-to-Point Tunneling Protocol (PPTP), 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.

Firewall Setup

Aligns with PCI DSS Requirements 1 and 12.3.9

The Connected Payments solution requires a direct internet connection from each point of sale lane to the data centers; a properly configured firewall is essential to maintain the safety and security of the network on which OpenEPS is deployed.

The goal of this section is to provide basic instructions on how to set up the network firewall for a production store environment to allow specific and limited outbound connections while eliminating undesired incoming connections from the internet.

Outbound and Inbound Connections

An outbound communication is one that originates within the network and connects to a provider outside the network. Inbound or incoming connections originate outside the network with a target host computer that is inside the network.

Inbound connections generally represent the most common threat to network security; hackers on the internet can use scanning software to locate misconfigured or unprotected open ports and use these ports to bypass security. Most firewall hardware and software limit or eliminate inbound traffic as part of their default settings; this is the main reason that use of firewalls is required by PCI regulations.

Outbound connections are commonly thought to pose less of a security risk due to the belief that the software initializing the connection is known and trusted. Outbound connections are actually the most common means of exfiltrating stolen cardholder data from POS devices. The security of even known and trusted software can be augmented with the proper use of firewalls and Access Control Lists (ACLs), while at the same time ensuring outbound access from unknown or untrusted software is completely denied.

The Connected Payments solution has been designed with network security in mind. As such it does not require any inbound connections; when a lane starts up, that lane initiates an outbound connection to the payments host – no incoming connection is required.

With that in mind, it is a simple matter to configure your firewall to allow the Connected Payments software to connect to just the designated data centers, and to prevent all other network traffic either inbound or outbound.

Firewalls

A firewall can come in the form of software loaded onto a computer, or as a separate piece of hardware that connections are routed through. PCI requires the use of a firewall in the payments environment, and firewalls themselves are easy to obtain by searching online for free software firewalls or locating a hardware firewall at your local electronics store.

The benefit of software firewalls is that they are inexpensive and often free. Software firewalls do tend to require an installation and configuration on each system to be protected; this can mean installing a software firewall at each POS lane.

If you are running a Windows system, do not rely solely on the inbuilt Windows firewall for security.

Hardware firewalls come in a variety of grades ranging from protecting a small home network to a large company network. Linksys, Belkin and Netgear all offer low cost ($50 to $60) consumer-grade router/firewalls for small networks that provide the ability to restrict access based on network IP addresses. Somewhat more expensive business grade firewalls will offer more options for limiting the connectivity by start and destination IP address and by port number.

One significant advantage a hardware firewall has over software firewalls is a central location for management. While software firewalls generally require setup on each machine they are installed on, a hardware firewall can be configured to allow or deny access to a range of IP addresses, making configuration of rules for a large number of POS lanes much simpler.

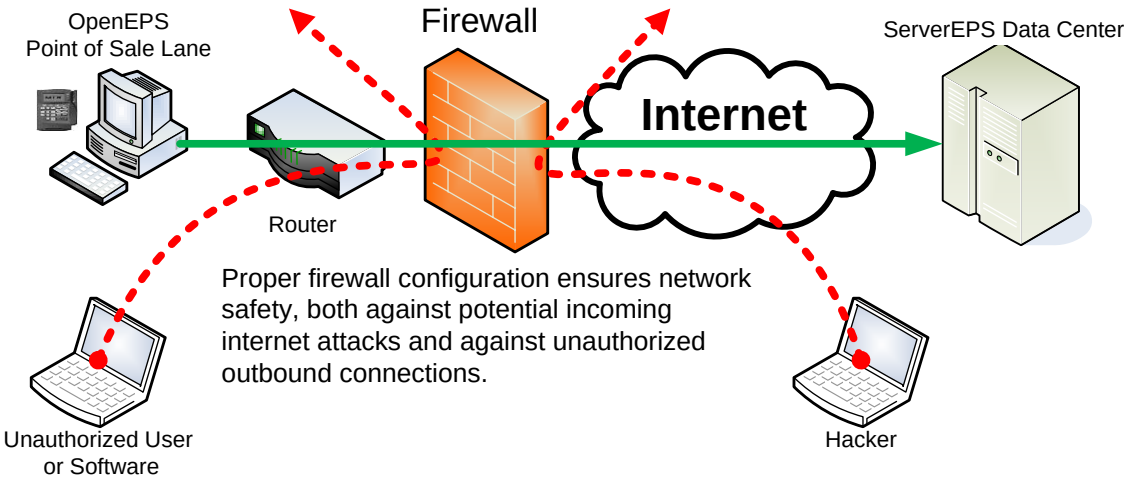
Keep in mind that PCI DSS requires that payments hardware be kept in a safe location. As a part of the payments network, your firewall hardware should be placed in a secure location, such as a locked server closet.

Additional Safety Measures

In addition to a firewall, use of File Integrity Monitoring Systems (such as Tripwire Security Suite, and GFI) or software such as Solid Core to prevent file changes or adds an extra layer of security. Solid Core 'locks' a system at a set point, preventing the modification or execution of any file you specify; File Integrity Monitoring software sends an alert to network administrators whenever files are changed.

Knowing Your Connections

Firewalls keep a network safe by denying access. To properly configure a firewall it is important to focus on what software you want to use and to what host(s) that software needs to connect. The more information you have about your software and connections, the more specific you can make your firewall rules, and the more secure your network becomes.



As you can see from the diagram above, it is possible to configure a firewall to deny unauthorized outbound connections from within the network, as well as unwanted connections from the internet while allowing the required connection from OpenEPS to the payment host provider.

The connection details that follow should allow you to configure your firewall to maximize network protection. Precisely what options you have for firewall connection rules is dependent on what your firewall allows, but the more specific you can make the rules the better the network is protected.

POS Lane Connections

The Connected Payments solution resides at each POS lane, and connects to ServerEPS Data Centers with fixed DNS names such as Trn1.ServerEPS.com, Trn2.ServerEPS.com, Svc1.ServerEPS.com,

Svc2.ServerEPS.com and Bin1.MTXEPS.com. These connections occur on port 443 as shown on the chart below.

Host DNS Name	Service	Host Port
Trn1.ServerEPS.com through Trn6.ServerEPS.com	Primary and Backup Transaction Processing	443
Svc1.ServerEPS.com through Svc3.ServerEPS.com	Primary Configuration Download	443

IP Address Ranges	Location	Host Port
4.79.143.162 – 4.79.143.174	Data Center 1	443
208.80.28.162 – 208.80.28.190	Data Center 2	443

Additional servers are added from time to time and the IP address of existing servers may change; therefore, it is recommended that a DNS server be used instead of utilizing the IP address. The IP addresses are included for completeness.

Using this information, it is possible to configure your network firewall to allow the Connected Payments software to connect out to only the payments host addresses listed and prevent any other connection from being established.

Report Service, Web Site Access

In addition to the POS lanes, it is likely necessary that at least one PC at the store will need to be able to log into the online Report Service for the Connected Payments product. The report service is available at www.servereps.com and communicates on port 443.

Report Service Host DNS Name	IP Address	Host Port
www.ServerEPS.com	4.79.143.167	443
www.ServerEPS.com	4.79.143.167	80

When a user signs on to www.servereps.com using their internet browser, the initial connection is generally established on port 80 (http protocol) and then switches over to secure port 443 (https protocol) automatically as the session begins.

If it is desirable to entirely block outbound traffic on port 80, then a simple desktop shortcut should be included that points to https://www.servereps.com to initiate the connection on secure port 443 to begin with.

Secure Desktop Shortcut Link
https://www.servereps.com

Similar to the POS lanes, this connection can be limited to only the computers that require it and the connection can be limited to only the required site.

CRL Validation

Connected Payments uses SSL server certificates in order to provide secure communication between OpenEPS client and ServerEPS server. SSL/TLS protocol uses server certificates in order to authenticate the server as well as encrypt the network traffic. As part of the secure communication protocol, before establishing the communication session, the client SSL implementation is required to validate the server certificate in order to make sure it was not compromised and revoked by Certificate Authority.

In recent Windows OS versions (Windows 7), the certificate revocation validation is mandatory by default. If Certificate Authority's online certificate validation servers are inaccessible for any reason (for example, blocked by firewall), Windows is unable to check the validity of the server certificate and does not allow the OpenEPS to establish the connectivity with the ServerEPS. In order to avoid this issue, the following server addresses should not be blocked by firewalls:

It is strongly recommended that any firewall policies and/or access control devices use URLs and not IP addresses. Certificate Revocation List (CRL) authorities can change their IP addresses at any time without notification.

Server Name	IP Address	Host Port
ocsp.comodoca.com ocsp.usertrust.com	178.255.83.1	80
crl.comodoca.com crl.usertrust.com	178.255.83.2	80
Whitelist the following: *.verisign.com *.ws.symantec.com *.symcb.com *.symcd.com If white listing wildcard entries is not permitted, whitelist the following: crl.ws.symantec.com	dynamic dynamic	80 80
ocsp.verisign.com	199.7.55.72	80
crl.entrust.net ocsp.entrust.net	dynamic	80

If your corporate firewall is configured to allow only a certain set of IP addresses to be accessed from your network, you'll need to take the following actions:

1. **Get the full list of IP addresses** for the new sites from Verisign/Symantec (https://knowledge.verisign.com/library/VERISIGN/ALL_OTHER/Symantec/crl_list.txt). You may need to complete a short form to gain access to the site list
   - The original Verisign/Symantec advisory is located at: https://knowledge.verisign.com/support/ssl-certificates-support/index?page=content&id=AD596
2. Install or add the IP addresses to your existing list – do not replace the old IP addresses and your existing rules for Symantec CRL IP addresses should not be deleted.

3. Test outbound connectivity – Verisign/Symantec will provide a test page after April 2, 2013. The **List of Test URLs** are located at https://knowledge.verisign.co.uk/support/ssl-certificates-support/index?page=content&id=SO25123&actp=AGENT_REFERAL.

Disable Restore Point: Server 2003/Vista/Win7

Visa has identified a potential insecurity issue with the Restore Point option in Windows Server 2003, Windows Vista, and Windows 7. According to Visa, while there is no specific vulnerability in the restore point itself, there is a high probability that the c:/pagefile.sys (or root directory) page file on the windows system could contain cardholder information, including full track data.

As such, it is recommended that the restore point option on Windows be disabled.

Security Policy

It is mandatory for PCI compliance that a comprehensive information security policy be in place in a production environment. Review section 12 of the PCI document for complete information on the current requirements.

Software Patches

Patch Information

A patch or update generally consists of one or more modules (files) that replace existing files within the software suite to provide enhanced functionality, correct problems, or in the case of a security related patch, change encryption keys or methods.

Retalix releases product update patches from time to time, as part of the ongoing product lifecycle. All merchants can contact Connected Payments support for a list of available patches.

Automated Patching Process

In most cases, within the Connected Payments environment, patching is an automated process initiated by either the Connected Payments Support or Connected Payments Operations group, and as such required no customer intervention.

In the rare case where manual patching is required, refer to the following section.

Manual Patching Process

In the event that a manual patch is required, merchants must receive patches either directly from Retalix support staff, or through a known and trusted chain of personnel. This will ensure authenticity and that the received patch is the most recent.

The patch received will include instructions on deployment; typically this will include the need to copy the patch module into the OpenEPS folder on each affected POS lane. Additional instructions will be supplied as needed on a case by case basis.

Notification of Security Patches

Should it become necessary, Retalix will release a Security Patch for any breach reported to Retalix by a merchant or reseller. Retalix delivers security/encryption related patches within 7 business days after notification of the security breach. The patch will be made available to all affected Retalix customers.

If a security related patch is released, Retalix will utilize current contact information to contact affected customers. Retalix may choose to automatically deploy a security patch in order to prevent further security issues from arising.

Connected Payments and OpenEPS PCI Settings

Settings Required by PCI

The following section details setting and configuration recommendations for the Connected Payments software.

The merchant is responsible for setting up all computer user accounts in a secure fashion, according to the PCI requirements detailed below.

Connected Payments Settings

The Connected Payments web service allows users to configure store and company information along with viewing report information. No full card numbers or other PCI-restricted data fields are available to users through this service.

Connected Payments runs in Retalix data centers and is certified with PCI DSS. No special security configuration is required from the user.

For more information on Connected Payments, refer to the Connected Payments Users Guide.

OpenEPS (Lane) Settings

Network and User Account Setup

Physical Security

Systems containing customer card information, such as the computer on which the POS runs, must be protected physically. Such physical protection should be as complete as possible, and may entail placing the POS machine inside a locked cabinet at the lane.

Remote Connections

As per the WAN Setup / External Connections section above, payments computers may never be directly accessible from the internet, nor allow incoming connections.

In the event that remote access is needed, it must obey these restrictions and must utilize secure technologies such as SSH, VPN, or SSL/TLS (transport layer security) for this purpose.

Windows User Accounts

When installing the local Connected Payments components on a POS lane, the merchant should log on as a Windows administrator. This allows the install process to perform actions like writing to the registry. The account that the POS runs under is not required to be an administrator; it does, however, require access to the OpenEPS directory in order to perform read/write operations there. It is recommended that the account under which the POS runs be defined as a member of the Window's Users group (unless greater permissions are required by the POS itself).

Other than administrative Windows accounts, no other account should be given access to the OpenEPS directory on the POS lanes. Restricting access to this directory will assist in preventing unauthorized access, and potential manipulation of the program or configuration files contained therein.

Account Information Summary	OpenEPS runs under the same user account as the account under which POS runs. This account should have following permissions: • read/write access to C:\Program Files\MicroTrax\OpenEPS\ folder • read/write access to HKEY_LOCAL_MACHINE\SOFTWARE\MTXEPS Registry key. The user account should not have administrative privileges, and should disable by default all access permissions that are not required.

Directory and Registry Access

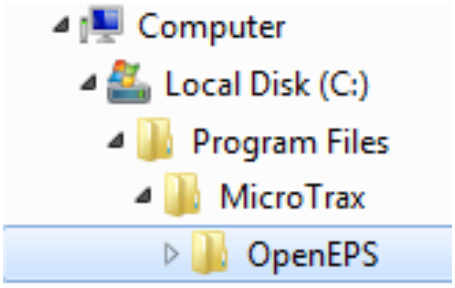
It is recommended that only administrative personnel be allowed to directly modify program files, or the registry keys; user accounts other than administrators must be prevented from making changes directly to the Connected Payments / OpenEPS software, its configuration files, or to the registry. To prevent this, the use of Access Control Lists is suggested.

PCI-DSS Requirement	PCI -DSS Testing Procedure
10.5.5 Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).	**10.5.5** Verify the use of file-integrity monitoring or change detection software for logs by examining system settings and monitored files and results from monitoring activities.

All directories listed must deny access to non-administrative user accounts access and be monitored by a File Integrity Monitoring System.

All Registry keys must likewise be restricted to deny access to non-administrative users.

Directory Structure



Default Directories

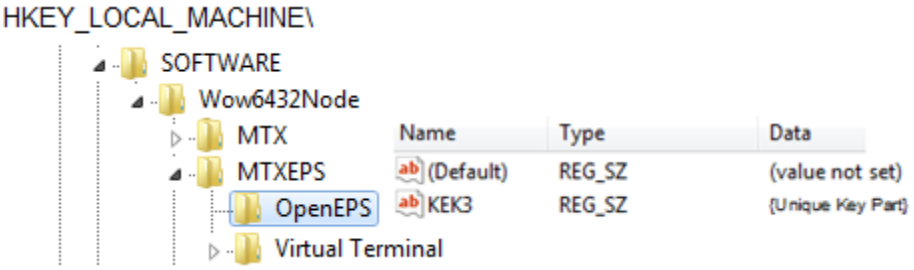
The Connected Payments OpenEPS software is installed by default to the following location:

C:\Program Files\MicroTrax\OpenEPS

Registry Keys

On Windows machines, the Windows Registry contains installation information and the unique key part (KEK3) that is stored on the machine in order to access transaction information that is written to disk.

The key part may either be in the HKEY_LOCAL_MACHINE\SOFTWARE\ MTXEPS\OpenEPS\ node, or the HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\MTXEPS\OpenEPS\ node as shown below.



HKEY_LOCAL_MACHINE\SOFTWARE\MTXEPS\OpenEPS

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\MTXEPS\OpenEPS

- KEK3

Directories and Permissions

OpenEPS environments, such as the POS lanes, have a default directory structure of C:\Program Files\MicroTrax\OpenEPS\. This directory is populated from a combination of the files installed during the initial installation process and files downloaded from the Connected Payments servers.

Only administrators should be given direct access to any file or folder from the \MicroTrax\OpenEPS\ directory and below; administrators will require access to these folders to in order to install patches and performs upgrades.

PCI-DSS Requirement	PCI -DSS Testing Procedure
11.5 Deploy file-integrity monitoring tools to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly. ***Note:*** *For file-integrity monitoring purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. File-integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider).*	**11.5.a** Verify the use of file-integrity monitoring tools within the cardholder data environment by observing system settings and monitored files, as well as reviewing results from monitoring activities. Examples of files that should be monitored: _ System executables _ Application executables _ Configuration and parameter files _ Centrally stored, historical or archived, log and audit files
	11.5.b Verify the tools are configured to alert personnel to unauthorized modification of critical files, and to perform critical file comparisons at least weekly.

In addition, it is highly recommended that the \OpenEPS\ directory be protected through the use of a File Integrity Monitoring System. The \OpenEPS\ directory contains configuration information that could potentially be altered with malicious intent. File Integrity Monitoring Systems keep track of changes to files or applications and can alert technical staff when changes are made; undesirable changes can be easily tracked and removed.

When using a File Integrity Monitoring System, be aware that certain files (typically log or database files: *.tor, Spool*, actlog*, jrnl*, Offlines) are constantly changing. It is often useful to either exclude these files from alerts completely, or configure the alerting software to allow the OpenEPS software to freely manipulate files within its directory structure, and to configure alerts for when files are directly manipulated by user accounts or when manipulated by other software.

OpenEPS Specific Directory Permissions

OpenEPS lane do have an extra requirement, and that is that the user account which launches the POS software must have read/write permissions to the OpenEPS directory. This is because OpenEPS is a DLL which the POS software loads, and therefor OpenEPS derives its permissions from the user account the POS is started under.

It is important to note, however, that the cashier, or other users of the POS must NOT have access to the OpenEPS folder. It is important for security that the casher or other daily users do not have the ability to modify OpenEPS configuration files. This generally requires that the POS be run under a separate specific user account, which is different from the user account actually used to log into the system by the cashier.

Here is a quick breakdown of recommended access rights for the OpenEPS folder:

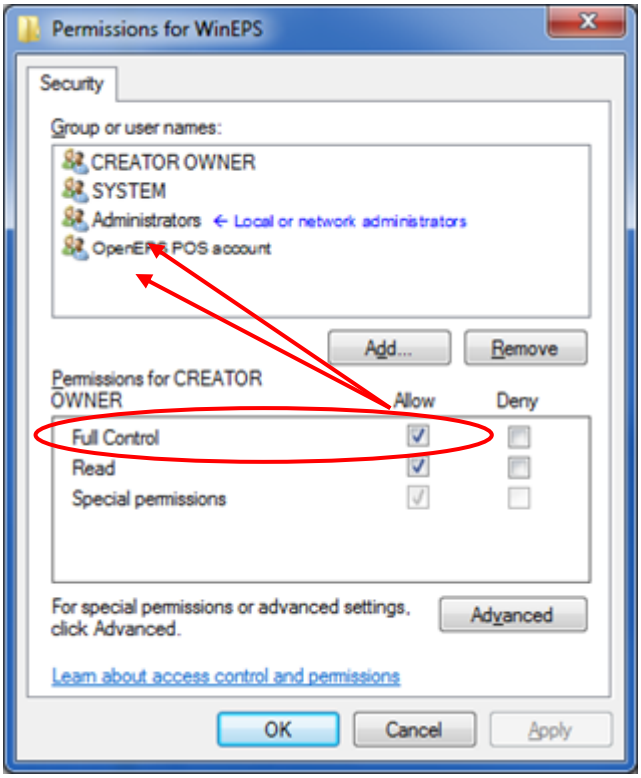
Windows:

- Admins: read/write
- POS account: read write
- Cashier: no access
- All others: no access

Registry Permissions

The Connected Payments software suite writes information to the Windows Registry locations noted above; specifically the HKEY_LOCAL_MACHINE\SOFTWARE\MTXEPS\OpenEPS\ or HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\MTXEPS\OpenEPS\ nodes contain the key-part used to store transaction data to file.

As such, the registry must be accessible to OpenEPS, however the keys noted above should not be accessible to any non-administrative user account. The registry key can be protected by limiting the permissions to the OpenEPS key to only those Windows accounts that require access.



Administrator accounts and the account under which the POS runs will require Full Control permissions to the registry key. Other accounts should be given NO permissions to access these keys.

Sensitive Data Handling and Trouble Shooting

After a transaction has been completed, the Connected Payments software stores only the data allowed by PCI. Information for transactions that have not yet been completed may be stored locally in encrypted format until they are resolved, such as in the case of offline transactions.

In all cases, the merchant will not have access to sensitive data. Sensitive data is stored in encrypted format and is not available to the merchant.

Even encrypted, files that can potentially contain card information must be handled carefully. Specifically, files of this nature must never be sent over e-mail, even to Retalix Support.

The following file types must be treated as sensitive:

- off*.eft

- tor*.eft
- ofline01.*
- towineps*.eft

These files are stored in the C:\Program Files\MicroTrax\OpenEPS\ directory on the POS lane.

If any of these files are required for troubleshooting by Retalix Support, an upload location will be assigned to you – do not send these files to Retalix prior to receiving a confirmed upload location. Upload the required files to the location specified, and securely delete the files when they are no longer necessary.

Merchants should only collect and transmit these files as needed as part of troubleshooting, and should collect only the files required by the specific issue.

Encryption Keys

Connected Payments is designed to follow the PCI requirements for the retention of cardholder data. The encryption methods in use for all file and data encryption are completely integrated into the software suite.

Each OpenEPS lane utilizes their own, separate, Key Encryption Keys (KEK's) to encrypt randomly generated Data Encryption Keys (DEK's). This ensures that data is stored securely and that the compromise of a key at one location will not compromise any other location.

Merchants may change their keys at will. Connected Payments has an option to allow the merchant to choose to update the keys, and when that option is selected, the encryption is then rotated automatically, with new keys generated using cryptographically sound pseudo-random number generation. This method has the advantage of guaranteeing the use of strong keys, as well as removing the need for key-part management from the merchant.

PCI requires encryption keys to be changed at least annually in order to remain PCI compliant.
The Connected Payments software will automatically rotate keys each year, without the need for merchant intervention.

In order to rotate the keys at a location, follow the instructions provided below in the Changing the Encryption Keys section.

Additional Key Change Requirements

Beyond being change annually, PCI PA-DSS requires that keys be changed in at least two other instances: when the integrity of a key is weakened, and at any time is it known or suspected that a key is compromised.

PA-DSS Testing Procedure
2.6.5.a Verify that key-management procedures are implemented to retire keys when the integrity of the key has been weakened.
2.6.5.b Verify that key-management procedures are implemented to replace known or suspected compromised keys.

In the event that a key needs to be changed, follow the key change procedure outlined below, in the Changing the Encryption Keys section.

Changing the Encryption Keys

Each OpenEPS lane utilizes their own separate Key Encryption Keys (KEK's) to encrypt randomly generated Data Encryption Keys (DEK's). This ensures that data is stored securely and that the compromise of a key at one location will not compromise any other location.

The Key will automatically be regenerated when it expires, one year after it was created, as required by PCI DSS, so no manual intervention should be required.

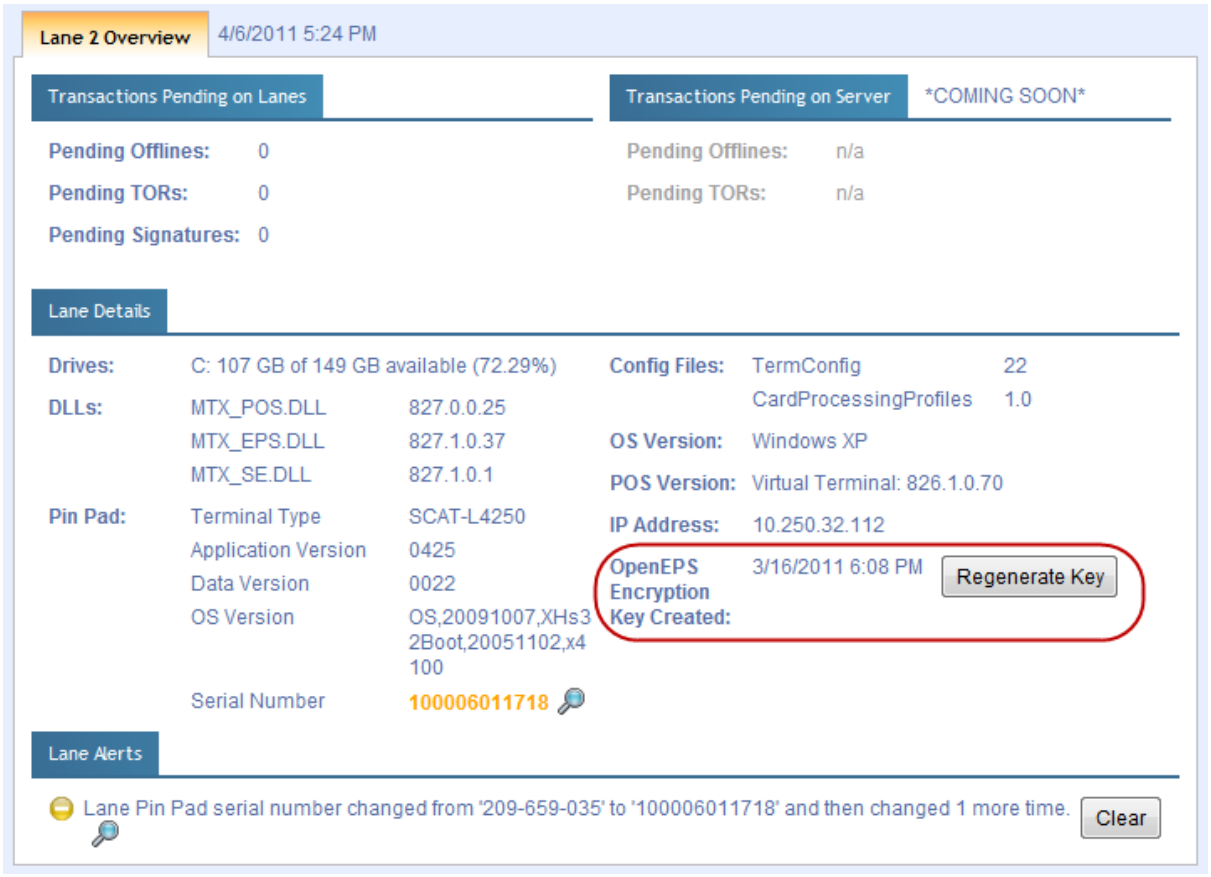
However, the option to regenerate the key manually is also available to the user, so that users have the ability to manually cycle the key at any time.

Encryption Key Manual Regeneration

To support the implementation of unique encryption per lane, the encryption status of each lane is displayed on the Lane information screen. This screen displays the date and time when the unique encryption key was generated, and provides the user with a button that re-generates the key at the lane. This feature is available with OpenEPS version 827.3 and higher.

In order to manually generate new KEK:

- Log into the ServerEPS Web Portal
- Select Monitoring -> Store Status from the tab menu
- Search for desired Store
- Expand the desired Lane
- Note the date/time stamp of the current key, and press *Regenerate Key* button.
- The update process can take anywhere from 15 to 30 minutes.
- In order to validate that the lane is updated correctly, confirm that the date/time stamp has been updated with a recent date/time.


Lane 2 Overview
4/6/2011 5:24 PM
Transactions Pending on Lanes
Pending Offlines: 0
Pending TORs: 0
Pending Signatures: 0
Transactions Pending on Server
COMING SOON
Pending Offlines: n/a
Pending TORs: n/a
Lane Details
Drives: C: 107 GB of 149 GB available (72.29%)
DLLs: MTX_POS.DLL 827.0.0.25
MTX_EPS.DLL 827.1.0.37
MTX_SE.DLL 827.1.0.1
Pin Pad: Terminal Type SCAT-L4250
Application Version 0425
Data Version 0022
OS Version OS,20091007,XHs32Boot,20051102,x4100
Serial Number 100006011718
Config Files: TermConfig 22
CardProcessingProfiles 1.0
OS Version: Windows XP
POS Version: Virtual Terminal: 826.1.0.70
IP Address: 10.250.32.112
OpenEPS Encryption Key Created: 3/16/2011 6:08 PM
Regenerate Key
Lane Alerts
Lane Pin Pad serial number changed from '209-659-035' to '100006011718' and then changed 1 more time.
Clear

Operating Systems

PCI requires that the security patches for software in the payments environment be tested and installed in a timely fashion. Several Microsoft operating systems have passed their supported security update lifespan, and no additional security patches will be released. Due to the vulnerability that a lack of security patches represents, these operating systems are no longer supported for use with the Connected Payments product suite.

For each of the supported operating systems it is required by PCI DSS that they be updated with the latest security patches or relevant service packs in a timely fashion.

Systems that have passed their supported security update lifespan include Windows NT 4.0, Windows 95/98, Windows XP Professional Service Pack 1 or 2, and thus these operating systems are not supported.

Refer to information at http://support.microsoft.com/ for the most up to date security related articles and end of support dates for all Microsoft operating systems.

Unsupported Systems

The following operating systems and hardware are **not supported** since they passed their supported security update lifespan:

- Windows NT 4.0
- Windows Win95/Win98
- Windows 2000
- Windows XP Pro SP 2
- Windows Vista SP1

Refer to Connected Payments Installation and Setup Guide [2] for full list of supported and unsupported systems.

Virtual Terminal PCI Settings

Virtual Terminal is a software application that can be used to process payment transaction similar to a POS system. Follow instructions from previous section for secure configuration of VT.

If VT is installed to a non-POS computer, care should be maintained regarding the amount of access granted; like any payments software, unauthorized access must be restricted and the computer must be as physically secure as feasible.

When Virtual Terminal is used in a live payments environment, it is often intended to be utilized to process only a limited number of transaction types. To prevent access to payments types that were not intended to be processed through VT, it is highly recommended that the Virtual Terminal term configuration file in use be configured to only allow the desired transactions. If a tender or transaction type is not intended to be processed through VT, turn that tender off.

References

[1] *PCI PA-DSS Requirements and Security Assessment Procedures, v2.0*

Copyright 2010 PCI Security Standards Council LLC

[2] Connected Payments Installation and Setup Guide

Copyright 2012 Retalix Ltd.

Contact Information

Retalix Global Payments

85 Argonaut

Suite 150

Aliso Viejo CA, 92656

Tel: 949-614-1600

E-mail: ConnectedSupport@retalix.com

Web site: http://www.mtxeps.com/

NCR Corporation

NCR Corporation

Discovery Centre, 3 Fulton Road

Dundee, DD2 4SW

Scotland

Web site: http://www.info.ncr.com/