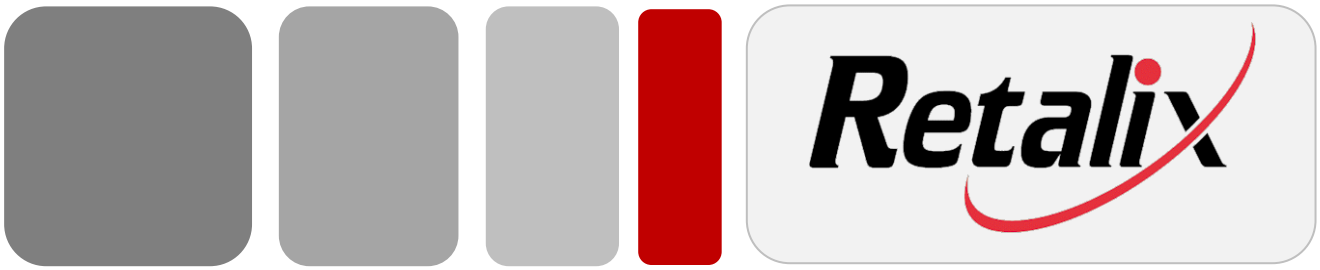
Connected Payments PCI Assessment Guide

Retalix Global Payments

Security Team



Version 1.0

Israel

10 Zarhin St.

P.O. Box 2282

Ra'anana 43000, Israel

Tel: +972 9 7766677

Fax: +972 9 7400471

Website: http://www.retalix.com

USA

6100 Tennyson Parkway

Suite 150, Plano, TX 75024 USA.

469-241-8400

Website: http://www.retalix.com

Table Of Contents

Revision History **2**
Introduction **3**
PCI Requirements **4**
Requirement 1 – Install and maintain a firewall configuration to protect cardholder data 4
Requirement 2 – Do not use vendor-supplied defaults for system passwords and other security parameters 5
Requirement 3 – Protect stored cardholder data 5
Requirement 4 – Encrypt transmission of cardholder data across open, public networks 7
Requirement 5 – Use and regularly update anti-virus software or programs 8
Requirement 6 – Develop and maintain secure systems and applications 9
Requirement 7 – Restrict access to cardholder data by business need to know 10
Requirement 8 – Assign a unique ID to each person with computer access 10
Requirement 9 – Restrict physical access to cardholder data 11
Requirement 10 – Track and monitor all access to network resources and cardholder data 11
Requirement 11 – Regularly test security systems and processes 12
Requirement 12 – Maintain a policy that addresses information security for all personnel 12
Appendix A – Encryption, Key Management, and Data Storage **13**
Encryption of Store and Forward file 13
Message Encryption – OpenEPS to ServerEPS 13
Message Encryption – Pinpad to OpenEPS 13
1 References **14**

Revision History

Version	Date	Changed By	Change Description
1.0 Draft	March 1, 2012	Jeff Maxton Slava Gomzin, CISSP	Initial Release

Introduction

The purpose of this document is to provide an overview of how Connected Payments adheres to the PCI DSS requirements. This document is intended to assist merchants with performing self assessments (PCI SAQ [1]) as well as answering the questions posed during an audit. Certain requirements outlined are out of the scope of Connected Payments and are the responsibility of the merchant to maintain. This guide is current as of PCI DSS 2.0.

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

PCI Requirements

Requirement 1 – Install and maintain a firewall configuration to protect cardholder data

Connected Payments architecture prevents cardholder data from being directly accessible via the internet or OpenEPS; however it is the merchant's responsibility to prohibit direct public access between the internet and any system components. Following the Firewall Setup Guide instructions provided by Retalix in Connected Payments PCI PA-DSS Implementation Guide [2] will prohibit such access. The Connected Payments PCI PA-DSS Implementation Guide [2] is available on the ServerEPS Web Portal under the Customer Service tab. Connected Payments facilitates a secure configuration by requiring only port 443 to be open to our data centers. All data sent to the ServerEPS datacenters is protected by SSL/TLS encryption as well as sensitive field encryption.

It is the merchant's responsibility to establish firewall and router configuration standards that include the following:

- A formal process for approving and testing all network connections and changes to the firewall and router configurations
- Current network diagram with all connections to cardholder data, including any wireless networks
- Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone
- Description of groups, roles, and responsibilities for logical management of network components
- Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure. Examples of insecure services, protocols, or ports include but are not limited to FTP, Telnet, POP3, IMAP, and SNMP.
- Requirement to review firewall and router rule sets at least every six months

In addition, the merchant must build firewall and router configurations that restrict connections between un-trusted networks and any system components in the cardholder data environment.

Requirement 2 – Do not use vendor-supplied defaults for system passwords and other security parameters

It is the responsibility of the merchant to always change vendor-supplied defaults before installing on the network, including but not limited to passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts. Connected Payments assists with this by requiring that the merchant change the default password supplied to them.

In addition, the merchant must develop configuration standards for all system components and assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Finally, the merchant must encrypt all non-console administrative access using strong cryptography (SSH, VPN, SSL).

Requirement 2.4 holds that shared hosting providers must protect each entity's hosted environment and card holder data and as the merchant is not a shared hosting provider, this does not apply to them. However, as a shared hosting provider Retalix Global Payments is PCI DSS compliant [3]

Requirement 3 – Protect stored cardholder data

Connected Payments is designed to follow the PCI requirements for the retention of cardholder data. The table included below outlines how Connected Payments meets the specific requirements outlined in the PCI DSS 2.0 document (requirements 3.1-3.4.1). Requirements 3.5-3.6.8 refers to the specific requirements for the protection of keys used to secure cardholder data. As OpenEPS properly protects these keys, the merchant does not have access to these keys via OpenEPS and as such these requirements are out of scope for Connected Payments.

3.1 Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes, as follows.	
3.1.1 Implement a data retention and disposal policy that includes: • Limiting data storage amount and retention time to that which is required for legal, regulatory, and business requirements • Processes for secure deletion of data when no longer needed • Specific retention requirements for cardholder data • A quarterly automatic or manual process for identifying and securely deleting stored cardholder data that exceeds defined retention requirements	• The only card holder data stored at the lane is the store and forward file (offline file) no other card holder data is stored. • OpenEPS securely deletes records upon forwarding to the Server • No retention of card holder data at store level (other than offline file - this is optional) • Customer must have a quarterly process in place.
3.2 Do not store sensitive authentication data	OpenEPS does not store sensitive authentication data past

PCI Requirements

after authorization (even if encrypted). Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3: ***Note:*** *It is permissible for issuers and companies that support issuing services to store sensitive authentication data if there is a business justification and the data is stored securely.*	authorization and is compliant per PA DSS (this has been validated by a third party [4])
3.2.1 Do not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data. ***Note:*** *In the normal course of business, the following data elements from the magnetic stripe may need to be retained:* • *The cardholder's name* • *Primary account number (PAN)* • *Expiration date* • *Service code* *To minimize risk, store only these data elements as needed for business.*	The full content of any track is not stored locally after authorization and is always encrypted. Any Card Holder Data not allowed to be stored post authorization is securely deleted after the transaction is authorized. During receipt and while authoring any sensitive data is securely encrypted. Connected Payments only stores track data to the point of authorization, encrypted and validated as PA DSS compliant [4] by a QSA (qualified security assessor.)
3.2.2 Do not store the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not present transactions.	OpenEPS does not store CVC beyond authorization.
3.2.3 Do not store the personal identification number (PIN) or the encrypted PIN block.	Pin is encrypted in pinpad and is not retained past authorization.
3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed). ***Notes:*** • *This requirement does not apply to employees and other parties with a legitimate business need to see the full PAN.* • *This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, for point-of-sale (POS) receipts.*	The logging used in OpenEPS only exposes last 4 digits of PAN; the ServerEPS Web Portal will display only first 6 and last 4 of the PAN.
3.4 Render PAN unreadable anywhere it is stored (including on portable digital media,	

backup media, and in logs) by using any of the following approaches: • One-way hashes based on strong cryptography (hash must be of the entire PAN) • Truncation (hashing cannot be used to replace the truncated segment of PAN) • Index tokens and pads (pads must be securely stored) • Strong cryptography with associated key-management processes and procedures ***Note:*** *It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated versions of the same PAN are present in an entity's environment, additional controls should be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.*	The PAN is always rendered unreadable when stored by using encryption. For details on the encryption used in Connected Payments please refer to Appendix A.
3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed independently of native operating system access control mechanisms (for example, by not using local user account databases). Decryption keys must not be tied to user accounts.	This does not apply to OpenEPS as OpenEPS does not use Disk encryption.

Requirement 4 – Encrypt transmission of cardholder data across open, public networks

OpenEPS uses strong transport level encryption (SSL) as well as encrypting sensitive fields using AES-256. OpenEPS does not send unprotected PANs by end user messaging technologies.

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).	Connected Payments use strong transport level encryption (SSL) as well as encrypting sensitive fields using AES-256. Hardware P2PE (Point-To-Point Encryption) option is also available (depending on customer hardware and configuration). Hardware P2PE provides highest level of protection and renders disclosure of sensitive cardholder data virtually impossible. For more information on the Connected Payments encryption technologies please refer to Appendix A. Connected Payments encrypt the tunnel between OpenEPS and ServerEPS as well as encrypting sensitive fields within the

	message. AES = Advanced Encryption Standard
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.*	It is the merchant's responsibility to secure their network including any wireless networks. Please refer to the Connected Payments PCI PA-DSS Implementation Guide available on the Web Portal for additional information.
4.2 Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat, etc.).	The OpenEPS application does not send unprotected PANs by end-user messaging technologies. It is the merchant's responsibility to monitoring any end-user messaging technology they employ to confirm unprotected PANs are not being sent.

Requirement 5 – Use and regularly update anti-virus software or programs

The merchant is responsible to deploy anti-virus software on all systems commonly affected by malicious software, including personal computers and servers. In addition, it is the responsibility of the merchant to ensure that all anti-virus programs are capable of detecting, removing and protecting against all known types of malicious software. Finally, the merchant must ensure that all anti-virus software is current, actively running and generating audit logs. Third Party applications such as Solidcore have been used as a compensating control to this requirement.

Requirement 6 – Develop and maintain secure systems and applications

OpenEPS patches are pushed down to the lanes automatically as part of the ServerEPS service offering. It is the merchant's responsibility to ensure that operating system components and software other than OpenEPS have the latest security patches and that critical security patches are installed within one month of release. In addition, the merchant must establish a process to identify and assign a risk ranking to security vulnerabilities beyond the scope of OpenEPS and address those vulnerabilities. Finally, the merchant must follow change control processes and procedures for all changes to system components which must included the following:

- Separate development/test and production environments
- Separation of duties between development/test and production environments
- Production data (live PANs) are not used for testing or development
- Removal of test data and accounts before production systems become active
- Change control procedures for the implementation of security patches and software modifications. Procedures must include the following:
- Documentation of impact.
- Documented change approval by authorized parties.
- Functionality testing to verify that the change does not adversely impact the security of the system.

The development of OpenEPS has been PA-DSS validated by a QSA [4] as being compliant to PCI DSS requirements by incorporating information security throughout the software development life cycle. In addition, OpenEPS has been developed using secure coding guidelines outlined in PCI DSS 2.0 (requirement 6.5) and has also been validated.

Requirement 6.6 which requires new threats and vulnerabilities be addressed on an ongoing basis for public facing web applications. Since ServerEPS does not have a public facing web application that processes cardholder sensitive data this requirement does not apply. If a merchant is hosting their own public facing web application than they will be required to adhere to the requirements of 6.6.

Requirement 7 – Restrict access to cardholder data by business need to know

Requirement 7 does not apply to OpenEPS as customers do not have access to cardholder data through OpenEPS.

Requirement 8 – Assign a unique ID to each person with computer access

While there is no customer access to cardholder data through OpenEPS, it is the merchant's responsibility to assign all users a unique ID before allowing them to access system components. In addition, the merchant must employ one of the following methods to authenticate 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

The merchant must also render all passwords unreadable during transmission and storage using strong cryptography and ensure proper user identification and authentication by following the below sub-requirements:

- Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.
- Verify user identity before performing password resets.
- Set passwords for first-time use and resets to a unique value for each user and change immediately after the first use.
- Immediately revoke access for any terminated users.
- Remove/disable inactive user accounts at least every 90 days.
- Enable accounts used by vendors for remote access only during the time period needed. Monitor vendor remote access accounts when in use.
- Do not use group, shared, or generic accounts and passwords, or other authentication methods.
- Change user passwords at least every 90 days.
- Require a minimum password length of at least seven characters.
- Use passwords containing both numeric and alphabetic characters.
- 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.
- Limit repeated access attempts by locking out the user ID after not more than six attempts.
- Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.
- If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.
- Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users. Restrict user direct access or queries to databases to database administrators.

Requirement 9 – Restrict physical access to cardholder data

Requirement 9 is out of scope for OpenEPS as OpenEPS does not allow access to card holder data.

Requirement 10 – Track and monitor all access to network resources and cardholder data

Requirements 10.1-10.3 are out of scope for OpenEPS as OpenEPS does not allow access to card holder data. It is the merchant's responsibility to maintain the following:

- Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time. Note: One example of time synchronization technology is Network Time Protocol (NTP).
- Critical systems have the correct and consistent time.
- Time data is protected.
- Time settings are received from industry-accepted time sources.
- Secure audit trails so they cannot be altered.
- Limit viewing of audit trails to those with a job-related need.
- Protect audit trail files from unauthorized modifications.
- Protect audit trail files from unauthorized modifications.
- Promptly back up audit trail files to a centralized log server or media that is difficult to alter.
- Write logs for external-facing technologies onto a log server on the internal LAN.
- 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).
- Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion-detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS). Note: Log harvesting, parsing, and alerting tools may be used to meet compliance with Requirement 10.6.
- Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from back-up)

Requirement 11 – Regularly test security systems and processes

It is the merchant's responsibility to regularly test security systems and processes by maintaining the following sub requirements outlined in PCI DSS 2.0:

- Test for the presence of wireless access points and detect unauthorized wireless access points on a quarterly basis.
- 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).
- Perform external and internal penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub network added to the environment, or a web server added to the environment).
- Use intrusion-detection systems, and/or intrusion-prevention systems to monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up-to-date.
- 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.

Requirement 12 – Maintain a policy that addresses information security for all personnel

It is the merchant's responsibility to establish and maintain an information security policy that includes all of the following:

- Establish, publish, maintain, and disseminate a security policy that addresses all PCI DSS requirements, includes an annual process that identifies threats and vulnerabilities in a formal risk assessment and includes at a review at least annually or when the environment changes.
- Develop daily operational security procedures that are consistent with PCI DSS requirements.
- Develop usage policies for critical technologies (for example, remote access technologies, wireless technologies, removable electronic media, laptops, tablets, personal data/digital assistants (PDAs), e-mail usage and Internet usage) and define proper use of these technologies.
- Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.
- Assign to an individual or team the following information security management responsibilities.
- Implement a formal security awareness program to make all personnel aware of the importance of cardholder data security.
- Implement a formal security awareness program to make all personnel aware of the importance of cardholder data security.
- Screen potential personnel prior to hire to minimize the risk of attacks from internal sources.
- Maintain a list of service providers with whom cardholder data is shared.
- Implement an incident response plan. Be prepared to respond immediately to a system breach.

Retalix Global Payments is a compliant service provider and has been validated as being PCI DSS compliant by a QSA as of October 31, 2011 [3].

Appendix A – Encryption, Key Management, and Data Storage

This section is designed to give an overview of the encryption utilized by the ServerEPS payments suite within the merchant environment. There is an additional document available to auditors under NDA that covers specifics of the encryption.

Encryption of Store and Forward file

OpenEPS typically does not store any cardholder data. The only exception to this is if the merchant elects to perform Store and Forward (also called Stand-In) processing. In this situation the communications to ServerEPS are down and the lane will locally approve the transaction and forward to ServerEPS as soon as communications are restored. This is permitted under PCI as the transaction has not yet been authorized (PCI requires that no sensitive authentication data be stored post-authorization).

For encryption of the store and forward file, OpenEPS dynamically generates a data encryption key for each record in the file. This provides a unique encryption key for every transaction record. The data encryption key is stored in the SNF file encrypted under a key encryption key. The key encryption key is hardcoded within the OpenEPS application as components and combined at runtime to form the actual key.

Message Encryption – OpenEPS to ServerEPS

Messages from OpenEPS to the ServerEPS datacenters are protected by SSL/TLS encryption (minimum SSL v3, automatically negotiated to the highest level supported by both client and server).

For implementations in which OpenEPS has access to full track data, the track data fields are encrypted using AES-256 encryption before being sent. The key for this encryption is hardcoded within the OpenEPS application as components and combined at runtime to form the actual key.

For implementations in which OpenEPS does not receive the full track data (i.e. a point-to-point encryption solution), the encryption is handled by the pinpad.

Message Encryption – Pinpad to OpenEPS

Depending on the pinpad and implementation, a number of different encryption schemes are used. These range from a hardcoded key shared between the pinpad and OpenEPS, to a dynamically generated session key between the pinpad and OpenEPS, all the way to a key injected into the Tamper Resistant Security Module (TRSM) of the pinpad with the key for decryption residing only on a Hardware Security Module (HSM) inside the ServerEPS datacenter (Hardware P2PE - Point-To-Point Encryption).

References

[1] *PCI PA-DSS Requirements and Security Assessment Procedures, v2.0*
Copyright 2010 PCI Security Standards Council LLC

[2] *Connected Payments PCI PA-DSS Implementation Guide v1.00*
Copyright 2012 Retalix Ltd

[3] *Visa's Global Registry of Service Providers - PCI DSS Validated Entities*
http://usa.visa.com/download/merchants/cisp-list-of-pcidss-compliant-service-providers.pdf
Copyright 2012 Visa Inc.

[4] *PCI SSC List of Validated Payment Applications*
https://www.pcisecuritystandards.org/approved_companies_providers/validated_payment_applications.php
Copyright 2012 PCI SSC, LLC