Miva Merchant PA-DSS Implementation Guide

For MIVA MERCHANT 5.5

Version 1.0
December 2009

Miva Merchant Contact Information

For general information about our company, products, and services, go to http://www.mivamerchant.com.
For questions about Miva Merchant, email support@mivamerchant.com or call 1.866.284.9812

Table of Contents

Chapter 1 - Introduction

Purpose

This guide is intended for Merchants and 3rd Party Installers implementing Miva Merchant 5.5. The purpose of this guide is to aid Merchants and installers in their efforts to implement Miva Merchant 5.5 in a PCI DSS compliant manner. Merchants accepting credit card information (cardholder data) are required to follow guidelines defined in the PCI Data Security Standard (DSS) to protect cardholder data. This guide is intended to make Merchants aware of implementation and environment issues that affect PCI Data Security Standard compliance. The PCI DSS program was created by Credit Card Brands, Banks, and Credit Card Processors. The PCI DSS program aims to protect cardholder data and sensitive authentication data during the life cycle of a credit card payment transaction.

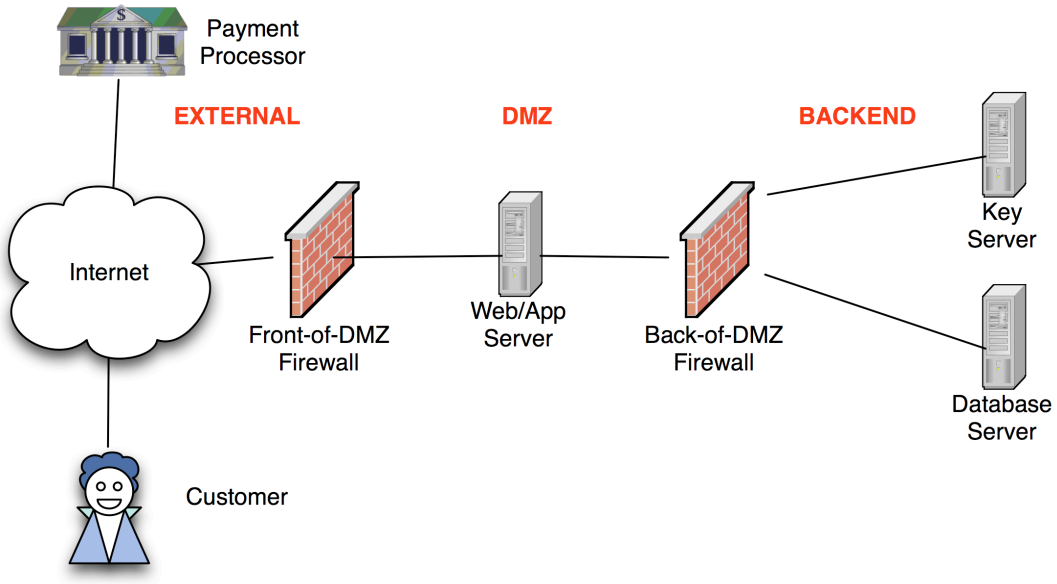
The PA-DSS security program is based on the requirements of PCI DSS and applies specifically to payment applications. Payment applications that have been accepted under the PA-DSS program have been validated to ensure they can be installed in a PCI DSS compliant manner when properly installed.

Standard Configurations

A standard configuration of Miva Merchant would include the following attributes:

- A DMZ firewall zone which includes the web servers running the Miva Merchant software
- A second firewall zone, with no access from or to the Internet containing the database server.
- A key server separated from the database server

An example compliant configuration would be:



How Do I Know that I Comply?

Miva Merchant 5.5 monitors key settings within itself to help you comply with PCI DSS. Default settings meet or exceed the requirements of this Implementation Guide and PCI DSS. You can see whether your settings comply by logging into your Miva Merchant 5.5 administrative interface and navigating to the PA-DSS Checklist tab located in Domain Settings. Any setting which does not meet the minimum requirements for compliance with PCI DSS is shown in red on this tab. To be compliant with PCI DSS, you are required to change any noncompliant setting to a level that complies with the minimum required. All Miva Merchant 5.5 settings will change to green when your Miva Merchant 5.5 settings are all fully compliant with PCI DSS requirements however this checklist should not be relied on to determine overall PCI DSS compliance status as it only covers a small subset of PCI requirements. If, however, you have settings marked as failed, you can be assured that you are most likely out of compliance with PCI DSS.

You may have added modules to Miva Merchant 5.5 or other systems that store credit card information and you should ensure that each of these systems complies with PCI DSS. Miva Merchant does not monitor any system other than itself so it is your sole responsibility to ensure PCI DSS compliance for any system other than Miva Merchant 5.5. The payment modules that have been tested as part of this assessment are:

- Authorize.net Payment Services v3.1
- CHASE Paymentech Orbital Gateway
- Innovative Gateway
- First Data Global Gateway
- Payflow Pro

Any other payment module or acquirer interface has not been tested as part of PA-DSS and should be individually evaluated for its PCI DSS compliance status.

Minimum security is required for the way you access cardholder data, including the way you access Miva Merchant 5.5. Review this Implementation Guide to ensure that minimum-security settings are met for devices such as servers, routers, firewalls and wireless networks that you use to access Miva Merchant 5.5.

All installation instructions specific to PCI DSS and PA-DSS must be followed. These instructions are listed in the distributed vm-README.txt file. Please ensure that you read this document and deploy the Miva Empresa Virtual Machine per the instructions contained therein.

Cardholder Data

The following table from the PCI Data Security Standard (DSS) illustrates commonly used elements of cardholder and sensitive authentication data; whether storage of each data element is permitted or prohibited; and if each data element must be protected. This table is not exhaustive, but is presented to illustrate the different types of requirements that apply to each data element.

	Data Element	Storage Permitted	Protection Required	PCI DSS REQ. 3.4
Cardholder Data	Primary Account Number (PAN)	YES	YES	YES
	Cardholder Name*	YES	YES*	NO
	Service Code*	YES	YES*	NO
	Expiration Date*	YES	YES*	NO
Sensitive Authentication Data**	Full Magnetic Stripe	NO	N/A	N/A
	CVC2/CVV2/CID	NO	N/A	N/A
	PIN / PIN Block	NO	N/A	N/A

* These data elements must be protected if stored in conjunction with the PAN. This protection must be consistent with PCI DSS requirements for general protection of the cardholder environment. Additionally, other legislation (for example, related to consumer personal data protection, privacy, identity theft, or data security) may require specific protection of this data, or proper disclosure of a company's practices if consumer-related personal data is being collected during the course of business. PCI DSS, however, does not apply if PANs are not stored, processed, or transmitted.

** Sensitive authentication data must not be stored subsequent to authorization (even if encrypted).

More Information about PCI and PA-DSS

More information about the PCI DSS and PA-DSS programs can be found at the PCI Security Standards Council website:

https://pcisecuritystandards.org/

More information about the Visa cardholder information data security program can be found at the Visa website:

http://www.visa.com

More information about the MasterCard secure data program can be found at the MasterCard website:

http://www.mastercard.com

Chapter 2 – Delete Sensitive Authentication Data

Miva Merchant 5.5 does not retain any sensitive authentication data post-authorization. Sensitive authentication data such as complete track1 or track 2 data and card-verification codes printed on the card (CVV2, CVC2, CID, or CAV2) should never be retained post-authorization even if it is encrypted.

If required for business the following data elements may be stored post-authorization when they are properly secured:

- Cardholder's name
- Primary account number (PAN)
- Expiration date
- Service code

Merchants should be aware of the following PCI requirements when integrating Miva Merchant 5.5 into their application environment.

Historical Data

It is required that Merchants securely delete any magnetic stripe data, card validation values or codes, and PINs or PIN block data stored by previously installed versions of software as required by PCI Data Security Standard 3.2. Any such historical data stored in files should be removed with a secure file wipe tool, which overwrites all data before the file is deleted. While you may select any secure wipe tool that complies with the DoD 5220.22M data destruction specification, for Unix or Linux systems the srm tool is recommended. This tool is located at http://srm.sourceforge.net/ . Proper usage of the tool is:

$ srm –dod *filename*

Test Data

Any sensitive data retained for debugging or troubleshooting purposes must be securely deleted when no longer needed. This includes any log files, debugging files, and other data sources used for debugging or troubleshooting purposes. This is required to ensure that magnetic stripe data, card validation codes or values, and PINS or PIN block data are not stored. These data sources must be collected in limited amounts and only when necessary to resolve a problem, encrypted while stored, and securely deleted immediately after use.

Chapter 3 – Secure Cardholder Data

Miva Merchant 5.5 allows Merchants to process payments securely. If the Merchant does store cardholder data in other systems then the credit card account number also known as primary account number (PAN), must always be stored in an unreadable form such as strong encryption (AES, 3DES) or a strong one-way salted hash (SHA-1). This is as required by PCI Data Security Standard 3.4.

The Merchant should also be aware of the following PCI requirements regarding the need to securely delete cardholder data and encryption keys.

Cardholder Data

Merchants are required to securely purge cardholder data, including credit card account number (PAN), after it is retained for a time that exceeds the Merchant-defined data retention period. This requirement also applies to data that has been encrypted.

Within the Manage Orders screen of Miva Merchant 5.5 select the Order(s) that you'll need to archive. This can be done using the search filters to limit orders to a specific date range (e.g. older than 180 days). Once you've applied the filter, select the checkbox in the upper left corner of the results screen to select all on that page (make sure you work through all of your pages, or change you display settings to show all of your orders on one page). Once all of your Orders are selected, click the Archive button in the upper right section of the results screen. This will delete all payment information associated with these orders.

Cryptographic Keys

Merchants are required to securely delete any cryptographic key material or cryptogram stored by previous versions of payment software. This could be cryptographic keys used for computation or verification of cardholder data or sensitive authentication data.

While you may select any secure wipe tool that complies with the DoD 5220.22M data destruction specification, for Unix or Linux systems the srm tool is recommended. This tool is located at http://srm.sourceforge.net/ . Proper usage of the tool is:

$ srm –dod *filename*

Chapter 4 – Use Secure Passwords

Miva Merchant 5.5 requires the use of unique usernames and secure authentication to access Miva Merchant 5.5 installations. To comply with PCI-DSS requirements it is important that the Merchant use secure passwords or other forms of secure authentication.

Passwords for Payment Applications

Use unique usernames and secure authentication for administrative access to all payment applications and access to cardholder data. Password requirements are defined in PCI DSS Requirements 8.1, 8.2, 8.4, and 8.5.8–8.5.15 as shown below. Password settings may be viewed on the PA-DSS Checklist screen. Changing the out of the box installation settings will result in non-compliance with PCI DSS.

Passwords for Payment Systems

Establish and maintain unique usernames and secure authentication to access any system that supports a payment application or stores cardholder data. This includes PCs, servers, or databases with payment applications and/or cardholder data. Password requirements are defined in PCI DSS Requirements 8.1, 8.2, 8.4, and 8.5.8–8.5.15 listed below.

PCI DSS Password Policy Requirements

- Assign all users a unique ID [PCI DSS 8.1]
- In addition to assigning a unique ID, employ additional authentication (for example, a password) for access to the cardholder data environment [PCI DSS 8.2]
- All passwords must be rendered unreadable during transmission and storage on all payment system components using strong cryptography [PCI DSS 8.4]
- Do not use group, shared, or generic accounts and passwords [PCI DSS 8.5.8].
- Change user passwords at least every 90 days [PCI DSS 8.5.9].
- Require a minimum password length of at least seven characters [PCI DSS 8.5.10].
- Use passwords containing both numeric and alphabetic characters [PCI DSS 8.5.11].

- When changing passwords, 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 [PCI DSS 8.5.12].
- Lock the user's ID if more than six unsuccessful attempts have been made to access the system [PCI DSS 8.5.13].
- Set the lockout duration to 30 minutes or until administrator enables the user ID [PCI DSS 8.5.14].
- If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal [PCI DSS 8.5.15].

Chapter 5 – Log application activity

Miva Merchant 5.5 supports PCI DSS required logs for access to cardholder data. The Merchant should confirm that they have logging procedures in place to access audit log information. The Merchant is required to ensure that all access to cardholder data is logged in accordance with PCI DSS requirement 10.2 and 10.3 listed below.

PCI DSS 10.2 requires automated audit trails for all system components to reconstruct the following events:

- All individual accesses to cardholder data [PCI 10.2.1]
- All actions taken by any individual with root or administrative privileges [PCI 10.2.2]
- Access to all audit trails [PCI 10.2.3]
- Invalid logical access attempts [PCI 10.2.4]
- Use of identification and authentication mechanisms [PCI 10.2 5]
- Initialization of the audit logs [PCI 10.2.6]
- Creation and deletion of system-level objects [PCI 10.2.7]

PCI DSS 10.3 requires that logs record at least the following audit trail entries for all system components for each event:

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

These logs must be retained for a period of 1 year. Failure to maintain these logs will result in non-compliance with PCI DSS.

Chapter 6 – Protect wireless transmissions

If the Merchant implements or accesses Miva Merchant 5.5 in a Wireless Environment the Merchant is required to maintain the security of the wireless network per the following PCI DSS requirements.

Merchants using wireless networks must install perimeter firewalls between any wireless networks and systems that store cardholder data, per PCI DSS

Requirement 1.2.3 and configure these firewalls to deny or control any traffic from the wireless environment into the cardholder data environment.

Merchants using wireless networks must ensure that wireless vendor default settings are changed, per PCI DSS Requirement 2.1.1.

For wireless implemented in the payment environment by Merchants, use secure encrypted transmissions, per PCI DSS Requirement 4.1.1.

Note: The use of WPA or WPA2 encryption is required for all new wireless installations in cardholder data processing environments. WEP encryption is not effective and not allowed by PCI DSS. Failure to do so will result in a wireless installation that is not compliant with PCI DSS.

Chapter 7 – Cardholder data must never be stored on a server directly accessible from the Internet

Miva Merchant 5.5 allows Merchants to process payment transactions securely when installed according to the recommended procedure. If Merchant storage of cardholder data is required then Merchants should not store cardholder data on Internet-accessible systems (e.g., A database server storing cardholder data must not be on same server as an Internet accessible web application.), per PCI DSS Requirement 1.3.7.

Chapter 8 – Facilitate secure remote software updates

Miva Merchant 5.5 delivers updates to itself using remote access to the Merchant's systems. Such updates are delivered to your Miva Merchant 5.5 securely via a signed software package and SSL. If the Merchant works with 3rd party vendors that access payment applications remotely to provide support or software updates then the Merchant must ensure that the vendor does so securely and are only allowed access during the time period required to complete their work, per PCI DSS Requirements 1, 1.4, and 12.3.9.

Chapter 9 – Secure remote access to application

Merchants that maintain their own payment application must use two-factor authentication if the payment application may be accessed remotely, per PCI DSS Requirement 8.3. Two-factor authentication combines a username and password with and an additional authentication item such as a hardware token or a unique certificate for each user.

Note: The PCI requirement for two-factor authentication cannot be met by requiring the user to login twice with a login and password. For example, requiring a user to login first on a VPN and then use SSH or Remote Desktop login to access a server in the cardholder data environment is not considered PCI compliant two-factor authentication.

If you utilize remote access software to access the Miva Merchant servers, some or all of the following security features must be implemented:

1. Customers must change default settings for remote access passwords per PCI 8.1
2. Use unique passwords for each user PCI 8.2
3. Use Strong Authentication and complex passwords PCI 8.1, (PCI 8.5.8) no generic accounts used, (PCI 8.5.9) reset password after 90 days, (PCI 8.5.10) password must be of at least 7 characters in length, (PCI 8.5.11)

complex passwords must be set, (PCI 8.5.12) and users cannot reuse last the last four passwords

4. Implement 2 factor authentication using a VPN as per PCI 8.3
5. Implement communication data transmission encryption using SSL as per PCI 4.1
6. Establish and protect passwords according to PCI, 8.4 and 8.5
7. Enable lockout after a certain number of failed login attempts PCI 8.5.13 with a lockout for 30 minutes PCI 8.5.14 and auto disconnect after 15 minutes of inactivity PCI 8.5.15
8. Log all access in accordance with PCI DSS requirements
9. Restrict access for all passwords to only authorized personnel
10. Store passwords securely, per PCI 8.4
11. Allow connections from only known IP/MAC addresses

Chapter 10 – Encrypt traffic over public networks

Miva Merchant 5.5 uses secure cardholder data transmission over public networks. Merchants implementing Miva Merchant 5.5 must ensure that they comply with PCI DSS DSS Requirement 4.1, 4.2.
In addition to the Internet, public networks include wireless networks such as publicly accessible Wi/Fi, GSM or CDMA wireless phone networks, and wireless modems.

Secure Transmission on Public Networks

Merchants must ensure that any payment application they implement that accepts or transmits cardholder data over a public network, such as the Internet, must use secure encrypted transmission. For example, a front-end web application that accepts cardholder data must use secure transmission (SSL) for all cardholder data, per PCI DSS Requirement 4.1.

Email and Messaging Technologies

Merchants should never send cardholder data via end user messaging technologies such as instant messaging or emails. If however they choose to do this, they must ensure that they implement and use an encryption solution if credit card account numbers (PANs) are sent with end-user messaging technologies such as email or instant messaging, per PCI DSS Requirement 4.2. Merchants must establish a policy prohibiting messaging of unencrypted PANs and communicate this policy to all staff.

Chapter 11 – Encrypt administrative access

Merchants accessing payment applications must ensure that they implement and use SSH, VPN, or SSL/TLS or other strong encryption for any non-console administrative access to payment applications or servers in cardholder data environment, per PCI DSS Requirement 2.3.