Midax EFT Management 3.3.x PA DSS Implementation Guide

Revision 1.4
October 21, 2020

Midax Inc.
106 Heron Pointe Drive
Cape Charles, VA 23310
1-757-620-4168
Technical Support line: 1-800-6432-991
www.midax.com

Copyright © 2020 by Midax Inc.

Information in this document is subject to change without notice. No part of this document may be reproduced or transmitted in any form without prior written permission of Midax Inc.
Midax Infinite Possibilities is a registered trademark of Midax Inc.

All brands and product names are trademarks, registered trademarks or trade names of their respective holders.

Table of Contents

1. Overview

This document describes how the Midax EFT Management 3.3.x suite of applications processes PCI DSS sensitive data and gives recommendations to Midax customers how to build and maintain a PCI DSS compliant environment. It is supposed to help the Midax customers with their PCI DSS audits.

All Midax payment applications are developed in compliance with the latest standards and documents published by PCI Security Standards Council (Payment Application Data Security Standard Ver. 3.2 as of this writing). Having a PA DSS certified payment application is a necessary but not sufficient condition to be PCI DSS compliant. Many parts of the production systems are outside of the Midax control and need additional special care. This document will help with recommendations how the production environment should look like.

The applications from the Midax EFT Management 3.3.x are installed and maintained by the Midax support team in the same way as with the old versions. The support team is instructed how to install the new version from scratch as well as how to upgrade the old version in a PCI DSS compliant manner. That offloads the responsibility from you as a merchant to take care of some PCI DSS requirements like controlling the cryptographic key management policies and the proper deletion of old cryptographic data. Nevertheless this document describes the general dataflow of the PCI DSS sensitive information within Midax applications. That keeps you aware of the way the system works and allows you to build properly your infrastructure in a PCI DSS compliant way.

Midax development team took special measures to limit the locations and the applications which have access to PCI DSS sensitive information. The new version significantly reduces the attack surface for the potential hackers and should help you limit the scope of your PCI DSS audits to a smaller number of machines and/or applications.

Please note that if the POS system at your store or gas station has a separate payment channel for proprietary cards (like Gilbarco Passport or Verifone Commander), the whole Midax infrastructure should be out of scope of the PCI DSS audit since it never sees or processes any credit or debit card information.

Midax EFT Management 3.3.x Configurations describes the path of the PCI DSS sensitive data through the Midax applications.

Midax PCI DSS Sensitive Information Handling describes what is done by Midax and what needs to be done by the merchant in order to protect the PCI DSS sensitive data on the disks and the networks.

PA DSS Implementation Instructions goes through PA DSS requirements and shows how the compliance responsibility is split between the Midax support team and the merchant.

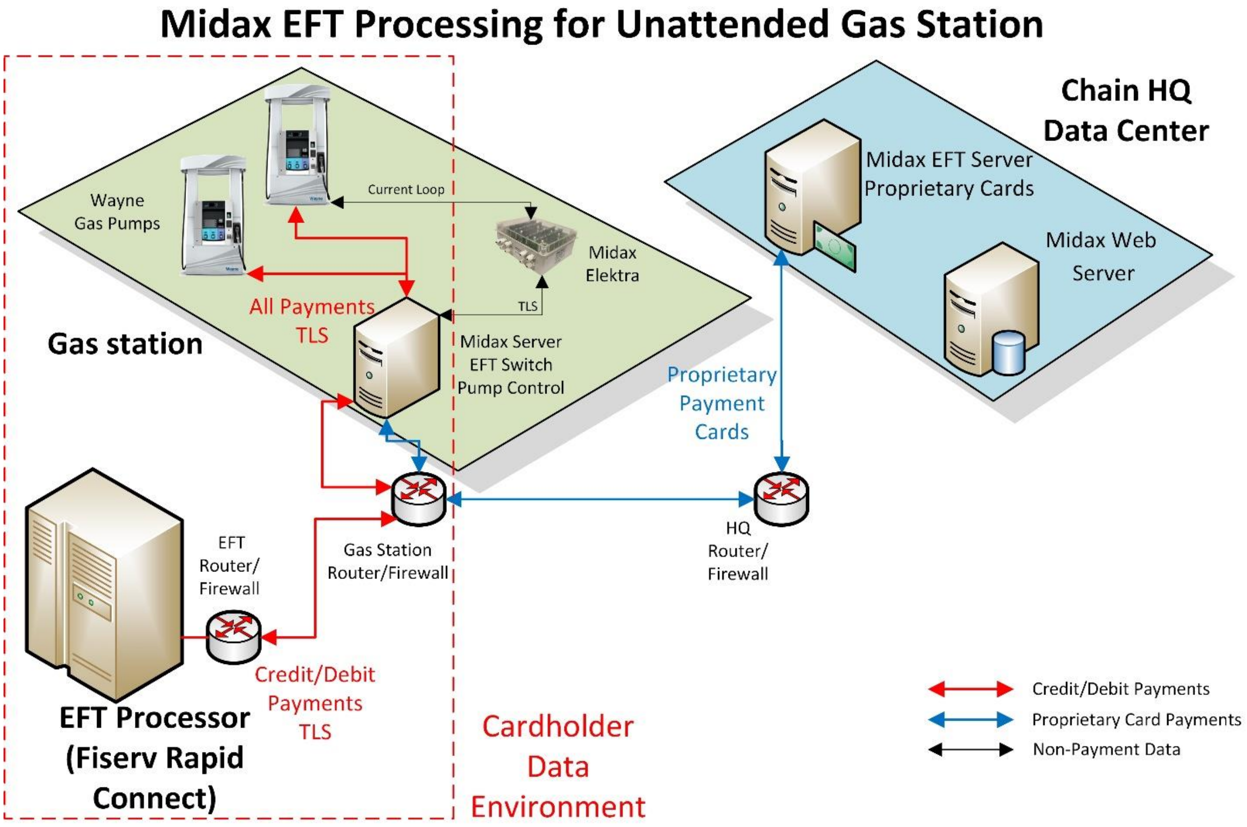
2. Midax EFT Management 3.3.x Configurations

Midax EFT Management Suite 3.3.x supports pumps payments for unattended Wayne gas stations. In this configuration there is no POS system and Midax takes care of all pump control and transactions.

Each gas station is controlled by a central HQ data center. If you are a big chain with many locations you probably host the HQ data center yourself. If you have one or only a few locations and can't afford your own HQ data center, Midax suggests your payment processing to be hosted at Midax Data Center. This is a PCI DSS certified data center which has Midax HQ EFT switch installed and configured to support multiple merchants. The version 3.3.x of Midax EFT Management suite isolates the HQ from the payment card holder environment and as a result the server doesn't see any PCI DSS related data – all card numbers are masked at store level and the full numbers don't reach the HQ at all. The HQ server only sees the full card number of Midax processed cards – gift cards, scrip cards etc.

2.1. Midax EFT for Unattended Gas Stations

There is no POS system at an unattended gas station. The pumps are completely under Midax control. The same EFT payment switch that is used in grocery store configurations is used to process pump payments.



Midax EFT Processing for Unattended Gas Station
Chain HQ Data Center
Midax EFT Server Proprietary Cards
Midax Web Server
Wayne Gas Pumps
Current Loop
Midax Elektra
TLS
All Payments TLS
Gas station
Midax Server EFT Switch Pump Control
Proprietary Payment Cards
EFT Router/ Firewall
Gas Station Router/Firewall
HQ Router/ Firewall
Credit/Debit Payments TLS
EFT Processor (Fiserv Rapid Connect)
Cardholder Data Environment
Credit/Debit Payments
Proprietary Card Payments
Non-Payment Data

Figure 2-1 Midax EFT Processing for Unattended Gas Station

Figure 2-1 shows the general infrastructure of the gas station and the payment transaction paths. The red line shows the PCI DSS sensitive data path. It includes the following components:

- Wayne Pumps equipped with iX Pay payment device. The iX Pay payment device connects directly to Midax in-store server using TLS protocol over a LAN connection.
- Midax Server with Midax EFT Switch and Midax Pump Control modules.
- Payment provider (EFT processor) which takes care of all credit/debit transactions. Midax talks with Fiserv Rapid Connect payment provider using Fiserv Secure Transport protocol over encrypted HTTPS connections.

This data path and components represent the Cardholder Data Environment (CDE) for the store. It should be segmented from the general network used by the store and for Midax proprietary cards (the blue line shows the proprietary card transaction path).

There are three Midax modules on the Midax store server participating in the Midax EFT Management Suite 3.3.x which see and process PCI DSS sensitive data:

- Midax Pump Control. This module controls completely the gas pumps. It takes care of all the interaction between the end users and the pumps including the payment process. Wayne pumps' iX Pay payment devices connect directly to Midax Pump Control using TLS connection over LAN. That connection is used to process all payments. The pump control module does minimal payment processing. It sends the payment transactions to the Midax EFT switch which is responsible for the complex EFT operations and protocols.
- Midax EFT Switch. This module receives all payments from the pump control and decides how to process them. Generic credit / debit card path is part of the CDE – the EFT switch communicates with Midax Secure Transport Interface to process those payments via Fiserv Rapid Connect protocol. Midax proprietary cards do not process PCI DSS sensitive data and are sent to Midax HQ via separate communication line.
- Midax Secure Transport Interface. The module provides an encrypted connection to Fiserv in order to process Rapid Connection protocol wrapped in Fiserv Secure Transport transactions. It receives transaction requests from Midax EFT Switch and process them through Fiserv.

Midax pump control currently supports Wayne pumps with iX Pay payment devices.

Midax EFT switch will send transaction log data for all processed transactions to the HQ data center. The card numbers for these transaction logs are masked before they leave the store's EFT server and don't have any PCI DSS sensitive data. That means Midax HQ server doesn't see any full credit/debit card numbers.

The pump control module communicates also with a hardware box called Midax Elektra Distribution Box in order to manage the pumps. That connection takes care of the physical part of the fueling - nozzles, gas grades, and prices. It has no access to user interface devices like screen, keyboard, and card readers. As a result, it doesn't process any payment data.

3. Midax PCI DSS Sensitive Information Handling

Midax EFT applications are developed with PCI DSS requirements in mind. They never store unencrypted credit card numbers or any information which is prohibited by the security standard.

There are 2 main areas which should be properly configured and maintained in order to protect the credit card sensitive data processed by Midax applications:

- Protect the data which is saved on the hard disks.
- Protect the data while it is being transmitted/received on the participating networks.

The protection of the saved data on the disks is done by the Midax EFT Management Suite of applications. Only one of the 3 Midax applications which process PCI DSS sensitive data (Midax Pump Control, Midax EFT Switch, and Midax Secure Transport Interface) stores PCI DSS sensitive data on a disk:

- Midax EFT switch. The application uses a proprietary database and 192-bit AES encryption for all the sensitive data kept on disk. It automatically deletes all the obsolete data using a secure algorithm. The encryption happens before the data is sent to the database. The system is designed so that the information from the database alone is not enough to decrypt any sensitive data.

Midax EFT switch keeps encrypted card numbers and expiration dates in order to be able to generate reversals in case the POS system requires them. They are kept for a maximum of 48 hours. All expired records are deleted from the disk using a secured algorithm that prevents the attempts to restore the deleted data using special low-level tools.

The encryption key management is done by Midax support team according to the PCI DSS requirements. You as a merchant don't have access and shouldn't be kept responsible for those keys. However if you experience a breach or any security issue with the systems on which Midax is installed, you should call immediately the Midax support team (1-800-MIDAX-911). They know how to force a change of the encryption keys in order to prevent any future exposure. These are the principles which Midax applications and support team follow regarding the encryption key management:

- Midax support team follows a special key management policy to take care of the encryption keys in your systems. You as a merchant are not responsible for storing or changing the encryption keys.
- The encryption keys are 192-bit AES keys. They are automatically generated using a strong cryptographic provider (via Microsoft Crypto API).
- The keys are generated by Midax EFT Switch and they are stored on the system on which the application is installed. They are not transmitted or otherwise moved to any other location.
- There are no open encryption keys stored anywhere on your system. All keys are protected and kept in a secure way on the disks.

- The encryption keys used by the Midax EFT switch are changed automatically every 6 months. The application can change the keys immediately if you call the support team and request that.
- The old encryption keys are deleted in a secure way after the last record using them is deleted from the system (no more than 48 hours later). The only exception is a key change forced by you because you believe the system is compromised – in this case the old keys and all pending records using them will be deleted immediately.
- Midax applications control the integrity of the used encryption keys. If an attempt to manipulate the key data is detected, the system automatically will destroy all existing keys and the corresponding encrypted records and will generate new encryption keys.
- Midax support team members know how to change the current encryption keys. However they can't decrypt any records using those keys and they can't see any real card numbers.

Protecting the data while it is transmitted on the networks means to prevent a hacker from stealing credit card numbers and other sensitive data by using a network sniffer. It requires cooperation and efforts from you.

All existing EFT provider protocols require a secure connection to their servers. Midax communicates with Fiserv using Fiserv's Secure Transport (a.k.a. DataWire) protocol over an encrypted https connection. All Rapid Connect transactions to and from Fiserv are wrapped in Secure Transport requests/responses.

The best way to protect the network data is by segmenting the network as recommended by PCI DSS. Most of the available routers at store level can do virtual LANs. It's quite possible that the proper segmentation is only a configuration matter. Even if you need to buy some additional devices (network card, switches etc.), usually it's less expensive to do that than to pay more to the PCI DSS auditors because the scope of the audit is significantly extended and covers non EFT related machines and applications. Midax strongly recommends the network connections which carry sensitive data (the red lines on the figure) to be put in a separate protected network segment. Midax guarantees that no PCI DSS sensitive data will ever be sent by Midax applications outside of the red transactions paths.

The exact sensitive data locations on the disks and the corresponding network information (tcp socket addresses and ports) are configurable and vary from system to system. Midax support team will be happy to provide that information for your particular system to your authorized administrators.

4. PA DSS Implementation Instructions

Midax EFT Management Suite 3.3.x is PA DSS compliant. It takes care of many of the PCI DSS requirements that you should fulfill. Other requirements are outside of Midax control – they typically affect your operational environment and are managed by your system and/or network administrators. We can only recommend measures to build and maintain that environment in a PCI DSS compliant manner, but we have no right to enforce them.

This guide covers only the Midax application installation and maintenance. If there are third party systems (independent POS systems with their own payment terminals), please follow their PCI DSS implementation guides too. We don't expect them to be in conflict with this guide since they are based on the same PCI standards.

The following list explains how certain PA DSS requirements are implemented in the Midax suite of applications and how the responsibility is split between the Midax support team and your system/network administrators:

- 1.1.4 Delete sensitive authentication data stored by previous payment application versions.
  Midax support team members do the installations and the upgrades of all Midax applications for you. They are instructed how to delete in a secured way the data stored by the previous versions of the application. You are not responsible to do that.
- 1.1.5 Delete any sensitive authentication data (pre-authorization) gathered as a result of troubleshooting the payment application.
  Midax applications don't store sensitive authentication data anywhere once the transaction is completed.
  The trace files used by the Midax support to troubleshoot an application don't have any PCI DSS sensitive authentication data or any unmasked card holder data. They can be used to localize a transaction based on its source (lane/pump), transaction or system trace number, date/time etc. However, the card numbers are masked (only the first 6 and the last 4 digits are visible) and no other PCI DSS sensitive information is kept there in any form. You are not responsible to do that.
- 2.1. Securely delete cardholder data after customer-defined retention period.
  Midax EFT switch keeps the encrypted card numbers and the expiration date for no more than 48 hours. That data is deleted automatically in a secured way after the retention period expires. Midax support team is instructed to make sure that everything is working as designed during their quarterly maintenance procedures. You are not responsible to do that except if you believe your system is compromised – in that case please call Midax support team to force a key change which will delete the old data.
- 2.2. Mask PAN when displayed so only personnel with a business need can see more than the first six/last four digits of the PAN.
  All PCI DSS related PANs are masked according to this requirement. There is no way for any personnel (Midax or yours) to see full card numbers. You are not responsible to do that.

- 2.3. Render PAN unreadable anywhere it is stored
  All PCI DSS related PANs are masked before they are written to the logs and/or front-end database. You are not responsible to do that.
- 2.4. Protect keys used to secure cardholder data against disclosure and misuse.
  The encryption keys are generated and handled automatically as described in the Midax PCI DSS Sensitive Information Handling chapter. Neither you as a merchant nor Midax support team members know how to disclose or use those keys. You are not responsible to do that.
- 2.5. Implement key management processes and procedures for cryptographic keys used for encryption of cardholder data.
  The cryptographic keys are generated automatically by Midax applications using a secured cryptographic provider. Midax support team has special instructions how to change and/or delete these keys during their annual maintenance procedures or as a result of your call about a compromised system (as described in the Midax PCI DSS Sensitive Information Handling chapter). You are not responsible to do that.
- 2.6. Provide a mechanism to render irretrievable any cryptographic key material or cryptogram stored by the payment application, in accordance with industry-accepted standards.
  Midax support team members do the installations and the upgrades of all Midax applications for you. They are instructed how to delete in a secured way the cryptographic key material or cryptograms stored by the previous versions of the applications. You are not responsible to do that.
- 3.1. Use unique user IDs and secure authentication for administrative access and access to cardholder data.
  Midax front end applications provide only masked card numbers and no other PCI DSS sensitive data. They are designed according to the PA DSS password management requirements. However, since they don't have any access to sensitive information, those policies are irrelevant from the PCI DSS perspective. You are not responsible to do that. However, you are responsible for the proper Windows credentials of the Midax store machine which sees PCI DSS cardholder data and is controlled by your system/network administrators.
- 3.2. Use unique user IDs and secure authentication for access to PCs, servers, and databases with payment applications.
  Typically, the administration of machines on which Midax applications are installed is done by your system administrators and is outside of the Midax control. Therefore, they are your responsibility. The only exception is Midax HQ servers located at Midax datacenter which are controlled by Midax support team – you are not responsible for their maintenance.
  These are the computer access requirements you should implement along with their PA DSS and PCI DSS numbers:
    - Assign unique ID for every user account (PA DSS 3.1.1, PCI DSS 8.1).
    - Employ at least one of the following methods to authenticate all users (PA DSS 3.1.2, PCI DSS 8.2):
        - 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.
  - Do not use group, shared, or generic accounts and passwords or other authentication methods (PA DSS 3.1.3, PCI DSS 8.5.8).
  - Change user passwords at least every 90 days (PA DSS 3.1.4, PCI DSS 8.5.9).
  - Require a minimum password length of at least seven characters (PA DSS 3.1.5, PCI DSS 8.5.10).
  - Use passwords containing both numeric and alphabetic characters (PA DSS 3.1.6, PCI DSS 8.5.11).
  - 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 (PA DSS 3.1.7, PCI DSS 8.5.12).
  - Limit repeated access attempts by locking out the user ID after not more than six attempts (PA DSS 3.1.8, PCI DSS 8.5.13).
  - Set the lockout duration to a minimum of 30 minutes or administrator enables the user ID (PA DSS 3.1.9, PCI DSS 8.5.14).
  - If the session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session (PA DSS 3.1.10, PCI DSS 8.5.15).
- 4.1. Implement automated audit trails.
  Midax EFT applications which see PCI DSS sensitive data are Windows services. They don't allow any users to log in or access the sensitive data. They write automatically critical information like starting the service (or failure to start the service), stopping the service, installing or uninstalling the service etc. to the Windows Application Event Log. Windows Service Control Manager writes independently similar information in the Windows System Even Logs. Apart from this Midax EFT applications generate trace files which can be used to investigate transactions. There is no PCI DSS sensitive information in any of these files. All these audit trails are generated automatically. You are not responsible to do that.
- 4.4. Facilitate centralized logging.
  As already mentioned, Midax log files don't have any PCI DSS sensitive information. There is no problem for them to be collected centrally using FTP or third-party applications like EventSentry. It's Midax responsibility to generate these files. It's your responsibility to collect them in a central place – Midax support team can help you localizing the files and organizing the process.
- 5.4.4. Implement and communicate application versioning methodology.
  Midax applications use 3 digits for version numbering: X.Y.Z where X is the major version, Y is minor version, and Z is release version and is used for bug fixing and no security impact changes. The major version X is changed only when radical changes of the application are made – use a new platform, libraries, database etc. The minor version Y is changed whenever there is a high impact change like adding a new payment processor or protocol that has a significant impact on the payment infrastructure. The release version is increased every time the application is changed in any way.

- 6.1. Securely implement wireless technology.
  Midax applications don't require any wireless connections. We strongly discourage you from using any wireless connections especially in the EFT sensitive segment of the network. However, if you ignore that recommendation and a wireless network is installed, you should take at least the following measures:
  - Change all vendor default settings:
    - 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.
    - Verify default SNMP community strings or wireless devices were changed.
    - Verify default passwords/passphrases on access points were changed.
    - Verify firmware on wireless devices is updated to support strong encryption for authentication and transmission over wireless networks.
    - Verify other security-related wireless vendor defaults were changed, if applicable.
  - Install a firewall between any wireless networks and the systems participating in the EFT sensitive segment of the network.
  - Configure the firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.
- 6.2. Secure transmissions of cardholder data over wireless networks.
  You are responsible to use industry best practices (for example IEEE 802.11i) to implement strong encryption for authentication and transmission. Please note that the WEP security is prohibited since it's considered broken.
- 6.3. Provide instructions for secure use of wireless technology.
  Midax doesn't have any built-in configuration parameters or settings related to wireless technology. If you choose to use wireless connections, you are responsible to do it using PCI DSS compliant settings.
- 7.2.3. Provide instructions for customers about secure installation of patches and updates.
  Midax support installs all patches and updates of Midax applications. You are not responsible to do that – you are only responsible to provide access for Midax support when they inform you about a new update.
- 8.2. Use only necessary and secure services, protocols, components, and dependent software and hardware, including those provided by third parties.
  Depending on the chosen communication between each store and the payment provider Midax may require the following third-party software and hardware:
  - Midax applications depend on a database installation as a prerequisite. Midax HQ uses Oracle database but there is no PCI DSS sensitive information in it. Midax Pump Control uses Microsoft SQL Server Express database and it doesn't store anymore PCI DSS related data in it. Midax support is responsible for the database installation and updates. You are not responsible to do that.

  - Your system/network administrators are responsible to stop any other services, protocols and components which they don't use.

- 9.1. Store cardholder data only on servers not connected to the Internet.
  The machines on which Midax EFT switch or Midax Pump Control modules are installed are not supposed to allow Internet connections. The only Midax application which is part of the Midax EFT Management 3.3.x Suite and needs an Internet connection is the external web service which allows end customers to use your web site to check their proprietary card balances. The communication between this web service and the Midax HQ EFT server is organized in such a way that no inbound connection from Internet is necessary. A special service on the Midax HQ server machines opens an outbound connection to the web server where the web service resides. No PCI sensitive data is ever sent through this line.
  It's a responsibility of your system/network administrators to make sure that no inbound Internet connections are allowed to the machines on which Midax EFT switch or Midax Pump Control modules are installed.
- 10.1. Implement two-factor authentication for remote access to payment application.
  Midax support team typically will access the Midax payment applications for upgrades and troubleshooting by using your VPN and then some desktop access software such as remote desktop. You are responsible to provide multi-factor authentication to the VPN by implementing at least two of the following three authentication methods:
  - 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.

  For example, Midax development lab uses two-factor authentication both to access the lab VPN and the remote desktop machines. The VPN access second factor is based on an individual certificate for each eligible developer and is enforced by the router. Rohos is used as a second factor for remote desktop access. It requires Google Authenticator mobile app on top of the username/password authentication.
- 10.2.1. Securely deliver remote payment application updates.
  Midax support team makes all the updates of the payment applications by accessing the corresponding systems remotely. When such an update is available a support team member will contact you and ask for an access. You should turn on the remote access only for the period necessary to do the update. You should close the access once the support team member informs you that the work is done. Midax support team will use your VPN and any other security features you provide in order to do the update.
  If you provide an "always on" VPN remote connection, you should have a securely configured firewall or a personal firewall product to protect your machines.
- 10.2.2. Securely implement remote access software.
  You are responsible to implement and use the remote access software security features.
  For example, Midax development lab uses remote desktop for a remote access to the machines protected additionally by Rohos phone authentication. The guys who are authorized to access the machines have to confirm the access on their smart phones before the access is granted.

- 11.1. Secure transmission of cardholder data over public networks.
  Midax communicates with Fiserv payment provider via “Midax Secure Transport Interface” module. It uses secured TLS connection via https to connect to Fiserv payment servers. Midax support is responsible for configuring and maintaining the “Secured Transport” related software on Midax store server.
  Midax receives cardholder data via secured TLS connection from the Wayne pump iX Pay device. It’s your pump technician’s responsibility to configure properly the pump to talk to Midax Pump Control application on Midax in-store server.
  As already described in the Midax PCI DSS Sensitive Information Handling chapter the part of the network which carries unencrypted PCI DSS sensitive data (the red lines on the figures) should be protected by one of the above methods. Under NO conditions these parts of the network should be exposed to any public networks without being encrypted and protected.
- 11.2. Encrypt cardholder data sent over end-user messaging technologies.
  Midax doesn’t provide any way for the users to see or send unmasked PAN numbers or any other PCI DSS sensitive data. Therefore, you are not responsible for this point relative to the Midax suite of applications. However, if you obtain cardholder data directly from the customer or from other system outside of Midax applications, you are responsible never to send it over end-user messaging technologies unencrypted.
- 12.1. Encrypt non-console administrative access.
  Midax support needs remote (non-console) access to Midax machines in order to do updates and troubleshooting. The remote access application that you provide for that purpose should use encrypted connections. Midax lab uses Windows remote desktop which uses encrypted connections by default. It’s your responsibility to make sure that your remote access application uses encrypted connections.
- 12.2. Use multi-factor authentication for all personnel with non-console administrative access.
  It’s your responsibility to provide multi-factor authentication both for Midax support and your personnel when they need remote access to Midax servers. Midax uses a two-factor authentication via Rohos for the remote desktop connections.