Sage Exchange Desktop v2.0 PA-DSS Implementation Guide

Sage Payment Solutions

July 2016

Contents

Introduction

The purpose of this document is to instruct merchants, systems integrators, resellers and other independent software vendors on how to implement Sage Payment Solutions' Sage Exchange Desktop (SED) v2.0 in a Payment Application Data Security Standard (PA-DSS) compliant environment. It is not intended to be a complete installation guide. If installed according to the guidelines documented here, Sage Exchange Desktop should facilitate and support a merchant's compliance.

Understanding PA-DSS

PA-DSS is a set of security standards created by the PCI Security Standards Council (PCI SSC) to guide payment application vendors to implement secure payment applications.

Distribution and updates

This document is applicable to all SED users including merchants, resellers, and integrators. It should be updated at least annually and after changes in the software. The annual review and update should include new software changes as well as any changes in the PA-DSS standard. Notifications of updates to this document are sent via release notifications to registered customers via email and can be obtained on the support portal website or contacting Sage Payment Solutions Customer Support at:

https://www.sage.com/us/sage-payment-solutions

Security standards versioning

This document references the PA-DSS and PCI DSS requirement standards (shown in italics), both of which play an important role for implementation of solutions meeting PCI Security and Compliance goals. The following versions are referenced in this guide:

- PCI DSS version 3.1
    - Merchants and Service Providers
    - Secure Environments
- PA-DSS version 3.1
    - Software Developers
    - Payment Applications

Securing systems and sensitive data

This section discusses the secure deletion of sensitive data and the protection of stored cardholder data.

PA-DSS 1.1.4 *Securely delete any magnetic stripe data, card validation values or codes, and PINs or PIN block data stored by previous versions of the software.*

Sage Exchange Desktop does not store sensitive authentication data (including magnetic stripe data and card validation values or codes). PCI DSS has strict requirements on the processing and storage of sensitive authentication and cardholder data, including historical data.

PA-DSS 1.1.5 *Securely delete any sensitive authentication data (pre-authorization data) used for debugging or troubleshooting purposes from log files, debugging files, and other data sources received from customers, to ensure that magnetic stripe data, card validation codes or values, and PINS or PIN block data are not stored on software vendor systems.*

Sage Exchange Desktop does not store sensitive authentication data (including magnetic stripe data and card validation values or codes). The application vendor does not collect sensitive account data during troubleshooting and will never ask for such information. It is strongly recommended that sensitive data never be collected for troubleshooting or as part of the troubleshooting process.

PA-DSS 2.1 *Securely delete cardholder data after customer-defined retention period.*

Sage Exchange Desktop does not store cardholder data, and has no configuration options to allow capture or retention of cardholder data.

All cardholder data must be handled in accordance with PCI DSS requirements, including secure deletion after customer-defined retention periods, when no longer required for legal, regulatory, or business purposes. All underlying software or integrated systems (such as OS, databases, etc.) should be configured to prevent inadvertent capture or retention of cardholder and sensitive data.

PA-DSS 2.2 *Mask PAN when displayed so only personnel with a business need can see the full PAN.*

Sage Exchange Desktop masks PAN by default for display only purposes. It captures credit card data via two entry methods on the Payment Information Screen. The credit card data may be entered manually or using the **Swipe Card** button will initiate a configured PTS PINPad device to capture card present transactions. When selected, the **Automatically Start Card Swipe** configuration option will automatically initiate the device capture upon receiving the calling application transaction request.

The PAN entry field displays the full PAN as typed for the business reason of the user ensuring the correct card number is entered before submitting the payment authorization request. The PAN is not masked on entry to support the business need for personnel to verify upon manual entry accurate and correct card information.

Sage Exchange Desktop does not have any other screens that display PAN and unmasked PAN is never logged to log files or error messages. The response XML data returned from Sage Exchange to the calling application may contain masked PAN in the field Last4 for the purpose of printing receipts and other functions as may be required. An example of how PAN data is formatted with 'X' as the mask character in the Last4 data element:

<Last4>XXXXXXXXXXXX5454</Last4>

In the case of the Moneris specific configuration of the Ingenico iPP320 PINPad device, Sage Exchange Desktop will format both a customer and merchant receipt and facilitate printing upon completion of the transaction request. The receipt data is written in the user's Microsoft Windows application local data path under:

<USER APP DATA PATH>\Sage Payment Solutions\Sage Exchange\Receipts\

The PAN is masked to only show the last 4 digits as in the XML output response. The following receipts files are created:

File name	Description
receiptdata.xml	Transaction receipt data values.
mmddyyyy_999999_CustomerCopy.htm	Customer HTML receipt.
mmddyyyy_999999_MerchantCopy.htm	Merchant HTML receipt.

The receipt HTML files are opened for printing using the system registered program for .htm files (the default program for Microsoft Windows is Internet Explorer).

PA-DSS 2.3 *Render PAN unreadable anywhere it is stored (including data on portable digital media, backup media, and in logs).*

Sage Exchange Desktop does not store PAN data. It is not written out to log files and is masked in any receipt files or XML responses. There are no configurable options that alter the treatment of PAN data within the software.

The XML response from Sage Exchange Desktop output to the calling application contains masked PAN data that may be stored or used for printing receipts or other purposes.

Below is an example of how PAN data is formatted with 'X' as the mask character in the XML responses:

<Last4>XXXXXXXXXXXX5454</Last4>

<PaymentDescription>545454XXXXXX5454</PaymentDescription>

PAN data must be rendered unreadable in any case a business application may have access to the full PAN and stored or displayed. The maximum allowed unmasked characters are first six and last four digits.

PA-DSS 2.4 *Protect keys used to secure cardholder data against disclosure and misuse.*

Sage Exchange Desktop does not store any cardholder data. There is no cryptographic key material stored by Sage Exchange Desktop.

PA-DSS 2.5 *Implement key management processes and procedures for cryptographic keys used for encryption of cardholder data.*

Sage Exchange Desktop does not store any cardholder data. There is no cryptographic key material stored by Sage Exchange Desktop.

PA-DSS 2.6 *Provide a mechanism to render irretrievable cryptographic key material or cryptograms stored by the payment application.*

Sage Exchange Desktop does not store any cardholder data. There is no cryptographic key material stored by Sage Exchange Desktop.

Password and account settings

Access control

Merchants, resellers, and integrators are advised to control access, via unique user name and PCI DSS compliant complex passwords, to any computers, servers, and databases with payment applications and cardholder data.

Sage Exchange Desktop does not have administrative user accounts or store cardholder data. However, merchants must control access, via unique user name and PCI DSS compliant complex passwords, to any computers or servers running SED.

PA-DSS 3.1 *Use unique user IDs and secure authentication for administrative access and access to cardholder data.*

Sage Exchange Desktop does not manage unique user IDs or have a user authentication method. The calling application shall manage user-level secure authentication in accordance with PA-DSS Requirements 3.1.1 through 3.1.11. These include but are not limited to:

Operating system

The following guidelines should be followed to protect the operating system. User accounts and passwords should meet the PCI requirements in PCI DSS section 8.1 and 8.2 including those listed below:

PCI DSS 8.1 *Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components as follows, in requirements 8.1.1 through 8.1.8.*

PCI DSS 8.1.1 *Assign all users a unique ID before allowing them to access system components or cardholder data.*

PCI DSS 8.1.2 *Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.*

PCI DSS 8.1.3 *Immediately revoke access for any terminated users.*

PCI DSS 8.1.4 *Remove/disable inactive user accounts within 90 days.*

PCI DSS 8.1.5 *Manage IDs used by vendors to access, support, or maintain system components via remote access as follows:*

- Enabled only during the time period needed and disabled when not in use.
- Monitored when in use.

PCI DSS 8.1.6 *Limit repeated access attempts by locking out the user ID after not more than six attempts.*

PCI DSS 8.1.7 *Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.*

PCI DSS 8.1.8 *If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

PCI DSS 8.2.3 *Passwords/phrases must meet the following complexity or equivalent:*

- Require a minimum length of at least seven characters.
- Contain both numeric and alphabetic characters.

PCI DSS 8.2.4 *Change user passwords/passphrases at least once every 90 days.*

PCI DSS 8.2.5 *Do not allow an individual to submit a new password/phrase that is the same as any of the last four passwords/phrases he or she has used.*

PCI DSS 8.2.6 *Set passwords/phrases for first-time use and upon reset to a unique value for each user, and change immediately after the first use.*

PA-DSS 3.1.1 *The payment application does not use (or require the use of) default administrative accounts for other necessary software (for example, the payment application must not use the database default administrative account).*

Aligns with PCI DSS Requirement 2.1 (Below)

PCI DSS 2.1 *Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network.*

This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, Simple Network Management Protocol (SNMP) community strings, etc.).

To maintain PCI DSS compliance, any changes made to authentication configurations would need to be verified as providing authentication methods that are at least as rigorous as PCI DSS requirements.

Assign secure authentication to all default accounts in the environment

For any default accounts that won't be used, assign secure authentication and then disable or do not use the accounts.

PA-DSS 3.2 *Use unique user IDs and secure authentication for access to computers, servers, and databases with payment applications.*

The controlling business application and PCI solution should use unique user names and secure authentication to access any computers, servers, and databases with payment applications and/or cardholder data, per PA-DSS requirements 3.1.1 through 3.1.11. Sage Exchange Desktop software does not manage unique user IDs or have a user authentication method.

Logging

Merchant applicability

Currently, for Sage Exchange Desktop, there is no end-user, configurable, logging settings that fall under the PA-DSS Audit Log requirements as defined in Requirement 4.1. For support and troubleshooting purposes it is recommended that all installations configure trace logging by default. A trace log file may be enabled via the **Settings > Tracing > On** configuration option. EML trace log file may be enabled via the **Settings > EMV Tracing > On** . All log and runtime files written by the application are written to the current user's Application Data folder or Temp directory. The Application Data folder is hidden by default in most Windows systems, and may be viewable by configuring the applicable folder view options. Usually the Application Data and Temp folders are:

<Application Data> = %User Profile%\AppData\Local\

<Temporary Data> = %User Profile%\AppData\Local\Temp\

Temporary files are created for certain functions, for example the signature image for healthcare acknowledgments:

Signature Image – "Signature_<ID>_.bmp" (Equinox device only)

The directory structure created for Sage Payment Solutions applications is:

<Application Data>\Sage Payment Solutions\

The following subdirectories and files are created here:

- Application Deployment
    - Installation Log files in format "mmddyyyy.log"
    - Application Version Manifest log in format "<App ID>.txt"
- Sage Exchange
    - Receipt Files in subdirectory "\Receipts\" (Moneris IPP320 only)
        - Customer - "mmddyyyy_<ID>_CustomerCopy.htm"
        - Merchant - "mmddyyyy_<ID>_MerchantCopy.htm"
        - Receipt Data File – "ReceiptData.xml"
- Sage Exchange Desktop
    - User Profile Data – "ApplicationProfiles.dat"
    - Trace File – "SageExchange.log"
    - User Settings – "SageExchangeDesktop.settings"

- Equinox Log – “Equinox.log” (Equinox L5300 only)

PA-DSS 4.1 *Implement automated audit trails.*

Sage Exchange Desktop software does not allow access to stored PAN or stored sensitive cardholder data and does not manage user-level authentication. Sage Exchange Desktop payment application does not use any administrative accounts. It also does not provide administrative access to any functions that change settings that may affect PA-DSS compliance. Cardholder data is not stored by the application. Since log settings are built around access to cardholder data and administrative functions that affect PA-DSS compliance, audit logging does not apply to the Sage Exchange Desktop payment application. The exception is PA-DSS requirement 4.2.7 in which the creation and deletion of system level objects need to be logged.

PA-DSS 4.2.7 *Creation and deletion of system-level objects within or by the application.*

Since the application itself does not create or delete system level objects, this logging ability must be handled at the operating system level by enabling “File Auditing” within the Windows Operating system for the application’s directories:

“<USER PROFILE>\AppData\Local\Temp*.*”

“<USER PROFILE>\AppData\Local\Sage Payment Solutions*.*”

“<PROGRAM FILES>\Sage Payment Solutions*.*”

These directories are base directories and should be configured such that auditing occurs recursively for all sub folders. This auditing MUST be enabled in order to maintain PA-DSS and PCI DSS compliance. The following links provide instruction for enabling file auditing on the supported Microsoft Windows Platforms.

https://technet.microsoft.com/en-us/library/dn319056.aspx

PA-DSS 4.4 *Facilitate centralized logging.*

Sage Exchange Desktop logs are generic text files and do not use any proprietary format. Most centralized logging solutions can support text based log file formats as a source file when aggregating or centralizing logs.

Securely developed payment applications

Merchant applicability

Sage Exchange uses a versioning methodology that contains four nodes in the format in which delineate various types of updates to the application.

PA-DSS 5.4.4 *Implement and communicate application versioning methodology.*

The versioning methodology for Sage Exchange Desktop v2.0 is 2.0.x.n where the components are as follows:

- **First node.** Major version number (2) and would represent a significant application design change and/or major product enhancement.
- **Second node.** Minor version number (0) and would represent a relatively small enhancement to the application, with no or low potential impact to design/functionality related to PA-DSS requirements.
- **Third node.** This is the wildcard patch version number (x). Updated for patch level fixes for minor issues or dependencies. Changes at this level of the version indicate only minor changes and no impact to security design and other PA-DSS related requirements.
- **Fourth node.** This is build version number (n) for internal tracking use having no meaning in a public context for external releases, updates to this node are not impact full to PA-DSS requirements.

Wildcards are used for patches and tracking builds internally. Any PA-DSS or security impactful change will have at least a Minor Version level version update. All updates are automatically downloaded and user prompted for installation. All releases are communicated in advance with release notifications emailed to registered customers and integrators.

Wireless networks

Merchant applicability

If wireless is used or implemented in the payment environment or application, the wireless environment must be configured per if wireless technology is used with the payment application, the wireless vendor default settings must be changed per PA-DSS Requirement 6.1. For any wireless transmission implemented into the payment environment, all vendor default settings must be changed per PA-DSS Requirement 6.1. Additionally, a firewall must be installed and configured per the PCI DSS Requirement 2.1.1. Wireless technology must be securely implemented and transmissions of cardholder data over wireless networks must be secure.

PA-DSS 6.1 *Securely implement wireless technology.*

Sage Exchange Desktop software does not use or rely on any wireless technology.

PA-DSS 6.2 *Secure transmissions of cardholder data over wireless networks.*

Sage Exchange Desktop software does not use or rely on any wireless technology.

PA-DSS 6.3 *Provide instructions for secure use of wireless technology.*

Sage Exchange Desktop does not use or rely on any wireless technology. Any integrated solutions with wireless technology need to provide instructions for PCI DSS-compliant wireless settings, including:

- Instructions to change all wireless default encryption keys, passwords, and SNMP community strings upon installation.
- Instructions to change wireless encryption keys, passwords, and SNMP strings anytime anyone with knowledge of the keys/passwords leaves the company or changes positions.
- Instructions to install a firewall between any wireless networks and systems that store cardholder data, and to 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.
- Instructions to use industry best practices (for example, IEEE 802.11.i) to provide strong encryption for authentication and transmission.

PCI requirements

PCI DSS 1.2.3 *Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the Cardholder Data Environment.*

PCI DSS 2.1.1 *For wireless environments connected to the cardholder data environment or transmitting cardholder data, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.*

- Encryption keys should be changed from default at installation and are changed anytime anyone with knowledge of the keys leaves the company or changes positions.
- SNMP community strings on wireless devices should be changed.
- Passwords/passphrases on access points should be changed.
- Firmware on wireless devices should be updated to support strong encryption for authentication and transmission over wireless networks (for example, WPA/WPA2).
- Other security-related wireless vendor defaults should be removed.

PCI DSS 2.2.3 *Implement additional 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, TLS, or IPSec VPN to protect otherwise insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

Note SSL and early TLS (TLS 1.0 and 1.1) are not considered strong cryptography and cannot be used as a security control after June 30, 2016. Prior to this date, existing implementations that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place.

Effective immediately, new implementations must not use SSL or early TLS.

POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits for SSL and early TLS may continue using these as a security control after June 30, 2016.

Secure networking

Merchant applicability

Sage Exchange Desktop must be implemented in a Secure Networking environment that implements PCI DSS 3.1 compliant encryption protocols, encryption key lengths, and strong cryptographic algorithms. Network components must have properly installed and configured firewalls and appropriate network segmentation to limit the scope of the Cardholder Data Environment. Only necessary and known protocols and ports should be allowed as required to connect between network zones and the public internet. Sage Exchange Desktop relies on establishing TLS 1.2 only secure encryption channels via Microsoft OS and .NET Schannel and is only supported on operating systems and environments that support and allow TLS 1.2.

PA-DSS 8.2 *Use only necessary and secure services, protocols, components, and dependent software and hardware, including those provided by third parties.*

Sage Exchange Desktop requires one of the following versions of Microsoft Windows operating system, with .Net Framework 4.6 required or installed as part of the installation process:

- v 7 SP1
- v8.1

Sage Exchange Desktop requires HTTPS connectivity over port 443 to SageExchange.com webservers. Only HTTPS TLS 1.2 secure cryptographic mechanisms are supported by our host servers and the application code relies on the Microsoft .NET Schannel OS level secure networking implementation of TLS 1.2 encryption channels.

USB connectivity and PINPad device driver components are required for any solution including one of the certified PINPad devices. The driver components required by each PINPad must be installed to support their proprietary protocols. PA-DSS 3.1 certified PTS PINPads supported are:

- Ingenico iPP320
- Equinox L5300

Sage Exchange Desktop relies on the HyperCom Windows service that is installed by the Equinox installation process, this windows service allows communication via USB to the L5300 PINPad Terminal.

Network segmentation

Credit card data cannot be stored on systems directly connected to the Internet as per PA-DSS Requirement 9. For example, web servers and database servers should not be installed

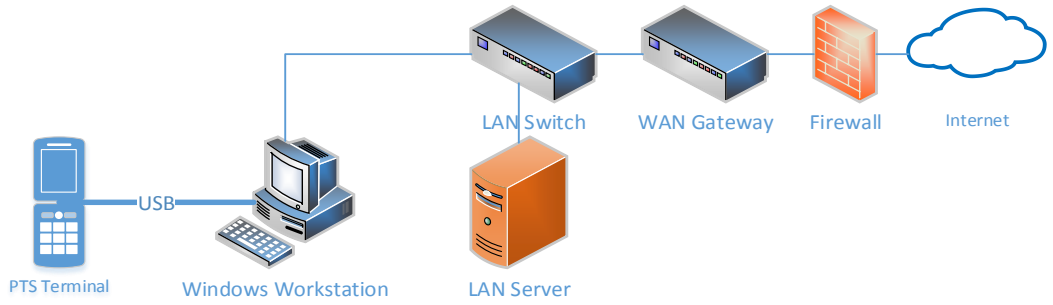
on the same server. A DMZ must be set up to segment the network so that only machines on the DMZ are Internet accessible.

PA-DSS 9.1 *Store cardholder data only on servers not connected to the Internet.*

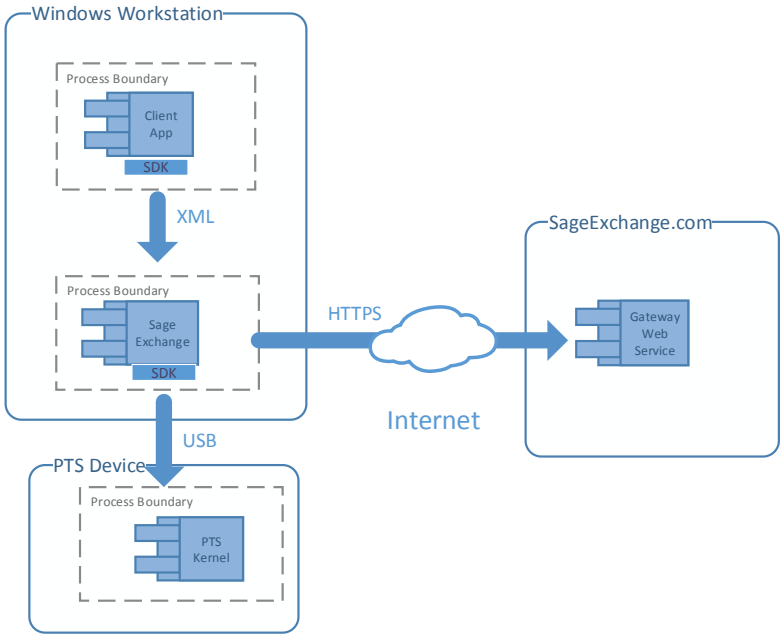
Sage Exchange Desktop does not store cardholder data. Any integrated solution that stores cardholder data must reside in a separate network segment protected by a firewall and not within the DMZ:

- Sage Exchange Desktop does require access to the internet to communicate with the Sage Exchange Gateway to process payment transactions and poll for messages. All communications is TCP/IP port 443 to SageExchange.com domain servers.
- Sage Exchange Desktop does not require access to any servers that store cardholder data, any such servers should not be located in the DMZ and should be protected in the internal network zone.

Physical implementation



Logical implementation



Secure remote software updates

Merchant applicability

Sage Payment Solutions securely delivers remote payment applications by high-speed connections. Merchants should develop an acceptable use policy for critical employee-facing technologies, per the guidelines below.

For high-speed connections, updates are received through a firewall or personal firewall, per PCI DSS 3.1.

Customers are recommended to use a firewall a personal firewall product if computer is connected via VPN or other high-speed connection. In order to enable the operation of the update application, the end- user must only configure their firewall to provide outbound connections on the https standard port 443 and the environment must support TLS 1.2 encryption on both the Windows OS level and LAN network and firewall.

Personal firewall

Any "always-on" connections from a computer to a VPN or other high-speed connection should be secured by using a personal firewall product, per PCI DSS 1.4. The firewall is configured by the organization to meet specific standards and not alterable by the employee.

Remote update procedures

Sage Exchange Desktop is updated via published patches made available on the install web site. The application deploy process checks for new versions and will prompt the user to install, updates can be mandatory or optional. Mandatory updates, when detected, prevent the previous version from running until the updated version is installed. Updates require Admin level privileges on the local workstation and are installed per machine. The update process uses a public key of a public/private key pair to check the integrity and source of the new update files are intact. All update files are signed with the private key certificate by Sage at the time of building the release. The application installer module and main Sage Exchange executable are signed with a GoDaddy.com CA issued code-signing certificate.

There are two ways in which these patches can be applied to existing installations:

- **Automatic update.** The automated update runs every hour starting from the time Sage Exchange is started. In the event a new version becomes available, Sage Exchange Desktop will prompt the user to download the update. The user can either accept and download the update or decline and download the update later. After an update is downloaded the user is prompted to restart Sage Exchange Desktop to apply the update.
- **Manual update.** A manual update check can be started by right clicking the Sage Exchange icon in the taskbar and selecting **Restart application**. In the event a new

version is detected, Sage Exchange Desktop will prompt the user to download the update. The user can either accept and download the update or decline and download the update later. After an update is downloaded the user is prompted to restart the Sage Exchange to apply the update.

The PA-DSS requirement states that if software updates are delivered via remote access into customers' systems, software vendors must tell customers to turn on modem only when needed for downloads from vendor, and to turn off immediately after download completes. Alternatively, if delivered via VPN or other high-speed connection, software vendors must advise customers to properly configure a firewall or personal firewall product to secure "always-on" connections, per PCI DSS.

PA-DSS 10.1 *Implement two-factor authentication for all remote access to payment application that originates from outside the customer environment.*

Sage Exchange Desktop does not allow remote access as part of the payment application.

- Any remote access solution used for customer and technical support must use two-factor authentication in order to meet PCI DSS requirements.
- Description of the two-factor authentication mechanisms supported by the application.
- The customer may initiate a shared session request via a link provided by the customer support representative via email for the Cisco WebEx Support tool. In this case an email with an embedded link requesting a support WebEx session and a password verbally communicated during a live phone call are the two factor authentication mechanisms.

PA-DSS 10.2.1 *Securely deliver remote payment application updates.*

Sage Exchange Desktop does not require a remote access into customers systems for payment application updates. Application updates are securely delivered over HTTPS TLS1.2 downloads from SageExchange.com remote deployment server. The application verifies the manifest files and using public key cryptography verifies an HMAC checksum on file signatures to ensure application integrity. New updates will automatically be downloaded and user prompted to install. Installation will require system administrator level access elevation.

PA-DSS 10.2.3 *Securely implement remote-access software.*

Sage Exchange Desktop does not allow remote access or rely on remote-access software. Any remote access to a payment application must be implemented securely, in the case of Sage Payment Solutions support, the Cisco WebEx remote support tool.

- Uses a strong encryption TLS 1.2 connection over HTTPS port 433 initiated from the web browser of the customer computer.
- Uses a one-time use token embedded in an email URL link and one-time use password.
- Use of the WebEx Remote Support application is restricted to only Sage Payment Solutions trained support personnel.

PA-DSS 11.1 *Secure transmissions of cardholder data over public networks.*

Sage Exchange Desktop securely transmits cardholder data to Sage Payment Solutions SageExchange.com webservers using only PA-DSS 3.1 approved encryption communications protocols like HTTPS TLS 1.2. This level of strong encryption communication is enforced by SageExchange.com network security infrastructure.

- Strong cryptography and security protocols are required and used to transmit card data over public networks. Currently strong cryptography includes TLS 1.2 and excludes TLS 1.1, TLS 1.2 and all SSL versions.
- Microsoft Windows Updates should be applied with all current security updates. Internet Explorer Internet Options, Advanced Tab, Security settings should be checked to only allow “Use TLS 1.2”. The following settings should be unchecked:
    - **Use SSL 2.0**
    - **Use SSL 3.0**
    - **Use TLS 1.0**
    - **Use TLS 1.1**
- Weak RC4 ciphers should be disabled via setting the following Registry Settings. (See Microsoft Security Advisory 2868725:

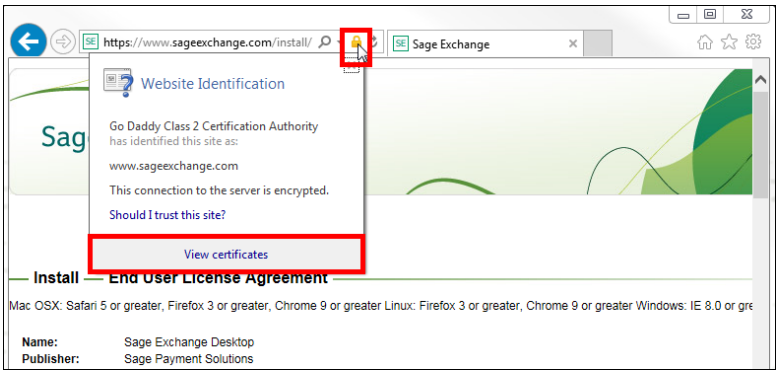
```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders
\SCHANNEL\Ciphers]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders
\SCHANNEL\Ciphers\RC4 128/128]

"Enabled"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders
\SCHANNEL\Ciphers\RC4 40/128]

"Enabled"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders
\SCHANNEL\Ciphers\RC4 56/128]

"Enabled"=dword:00000000
```

Security Advisory 2868725: Recommendation to disable RC4

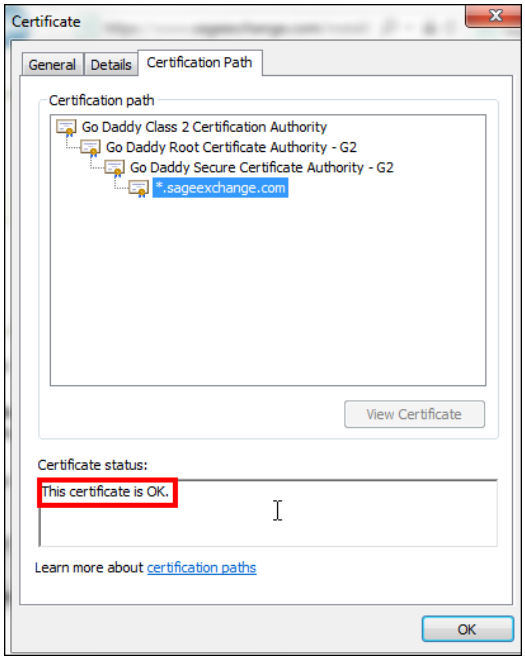
In light of recent research into practical attacks on biases in the RC4 stream cipher, Microsoft is recommending that customers enable TLS1.2 in their services and disable RC4. See http://blogs.technet.com/b/srd/archive/2013/11/12/security-advisory-2868725-recommendation-to-disable-rc4.aspx for additional information. Additionally:

- Follow the steps below to verify that only trusted certificates are accepted and from Sage Payment Solutions and SageExchange.com:
    1. Go to https://www.sageexchange.com/install/.

2. Click on the padlock icon in the browser **Address** bar and then select **View certificates**.

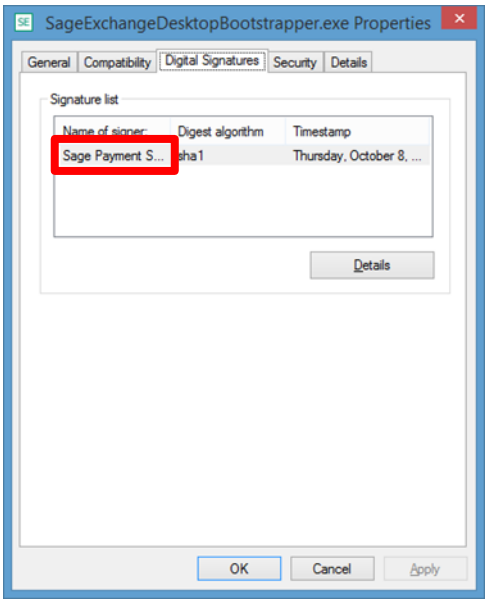


3. Open the **Certification Path** tab then click ***.sageexchange.com**.
4. The **Certificate status** field reads **The certificate is OK**.

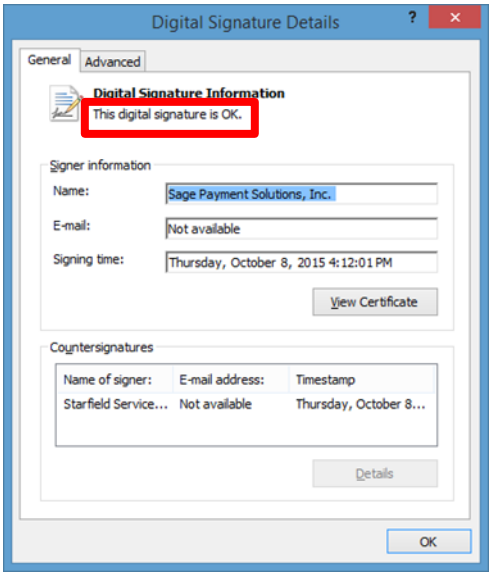


5. Click **OK** to close the **Certificate** window.
    - Sage Exchange Desktop is automatically configured to use only secure TLS 1.2 HTTPS communications with SageExchange.com and Sage Payment Solutions servers.
    - Sage Exchange Desktop is automatically configured to use TLS 1.2 and does not allow fallback to SSL or early TLS versions, TLS 1.0 and TLS 1.1.
    - After downloading the Sage Exchange Desktop installation program and extracting the zipped folder, follow the steps below to verify the digital signature:

6. Right-click **SageExchangeDesktopBootstrapper.exe** and then select **Properties** to open the **SageExchangeDesktopBootstrapper.exe Properties** window.
7. To ensure the source and integrity of the installation program, verify that it is signed by **Sage Payment Solutions, Inc.**

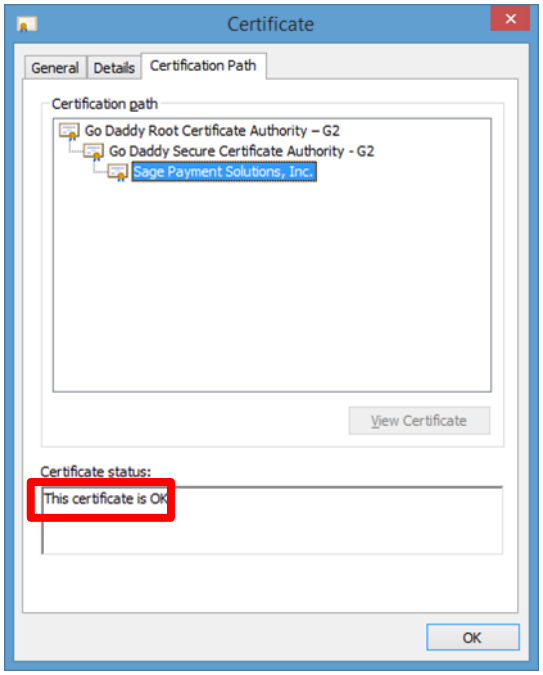


8. Click **Details** to open the **General** tab of the **Digital Signature Details** window.
9. Under **Digital Signature Information**, verify that the status is **OK**.



10. Click **View Certificate**.
11. Click **Sage Payment Solutions, Inc.** in the **Certification path** field.

12. Verify that the **Certificate status** field displays **This certificate is OK**.



13. Click **OK** to close the **Certificate** window.
14. Click **OK** to close the **SageExchangeDesktopBootstrapper.exe Properties** window.

PA-DSS 11.2 *Encrypt cardholder data sent over end-user messaging technologies.*

Sage Exchange Desktop does not use or rely on any end-user messaging technology.

PA-DSS 12.1 *Encrypt non-console administrative access.*

Sage Exchange Desktop does not use or rely on any non-console administrative access or technology.

PA-DSS 12.2 *Encrypt non-console administrative access.*

Sage Exchange Desktop does not use or rely on any non-console administrative access or technology. Any integrated solution or support relying on non-console admin access must include instructions for customers and integrators/resellers to implement strong cryptography, using technologies such as SSH, VPN, or TLS 1.2, for encryption of all non-console administrative access.

Disable Windows System Protection/Restore Points

On Windows v7 and Windows v8 systems, the System Restore Points feature must be disabled. Follow the steps below to disable the feature:

1. Sign on to the Windows computer as an administrator.
2. Click **Start**.

3. Right-click **My Computer** and then select **Properties**.
4. On the **System Protection** tab, click **Configure**.
5. On the **System Restore Settings** window, click **Disable system protection**.
6. Click **Apply** and then click **Yes**.
7. Click **OK**.

See https://support.microsoft.com/en-us/kb/264887 for additional information.