

PA-DSS Implementation Guide for Keystroke POS and Keystroke Payment Module

Applicable Application Version

This document supports the following application version:

6.3

Introduction

Systems which process payment transactions necessarily handle sensitive cardholder account information. The Payment Card Industry (PCI) has developed security standards for handling cardholder information in a published standard called the PCI Data Security Standard (DSS). The security requirements defined in the DSS apply to all members, merchants, and service providers that store, process or transmit cardholder data.

The PCI DSS requirements apply to all system components within the payment application environment which is defined as any network device, host, or application included in, or connected to, a network segment where cardholder data is stored, processed or transmitted.

The following high level 12 Requirements comprise the core of the PCI DSS:

Build and Maintain a Secure Network

1. Install and maintain a firewall configuration to protect data
2. Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

3. Protect Stored Data
4. Encrypt transmission of cardholder data and sensitive information across public networks

Maintain a Vulnerability Management Program

5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications

Implement Strong Access Control Measures

7. Restrict access to data by business need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data

Regularly Monitor and Test Networks

10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes

Maintain an Information Security Policy

12. Maintain a policy that addresses information security

The remainder of this document describes the essential guidance for implementing Keystroke Payment Module in a PCI compliant environment.

PCI DSS Payment Application Environment Requirements

Access Control

The PCI DSS requires that access to all systems in the payment processing environment be protected through use of unique users and complex passwords. Unique user accounts indicate that every account used is associated with an individual user and/or process with no use of generic group accounts used by more than one user or process. Additionally any default accounts provided with operating systems, databases and/or devices should be removed/disabled/renamed, or at least should have PCI DSS compliant complex passwords and should not be used. Examples of default administrator accounts include KEYSTROKE (Keystroke software), "administrator" (Windows systems), "sa" (SQL/MSDE), and "root" (UNIX/Linux).

The PCI standard requires the following password complexity for compliance:

- Passwords must be at least 7 characters
- Passwords must include both numeric and alphabetic characters
- Passwords must be changed at least every 90 days
- New passwords can not be the same as the last 4 passwords

PCI user account requirements beyond uniqueness and password complexity are listed below:

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

These same account and password criteria must also be applied to any applications or databases included in payment processing to be PCI compliant.

In Keystroke, the default user account can be changed by editing the clerk record. Or, after a new administrative clerk has been created, it can be removed in the database manager. Select the Clerk database, then Record and Delete. In Keystroke, the password parameters are set in the Configuration manger under settings and parameters.

Remote Access

The PCI standard requires that if employees, administrators, or vendors are granted remote access to the payment processing environment; access should be authenticated using a two-factor authentication mechanism (username/ password and an additional authentication item such as a token or certificate).

In the case of vendor remote access accounts, in addition to the standard access controls, vendor accounts should only be active while access is required to provide service. Access rights should include only the access rights required for the service rendered, and should be robustly audited.

- KeystrokePOS does not require the use of remote access software.
- If the customer should decide to remotely access the application, the PA-DSS Implementation Guide document includes merchant guidance on using

- security options for common Remote Assistance products and lists all associated requirements for use only in conjunction with two factor authentication scenarios such as VPN with digital certificates for access outside the payment application environment. Remote access is not required or enabled directly by the application or server as indicated in the PA-DSS Implementation Guide.
- Additionally, the vendor-supplied *PA-DSS Implementation Guide* advises customers and resellers/integrators to use all available remote access security features. Examples of security features that may be supported by remote access software are as follows:
 - All users are assigned a unique ID for access to system components or cardholder data. Two-factor authentication was observed to be implemented for remote network access
 - Generic user IDs and accounts were observed to be disabled or removed
 - Shared user IDs for system administration activities and other critical functions were not observed to exist
 - Shared and generic user IDs were not observed to be in use to administer any system components.
 - Vendor ID has password policies/procedures that group and shared passwords are explicitly prohibited.
 - System administrators were interviewed to verify that group and shared passwords are not distributed, even if requested
 - Passwords are changed every 90 days.
 - A minimum password length of at least seven characters are required
 - Passwords containing both numeric and alphabetic characters are required
 - New passwords that are the same as any of the last four are not allowed
 - Repeated access attempts are blocked by locking out the user ID after not more than six attempts
 - The lockout duration is set to a minimum of 30 minutes or until administrator enables the user ID
 - If a session has been idle for more than 15 minutes, the user must re-enter the password to reactivate the terminal
 - Change default settings in the remote access software (for example, change default passwords and use unique passwords for each customer).
 - Allow connections only from specific (known) IP/MAC addresses.
 - Use strong authentication and complex passwords for logins according to PCI DSS Requirements 8.1, 8.3, and 8.5.8–8.5.15
 - Enable encrypted data transmission according to PCI DSS Requirement 4.1:
 - Strong encryption is used during data transmission
 - The server can support the latest patched versions of SSL
 - HTTPS appears as a part of the browser Universal Record Locator
 - No cardholder data is required when HTTPS does not appear in the URL
 - Transactions were observed to encrypt cardholder data during transit.
 - Only trusted SSL/TLS keys/certificates are accepted.
 - Proper encryption strength was verified to be implemented for the encryption methodology in use
 - For wireless networks transmitting cardholder data or connected to the cardholder data environment, guidance on industry best practices (for example, IEEE 802.11i) is provided to implement strong encryption for authentication and transmission.
 - Enable account lockout after a certain number of failed login attempts according to PCI DSS Requirement 8.5.13

- Configure the system so a remote user must establish a Virtual Private Network (“VPN”) connection via a firewall before access is allowed.
- Enable the logging function.
- Restrict access to customer passwords to authorized reseller/integrator personnel.
- Establish customer passwords according to PCI DSS Requirements 8.1, 8.2, 8.4, and 8.5.

Non-Console Administration

Users and hosts within the payment application environment may need to use third-party remote access software such as Remote Desktop Protocol (RDP)/Terminal Server, pcAnywhere, etc. to access other hosts within the payment processing environment. However, to be compliant, every such session must be encrypted with at least 128-bit encryption (in addition to satisfying the requirement for two-factor authentication required for users connecting from outside the payment processing environment). For RDP/Terminal Services this means using the high encryption setting on the server, and for pcAnywhere it means using symmetric or public key options for encryption. Additionally, the PCI user account and password requirements will apply to these access methods as well.

Wireless Access Control

The PCI standard requires the encryption of cardholder data transmitted over wireless connections. The following items identify the PCI standard requirements for wireless connectivity to the payment environment:

- Firewall/port filtering services should be placed between wireless access points and the payment application environment with rules restricting access
- Use of appropriate encryption mechanisms such as VPN, SSL/TLS at 128 bit, WEP at 128 bit, and/or WPA
- If WEP is used the following additional requirements must be met:
 - Another encryption methodology must be used to protect cardholder data
 - If automated WEP key rotation is implemented key change should occur every ten to thirty minutes
 - If automated key change is not used, keys should be manually changed at least quarterly and when key personnel leave the organization
- Vendor supplied defaults (administrator username/password, SSID, and SNMP community values) should be changed
- Access point should restrict access to known authorized devices (using MAC Address filtering)

Transport Encryption

The PCI DSS requires the use of strong cryptography and encryption techniques with at least a 128 bit encryption strength (either at the transport layer with SSL or IPSEC; or at the data layer with algorithms such as RSA or Triple-DES) to safeguard sensitive cardholder data during transmission over public networks (this includes the Internet and Internet accessible DMZ network segments).

Additionally, PCI requires that cardholder information is never sent via email without strong encryption of the data.

Network Segmentation

The PCI DSS requires that firewall services be used (with NAT or PAT) to segment network segments into logical security domains based on the environmental needs for internet access. Traditionally, this corresponds to the creation of at least a DMZ and a trusted network segment where only authorized, business-justified traffic from the DMZ is allowed to connect to the trusted segment. No direct incoming internet traffic to the trusted application environment can be allowed. Additionally, outbound internet access from the trusted segment must be limited to required and justified ports and services.

Information Security Policy/Program

In addition to the preceding security recommendations, a comprehensive approach to assessing and maintaining the security compliance of the payment application environment is necessary to protect the organization and sensitive cardholder data.

The following is a very basic plan every merchant/service provider should adopt in developing and implementing a security policy and program:

- Read the PCI DSS in full and perform a security gap analysis. Identify any gaps between existing practices in your organization and those outlined by the PCI requirements.
- Once the gaps are identified, determine the steps to close the gaps and protect cardholder data. Changes could mean adding new technologies to shore up firewall and perimeter controls, or increasing the logging and archiving procedures associated with transaction data.
- Create an action plan for on-going compliance and assessment.
- Implement, monitor and maintain the plan. Compliance is not a one-time event. Regardless of merchant or service provider level, all entities should complete annual self-assessments using the PCI Self Assessment Questionnaire.
- Call in outside experts as needed. Visa has published a Qualified Security Assessor List of companies that can conduct on-site CISP compliance audits for Level 1 Merchants, and Level 1 and 2 Service Providers. MasterCard has published a Compliant Security Vendor List of SDP-approved scanning vendors as well.

Sensitive Credit Card Data Requires Special Handling

Sensitive Credit Card data handling and storage considerations:

- Only collect sensitive authentication only when needed to solve a specific problem
- Store data only in specific, known locations with limited access
- Collect only the limited amount of data needed to solve a specific problem
- Encrypt sensitive authentication data while stored
- Delete such data immediately after use

SBS Procedure for Handling User Data with Credit Card Information

- Always first attempt to solve any problem over the telephone.
- Do not accept data containing credit card information transferred via the internet.
- Any data received from a user or dealer containing credit card data must be checked-in and logged by an Application Security Manager (currently David Hunsinger or Mike Taber).
- Data will be placed on the Secure Data Workstation (SDW) which is an independent machine dedicated to the task of analyzing customer data. This workstation is not connected to an internal network, an external network or the internet.
- Access to the SDW is controlled by the Application Security Manager. A secure login and password is controlled by the Application Security Manager and follows the PCI guidelines for passwords.
- Data is stored in Keystroke data files and securely encrypted and the PAN is rendered unreadable in accordance with PCI DSS Requirement 3.4. No support or debugging files are created with PAN data.
- Data will be copied to SDW and analyzed. Upon completion data will securely wiped from the SDW.
- The original data will be destroyed or returned.
- SBS will use CardRecon from Ground Labs to scan the SDW before and after each data set is placed onto and removed from the SDW. These scans will ensure a compliant method of encryption is used.

Payment Application Configuration

Baseline System Configuration

Below are the operating systems and dependent application patch levels and configurations supported and tested for continued PCI DSS compliance:

- Microsoft Windows 2003/2000 Service Pack 4, Windows XP Professional with Service Pack 2 or 3. All latest updates and hot-fixes should be tested and applied.
- 256 MB of RAM minimum, 512 MB or higher recommended
- 200 MB of available hard-disk space
- TCP/IP network connectivity.

Data Encryption over Public Networks

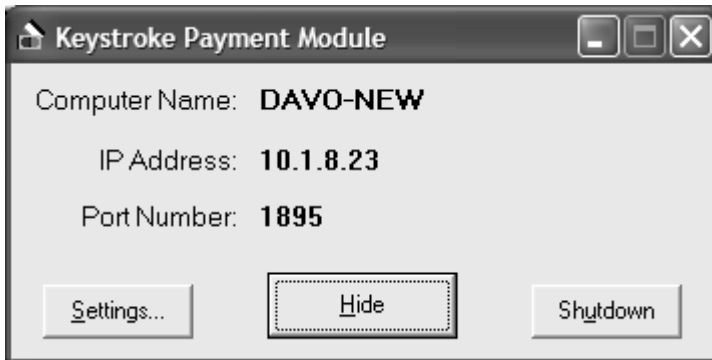
Keystroke POS facilitates the sending and transmission of data over public networks (the internet) via DataCap/Mercury Payment Systems DSI client. This uses secure encryption transmission technology and is PA-DSS validated.

Keystroke POS does not allow or facilitate the sending of cardholder data or PANs by end-user messaging technologies. If a Keystroke user needs to send this information via messaging they must use an encrypted solution.

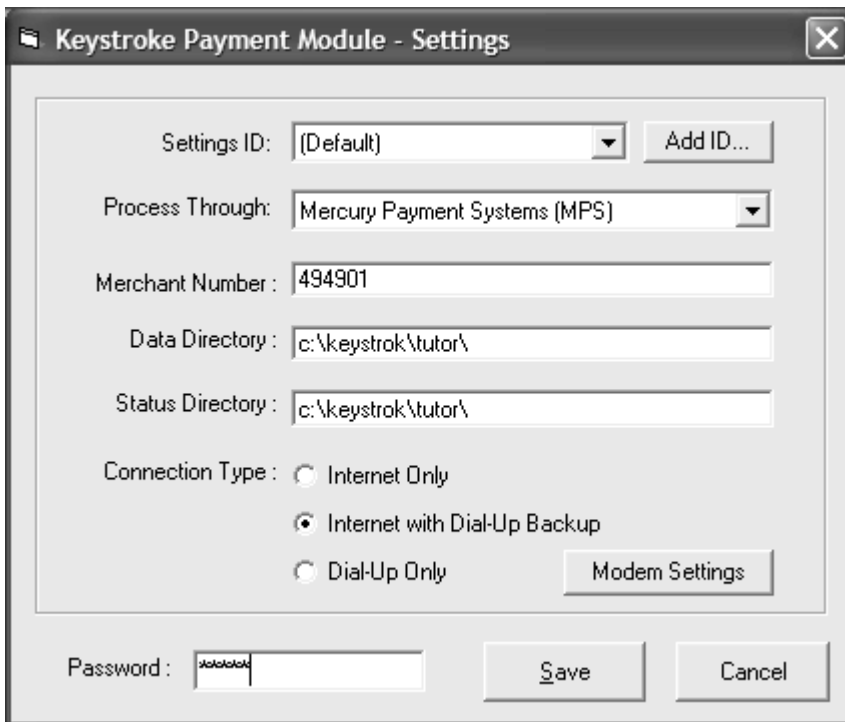
Application Configuration

The Keystroke Payment Module (KeyPay) can be installed either as a conventional Windows program (KeyPay.exe) or as a Windows Service (KPsvc.exe). SBS recommends the Service method for most users. Whichever method is used, the KeyPay module should be installed on a single computer only to handle payment requests for all workstations.

It is important to select a computer physically located in a secure location with access limited to authorized personnel only. This computer, the primary file server, and all POS workstations should also be protected by a secure firewall. Whether the computer hosting KeyPay is a file server itself or an office workstation, it must always be started before other POS workstations in order to ensure payments can be reliably processed.



Click setting to enter unique user information (settings will automatically run upon initial installation).



Enter the Merchant Number and typically use the default Data and Status Directories. Keystroke Payment Module will use your Internet connection to process payments. You can select Dial-Up Backup or Dial-Up Only if you have a Windows modem installed on the computer running Keystroke Payment Module.

Multiple merchant settings can be created by selecting the Add ID button. This allows the Keystroke Payment Module to process transactions for more than one merchant ID or multiple locations running on a wide area network. If using ID's, you must specify the correct ID in the Authorization Method selected in the Keystroke POS program.

Data Logs

In Keystroke all payment activity is logged by audit entries. The settings are in the Configuration manger under Settings – Parameters – Audit. The "Payment Processing" log is always turned on. In additional, the Keystroke Payment Module also generates logs that are stored in the LOGS directory below the Keystroke data directory.

Data Storage

Magnetic strip data has never been stored by SBS/Keystroke Products. Key pay stores cardholder data for 72 hours in encrypted format using secure, random encryption keys. The data is automatically purged after 72 hours. Recurring payment data is also stored by Key pay using the same secure, random encryption keys. It can be removed by deleting the payments off of the recurring transactions.

Historical Data Storage

Magnetic strip data has never been stored by SBS/Keystroke Products. It is absolutely necessary to remove historical payment data to comply with PA-DSS. To purge all historical data:

1. Goto the Keystroke Sales Manger and select Special and Closeout from the top menu bar.
2. Enter any date range or just select OK (date range does not effect data purge).
3. Select Closeout and Parameters from the top menu bar.
4. In the Purge Payments section, set "On Save" to Automatic, Minimum Interval to 0 days and Payments Over to 0 days. Select OK to save.
5. Select Closeout and Purge Payments from the top menu bar. Select Yes on the Run Purge Payments.

This process must be run on all historical data sets you have on your network. There are no legacy cryptographic key materials to remove.

Data sets that are loaded using the v6.30 (or later) of Keystroke POS, will have this data purged automatically as part of the update process.

Remote Access

Remote network access is not required or enabled by the Keystroke POS application or server. If a Keystroke POS user employees outside software for remote access, be sure to follow the following PCI/PA-DSS guidelines

1. Change all default settings in the remote access software.
2. Allow connections from only specific IP/MAC addresses.
3. Use strong authentication and complex passwords for logins as stated earlier in this document and according to PCI-DSS requirements 8.1, 8.2, 8.3, 8.4 and 8.5.
4. Enable encrypted data transmission according to PCI-DSS requirement 4.1.
5. Enable account lockout after a certain number of failed login attempts according to PCI-DSS requirement 8.5.13.
6. Configure the system so a remote user must establish a Virtual Private Network (VPN) connection via a firewall before access is allowed.
7. Enable the logging function.
8. Restrict access to passwords to authorized reseller/integrator/owner personnel.

Vulnerability Testing and Patch/Update Deployments

Timely Development and Deployment of Security Patches

SBS is committed to timely development and deployment of security patches. When a vulnerability is detected, we will develop and deploy a patch and/or update within 30 days of discovery. These patches will be delivered using a known chain of trust. A technical notice will be sent out via email and the patch will be made available on our web site. The patch can then be downloaded directly or automatically using the provided Update.exe program. The patch files are digitally signed to verify their authenticity.

About This Guide

This Guide will be disseminated to all SBS customers and resellers. It covers all PA-DSS requirements and identifies any that are not applicable to SBS Software. This document is reviewed on an annual basis and updated as need for all major and minor changes to the payment application. It is also reviewed and updated on an annual basis for any software changes made because of changes in PA-DSS requirements.

More Information

A copy of the Payment Card Industry (PCI) Data Security Standard from VISA's security website is available at the following Internet address:

https://www.pcisecuritystandards.org/tech/download_the_pci_dss.htm

Additional information for merchants from VISA is available at the following Internet address:

http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_merchants.html?it=il|/business/accepting_visa/ops_risk_management/cisp.html|Merchants

A listing of qualified security assessors from VISA is available at the following Internet address:

http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_assessors.html?it=I2|/business/accepting_visa/ops_risk_management/cisp_merchants%2Ehtml|Assessors