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

Applicable Application Version

This document supports the following application version:

8.0x.xx

1.0 Introduction

Systems which process payment transactions necessarily handle credit card sensitive authentication data. 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 and Systems

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 credit card sensitive authentication data 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.

2.0 PCI DSS Payment Application Environment Requirements

2.1 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 must be removed/disabled/renamed, or at least have PCI DSS compliant complex passwords. Examples of default administrator accounts that are not part of the Keystroke software but may exist on your system or network include "administrator" (Windows systems), "sa" (SQL/MSDE), and "root" (UNIX/Linux). Control access, via unique user ID and PCI DSS compliant secure authentication, to any PCs, servers, and databases with payment applications and cardholder data.

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

- If an incorrect password is provided 6 times the account must be locked out
- Account lock out duration is at least 30 min. (or until an administrator resets it)
- Sessions idle for more than 15 minutes 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.

Keystroke enforces strong authentication by the completion of the installation and for any subsequent changes. To maintain PCI DSS compliance, any changes made to authentication configurations must be verified as providing authentication methods that are at least as rigorous as PCI DSS requirements. Assign secure authentication to any default accounts (even if they won't be used), and then disable or do not use the accounts. All authentication credentials used by the payment application are generated and managed by the application.

In Keystroke, when entering the program for the first time, the user is prompted to create a strong password for the Keystroke Clerk #1. Access to administrative functions is based on security levels. The levels range for zero (0) to ten (10) with zero having complete access and ten having very limited access. For PCI DSS, security levels 0-5 have access to administrative functions and require strong passwords.

To create unique users (or clerks), go to the Keystroke POS Database Manager and select Clerk and Add. The security level for a new user is 10 and would have to be changed to allow greater access. Each user record is assigned a unique Clerk Number. An initial, unique password is entered then is changed by the user.

Biometric identifiers may also be used in addition to passwords. Installed biometric devices must meet PCI DSS requirements for strong authentication. In the Configuration Manager of Keystroke go to Hardware and Biometrics Reader. Set the Reader Type to Generic OPOS, then the Port setting will be displayed. Under the Port setting, select the OPOS device listed (i.e. DPFingerprintReader). Typically both the "Use as Clerk Number" and "Use as Password" will be turned on. The program will look up the clerk based on the biometric scan and the clerk will not be asked for a password. This allows the clerk to only provide a fingerprint scan to log in.

Keystroke Security Level "0" (zero) is for store owners and has the most access. We recommend a clerk with security level 0 to be used for administrative and setup functions only. Day to day managers should have a security level from 1 to 5 (with 1 having more access). Workers entering sales and new employees should have a security level from 6-10. Administrators can run the Security Levels report from the Keystroke Report Manager by selecting Tables then Security Levels. This will show functions available to clerks at each security level (e.g. a clerk with Security Level 2 has access to any function marked as 2 or higher).

In Keystroke, the Clerk #1 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.

2.2 Remote Access

The PCI DSS requires that if employees, administrators, or vendors are granted remote access to the payment processing environment; access originating from outside the customer's network must be authenticated using a two-factor authentication mechanism (username/password and an additional authentication item such as a token or certificate). All remote access must originate from within the customer's environment and the customer must install the client, initiate communication, and provide a password or key.

Two-factor authentication is an approach to authentication which requires the presentation of two or more of the three authentication factors: a knowledge factor ("something only the user knows"), a possession factor ("something only the user has"), and an inherence factor ("something only the user is"). After presentation, each factor must be validated by the other party for authentication to occur.

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

- Keystroke POS does not require the use of remote access software.
- No configuration options are necessary in Keystroke or Keypay to do two-factor authentication.

- Additionally, customers and resellers/integrators must use 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 TLS
    - 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 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.

2.3 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, 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.

Always implement strong cryptography, using technologies such as SSH, VPN, or TLS, for encryption of all non-console administrative access.

2.4 Wireless Access Control

Keystroke and Keypay does not require or support the use of wireless networks. SBS does not recommend the use of wireless networks, but if you do, follow the following guidelines.

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

- Change all wireless default encryption keys, passwords, and SNMP community strings upon installation.
- Change all wireless default encryption keys, passwords, and SNMP community strings anytime anyone with knowledge of the keys/passwords leaves the company or changes positions.
- Install a firewall between any wireless networks and systems that store cardholder data and configure firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.
- Use strong encryption, such as WPA2 or IEEE 802.11.i, to protect authentication and transmission.
- Vendor supplied defaults (administrator username/password, SSID, and SNMP community values) must be changed
- Access point must restrict access to known authorized devices (using MAC Address filtering)

2.5 Transport Encryption

The PCI DSS requires the use of strong cryptography and encryption techniques to safeguard credit card sensitive authentication 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.

Keystroke POS facilitates the sending and transmission of data over public networks (the internet) via DataCap/Mercury Payment Systems DSIClient, HTTPS and PCCharge. These use secure encryption transmission technology and are PA-DSS validated.

Keystroke POS uses protocol TLS 1.2, ciphers Triple DES, AES 128 or AES 256 and hashes SHA, SHA 256, SHA385 or SHA 512. When KeyPay is installed non-secure protocols, ciphers and hashes are disabled. The installation program automatically disables the protocols below TLS 1.1 (TLS 1.0, SSL and PCT), ciphers with less than 128 bits and RC4, and hashes using MD5. This could cause non-secure websites to not function (these websites are never used by Keystroke or KeyPay and should not be visited in a secure payment processing environment). There is no configuration necessary to ensure the use of secure versions, secure protocols, proper encryption strength and proper encryption methodology.

Keystroke POS and KeyPay requires Microsoft .NET Framework 4.5.2 or later.

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. Keystroke automatically uses and verifies that only trusted keys and certificates are accepted.

2.6 Storage Encryption

Encryption keys are never distributed and no user interaction is required. Keystroke uses AES 256 encryption and the amount of data encrypted is small. Keys are changed at least annually. Because of strong encryption the cryptoperiod is well beyond a year. Actually the defined cryptoperiod for the encryption used in the application is over three years, but that data encryption keys are automatically changed for each transaction.

Every year you must update your key-encrypting key in KeyPay. Do this by going into the KeyPay settings and selecting the "Change Cryptographic Keys" button. Also use this procedure to retire or replace keys if the integrity has been weakened or there is a known or suspected compromise of the key. "Change Cryptographic Keys" renders keys and any previously used cryptographic material irretrievable. Not only does this destroy keys that are no longer used in accordance with key management requirements of PCI DSS, it re-encrypts data with new keys and maintains security of and clear-text data during the decryption/re-encryption process.

All cardholder data is strongly encrypted and there are no settings to change that. Key-encrypting keys are at least as strong as the data encrypting keys they protect. Keys are managed and stored automatically by the application; therefore there are no key custodians. No action is required by the customer. There are no steps required to restrict access to the keys, it is configured automatically by the application. Keys are securely stored in the fewest possible locations. Security restrictions are placed on storage files to protect them. These safeguards are in place as long as the data is being stored on Windows NTFS hard drives.

2.7 Dependencies

KeyPay is dependent on the KeyPay server (KEYSTROE.EXE) or the KeyPay Service (KPSVC.EXE). It is also dependent on the following protocols, services, components, software and/or hardware.

- TLS 1.2
- HTTPS – Secure Communications Protocol.
- Datacap Systems, Inc., NETePay 5, 5.06.XX
- Verifone Inc, PC Charge, 5.10.0
- NET Framework 4.5.2 or later from Microsoft.
  Including the System.Net.ServicePoint objects.
- PA-DSS validated with Windows 7 and Windows 8
- Supports Windows 10, Windows Server 2008 or Windows Server 2012 or newer from Microsoft with all available updates and hotfixes.
- Cayan LLC, Genius, 5.0.*.*
- Ingenico, iPP310, iPP320, iPP350 Ingenico, iSC250
- Ingenico, iSC350
- ID Tech, Sign&Pay IDFA-3123 and IDFA-3153
- MagTek Inc, IPAD 100/ IPAD 100SC/ IPAD 100KB
- Verifone Inc, PP1000SE

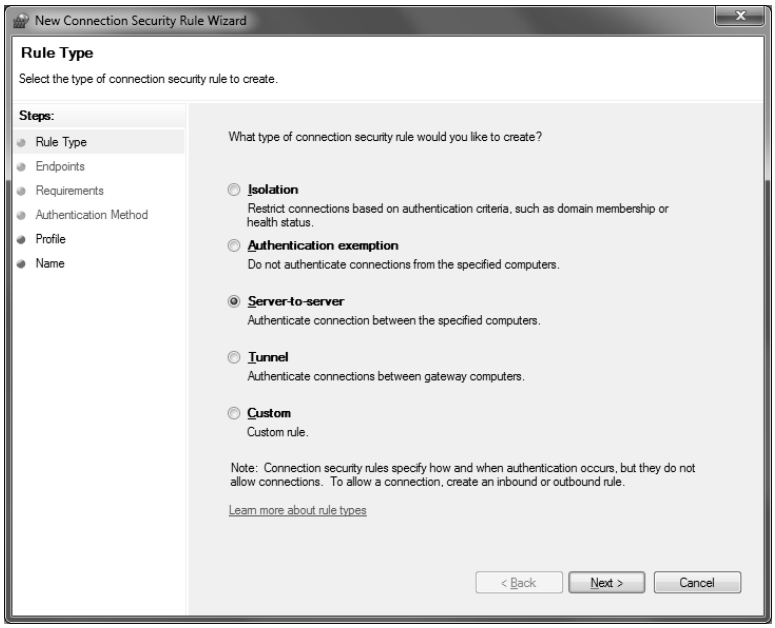
2.7.1 Windows File Sharing

If Windows file sharing is used in conjunction with Keystroke, PCI DSS Requirement 2.2.2 requires the connection be secure. When using Windows sharing follow these few simple steps to ensure secure and encrypted data transmission; and reduce the threat of an outside network attack.

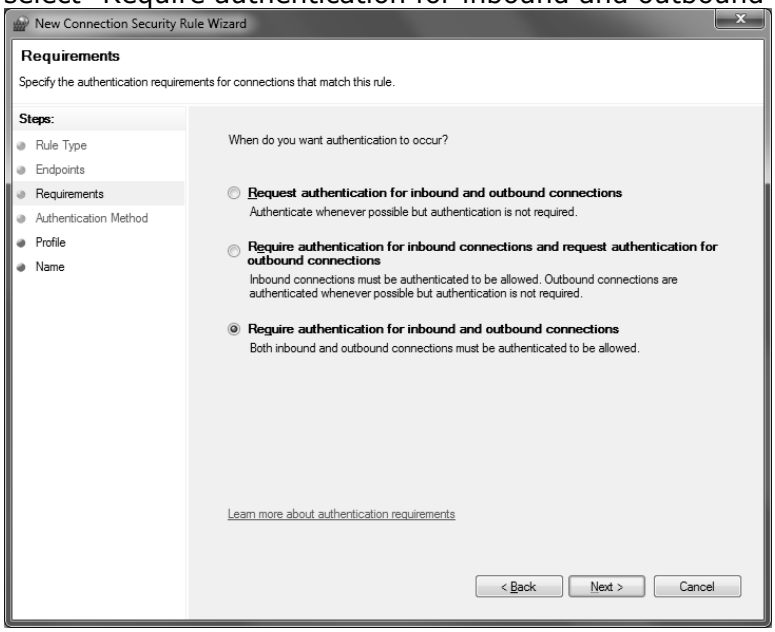
- On the server, in Windows Control Panel\Network and Internet\Network and Sharing Center\Advanced sharing settings be sure "File sharing connections" is set to "Use 128-bit encryption…" and "Password protected sharing" is set to "turn on…"

  Unique user should be setup on the server for each workstation with strong passwords.

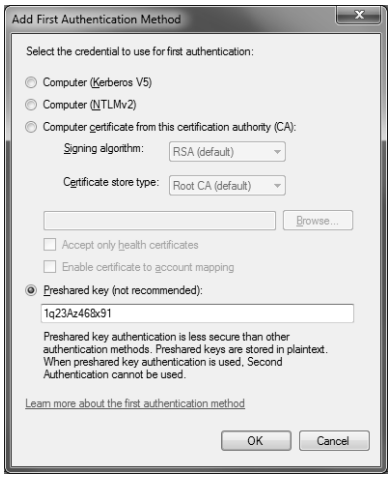
- On the server and all workstations, in Windows Control Panel\System and Security\Windows Firewall select Advanced Settings. Under Windows Firewall with Advanced Settings, click on Connection Security Rules, then right-click Connection security Rules and select New Rule. For Rule Type select "Server-to-server".



For Endpoints leave both settings at "Any IP address". For Requirements select "Require authentication for inbound and outbound connections".



- For Authentication Method select "Advanced" and click the Customize button. Under "First authentication" click the Add button and select "Preshared key". Enter an encryption key for the business and select OK.



  For Profile leave Domain, Private and Public all selected. For name enter an appropriate title like "Secure File Sharing".

2.8 Network Segmentation

Keystroke and Keypay must not be installed on a public facing system with internet access. It must be on a secure internal network and not in a DMZ. 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. 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.

All internet communications are initiated by outbound requests using the HTTPS protocol on port TCP/443.

2.9 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 authentication data.

The following is a very basic plan for every merchant/service provider to 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 include 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 need to complete an annual self-assessment 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.
- No cardholder data encryption keys are accessible in Keystroke. They are randomly generated and rotated in Keystroke. PCI DSS Requirement 3.5 and PA-DSS Requirements in 2.4 and 2.5 do not apply.

2.10 Credit Card Sensitive Authentication Data Requires Special Handling

SBS policy is to never collect or store sensitive authentication data for troubleshooting or any reason. SBS also never collects cardholder PAN for troubleshooting or any reason.

2.11 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 with PAN or credit card sensitive authentication data.
- Any data received from a user or dealer containing credit card sensitive authentication 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.

2.12 SBS Procedure for End User Remote Access

- Always first attempt to solve any problem over the telephone.
- Use JoinMe.com to create a one-time use, user generated passphrase to log in.
- Only remain connected long enough to solve the problem.
- Never view or record SAD or PAN data.

2.13 Prevention of Inadvertent Data Storage

Secure electronic payment card processing requires the prevention of inadvertent data storage.

- Turn off Windows System Restore on all machines running KeyPay where encrypted PAN data is stored. Settings for System Restore can be accessed from the Windows Control Panel under System then System protection.

- Exclude the KeyPay data files, KP.TMP and KPREC.DAT from all backups.

3.0 Payment Application Configuration

3.1 Baseline System Configuration

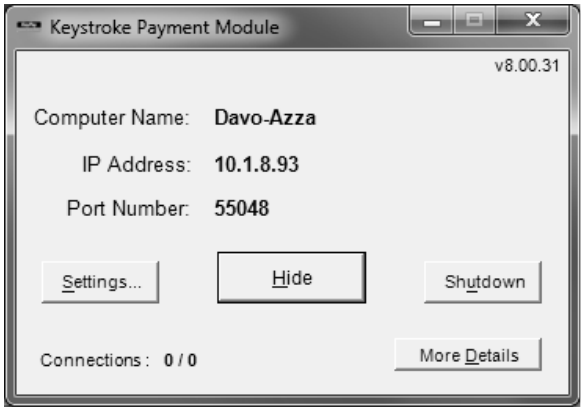
Below are the operating systems and dependent application patch levels and configurations supported and tested for continued PCI DSS compliance:

- Microsoft Windows 2008/2012 Server, Windows 7 Service Pack 1 or higher. All latest updates and hot-fixes must 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.

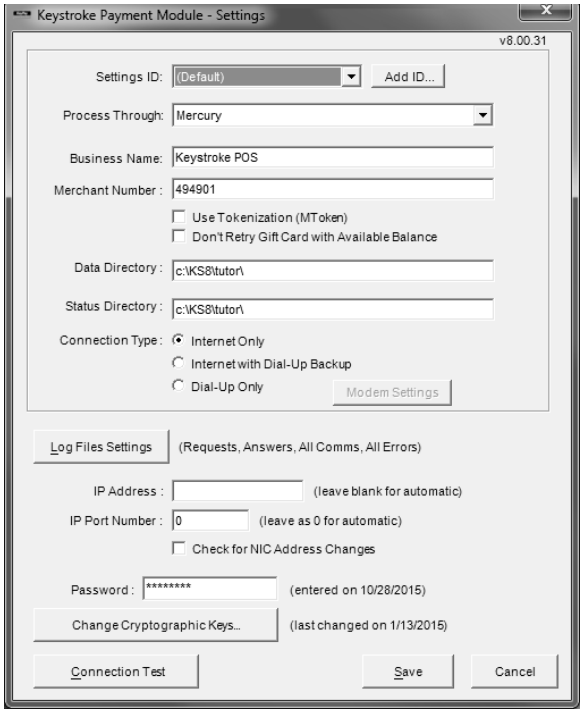
3.2 Application Configuration

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 is installed on a single computer only to handle payment requests for all workstations. If using KeyPay.exe, it should be added to the Windows Startup folder (or an automated Batch program) on a single designated computer only.

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 need to 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.



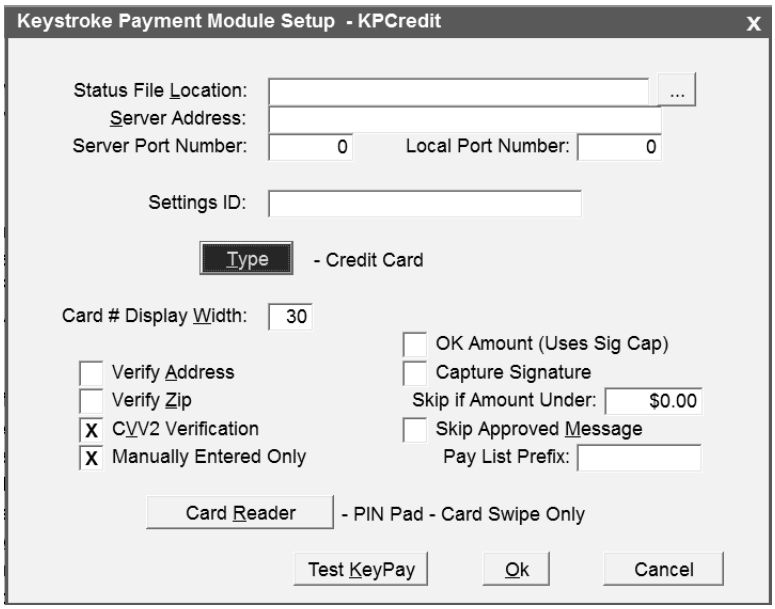
Click setting to enter unique user information (settings will automatically run upon initial installation).



Enter the Business Name and Merchant Number. Use Tokenization is turned on for End-to-End (E2E) encrypted devices, which are highly recommended by SBS. The default Data and Status Directories are typically used. 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.

In Keystroke, go to the Configuration Manager and select Tables then Sales Payment Types. Select the Visa/MC/Disc payment type. New payment types may be created if you want to separate card types for reporting. Click on the Auth Method button and select the KPCredit authorization method. While on the list press F3 to edit the method. Default settings should be appropriate, but review the choices to make sure they are functioning as desired.



Hit F10 twice to save the settings. Select American Express and set up in a similar fashion. Debit, Food Stamps, and EBT can also be set up using the authorization methods KPDebit, KPFood and KPEBT respectively.

3.3 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 mandatory and always turned on. In additional, the Keystroke Payment Module also generates centralized logs that are stored in the LOGS directory below the Keystroke data directory in tab delimited text. These logs are always active, cannot be disabled and no user intervention is required. For PCI DSS compliance merchants must maintain centralized logs. The log files created can be imported or combined with other information for a centralized logging environment.

Log Field Descriptions

- Date
- Time
- AuthType – StartUp, Shutdown, Sale, Return, AddRecord, DeleteRecord
- Name – Machine name making the request to KeyPay
- Address – IP Address of the machine making the request to KeyPay
- Port – Port used for the request
- Mach# - Machine number of the machine making the request to KeyPay
- Clerk# - Clerk in Keystroke making the request
- CalledBy – Type of Keystroke Software making the request – Keystroke Advanced POS, Keystroke POS, Keystroke Express POS
- Version – Keystroke version and build
- Total – Dollar amount of the request
- EntryType – Success or Failure for the request

If using PCCharge software, refer to their Implementation Guide for logging instructions.

Any logs (e.g. network, system, PCCharge or Keystroke) should not be disabled and doing so will result in non-compliance with PCI DSS.

3.4 Data Storage

Magnetic strip data and sensitive authentication data is not now and has never been stored by SBS/Keystroke Products. Keypay stores cardholder data for 72 hours in encrypted format using secure, random encryption keys. The data is automatically securely deleted after 72 hours.

Cardholder data must be securely deleted when no longer required for legal, regulatory or business purposes. All business must define a cardholder data retention period and must securely delete all data exceeding that retention period.

No instructions are necessary to securely delete cardholder data because it is automatically deleted after 72 hours. Tokenized cardholder data is stored in the files KP.TMP and KPREC.DAT in the KeyPay data directory. The KeyPay data directory location is specified in the KeyPay setting "Data Directory". No cardholder data is stored in underlying software or systems.

Recurring payment data is also stored by Keypay using the same secure, random encryption keys. It can be removed by deleting the payments off of the recurring transactions.

Keystroke does not ever display the full PAN, but only displays the last four digits. By default the PAN is masked on all POS devices, screens, logs, receipts and reports. To access the PAN please contact your merchant service provider. The Keystroke Export and Report functions never output PAN or any cardholder data. Data is output with the last four digits of the PAN.

The files KeyPay.xml and KeyPay.krf hold settings and information required to initialize the encryption for access to the data files. These files are hidden but should be included in your standard backup routine. KeyPay.krf is located in the KeyPay application directory and KeyPay.xml is located in the ProgamData\KeystrokePOS directory off the root drive where KeyPay in installed.

3.5 Historical Data Storage

Magnetic strip, PIN and security code data (i.e., Sensitive Authentication Data) is not now and has never been stored by SBS/Keystroke Products. In version prior to 6.3 or October 2009 PAN data was stored. It is absolutely necessary to remove this historical payment data if present to comply with PCI 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 affect 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 including all backups. 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.

3.6 Display of Primary Account Number (PAN)

The Primary Account Number (PAN) is always tokenized and masked (last four digits are displayed) in Keystroke and there is no way to display an unmasked PAN on computer screens, payment card receipts, faxes, or paper reports. There are no instances where the PAN or and secure cardholder data in output.

The displayed PAN is masked when entered manually, but can be unmasked if the clerk needs to view the PAN as it is entered. To achieve this, go to the Keystroke Configuration Manager and select Tables then Sales Payment Types. Choose the appropriate payment type, then select Security Levels. Change "Display Ref. Characters (Add)" to the appropriate security level (probably 10) and save.

4.0 Vulnerability Testing and Patch/Update Deployments

4.1 Timely Development and Deployment of Security Patches

SBS is committed to timely development and deployment of security patches. When 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.

4.2 Versioning Methodology

Every release of a product is identified by series of numbers that signify the difference between it and prior releases. This series of numbers is referred to as the Version and Build number where the Version is a combination of a Whole Number followed by a decimal point followed by a 2 digit number (e.g. "8.01") and the Build number is listed either as another 2 digit number following a decimal point (e.g. "8.01.20") or using the word "Build" to separate it from the Version number (e.g. "8.01 Build 20"). The Version Number may also be listed the small letter "v" in front of it to help identify the number as the Version Number (e.g. "v8.01.20").

When a higher number portion of the Version Number is changed, all other numbers reset to 0 (except the Build number which starts at 20). For example if the current release is "7.15.60" and the next release will change the whole number to 8, then the new release will be "8.00.20".

Major Releases:

- Normally 3-5 years apart (but could be sooner if required).
- Is the whole number numeric digit in front of the decimal point and the tenths digit.
- Major changes to data file structure and/or database engine, or the User Interface will require a change to the Whole Number portion of the Version Number.
- Any changes affecting PA-DSS require a change to the tenths digit of the Major Release number. These changes include anything that would affect the PA-DSS requirements including:
    - security system used to restrict and/or track users access to the program and/or data (including authentication of users)
    - encryption/hashing routines/methods
    - handling a payment information in RAM
    - storage of any payment related data
    - communications (especially those involving payment data)
    - interfaces from outside sources
- Large changes to the functionality of the program that would require additional training for most users will cause the tenths digit of the Major Release number to change.
- Changes to the data structure that would require any other programs that are using exported data to require being checked/updated will require the tenths digit of the version number to be changed.

Maintenance Releases:

- 6 months to 3 years apart.
- Is the 100s digit of the numeric number after the first decimal point and Build number.
- Changes affecting PA-DSS are NOT to be made in a Maintenance Release.
- Released as needed by market and customer demand for new features
- Small data file changes may be included (data files are not necessarily compatible between Minor releases).

When referring to compatibility and changes between versions, wild cards (the letter "x") can be used. For example, "v8.0x.xx" refers to all release of the program where the version number starts with "8.0" is applicable to all version and build numbers that were released with it. Note that PCI requirements do not allow wild cards to be used for any part of the Major Version number (e.g. "8.x" is not acceptable).

Wildcards are never used for changes impacting security or PCI DSS or PA-DSS requirements. Any parts of the version number representing a non-security impacting change are never used to represent a security impacting change. Also, wildcards and any elements right of a wildcard are not used to represent a security impacting change. All security impacting changes require a version number changes to the left of a wildcard.

Version and Build Numbers used internally (whether for development or testing) are the same as the numbers that are used for release. However, it is possible that a Version and Build numbers combination may be used internally but never released publicly if additional changes are made requiring the program to be assigned a new Version and/or Build number.

4.3 Keystroke POS Back-out/De-installation Procedures

To revert Keystroke to an earlier or previous version simply install the earlier or previous version on top on the unwanted updated version. No uninstall is necessary. This procedure is good as long as you are installing the same major version (e.g. 8.00.40 to 8.00.20 not 8.00.40 to 7.15.60). If you have to go back to a previous major version you need to remove the Keystroke program directory, do a fresh install on the desired version, and restore a backup of the Keystroke data.

About This Guide

This Guide will be disseminated to all Specialized Business Solutions customers and resellers. It covers all PA-DSS requirements and identifies any that are not applicable to SBS Software. This document is reviewed and updated at least annually. It is also reviewed and updated as needed for all major and minor changes to the payment application or it dependencies. It is also reviewed and updated for any software changes to PA-DSS requirements.

The PS-DSS Implementation Guide is installed with every copy of Keystroke and is available at www.KeystrokePOS.com. When Keystroke POS is installed or updated, the user, reseller and/or integrator is prompted to open the PA-DSS Implementation Guide. The document can also be emailed or mailed to any appropriate party upon request.

More Information

A copy of the Payment Card Industry (PCI) Data Security Standard is available at the following Internet address:

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

Revision History

Below are the dates of Implementation guide review and changes.

10/1/2014 – Initial release of PA-DSS 3.0 Implementation Guide.
12/5/2014 – Implementation Guide updated for programming changes.
4/23/2015 – Implementation Guide updated for PA-DSS 3.0 requirements.
5/15/2015 – Implementation Guide updated for PA-DSS 3.0 requirements and release of Keystroke v8.0.
6/24/2015 – Implementation Guide updated for PA-DSS 3.1 requirements.
9/18/2015 – Implementation Guide updated for errors and revision history.
4/14/2016 – Implementation Guide updated for errors and revision history.
5/02/2016 – Implementation Guide updated for errors, clarifications and revisions.
5/16/2016 – Implementation Guide updated for dependencies.
5/31/2016 - Implementation Guide updated for versioning methodology.
6/1/2016 - Implementation Guide updated for versioning methodology.