AutoClerk Inc.'s

Payment Card Industry (PCI)

Payment Application Data Security Standard (PA-DSS 3.2)

Implementation Guide

For AutoClerk Version 9

November 2019

Table of Contents

Copyright Information

AutoClerk, Inc.

Address: 1981 North Broadway, Suite 430, Walnut Creek, CA 94596

Phone: 925.284.1005

Fax: 925.284.3423

URL: www.autoclerk.com

Version	Date	Reviewed by	Changes made
3.0	8/22/16	Holly McGlothlin	First pass at document for PA-DSS ver. 3.2
3.1	9/16/2016	David Ferris, Holly McGlothlin	Updated for grammar and clarification.
3.2	9/20/2016	David Ferris	Updated after review.
3.3	12/8/2016	Holly McGlothlin	Corrections to match PCI Council changes
4.0	11/18/2019	Holly McGlothlin	Update for accuracy

Introduction

AutoClerk, Inc. is a software application developer and vendor. As a vendor that integrates and implements credit card processing for deposits, authorizations and payments, we are required to comply with the *Payment Card Industry's (PCI) Payment Application Data Security Standard (PA-DSS)*.

As a business entity that processes credit cards, in terms of both getting authorizations as well as processing sales, you are required to be compliant with *the Payment Card Industry Data Security Standard (PCI DSS)*. There are several levels of PCI DSS compliance. One criterion is the number of credit card transactions processed in a year. You need to review the compliance documentation at http://www.pcisecuritystandards.org and take the necessary steps to obtain and maintain your appropriate PCI DSS compliant status.

AutoClerk, Inc.'s PA-DSS compliance serves to support your PCI DSS compliance. Our being PA-DSS compliant does *not* make you PCI DSS compliant.

The PCI DSS consists of 12 Requirements, which cover the handling, processing and storage of credit card data. The following table lists the requirements.

Objective	**12 PCI-DSS Compliant Requirements**
Build and Maintain a Secure Network and Systems	Requirement 1: Install and maintain a firewall configuration to protect cardholder data Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	Requirement 3: Protect stored cardholder data Requirement 4: Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	Requirement 5: Use and regularly update anti-virus software or programs Requirement 6: Develop and maintain secure systems and applications
Implement Strong Access Control Measures	Requirement 7: Restrict access to cardholder data by business need to know Requirement 8: Identify and authenticate access to system components Requirement 9: Restrict physical access to cardholder data

Regularly Monitor and Test Networks	Requirement 10: Track and monitor all access to network resources and cardholder data Requirement 11: Regularly test security systems and processes
Maintain an Information Security Policy	Requirement 12: Maintain a policy that addresses information security for employees and contractors.

This PA-DSS Implementation Guide explains AutoClerk's role in the security of your guests' credit card data. It instructs you and your network administrator how to enable security settings in regards to both your network and hardware. It instructs you on secure AutoClerk product implementation; and defines some of your responsibilities for meeting PCI DSS requirements.

Following these guidelines does *not* make you PCI DSS compliant, nor does it guarantee your network's security. It is your responsibility, along with your network administrator, to ensure that your hardware and network systems are secure from internal as well as external intrusions.

AutoClerk makes neither claim on the security of your network, nor on the level of your PCI DSS compliance.

AutoClerk Version 9 can only be updated from AutoClerk Version 8, which does not allow the storing of legacy data even from previous versions of AutoClerk. (PA-DSS 1.1.4)

Anytime AutoClerk was installed at your property, you were required to follow AutoClerk's System Specifications (Specs). You must review the current Specs and have your network administrator verify that your AutoClerk system meets them. There may be changes which need to be made to bring your system to AutoClerk's current specs. Following AutoClerk's Specs does *not* make you PCI DSS compliant; however, it contributes to your PCI DSS compliance. AutoClerk's System Specifications can be found at http://myautoclerk.com. Once you have logged in, there is a link on the home page. AutoClerk's Specifications are also attached as "Appendix B" to this document.

This document is organized by the PA-DSS requirements, which AutoClerk must meet to be PA-DSS certified. Some of the measures you need to take are detailed in the AutoClerk System Specifications. This Guide also references the PCI DSS (Version 3.2 April 2016) and the attached Appendixes.

1. Do Not Retain Full Magnetic Stripe, Card Verification Code or Value (CAV2, CID, CVC2, CVV2) or PIN Block Data

The magnetic stripe on the back of a credit card contains sensitive data including the cardholder's name, Primary Account Number (PAN), expiration date, and other information necessary to process the card for an authorization and/or sale. The Card Validation Code or Value, or Card Security Code refers to either 1) the data element on a card's magnetic stripe or 2) the 3-digit number next to the signature field on the back of a Discover, JCB, MasterCard, and Visa payment card; or the 4-digit number on the face of an American Express card. A PIN (Personal Identification Number) is used when a debit card is processed as a debit transaction rather than a credit card transaction.

AutoClerk's credit card interface (Data capture) is certified with Shift4 and Heartland Payment Systems (Heartland) EMV (Europay, MasterCard and Visa) technology. Shift4 and its "Dollars on the Net™" is "a real-time payment gateway between merchants' point-of-sale systems and their bank/processor". By processing guests' credit cards through Shift4 or Heartland, the credit card number is kept by the AutoClerk PMS on your hardware as a masked number with a token. A token is a unique code, which represents and points to the actual card number, which resides at Shift4 or Heartland.

"Masked" is when a cardholder's PAN has been substantially replaced by X's. For example, XXXXXXXXXXXX4957 is a masked format used when viewing and/or printing a guest folio receipt in AutoClerk; 5474XXXXXXXX4957 is a masked format used by Shift4, Heartland Payment Systems, and/or AutoClerk for a hotel's internal reporting purposes, such as a Transaction report.

AutoClerk requires *all* properties which have the AutoClerk data capture interface use Heartland or Shift4 as the property's payment gateway.

When a credit card is used within the AutoClerk client for an authorization or sale it can be entered as a tap, swipe, manually or chip in the EMV pin pad; or the card data is manually entered in the AutoClerk program. The data is then sent by the AutoClerk client to Shift4's Universal Transaction Gateway (UTG) or to Heartland. Shift4 and Heartland Payment Systems process the card authorization and/or sale and return the number in encrypted format to AutoClerk as a truncated number and a token. The full magnetic stripe data is not kept on your hardware and the tokens that are returned by Shift4 Heartland Payment Systems are of no value to a thief.

When a credit card number is manually entered into the PMS for an authorization and/or sale, the staff has the ability to include the name on the card, the card's validation code or value as well as the billing address's zip code. If the card's code and/or value is entered, neither are retained anywhere within the AutoClerk PMS. They are passed to Shift4 or Heartland Payment Systems who uses them only to further validate the card. They are not returned to the PMS once an authorization or sale is obtained.

A debit card's PIN and/or PIN block data is one of the most dangerous numbers to retain. The AutoClerk PMS does not support pin-based debit transactions. AutoClerk's

credit card interface does not allow for the processing of debit cards as anything other than a credit card; therefore, transmitting the PIN is not possible.

When a reservation is entered in the PMS, a property typically requires a valid credit card number and expiration date to guarantee it. Once the credit card number is entered, it is sent in an encrypted format to either the Shift4 UTG or to Heartland. The processor then returns a token to AutoClerk along with only a partial credit card number. This token is used for all future authorizations, sales and refunds made to the card through AutoClerk. Any user looking at the reservation's credit card data only sees a masked credit card number and expiration date.

If a reservation was taken prior to AutoClerk's tokenization being enabled, when that credit card number and expiration date was entered, the AutoClerk PMS' encrypts the card information. Anyone looking at the reservation sees a masked credit card number and expiration date. Only a user with specific 'view rights' can see that unmasked card number. All credit card 'views' are logged by AutoClerk and reference the reservation's confirmation number. In addition, a clerk can go into the reservation and 'validate/tokenize' the card number.

AutoClerk's reservation form does not have a field to enter the Card Validation Code/Value and/or the PIN block data, so any card validation codes/values and PIN block data are also not kept within the PMS.

AutoClerk masks PANs and expiration dates on reports and also encrypts them on backups. The PMS' backups are compressed using zip and are kept on the AutoClerk server computer, on zip disks, on other removable media, and/or sent off site.

There may be instances when you need to retrieve a guest's full credit card number and expiration date. Depending on the situation, you will get the card number and expiration date from either Shift4's Dollars on the Net™ website, a phone call to Heartland Payment Systems or in limited circumstances, from within the AutoClerk PMS.

The AutoClerk PMS can show an unencrypted credit card number only on an existing reservation and only to specific staff. View ability is based on user permissions which are set by property management through the PMS' ACAdmin module. All views of unencrypted credit cards numbers held in the PMS are logged by AutoClerk. You must limit the number of staff who has access to this data. When setting up your users in AutoClerk, only those employees on a "need to know" basis should have access to read full card numbers, process refunds, etc. (PCI DSS Reqs. 7.1).

AutoClerk retains active reservations that do not have an advance deposit posted to them for 60 days past the arrival date. These reservations have a status of guaranteed, hold, share-with, wait list, checked in/out, no show, or canceled. During that time, an authorized staff member has the ability to go back and retrieve a guest's unmasked credit card information if they have 'view rights' and if the reservation was created prior to tokenization. If a reservation has an advance deposit posted to it and it is not checked in, it will remain in the reservation file until the Deposit balance is $0.00, and then will be purged based on its arrival date. The ability to see an unmasked credit card in a past reservation also depends on your property's retention period as discussed in Section 2 of this document.

Per PA-DSS 1.1.5.c, AutoClerk support staff, customers and integrators will: collect sensitive authentication only when needed to solve a specific problem; store such 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; and securely delete such data immediately after use.

A customer's dataset is only downloaded when necessary to troubleshoot a problem.

An AutoClerk Tier 2 support person downloads the dataset to a virtual computer (VM Island) via Bomgar. The dataset is 1) restored using the backupkeys provided by the property;2) cleaned by running a utility which replaces credit card numbers and expiration date information with bogus information; 3) the Users file is replaced; and 4) the backupkeys are changed. A new backup is then done. The cleaned and backed up dataset is placed in the client's folder on AutoClerk's server. The dataset on the virtual computer is then securely deleted.

The dataset on the AutoClerk server can then be used by programmers, operations and/or QA to troubleshoot the problem. Once the issue has been resolved, that hotel's data is securely removed from any support/development/QA computer it was restored on and deleted from the client folder on the server.

2. Protect Stored Cardholder Data

Protecting cardholder data includes the following: 1) Securely deleting cardholder data after a customer-defined retention period as well as when it is no longer required for business, legal, or regulatory purposes; 2) Masking and truncating card numbers when displayed; 3) Rendering the card's PAN unreadable; and 4) Protecting and managing cryptographic keys.

Cardholder data exceeding the customer-defined retention period must be securely deleted per PCI DSS. Cardholder data must also be securely deleted when it is no longer required for legal, business and/or regulatory purposes. Listed below are all the locations where AutoClerk stores cardholder data so you know the locations of data that will be deleted.

AutoClerk is configured so a property can define 1) How often AutoClerk checks; and 2) A retention period, after which, AutoClerk securely deletes cardholder data. Both parameters are expressed in days. The default settings are to check every 7 days and to retain 90 days.

AutoClerk stores credit card data in four files: Reservations, Group masters, Inhouse folios, and Folio history. When AutoClerk checks these files at the defined interval, cardholder data is selected for purging according to the following criteria:

1. All Reservations except Permanent Reservations: Departure date is older than today - <retentionperiod>.
2. Permanent Reservations: Reservation creation date is older than today - <retentionperiod>.

3. Group Masters: The later of (group departure date, last room block) is older than today - <retentionperiod>.
4. Inhouse folios: (1) Folio is checked out, and departure is older than today -2, or (2) Folio is checked in, and arrival is older than today - <retentionperiod>.
5. Folio History: Departure date is older than today - <retentionperiod>.

The credit card data is cleared by encrypting the truncated credit card number over the encrypted full card number and rewriting the record. A manager can also run the utility at any time to delete cardholder data past a defined number of days. Call AutoClerk support for the option codes and steps.

What does this mean to the hotelier? For example, let's assume a hotel manager defines a check interval of 14 days and retention period of 120 days. Then AutoClerk will, automatically, every 14 days, on the night audit, examine the cardholder data locations and clear sensitive cardholder data per the rules stated above.

The nalog.txt, which is produced at each night audit, logs the secure deletion which took place during that audit.

Prior to deleting, a user with view rights can see a full credit card number on a reservation created prior to tokenization being enabled. Post deletion, even with view rights, all the user will see is a truncated and masked credit card number on a reservation. Credit card data which is part of an advance deposit folio, inhouse folio credit card data, and historical folio history already is truncated and contains a token from Shift4 or Heartland.

AutoClerk's PMS responsibility is to make sure that any PAN is masked when displayed, but can be displayed "to those employees and other parties with a specific need to see full PAN". The PAN is unreadable anywhere it is stored. The PMS stores credit card PANs using encryption or tokenization. The full credit card data is stored at Shift4 or Heartland. The reports and historical data produced and maintained by the PMS contain only the truncated credit card numbers and expiration dates.

Displays of masked PANs include guest folios, daily sales transmittal batch, reservations, inhouse folios, receipts for non-guest charges and payments, credit card logs and advance deposit receipts. With tokenization enabled, the only place an unmasked PAN can be viewed is in a prior created reservation; and even then, the user must have 'view rights'.

When AutoClerk is installed at a property, the manager is instructed to set up all users with a unique login using AutoClerk's ACAdmin module. Part of the user set-up includes assigning users the 'right' to view unmasked credit cards. The manager is instructed to only assign that right to as few employees as necessary. With the introduction of tokenization from the card processors, the only unmasked PANs a user would be able to see would be on a reservation created prior to tokenization being enabled. The complete setup of users is detailed in the AutoClerk training document: ACAdmin Module.

Everywhere that AutoClerk stores a PAN, it is unreadable. There are no options the user can configure to make them unreadable as it is part of the program.

Every backup of the AutoClerk data is encrypted by two (2) user defined and changeable keys. Regardless of where these backups may be stored: on the server, on portable devices, off-site, the PAN is unreadable. These backup keys are different than the keys used to encrypt the credit card data.

There are no logs in AutoClerk which have readable PANs. They are all masked and encrypted.

AutoClerk uses two (2) cryptographic key elements: a Key-Encryption-Key (KEK) and a Data-Encryption-Key (DEK) which are used to encrypt credit card data. The KEK is composed of a 72 byte random key. The KEK is used to encrypt/decrypt the DEK; the DEK is used to encrypt/decrypt the data. Both keys are stored in the server registry in binary format. They are protected by the Windows registry protection mechanism which, when properly set up, prevents access by any network user or any user of the same computer without the correct credentials. The KEK is also protected by being obfuscated using an internal encryption routine. You must restrict access to these keys to the fewest number of people necessary and store them securely in the fewest possible locations and forms. (PA-DSS Req. 2.4)

The encryption keys expire every 365 days. AutoClerk's Encryption Key Expiration report is produced by the night audit. It lists the keys' expiration date when they need to be changed. The report can also be produced at will through the Utilities menu.

When the credit card encryption keys have expired, or on demand, an AutoClerk administrative user can invoke a program through ACAdmin that generates two (2) new keys, re-encrypts every cc number in the data set, including historical data, using the new DEK, and stores the new keys. The user does not have the ability to enter their own keys; they are automatically generated by the program.

Properties can change the encryption keys at any time. They must change them when they expire, anytime they suspect their data has been compromised, or when the integrity of the keys have been weakened or possibly compromised. (PA-DSS 2.6.5)

AutoClerk does not retain the retired or replaced cryptographic keys which make them irretrievable. (PA-DSS Reqs. 2.6.5, 2.7) Irretrievability is absolutely necessary for PCI DSS compliance.

AutoClerk's backups are also encrypted using two (2) separate keys. The backup encryption keys must be entered and kept by two separate employees. When the backupkeys are changed, each key custodian enters their key manually, and stores it per the property's security policy. When the keys are entered, they are not clear-text.

"Appendix B" is a sample Key Custodian form (PA-DSS Req. 2.5 and PCI DSS Req. 3.6) which all key custodians should complete and keep in a secure place.

The only cryptographic key material in earlier versions of the AutoClerk client was a built-in credit card encryption key in executables such as ac2g.exe. Part of the AutoClerk conversion/upgrade process to Version 8 included securely deleting all instances of the AutoClerk PMS client executables within the active data. This process securely deleted any cryptographic key material and/or cryptogram from previous versions in the active data and made them irretrievable.

3. Provide Secure Authentication Features

Per AutoClerk's System Specifications ("Appendix A"), and a requirement for your PCI DSS compliance, every employee who has computer access must have a unique user name and password on every computer they use. Your Network Administrator must assist you in setting up these computer users. The users must be standard and NOT administrator users. It is your responsibility, as staff members change, to ensure that the users are disabled/removed and added; as necessary.

AutoClerk's ACAdmin Module document details the requirements and procedures for setting up AutoClerk users; for both admin and general user purposes.

Every employee using AutoClerk must have a unique user name and password that is used when they log into an AutoClerk session. You cannot have duplicate user names or initials. AutoClerk passwords must be at least 7 characters and contain at least one number and one letter. In addition, they can contain upper and lower case letters, and/or special characters (e.g., punctuation). Setting up a user's login name and password must be done immediately upon their hire. Do *not* set up or use any default AutoClerk user accounts or passwords. A manager must have two user accounts in AutoClerk: one for everyday use and another to administer user names and passwords within AutoClerk's ACAdmin program. A user's name and password to log into AutoClerk will not allow them to log into ACAdmin.

AutoClerk enforces secure changes to authentication credentials by the completion of installation by providing the GM a user name with a one-time use password. This allows the manager to access ACAdmin to then set up all the AutoClerk users.

Properties and any third-party integrators must assign secure authentication to any default accounts (even if they won't be used), and then disable or do not use the accounts. (PA-DSS 3.2)

AutoClerk's users' passwords expire after 90 days and then must be reset. The new password cannot be any of the past four passwords. If an AutoClerk PMS user fails to log into a terminal 6 times, they will be locked out of that terminal for 30 minutes. Rebooting the terminal does not shorten the timeout of this feature. Your network vendor must set up all computers to require Windows logon if the station has been idle for more than 15 minutes. All AutoClerk PMS user passwords are encrypted and are never seen in clear-text. In addition, all login attempts are logged by the PMS server and are viewable through the ACAdmin module.

When an employee leaves your employment, you must immediately delete *all* their users' logins including Windows and AutoClerk. Take any other steps necessary depending upon the duties and/or access the ex-employee had, such as changing locks on storage areas for credit card data or being a key custodian.

AutoClerk strongly advises its customers to control access, via unique user ID and PCI DSS compliant secure authentication, to *all* systems, PCs, servers, and databases that contain payment applications and/or cardholder data. (PA-DSS 3.2)

Your property's written security policy must include your rules regarding users, passwords and access to ALL credit card data whether it is on the active dataset, within Shift4 or Heartland, on removable backup media, and/or on paper.

4. Log Payment Application Activity

The AutoClerk PMS automatically creates a variety of logs, such as credit card logs and user access logs. (PA-DSS 4.1) Credit card logs include the logged in user identification (clerk ID), type of event (I.e. Authorization), date and time, success or failure indication (I.e. Approved), origination of event (Shift and Station Number), Identify or name of affected data, system component, or resource (Room/Folio Code).

AutoClerk's PMS server application logs those events that affect security including each time a staff member logs into AutoClerk, successful or not, when an employee views an unmasked credit card PAN and expiration date; as well as actions taken by an AutoClerk PMS administrator. These logs are accessible to an AutoClerk administrator logged into AutoClerk's ACAdmin module.

Logs are automatically created; they cannot be configured or disabled by the user. (PA-DSS 4.1) Logs are automatically exported into a CSV or text file. The log files are located on the property's server computer in:
\app\autoclerk\060.002\[hotelid]\logs
\autoclerk\[hotelid]\data\credit

These logs can be imported into any standard centralized logging system. To access the logs, you must log onto the AutoClerk server computer as an administrator. From the centralized logging system, you can import the data. The file type should be CSV or text. (PA-DSS 4.4)

5. Develop Secure Payment Applications

This section of the *PA-DSS Requirements* applies to AutoClerk, Inc. and how we write, develop, test, and implement our software application. It is important you are made aware of how the PMS is developed, tested, released, and implemented to aide you in complying with PCI DSS.

Prior to release from Development to QA, all code is run through an analyzer to test for vulnerability. If any 'fails' are found, they are fixed before the code is passed. In addition, the developers go through yearly training on secure coding.

Prior to being released to our clients as either a beta or a production version, all upgrades to the AutoClerk PMS and interface applications are tested in-house under the direction of our QA department per their test plans. "Test only" credit cards are issued by Shift4 and Heartland for testing use. No active or "live" credit card numbers are used.

Development, QA, and Production are separate departments at AutoClerk. Any new code comes from Development and is passed to QA. QA oversees the testing of the new code. Once successfully tested, QA passes it to Production for implementation in the field. The code passed from QA to Production to be implemented in the field is an executable file. No test data is included.

When a new version is implemented at a property, the General Manager is advised they can go to http://www.myautoclerk.com for the version 'What's New' release notes.

AutoClerk releases follow a 'Versioning Methodology'. Release versions are numbered as follows:

Version 9 is the major version number; this is also referred to as 060

002 is the minor version number;

005 is the release number;

xxxx is the build.

The versioning methodology is:

A change in major version number indicates a change in application architecture, data structure, or both.

A change in minor version indicates a smaller change in data structure such as the addition of fields to a record.

A change in release number indicates a noticeable improvement to one executable. Programs with different release numbers are interoperable. Moving from one release to another involves changing only the executable concerned.

The build edition changes every time a bug or non-noticeable (behind the scenes) change is made. It is used to identify the exact version of each executable independently of the above versioning system. Build numbers change through the alpha and beta test cycle and stop when the program is released in its final form.

6. Protect Wireless Transmissions

Wireless connections to the AutoClerk network segment are not recommended or supported. AutoClerk has not been developed to be used in a wireless environment.

If *any* workstations are wirelessly connecting to your network, they *must* be configured to use industry best practices such as IEEE 802.11i to implement strong encryption for authentication and transmission. It is prohibited to implement WEP.

In addition, if wireless is used, customers, integrators and/or your network administrator must:

1) Verify all encryption keys are changed from default at the time of installation and are changed if anyone with knowledge of the keys leaves the company or changes positions

2) Change the SNMP community strings

3) Change all default passwords/passphrases on access points

4) Update firmware is updated to support strong encryption for authentication and transmission over wireless networks

5) Verify other security-related wireless vendor defaults are changed

6) Install a firewall between any wireless networks and systems that store cardholder data

7) 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.

Your network administrator must verify that the wireless technology is protected with personal firewall software. The firewall software secure configuration must not be alterable by an employee. All vendor defaults, including keys, are changed at installation and whenever the person knowing the key leaves or changes positions; SSID broadcast is disabled; default Simple Network Management Protocol (SNMP) community strings are changed; all access point passwords are changed; WPA or WPA2 are enabled, if possible. At all times, industry best practices to implement strong encryption for authentication and transmission of cardholder data must be implemented.

7. Test Payment Applications to Address Vulnerabilities and Maintain Payment Application Updates

This section of the PA-DSS refers to AutoClerk's internal processes, which keep AutoClerk up to date on potential security risks to the AutoClerk program and credit card data.

If any possible threats are found to the AutoClerk application, they are investigated, fixed, tested, and deployed to our customers in a timely manner.

It is your responsibility to do the same for your network, including having your network administrator run regular network scans to check for any intrusions and/or unauthorized access attempts. Internal and external network vulnerability scans must be run at least quarterly by a PCI approved scanning vendor, as well as after any significant change in your network. In addition, intrusion-detection systems must be installed to monitor all traffic in the cardholder data environment and to alert personnel to any suspected compromises.

All updates are delivered securely via two-factor authentication and through our internal "chain-of-trust."

When QA has completed testing of a new build, it advises Production via email that the build is ready for beta deployment. Production selects a beta property, advises them that a build is available, and schedules the update.

To install the update, an AutoClerk Support or Tech employee 1) initiates an AutoClerk Bomgar session with the property; 2) renames the old executable; 3) transfers over the new executable; 4) verifies the build with the property; 5) deletes the old executable; and 6) the Bomgar session is ended. Lastly, the manager is advised that the updated What's New documentation is available on www.myautoclerk.com

8. Facilitate Secure Network Implementation

You must have certain security tools in place. These tools include, but are not limited to, an external hardware firewall, anti-virus software, and traffic filtering devices.

Updates to these entities such as your Windows Operating System, anti-virus program, etc., need to be managed, monitored, and installed. Your network administrator must install these tools and train management and staff on their use, management, and maintenance.

Having these security tools implemented on your network computers does *not* interfere with the AutoClerk PMS when they are properly configured. They also do not interfere with AutoClerk's ability to remotely connect to your system via Bomgar.

The only third-party service, protocol, component, etc. that AutoClerk requires is Actian's Pervasive PSQL v12SP1 12.10.62 and above. AutoClerk technicians install Pervasive as part of your AutoClerk PMS installation.

9. Cardholder Data Must Never be Stored on a Server Connected to the Internet

AutoClerk does not use a web server or database server.

10. Facilitate Secure Remote Access to Payment Application

Multi-factor authentication must be used whenever *anyone* remotely accesses your network. Multi-factor authentication requires users to produce at least two (2) credentials to access a system. Credentials consist of something the user has in their possession e.g. smartcards or tokens; something they know e.g. a password; and/or

something they are e.g. a biometric such as a fingerprint or retina pattern. To access a system, the user must produce at least two (2) of the factors. (PA-DSS 10.1)

AutoClerk does not interfere with outside entities using multi-factor authentication to access your network. AutoClerk support staff use two-factor authentication whenever we need to gain access to a hotel's network. All remote access by AutoClerk support is facilitated by known secure solutions: Bomgar and secure tokens.

Bomgar is a security cloud application. AutoClerk has its own dedicated and protected segment on the application. Each AutoClerk Support employee has their own hardware (or software) token which generates a unique number every 60 seconds, and is used to initiate a Bomgar session and then connect with a property. Only authorized AutoClerk employees with a valid token generated number can access our segment.

Support and/or tech sessions with our customers can be conducted in the following ways:

1. Customers initiate an AutoClerk support session by visiting esupport.autoclerk.com from a browser and entering the pin code our support agent gives them over the phone. The pin is only good for that support session.
2. An AutoClerk support agent may email a link to the customer.
3. The link may be accessible via other locations.

The Bomgar connection does not interfere with RADIUS, TACACS, or corporate VPNs. All remote access is logged by Bomgar.

For all remote access, you *must* use and implement remote access software security features such as requiring a unique user name, authenticating all users, changing all default settings, enabling lockouts, enabling data encryption, enabling logging, allowing connections only from specific (known) IP/MAC addresses, and establishing customer passwords according to the PCI DSS requirements. PCI compliant use of all remote stations must be part of your property's security policy.

AutoClerk requires that the computer running AutoClerk's AutoServe program have high-speed Internet access. It must be persistent and static and must be accessible via public (not private) address. Examples of such broadband services would be: DSL, T1, or Cable Modem. AutoClerk does not access properties via a dial-up modem.
Because the server has a static and persistent IP, it must be secured behind your hardware firewall. Proper configuration of the firewall will allow access only to those approved vendors/persons/entities. Any Regional stations must also have at minimum, a personal software firewall installed and properly configured in a secure manner.

Properties must insist that any and all remote-access technologies used by their vendors and business partners be activated only when needed and immediately deactivated after use.

AutoClerk recommends its customers use a securely configured firewall or a personal firewall product if a computer is connected via VPN or other high-speed connection and to secure these "always-on" connections, per PCI DSS Requirement 1. (PA-DSS 10.3)

The access should be logged and be disabled when not in use, multiple incorrect log ins must lock out the account.

11. Encrypt Sensitive Traffic over Public Networks

Customers and integrators are to use strong cryptography and security protocols if they send any cardholder data over a public network. (PA-DSS 11.1)

AutoClerk has the ability to send guests a reservation, cancellation and/or thank you letter via email. However, even if the letters are formatted to send the guest's credit card number used to guarantee the reservation, it sends the masked PAN and only the last four digits of the number. The full PAN is never sent from the PMS. (PA-DSS 11.2.b) Full PANs are, in the limited areas they are viewable, viewable only. AutoClerk does not facilitate the sending of full PANs over public networks or any end-to-end messaging such as instant messaging. Any credit card information sent to the payment processor (Shift4 or Heartland) is encrypted and tokenized. In addition, communication to/from Shift4 goes through their UTG.

12. Secure All Non-Console Administrative Access

The AutoClerk program does not facilitate non-console administrative access.

13. Maintain a PA-DSS Implementation Guide for Customers, Resellers, and Integrators

AutoClerk's website for our customers is http://www.myautoclerk.com. It contains: AutoClerk's System Specifications, a link to our interactive training videos, training documentation, user documentation and the 'What's New' documents. The What's New is updated with each release. These are available under the "Documentation" tab. Customers can also select Help at the top of the PMS Main menu to access the documentation.

Prior to AutoClerk's installation, a link to this document is provided to the property. The *AutoClerk PA-DSS Implementation Guide* can also be found at http://www.myautoclerk.com.

It is reviewed and updated at minimum on a yearly basis, and is updated as needed to document all major and minor changes to AutoClerk.

14. Assign PA-DSS Responsibilities for Personnel, and Maintain Training Programs for Personnel, Customers, Resellers, and Integrators.

Mohammed Hansia, Director of Operations, is responsible for assigning PA-DSS responsibilities.

Appendix A: System Specifications

Note for all systems: Each user must be configured with their own standard Windows user with a "complex" password, in that they must contain at least 7 characters and include both letters and numbers. Passwords can be even more secure by including upper- and lower-case letters and/or special characters.

Those employees that need administrative level access to a computer must have a separate user and "complex" password with administrative access, which must only be used when that access level is needed.

Customers are strongly advised to control access, via a unique user ID and PCI DSS-compliant secure authentication, to any PCs, servers, and databases with payment applications and cardholder data. (PA-DSS 3.2)

Restore points must be disabled on all systems.

All users must be set to time out after 15 minutes of inactivity. (PA-DSS 3.2)

AutoClerk Minimum Requirements for a Single Computer

Computer running Windows 8.1 Pro or Windows 10 Pro

Anti-virus software

External hardware firewall

Intel Processor 2.0 GHz

4 GB Ram

Video Supporting 1024 x 768

Network Interface Card – Must be 3Com, Intel or Broadcom (1 GB)

Hard drive 40GB Disk storage available for AutoClerk.

Color Monitor

Keyboard

Mouse

Speakers or Headphones (For instructional Videos)

DB9 RS232 Serial Port - One is needed for each of most interfaces. Digi or Edgeport for multiple Serial Ports.

Laser Printer (must be local or network).

Dedicated USB Port

USB Printer Cable

Battery Backup

High Speed Internet Access with a Static IP address

Properly configured hardware systems for AutoClerk can be directly purchased from Technology At Work.

AutoClerk Minimum Requirements Non-Dedicated Server (4 stations max)

Two or more Computers running Windows 8.1 Pro or Windows 10 Pro

External hardware firewall on the computer running the AutoClerk autoserv.exe

Anti-virus software

Intel Processor 2.0 GHz

4 GB Ram

Video Supporting 1024 x 768

Network Interface Card – Must be 3Com, Intel or Broadcom (1 GB)

Hard drive 40GB Disk storage available for AutoClerk.

Color Monitor

Keyboard

Mouse

Speakers or Headphones (For instructional Videos)

DB9 RS232 Serial Port - One is needed for each of most interfaces only on the computer(s) running the interface(s). Digi or Edgeport for multiple Serial Ports.

Laser Printer (local or network)

Dedicated USB Port

USB Printer Cable

Battery Backup

High Speed Internet Access with a Static IP address

Network Switch (1 GB)

Category 5 (Cat 5) Cabling

Properly configured hardware systems for AutoClerk can be directly purchased from Technology At Work.

AutoClerk Minimum Requirements Dedicated Server. Required for 4 plus stations

Local Work Stations

Computers running Windows 8.1 Pro or Windows 10 Pro

External hardware firewall

Anti-virus software

Intel Processor 2.0 GHz

4 GB Ram

Video Supporting 1024 x 768

Network Interface Card – Must be 3Com, Intel or Broadcom (1 GB)

Hard drive 40GB Disk storage available for AutoClerk.

Color Monitor

Keyboard

Mouse

Speakers or Headphones (For instructional Videos)

DB9 RS232 Serial Port - One is needed for each of most interfaces only on the computer(s) running the interface(s). Digi or Edgeport for multiple Serial Ports.

Laser Printer (local or network)

Dedicated USB Port

USB Printer Cable

Battery Backup

Dedicated Application Server with Primary Domain Controller

Microsoft Server 2012 or Microsoft Server 2019 Standard

Anti-virus software

External hardware firewall

Intel Processor 2.0 GHz

8 Gig Ram

Video Supporting 1024 x 768

Network Interface Card – Must be 3Com, Intel or Broadcom (1 GB)

Hard drive 40GB Disk storage available for AutoClerk. It is highly desirable that redundant (RAID 1 or higher) disk storage be used.

Monitor

Keyboard

Mouse

DB9 RS232 Serial Port – One is needed for each of most interfaces. Digi or Edgeport for multiple Serial Ports.

UPS from APC with PowerChute

High Speed Internet Access with a Static IP address

Network Switch (1 GB)

Category 5 (Cat 5) Cabling

Properly configured hardware systems for AutoClerk can be directly purchased from Technology At Work.

Special Interface considerations:

Best Western Properties:

Best Western properties require a PMS-Router configured specifically for the Best Western 2-Way Interface.

Credit Card Processing:

EMV pin pads acquired either directly from Heartland Payment Systems or Technology At Work for Shift4.

Appendix B: Sample Key Custodian Form

The following is a sample of the Key Custodian form that must be signed by all Key Custodians:

The signee of this document acknowledges that he or she has been afforded access to key management devices, software, and equipment. I understand I have been chosen as a key custodian for one (1) AutoClerk backup encryption key.

I hereby agree that I:

1. Have read and understood the policies and procedures associated with key management and agree to comply with them to the best of my ability. I have been trained in security awareness and have had the ability to raise questions and have had those questions satisfactorily answered.
2. Agree to never divulge to any third party, especially including personnel who maintain the other half of the key management or related security systems, passwords, processes, security hardware, or secrets associated with the AutoClerk system, unless authorized by a manager, owner, or required to do so by law enforcement officers.
3. Agree to report promptly and in full to the correct personnel, any suspicious activity including but not limited to key compromise or suspected key compromise. Suspicious activity can include the following: Phone requests from unidentifiable callers for access to secure information, unidentifiable files found on computers, and unusual activity recorded in log files.
4. My duties are to generate my half of the AutoClerk backup encryption key when necessary and to protect the integrity of this password at all times. If it is written down, then the written password must be secured within a secure, locked area, preferably a safe, per my property's security policy

_____

Signature Date

_____

Print Name