AUTOCLERK

* It's how you manage.™

PCI SSF Vendor Security Guidance

For

acPMS

Contents

Copyright Information....2
Revision History....2
Introduction....3
PCI Secure Software Core Requirements....4
1. Minimizing the Attack Surface....4
Control Objective 1: Critical Asset Identification....4
Control Objective 2: Secure Defaults....5
Control Objective 3: Sensitive Data Retention....6
2. Software Protection Mechanisms....6
Control Objective 4: Critical Asset Protection....6
Control Objective 5: Authentication and Access Control....7
Control Objective 6: Sensitive Data Protection....8
Control Objective 7: Use of Cryptology....8
3. Secure Software Operations....8
Control Objective 8: Activity Tracking....8
Control Objective 9: Attack Detection....9
4. Secure Software Lifecycle Management....9
Control Objective 10: Threat and Vulnerability Management....9
Control Objective 11: Secure Software Updates....9
Control Objective 12: Software Vendor Implementation Guidance....9
Module A – Account Data Protection Requirements....9
Purpose and Scope....9
Control Objective A.1: Sensitive Authentication Data....10
Control Objective A.2: Cardholder Data Protection....10

Copyright Information

acPMS PCI SSF Vendor Security Guide

AutoClerk, Inc.

Address: 1990 N California Blvd, Suite 20 PMB1139, Walnut Creek, CA 94596

Phone: 925.284.1005

URL: www.autoclerk.com

Revision History

Date of Revision	Revision #	Editor	Purpose
3/23/22	1.0	H. McGlothlin	First draft of Guide
5/26/2022	1.1	T. Hannan, D. Ferris, G. Willkom, H. McGlothlin	Updated by Tech, Development and Security
6/9/2022	1.1	Mohammed Hansia	Reviewed and approved v1.1 for distribution.

This document is updated anytime there is a modification to the acPMS software and upon any updates to the PCI SSC standard for which it is validated against. In addition, the document is reviewed no less than annually. A copy is maintained on the AutoClerk support site, www.myautoclerk.com

Introduction

This security guide is for AutoClerk's acPMS POS version 060-002-005 payment application. The version is also known as Version 9. 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) Secure Software Standards.* acPMS previously certified under the PCI's Payment Application Data Security Standard (PA-DSS).

acPMS is a software product developed for use in hotels and resorts. It helps hotels efficiently organize, schedule, and manage their daily operations, enables hotels to handle front office workflow including booking of rooms, guest check-in & checkout, posting charges to guest folios such as room and occupancy tax, delegating housekeeping tasks and managing Accounts Receivable, etc. Hotel staff can perform credit card authorizations, sales, refunds, and voids using either an EMV device, manual entry of the card number (https); and/or the credit card token already received from their credit card processor. acPMS supports Shift 4 Payment Processing, Heartland payment processing and Elavon Payment Processing.

This guide is organized by the PCI's Software Security Framework (SSF) document. Please also refer to acPMS' PA-DSS Implementation Guide ver. 5.0, acPMS System Specifications (which is Appendix A to the Implementation Guide) and acPMS User Guide - ACAdmin for additional information on how acPMS handles credit card information, how to secure your system and other credit card and data security information.

PCI Secure Software Core Requirements

1. Minimizing the Attack Surface

Control Objective 1: Critical Asset Identification

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. These are also referred to as the CVC, CVV and/or CSC. A PIN (Personal Identification Number) is used when a debit card is processed as a debit transaction rather than a credit card transaction.

When a credit card is used within the acPMS 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 acPMS program. If a credit card number is manually entered in acPMS and not in the EMV device, the user can include the cardholder's name, the card's validation code or value as well as the billing address's zip code. These are not kept anywhere in the system. They are passed to the processor and are not returned to acPMS.

A debit card's PIN and/or PIN block data is one of the most dangerous numbers to retain. acPMS does not support pin-based debit transactions so they cannot be entered and/or transmitted.

acPMS uses cryptographic keys to encrypt cards. The keys' elements are a KEK and a DEK.

Credit card numbers are only stored if a token is not received by the processor. It is encrypted using ThreeFish-512. Full magnetic stripe data is not kept on the hardware. Once tokenized, the token is used for any future authorizations, sales, and refunds.

Storage, if any, of user and/or credit card information is stored on RAM discs and not in in any temp or non-volatile memory.

At the time of installation of the credit card interface, properties can opt to have 'res tokenization' enabled.

If enabled, when a reservation is taken and a credit card number is entered as a form of guarantee, it is sent in an encrypted format to the Shift4 UTG or to Heartland or Elavon. The processor returns a token which is used for all future transactions. Any user with permission to 'view cc' will only see a masked card number and expiration date.

acPMS users are created with a unique user name and password. They can only be created by a user with acPMS' ACAdmin user credentials. These are kept in volatile memory and database on the acPMS server. To see the file, you must be logged into the acPMS server PC as a Windows Admin user. The passwords are hashed during storage and in the file.

When users are created, they can be assigned to the 'User View' group. If a user is part of this group, he can only see an unmasked credit card number and expiration in an existing reservation and only if 'Res Tokenization' has not been enabled. Once a guest is checked in, only a masked card number can be viewed, regardless of ‘view’ status. All credit card views are logged.

‘Sensitive functions’ within acPMS include the reading of acPMS user credentials when staff log into acPMS, and the reading, writing and transmission of credit card data to the credit card processor.

A hotel employee with ACAdmin rights, can, at any time, go in and re-encrypt the encryption keys; change the ‘keys’ used to back up the data; and change a user permission to allow/disallow the viewing of a full credit card number.

Hotels are advised to change the keys at least once a year or if at any time they think their data may have been compromised. acPMS produces a report each night on the Night Audit that lists any keys that are expiring in the next 14 days.

acPMS requires Actian’s Pervasive 13.30 to run. It is installed at the time of initial acPMS installation with its own license key. If for any reason Pervasive shuts down, acPMS will not run.

Control Objective 2: Secure Defaults

At the time of installation, the acPMS On-boarder or Technician directs the GM/Hotel Owner to log into the ACAdmin module with a default user and password given to them. This default user and password can only access ACAdmin. It cannot log into acPMS. Once logged in, they are instructed to create their own ACAdmin user and password as well as acPMS users for each employee who will be using the system. The default user is then deleted. This is the only default user account acPMS.

When acPMS users are created, per the ‘User Guide – ACAdmin,’ only those staff with a ‘need to know’ should be allowed to see a full credit card number. Once card numbers are tokenized, that token is used to communicate with the credit card processor. Users can reach out to their credit card processor for card information if necessary

acPMS does not use any APIs.

acPMS Support and Technicians use Bomgar to remotely assist properties. Properties with a dedicated server PC can opt to have a Bomgar jump client installed on the server. Each jump client has its own user/password for access.

At the time of installation, the property’s dataset has default backupkeys and a ‘datakey.’ These are changed by the property at the end of the installation with the help of the On-boarder/Technician.

The property’s IT vendor is required to open port 11193 and ‘Allow the Connection’ so the computers can communicate on the network with the server.

The IT vendor must disable and/or remove any unnecessary and insecure services and protocols such as NetBIOS, file-sharing, Telnet, etc.

If a property is using Shift4 as their credit card processor, Shift4 works with the property to gain access to their acPMS server and install its Universal Transaction Gateway (UTG). Once installed, Shift4 works with the acPMS Technician to configure the UTG to interface with acPMS’ credit card interface.

After installation and prior to going ‘live,’ a property enters its existing reservations including the guest’s credit card number, if there is one. The card data is saved in non-volatile storage, e.g., the hard drive, in an encrypted format. Once the property is ‘live,’ when the credit card interface is installed and activated, the On-boarder/Technician works with the property to re-encrypt the dataset and change the encryption keys through the ACAdmin module. Only a user with ACAdmin rights can access the ACAdmin module and change the keys. The keys are changed within the system without user input to decide what the new keys are.

Control Objective 3: Sensitive Data Retention

acPMS retains active reservations that do not have an advance deposit posted to them for a default of 60 days past the arrival date. The retention date is configurable by the hotel in the ACConfig module. 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 can go back and see 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. acPMS is configured so a property can define 1) How often acPMS checks; and 2) A retention period, after which, acPMS securely deletes cardholder data. Both parameters are expressed in days. The default settings are to check every 7 days and to retain 90 days.

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.

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.

PANs are masked when displayed and unreadable anywhere they are stored. The PMS stores credit card PANs using encryption or tokenization. The full credit card data is securely stored at the processor. The reports and historical data produced and maintained by the acPMS contain only the truncated credit card numbers and expiration dates.

Displays of masked PANs include guest folios, daily credit card 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.’

2. Software Protection Mechanisms

Control Objective 4: Critical Asset Protection

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.

Control Objective 5: Authentication and Access Control

Every hotel employee who has computer access must have a unique username and password on every computer they use. Your network administrator must assist you in setting up these computer users. The users must be standard users and NOT administrator users.

Every employee using acPMS must have a unique user name and password for logging into an acPMS session. A manager may have two user accounts in acPMS: one for everyday use and another to administer user names and passwords within the ACAdmin module. A user's name and password to log into acPMS will not allow them to log into ACAdmin. acPMS does not maintain any client user names and/or passwords. It is important that at least manager level employee also have ACAdmin user credentials.

A property's IT vendor and any third-party integrators must assign secure authentication to any default accounts (even if they will not be used), and then disable or not use the accounts.

Wireless connections to the acPMS network segment are not recommended or supported. acPMS 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.

Multi-factor authentication must be used whenever *anyone* remotely accesses your network.

acPMS does not interfere with outside entities using multi-factor authentication to access your network. acPMS support staff use two-factor authentication whenever they need to gain access to a hotel's network.

All remote access by acPMS support is facilitated by known secure solutions: Bomgar and secure tokens.

1. Customers initiate an acPMS support session by visiting esupport.autoclerk.com from a browser and entering the session key the support agent gives them or clicking on a support agent's name. The pin code is only valid for that support session.
2. An acPMS support agent may email a link to the customer.
3. From within acPMS, on the Main Menu, customers click on Help, then click on Support. This redirects them to esupport.autoclerk.com where they can enter a session key given to them by the Support agent, or they can click on a Support agent's name.
4. The Bomgar client software may be permanently installed on hotel computers, such as dedicated server computers, or others.

Bomgar solutions are designed to work transparently through firewalls, enabling a connection with any computer with internet connectivity, anywhere in the world. However, with certain highly secured networks, some configuration may be necessary.

1. Ports 80, 443, and 8200 need to be open for outbound TCP traffic.

2. NOTE: Port 8200 is used as a rollover for port 443 and is not strictly required, though it is recommended.

Control Objective 6: Sensitive Data Protection

acPMS protects cardholder data by: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; 4) Protecting and managing cryptographic keys; 5) Using credit card processor issued tokens for transactions; and 6) encrypting backups with unique keys.

Control Objective 7: Use of Cryptology

acPMS 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 by the property's network administrator, 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.

When the credit card encryption keys have expired, or on demand, an acPMS administrative user can invoke a program through the ACAdmin module that 1) generates two (2) new keys; 2) re-encrypts every cc number in the data set, including historical data, using the new DEK; and 3) stores the new keys. The user does not have the ability to enter their own keys; the program automatically generates them.

acPMS does not retain the retired or replaced cryptographic keys, which make them irretrievable.

acPMS' backups are encrypted using two (2) separate keys. The backup encryption keys when created and/or changed, should 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.

Properties can change the backup 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 has been weakened or possibly compromised.

3. Secure Software Operations

Control Objective 8: Activity Tracking

Each time a credit card number is attempted to be viewed in a reservation, or inhouse guest folio, regardless of whether the full card number is displayed, it is tracked in the acPMS server logs. The logs can be viewed by an ACAdmin user through Tools – View logs.

The logs include the date, time, PC name, acPMS station number, who was logged into the acPMS session and the confirmation number of the reservation. An example is:

```
04/07/22 18:14:39 BOCWN76489.bwi.bestwestern.com[+1:HOLLY]: View credit card number for 220010
```

The logs are kept by default for 366 days. Only a user with Windows Administrator rights on the acPMS server has access to the file to change the number of days logs are kept.

Each time a credit card is authorized, a payment, refund or void is processed either through the acPMS software such as in a reservation, or through an EMV machine, that process is tracked in the credit card logs.

Control Objective 9: Attack Detection

If an acPMS user, when logging into the system, enters an incorrect user/password 6 times, they are automatically locked out of the system for 30 minutes.

4. Secure Software Lifecycle Management

Control Objective 10: Threat and Vulnerability Management

If a security issue is discovered, acPMS Developers can issue a patch the same day or within 48 hours at most. Technicians can deploy the patch the same day it is released to them by Development. If multiple acPMS properties share the same build for which the vulnerability was discovered, Technicians will inform those properties. Until the patch has been created, acPMS Technicians will produce a workaround and inform all properties using the affected build the same day they are informed of the threat.

Control Objective 11: Secure Software Updates

acPMS software updates are done by acPMS technicians in a secure manner by using Bomgar to access the property, install the update, delete the old executable(s) and re-lock the acPMS server.

When an update is produced and delivered, hotels can go to www.myautoclerk.com and view the 'What's New' document that is produced, as well as other User Guides and/or documents produced for an update and/or release.

acPMS Technicians maintain a list of properties who have reported bugs or requested features. When a build is available for those bug fixes or features, Technicians call those properties directly to schedule updates. When a build has been chosen for production, Technicians call all acPMS properties to schedule updates.

Control Objective 12: Software Vendor Implementation Guidance

acPMS produces an Implementation Guide that is reviewed and/or updated yearly or whenever changes need to be made due to changes in the software or credit card security requirements. It includes Appendix A – System Specifications which detail the requirements to have acPMS installed as well as security requirements such as no sharing of users, when and how to change passwords, the non-use of any defaults, etc.

The acPMS Implementation Guide is available to any user on the www.myautoclerk.com site.

Module A – Account Data Protection Requirements

Purpose and Scope

This section (hereinafter referred to as the "Account Data Protection Module"), defines security requirements and assessment procedures for software that stores, processes, or transmits account data. For the purposes of this module, account data is defined as follows: Cardholder Data includes: Primary Account Number (PAN), Cardholder Name, Expiration Date and Service Code. Sensitive Authentication Data includes: Full track data (magnetic-stripe data or equivalent on a chip), CAV2/CVC2/CVV2/CID, and PINs/PIN blocks. The primary account number (PAN) is the defining factor for cardholder data. If PAN is stored, processed, or transmitted or is otherwise present, the requirements in this module apply in addition to the Secure Software Core Requirements. The primary account number (PAN), cardholder name, expiration date and service code are permitted to be stored, but the PAN must be rendered to be unreadable. The full track data, CAV2/CVC2/CVV2/CID, and PINs/PIN blocks are never permitted to be stored. Account Data Protection

The software does not store sensitive authentication data after authorization even if encrypted unless the software is intended only for use by issuers or organizations that support issuing services. Only in those cases can sensitive authentication data be stored post-authorization.

Control Objective A.1: Sensitive Authentication Data

Sensitive authentication data consists of full trackdata, card validation code or value, and PIN data. Storage of sensitive authentication data after authorization is prohibited. This data is very valuable to malicious individuals as it allows them to generate counterfeit payment cards and create fraudulent transactions.

Control Objective A.2: Cardholder Data Protection

acPMS retains active reservations that do not have an advance deposit posted to them for a default of 60 days past the arrival date. The retention date is configurable by the hotel in the ACConfig module. 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 can go back and see 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. acPMS is configured so a property can define 1) How often acPMS checks; and 2) A retention period, after which, acPMS securely deletes cardholder data. Both parameters are expressed in days. The default settings are to check every 7 days and to retain 90 days.

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.

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.

PANs are masked when displayed and unreadable anywhere they are stored. The PMS stores credit card PANs using encryption or tokenization. The full credit card data is securely stored at the processor. The reports and historical data produced and maintained by the acPMS contain only the truncated credit card numbers and expiration dates.

Displays of masked PANs include guest folios, daily credit card 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.’