11 January 2010

PA-DSS 1.2 Validation & CISP Implementation Documentation

Since 1995, RPOWER has always been protective of cardholder data. It has never stored numbers, expiration dates, and track data unencrypted. It has always formatted its receipts to be secure according to the strictest requirements of the time.

With the release of RPOWER Restaurant POS Version 2008 and higher, RPOWER adheres to the PCI Security Council PA-DSS 1.2 guidelines and beyond. Furthermore, we can identify the following specific statements about credit card security and cardholder information with regards to RPOWER Restaurant POS.

- RPOWER never prints or displays a full credit card number to anyone under any circumstances.
- "Current day" card information is encrypted with 128-bit AES using a site-specific key.
- Card numbers and expiration dates are re-encrypted each day using a 2,048-bit RSA public key from K3 Software for problem resolution and batch reconstruction.

  RSA estimates these key strengths to be valid until at least 2030. See http://en.wikipedia.org/wiki/Key_size for an overview.
- All keys are known only to K3 Software Corp. and are stored and backed up on equipment physically separate from its regular company computers. The passwords to these computers are known to two senior executives in the company. Access to the keys is logged.
- Card verification code and PIN values are never stored.
- RPOWER's keystroke logs do not contain sensitive information, while at the same time allowing people to see that something was entered.
- All credit card data inaccessible to anyone outside of K3 Software. Even RPOWER-certified dealers with access to the highest level security passcodes cannot retrieve credit card data.

- RPOWER uses password-protected remote control software for direct support and maintenance. RPOWER recommends the use of Radmin with configuration settings defined later in this document.

PA-DSS 1.2 Implementation Guide for RPOWER System Networks

In addition to the security measure implemented by RPOWER in Version 2008, the following guidelines are CISP recommendations to further secure all data at each location.

Additional information on each of the following topics can be found in the Visa **PCI Data Security Standard** documentation located on their website at:

https://www.pcisecuritystandards.org/

Remove Potentially Sensitive Historical Information

For existing RPOWER customers upgrading to PCI-DSS 1.2 validated software, RPOWER Version 2008 or newer:

RPOWER deletes all previous existing historical sensitive data in its database, however previous "Daily Zip"(*.zip) and log files (*.txt) must be deleted to maintain CISP compliancy and remove all potentially sensitive information.

These files are typically located in the following directories:

Daily Zips: F:\RPOWER\ARCHIVE and/or

C:\SYS\RPOWER\ARCHIVE

System Logs: F:\RPOWER\WINRUN\Logs and/or

C:\SYS\RPOWER\WINRUN\Logs

Keystroke Logs:

F:\RPOWER\WINRUN\Logs_WORKSTATION_NAME and/or

C:\SYS\RPOWER\WINRUN\Logs_WORKSTATION_NAME

These files may be stored on both the "File Server" computer as well as alternate systems. Please check with your local RPOWER dealer to ensure removal of all potentially sensitive data from your systems.

Cryptographic Material

For existing RPOWER customers upgrading to PCI-DSS 1.2 validated software, RPOWER Version 2008 or newer:

RPOWER deletes all previous existing cryptographic data from its database and no longer locally stores means of recovering cardholder data.

Access and Storage of Sensitive Card Holder Data

For existing RPOWER customers upgrading to PCI-DSS 1.2 validated software, RPOWER Version 2008 or newer:

RPOWER does not allow for open recovery of encrypted cardholder data regardless of user privilege levels in RPOWER under any circumstances. Request for sensitive cardholder information will be made to K3 Software Corp. through your local RPOWER dealer. All requests must be accompanied by: the reason for submittal along with requesting individual full name and contact information. The request will be processed within 24 hrs of notification in most cases.

Cardholder data once provided to the site must:

- Be stored only in specific, known locations with limited access.
- Be limited to the amount needed to solve a specific problem.
- Be securely deleted immediately after use.

RPOWER may store credit card swipe data fully encrypted for retrieval using obscured card number entry, which means entering the first six and last four digits of a card number, with X's in between. Track 2 and AVS data is kept for the current day and cleared upon settlement. CVC data is never stored. After settlement, you may still use obscured card number entry to retrieve credit card numbers and expiration dates (as if manually keyed) for up to 10 days (two full weekends prior to any given Monday). You can change the number in RPOWER.ini by setting ICTDAYS=N where N is the number of days.

You can turn off current-day track 2 data storage by setting ICTDAYS=N,1 (for example, ICTDAYS=10,1) where ,1 causes RPOWER not to store track and AVS data.

Setting ICTDAYS=1 causes RPOWER only to store the current day.

Setting ICTDAYS=-1 turns off all storage, including track 2 and AVS.

Obscured card number entry means that if original the credit card number is, for example, 4003 0101 2345 6780, then:

- 400301xxxxxx6780 will print on merchant copies and reports.
- xxxxxxxxxxxx6780 will print on customer copies, and, optionally, merchant copies.
- With manager approval, you now can enter it (with the Enter CC# button) as 400301XXXXXX6780. If this card was used within the last ICTDAYS days, RPOWER will find it and use it.

This covers only the ability for RPOWER to recover access to the cardholder data at the restaurant for subsequent recovery and error correction, using the restaurant's own 128-bit AES encryption keys through RPOWER software only.

It is important to note that RPOWER still keeps daily Zips going back up to 1200 days (by default). Credit card information in these files (and the 200-day 911\DATA backup archive) is protected by 2,048-bit RSA public key encryption and recoverable only by K3 Software.

User Passwords and Logins

RPOWER recommends using unique user IDs for each RPOWER user via means of employee passcodes, magnetic stripe cards, or biometrics. Your RPOWER system can be configured to require magnetic stripe or biometric access only. Consult your RPOWER dealer for assistance implementing these options.

- Do not allow employees to share user IDs.
- Change employee passcodes every 90 days.
- Immediately edit terminated employee files to an "inactive" status to revoke all RPOWER application privileges.

For additional information on creating complex passwords for your windows environment and other non-RPOWER applications and networking components refer to the PCI Data Security Standard sections 8.5.8 through 8.5.15.

RPOWER System and Keystroke Logging

RPOWER logs all system activity, via keystroke logging and application logging.

All logs related to credit card swipes and manual entries are obscured in a non-recoverable manner.

RPOWER system logs are stored in F:\RPOWER\Winrun\Logs and track system operations, errors, and higher-level user activity. This includes each attempt to access the Manager Functions area of RPOWER.

RPOWER workstation logs record ALL user activity within the RPOWER application via means of a keystroke log. Whereas the entire activity of a given RPOWER workstation can be rebuilt step-for-step as the original actions were performed. These files are stored in F:\RPOWER\Winrun\Logs_Workstation_Name.

RPOWER in Wireless Networking Environments

RPOWER may be used in a wireless networking environment. Implement wireless security on networks transmitting or connected to cardholder data according to industry best practices (e.g., IEEE 802.11i) to implement strong encryption for authentication and transmission.

The following recommendations should be considered in order to preserve the utmost system security:

- Install, use, and maintain a personal firewall on all components using a wireless networking connection.
- Do not use wireless vendor defaults in any manner for passwords, users or any other means.
- Do not use the default SSID or broadcast the wireless SSID.
- Do not allow remote management of wireless networks.
- Restrict access to wireless access points by MAC address only.
- Static assign IP address for all wireless system components. Do not enable DHCP service for access points.
- Physical access to networking components such as wireless access points, gateways and unused handheld systems is restricted from non-essential personnel.
- For new wireless implementations, it is prohibited to implement WEP after March 31, 2009.
- For current wireless implementations, it is prohibited to use WEP after June 30, 2010.

Internet Accessible Systems

Sites utilizing a high-speed Internet connection should consider implementing the following to further secure their network:

- Install and maintain a network firewall.
- Do not use the RPOWER system or terminals on the network for general Internet activity.
- Do not send any cardholder information over the Internet.

RPOWER Remote Software Updates

RPOWER will not and cannot perform remote software updates without initiation and request from each site internally prior to execution. Contact your local RPOWER dealer for further information about software updates and upgrades.

Remote Software Access

For a site opting to use Remote Access Software for periodic system support by its local RPOWER dealer and/or RPOWER corporate, RPOWER recommends the use of Radmin Remote Access Software.

RPOWER recommends taking the following steps to ensure proper and secure use of Radmin Remote Access Software:

- Do not use the default listening port for access.
- Change the default login name and user password. Use unique, strong and complex passwords for each user login.
- Configure Radmin to limit remote access by remote users by their known local IP/MAC addresses. Contact your local RPOWER dealer for assistance in enabling the IP/MAC addresses required for direct RPOWER support.
- Enable the logging functionality of Radmin.

Contact your local RPOWER dealer for assistance in configuring your Radmin software to enable these functions and provide the securest means to allow remote access.

For additional information on Radmin and its security features visit:

http://www.famatech.com/products/radmin/index.php

and

http://www.famatech.com/products/radmin/security.php

Note: RPOWER and its authorized dealership channel do not and will not share their remote access connection information. Independent user connections must be created for third party access to your system. Contact your local dealership for assistance in creating a personal login or third party accounts.

Public Transmission of Secure Data Over The Internet

RPOWER recommends and uses only SSL communications for all transmission of secure data over the Internet when necessary.

PCI-DSS 1.2 Implementation Guide Review

RPOWER will review and update this guide annually to adhere to future CISP guidelines. Contact your local RPOWER dealership for an updated copy of our procedures at least once annually.

For Additional information regarding PCI-DSS 1.2 Validation for RPOWER Restaurant POS or additional information on updating your site to comply with CISP and PCI regulations please contact your local RPOWER dealership.