Oracle® Hospitality Oracle Hospitality RES 3700

PA-DSS 3.2 Implementation Guide
Release 5.7.X.X

May 2018

ORACLE

Contents

Preface

This document describes the steps that you must follow in order for your Oracle Hospitality RES 3700 installations to comply with Payment Application – Data Security Standards (PA-DSS). The information in this document is based on PCI Security Standards Council Payment Application - Data Security Standards program (version 3.2 dated June 2016). You can download the PCI PA-DSS 3.2 from the PCI SSC Document Library.

Oracle Hospitality instructs and advises its customers to deploy Oracle Hospitality applications in a manner that adheres to the PCI Data Security Standard (v3.2). Subsequent to this, you should follow the best practices and hardening methods, such as those referenced by the Center for Internet Security (CIS) and their various benchmarks, in order to enhance system logging, reduce the chance of intrusion, increase the ability to detect intrusion, and other general recommendations to secure networking environments. Such methods include, but are not limited to, enabling operating system auditing subsystems, system logging of individual servers to a centralized logging server, disabling infrequently-used or frequently vulnerable networking protocols, and implementing certificate-based protocols for access to servers by users and vendors.

You must follow the steps outlined in this Implementation Guide in order for your Oracle Hospitality RES 3700 installation to support your PCI DSS compliance efforts.

Revision History

Date	Description of Change
May 2018	• Initial publication.

This PA-DSS Implementation Guide is reviewed and updated on a yearly basis, when there are changes to the underlying application changes, or when there are changes to PA-DSS requirements. Go to the Hospitality documentation page on the Oracle Help Center at http://docs.oracle.com to view or download the current version of this guide, and refer to the Oracle Hospitality Oracle Hospitality RES 3700 Release Notes and this guide's Revision History to learn what has been updated or changed. In order to ensure your PCI DSS compliance, you need to subscribe to receive email Oracle Security Alerts by clicking the Critical Patch Updates link on the Oracle Technology Network at http://www.oracle.com/technetwork/index.html. This provides you timely information on any possible updates to the PA-DSS Implementation Guide that you need to know about in order to continue to use Oracle Hospitality RES 3700 in a PCI DSS compliant manner.

1 Executive Summary

Oracle Hospitality RES 3700 5.7.X.X has been Payment Application - Data Security Standard (PA-DSS) validated, in accordance with PA-DSS Version 3.2. For the PA-DSS assessment, we worked with the following PCI SSC approved Payment Application Qualified Security Assessor (PAQSA):

Coalfire Systems, Inc.
11000 Westmoore Circle, Suite 450,
Westminster, CO 80021

Coalfire Systems, Inc.
1633 Westlake Ave N #100
Seattle, WA 98109

This document also explains the Payment Card Industry (PCI) initiative and the Payment Application Data Security Standard (PA-DSS) guidelines. The document then provides specific installation, configuration, and ongoing management best practices for using Oracle Hospitality Oracle Hospitality RES 3700 Version 5.7.X.X as a PA-DSS validated application operating in a PCI DSS compliant environment.

PCI Security Standards Council Reference Documents

The following documents provide additional detail surrounding the PCI SSC and related security programs:

- Payment Card Industry Payment Applications - Data Security Standard (PCI PA-DSS) https://www.pcisecuritystandards.org/security_standards/index.php
- Payment Card Industry Data Security Standard (PCI DSS) https://www.pcisecuritystandards.org/security_standards/index.php
- Open Web Application Security Project (OWASP) http://www.owasp.org
- Center for Internet Security (CIS) Benchmarks (used for OS Hardening) https://benchmarks.cisecurity.org/downloads/multiform/

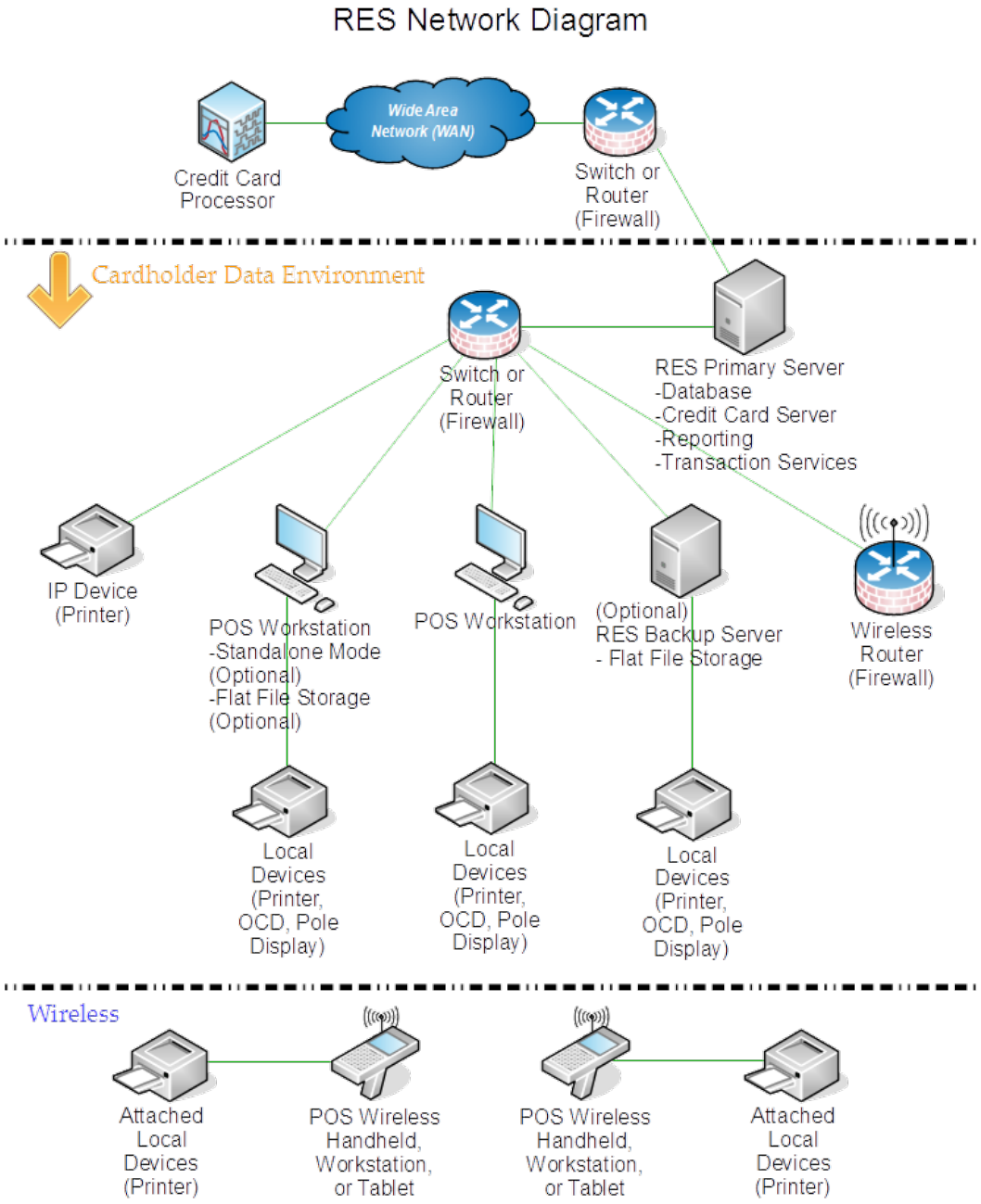
Payment Application Summary

Payment Application Name	Oracle Hospitality RES 3700	**Payment Application Version**	5.7.X.X		
Payment Application Description	RES 3700 is a complete Point-of-Sale (POS) application that is used by a variety of food and beverage merchants. It is capable of processing and reporting on electronic payments without any additional components.				
Typical Role of the Payment Application	RES 3700 is typically used in Full Service and Quick Service restaurants.				
Target Market for Payment Application (check all that apply)	☐ Retail	☐ Processors	☐ Gas/Oil		
	☐ e-Commerce	☐ Small/medium merchants			
	☒ Others (please specify): Restaurant and Hospitality				
Stored Cardholder Data	The following is a brief description of files and tables that store cardholder data.				
	File or Table Name	Description of Stored Cardholder Data			
	See Appendix B.				
	Individual access to cardholder data is logged as follows: No clear access to clear-text PAN is allowed by RES 3700.				
Components of the Payment Application	The following are the application-vendor-developed components which comprise the payment application:				
	See Appendix C.				
Required Third Party Payment Application Software	The following are additional third party payment application components required by the payment application:				
	None.				
Supported Database Software	The following are database management systems supported by the payment application:				
	SAP SQL Anywhere Version 17.				
Other Required Third Party Software	The following are other third party software components required by the payment application:				
	• Microsoft .NET Framework Version 4.6.2 • Microsoft Visual C++ Runtime Version 14 • SAP Crystal Reports Runtime for .NET 4.0 Version 13				
Supported Operating	The following are Operating Systems supported or required by the payment application:				

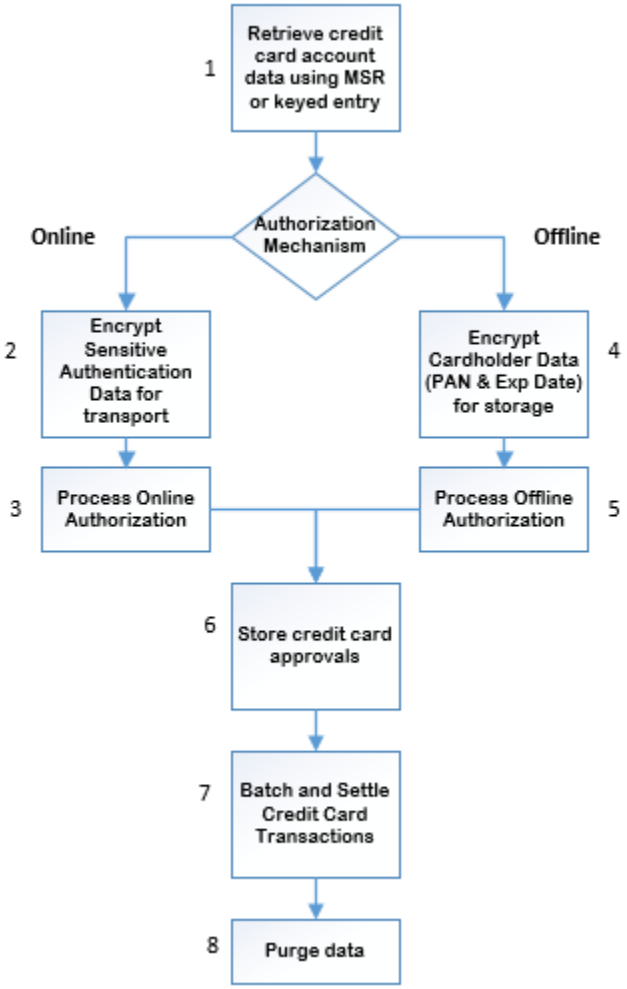
<table>
<tr><td>System(s)</td><td>RES 3700 Server:
Microsoft Windows 7
Microsoft Windows 10
Microsoft Windows Server 2008 R2
Microsoft Windows Server 2012 R2
Microsoft Windows Server 2016
RES 3700 Clients:
Microsoft Windows Compact Edition (CE) 6
Microsoft Windows Embedded Compact 7
Microsoft Windows 7
Microsoft Windows 8.1
Microsoft POSReady 2009
Microsoft POSReady 7</td></tr>
<tr><td>Payment Application Authentication</td><td>Application users are created and stored in the same database used by the core product. A user is assigned a password that must confirm to the standard complexity rules. This password is then hashed using: SHA-256, random salt, random number of iterations between 10,000 and 99,999 iterations.</td></tr>
<tr><td>Payment Application Encryption</td><td>The entire database is encrypted using AES-256.
Sensitive data stored within the database is encrypted at the column level with AES-256.
Sensitive data transmitted within the local, private POS network is encrypted with RSA-2048.
The details of this topic are covered in Cardholder Data Encryption & Key Management (PA-DSS 2.3, 2.4, and 2.5).</td></tr>
<tr><td>Supported Payment Application Functionality</td><td><table>
<tr><td>☐</td><td>Automated Fuel Dispenser</td><td>☐</td><td>POS Kiosk</td><td>☐</td><td>Payment Gateway/ Switch</td></tr>
<tr><td>☐</td><td>Card-Not-Present</td><td>☐</td><td>POS Specialized</td><td>☐</td><td>Payment Middleware</td></tr>
<tr><td>☐</td><td>POS Admin</td><td>☐</td><td>POS Suite/General</td><td>☐</td><td>Payment Module</td></tr>
<tr><td>☒</td><td>POS Face-to-Face/POI</td><td>☐</td><td>Payment Back Office</td><td>☐</td><td>Shopping Card & Store Front</td></tr>
</table></td></tr>
<tr><td>Payment Processing Connections</td><td>The architecture of the RES 3700 uses modules, known as Credit Card Drivers, to implement the details of interfacing to Payment Processors.</td></tr>
<tr><td></td><td></td></tr>
</table>

Description of Listing Versioning Methodology	Oracle implements wildcard versioning and follows a versioning methodology for the application in the format of [N].[N].[N].[N] (where N represents a number): • Changes made at the Major level include architectural changes to the application and impact PA-DSS requirements or the security of the application. • Changes made at the Minor level include minor changes to the application that may or may not impact PA-DSS requirements. o Additional hardware platform and OS support can be added at the Minor level that may result in high level impact to PA-DSS requirements. • Changes at the Patch level include one or more changes made at the Interim level, and do not impact PA-DSS requirements or the security of the application. • Changes at the Interim level do not impact PA-DSS requirements or the security of the application. The versions of the payment application listed on the PCI SSC web site are listed as Major.Minor.X.X.

Typical Network Implementation



Credit/Debit Cardholder Dataflow Diagram



1. Credit card data is entered into the RES Point-of-Sale (POS) in the following ways:
   - Operator manually enters the account number and expiration date.
   - An unencrypted Mag Stripe Reader (MSR) generates raw track data.
   - An encrypting MSR generates encrypted track data and a hashed account number that is used to determine whether the card has been previously used on the same guest check.

   RES may request additional information such as the Address Verification System (AVS) or the Card Verification Value (CVV).
2. The POS encrypts the Sensitive Authentication Data (including AVS and CVV if collected) for transport using a public key securely maintained by the POS.

   The POS does not encrypt the cardholder name, because it must be available for printing on a Credit Authorization Voucher.
3. The POS transmits the encrypted data and authorization amount to the Credit Card Server (CCS) on either the Primary Server or the Backup Server. The CCS decrypts and passes the data to the Credit Card Driver (CCD), which is an in-process dynamic

link library (dll). The CCD formats and sends the request to the Credit Card Processor (CCP) using the appropriate encryption for the processor-specific protocol. When the CCD receives a response from the CCP, it interprets the response and returns Approved or Decline to the POS.

4. The POS encrypts the PAN and Expiration date using a public key securely maintained by the POS. The POS assumes the authorization will be approved, and stores the encrypted data in a flat file database.

   The POS does not encrypt the cardholder name, because it must be available for printing on a Credit Authorization Voucher.

5. Upon returning to normal operation, the POS sends the offline transactions to the RES Server for insertion into the standard POS database.
6. The POS maintains the authorization data with the guest check and uses RESDBS to add the data to the database on the Primary Server. RESDBS decrypts the transport-encrypted authorization data and then re-encrypts it for storage in the RES database.

   If the transaction involves a Tender operation, the POS associates the tender with the authorization and applies the tender. Typically on a schedule of once per day, the POS groups credit card tenders on closed checks in a Batch, which can then be settled.

7. The settlement application passes the data encryption key to a stored procedure for each batch. The database decrypts the data and sends a result set to the CCS as a local, out-of-process COM server. The CCS sends the batch data to the CCD, which formats and sends the settlement messages to the CCP using the appropriate encryption for the processor-specific protocol.
8. RES deletes encrypted sensitive data from the transaction details along with the rest of the transaction details after 15 day.

   RES deletes encrypted sensitive data from batch detail tables after a configurable time, which by default is set to and recommended to be 14 days.

   If the environment uses Transaction Vault, sensitive data is only stored when performing an offline authorization. RES then deletes encrypted sensitive data when receiving the Transaction Vault key prior to settlement.

Difference between PCI Compliance and PA-DSS Validation

As the software and payment application developer, our responsibility is to be PA-DSS validated. We have tested, assessed, and validated the payment application against PA-DSS Version 3.2 with our independent assessment firm (PAQSA) to ensure that our platform conforms to industry best practices when handling, managing, and storing payment-related information.

The PA-DSS Validation is intended to ensure that Oracle Hospitality RES 3700 will help you facilitate and maintain PCI Compliance with respect to how the payment application handles user accounts, passwords, encryption, and other payment data related information.

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

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

PCI Compliance is an assessment of your actual server (or hosting) environment called the Cardholder Data Environment (CDE). It is the responsibility of you, as the merchant, and your hosting provider to work together to use PCI compliant architecture with proper hardware & software configurations and access control procedures.

The 12 Requirements of the PCI DSS:

Build and Maintain a Secure Network and Systems

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

Protect Cardholder Data

3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

5. Protect all systems against malware and regularly update anti-virus software or programs
6. Develop and maintain secure systems and applications

Implement Strong Access Control Measures

7. Restrict access to cardholder data by business need-to-know
8. Identify and authenticate access to system components
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 for all personnel

2 Considerations for the Implementation of Payment Application in a PCI-Compliant Environment

The following areas must be considered for proper implementation in a PCI-Compliant environment:

- Remove Historical Sensitive Authentication Data
- Handling of Sensitive Authentication Data
- Secure Deletion of Cardholder Data
- All PAN is masked by default
- Cardholder Data Encryption & Key Management
- Removal of Historical Cryptographic Material

Remove Historical Sensitive Authentication Data (PA-DSS 1.1.4)

Sensitive Authentication Data (SAD) includes security-related information (including but not limited to card validation codes/values, full track data (from the magnetic stripe or equivalent on a chip), PINs, and PIN blocks) used to authenticate cardholders and/or authorize payment card transactions. Refer to the Glossary of Terms, Abbreviations, and Acronyms in the PCI SSC for the definition of Sensitive Authentication Data.

The following previous versions of Oracle Hospitality RES 3700 stored SAD, including Track 1 / Track 2 data:

- RES 3.2 SP7 HF4 or lower

Historical SAD stored by previous versions of Oracle Hospitality RES 3700 must be securely deleted and removal is absolutely necessary for PCI DSS compliance. Older versions of Oracle Hospitality RES 3700 that stored SAD were only supported on operating systems that are no longer supported. Because of this limitation, there is no means for a system that may have stored SAD to be upgraded to the current version of Oracle Hospitality RES 3700.

Handling of Sensitive Authentication Data (PA-DSS 1.1.5)

Oracle Hospitality does not store Sensitive Authentication Data (SAD) for any reason, and we strongly recommend that you do not do this either. However, if for any reason you should do so, the following guidelines must be followed when dealing with SAD used for pre-authorization (swipe data, validation values or codes, PIN or PIN block data):

- Collect SAD 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 such data while stored
- Securely delete such data immediately after use

Secure Deletion of Cardholder Data (PA-DSS 2.1)

The following guidelines must be followed when dealing with Cardholder Data (Primary Account Number (PAN); Cardholder Name; Expiration Date; or Service Code):

- A customer defined retention period must be defined with a business justification.
- Cardholder data exceeding the customer-defined retention period or when no longer required for legal, regulatory, or business purposes must be securely deleted.
- For the locations of the cardholder data you must securely delete, see Appendix B Stored Cardholder Data.
- RES 3700 automatically securely deletes Cardholder Data by overwriting memory with 0's.
- All underlying software (this includes operating systems and/or database systems) must be configured to prevent the inadvertent capture of PAN. Instructions for configuring the underlying operating systems and/or databases can be found in Appendix A.

All PAN is Masked by Default (PA-DSS 2.2)

Oracle Hospitality RES 3700 masks all PAN by default in all locations that display PAN (screens, paper receipts, printouts, reports, etc.) by displaying only the last 4 digits.

The payment application displays PAN in the following locations:

- Operator Display
- Guest check receipt – masks all but the last four digits of the PAN. No expiration date.
- CA voucher receipt – masks all but the last four digits of the PAN. No expiration date.
- CC Batch Detail Report – masks all but the last four digits of the PAN. Masks the expiration date.

  Note: You can enable the **Do not mask the first 6** option under **Tender/Media** and then **CC Tender** to preserve the first 6 digits and the last 4 digits. When this option is enabled, the Credit Card Batch Detail Report displays the first 6 and the last 4 digits of the Account Number.

RES 3700 does not have the ability to display full PAN for any reason and therefore there are no configuration details to be provided as required for PA-DSS v3.2.

Cardholder Data Encryption & Key Management (PA-DSS 2.3, 2.4, and 2.5)

Oracle Hospitality RES 3700 does store cardholder data and does not have the ability to output PAN data for storage outside of the payment application. All PAN must be rendered unreadable anywhere it is stored (including data on portable digital media, backup media, and in logs). The payment application uses an encryption methodology with statically generated keys to automatically encrypt all locations/methods where cardholder data is stored.

The payment application does not output PAN for use or storage in a merchant's environment for any reason therefore there are no location or configuration details to provide as required by PA-DSS v3.2.

Oracle Hospitality RES 3700 does not have a debugging mode that could write PAN to debugging logs.

Oracle Hospitality RES 3700 uses a static key encryption methodology

- Generation of strong cryptographic keys.
    - RES generates AES-256 encryption keys using a proprietary algorithm that consists of SHA-2 hashing and a random iteration count.
    - The RSA-2048 keys are generated using the MS Crypto API.
- Secure cryptographic key distribution.
  RES 3700 programmatically generates keys and does not distribute them outside of the system.
- Secure cryptographic key storage.
    - The AES-256 encryption keys are never stored. The passphrases used to derive the AES-256 encryption keys are encrypted using the Microsoft DPAPI using entropy derived from a site-specific passphrase that is also encrypted using the MS DPAPI.
    - The RSA-2048 are stored encrypted using the Microsoft DPAPI using entropy derived from a site-specific passphrase that is also encrypted using the MS DPAPI.
- Cryptographic key changes for keys that have reached the end of their crypto period.
    - Oracle Hospitality RES 3700 does not enforce key changes at the end of the defined crypto period. Merchants can rotate any of the keys independently at will.
- Retire or replace keys when the integrity of the key has been weakened and/or when known or suspected compromise. Whenever a key/passphrase is changed, the new key/passphrase replaces the old key/passphrase and the old key/passphrase is no longer retained.
- Oracle Hospitality RES 3700 does not support manual clear-text cryptographic key-management. The passphrases used to derive the database encryption keys and sensitive data encryption keys are automatically generated for the user, and are unknown to any user.
- Oracle Hospitality RES 3700 does not allow substitution of cryptographic keys.

Removal of Historical Cryptographic Material (PA-DSS 2.6)

Oracle Hospitality RES 3700 has the following versions that previously encrypted cardholder data:

- Version 4.0 – 4.12
- Version 5.0 – 5.5

If the historical Cardholder data is no longer needed, the following must be completed to ensure PCI Compliance:

- All cryptographic material for previous versions of the payment application (encryption keys and encrypted cardholder data) must be rendered irretrievable when no longer needed.

- Oracle Hospitality RES 3700 automatically decrypts the historical passphrases and securely replaces them using the updated mechanisms for securing passphrases. The previously encrypted cardholder data is re-encrypted using the newer algorithm automatically during the upgrade process.
- You must restrict access to the encryption keys/passphrases to the fewest number of custodians necessary.
- You must store the encryption keys/passphrases securely in the fewest possible locations and forms.

Set up Strong Access Controls (PA-DSS 3.1 and 3.2)

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.

There are no default accounts within the application that have administrative access.

All authentication credentials are generated and managed by the application. Secure authentication is enforced automatically by the payment application for all credentials by the completion of the initial installation and for any subsequent changes (for example, any changes that result in user accounts reverting to default settings, any changes to existing account settings, or changes that generate new accounts or recreate existing accounts). To maintain PCI DSS compliance the following 11 points must be followed per the PCI DSS:

1. The payment application must not use or require the use of default administrative accounts for other necessary or required software (for example, database default administrative accounts) (PCI DSS 2.1 / PA-DSS 3.1.1)
2. The payment application must enforce the changing of all default application passwords for all accounts that are generated or managed by the application, by the completion of installation and for subsequent changes after the installation (this applies to all accounts, including user accounts, application and service accounts, and accounts used by Oracle Hospitality for support purposes) (PCI DSS 2.1 / PA-DSS 3.1.2)
3. The payment application must assign unique IDs for all user accounts. (PCI DSS 8.1.1 / PA-DSS 3.1.3)
4. The payment application must provide at least one of the following three methods to authenticate users: (PCI DSS 8.2 / PA-DSS 3.1.4)
    a. Something you know, such as a password or passphrase
    b. Something you have, such as a token device or smart card
    c. Something you are, such as a biometric
5. The payment application must NOT require or use any group, shared, or generic accounts and passwords (PCI DSS 8.5 / PA-DSS 3.1.5)
6. The payment application requires passwords must to be at least 7 characters and includes both numeric and alphabetic characters (PCI DSS 8.2.3 / PA-DSS 3.1.6)
7. The payment application requires passwords to be changed at least every 90 days (PCI DSS 8.2.4 / PA-DSS 3.1.7)

8. The payment application keeps password history and requires that a new password is different than any of the last four passwords used (PCI DSS 8.2.5 / PA-DSS 3.1.8)
9. The payment application limits repeated access attempts by locking out the user account after not more than six logon attempts (PCI DSS 8.1.6 / PA-DSS 3.1.9)
10. The payment application sets the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID. (PCI DSS 8.1.7 / PA-DSS 3.1.10)
11. The payment application requires the user to re-authenticate to re-activate the session if the application session has been idle for more than 15 minutes. (PCI DSS 8.1.8 / PA-DSS 3.1.11)

You must assign strong passwords to any default accounts (even if they won't be used), and then disable or do not use the accounts.

Changing the Default Database Encryption Key

1. Launch the Database Manager and click **Encryption Keys**.
2. Select or deselect the following:
   - **Change Database Key**: change the passphrase used to generate the database encryption key that is required for starting the database. If you select this option, a new random passphrase is generated and the current one is replaced.
   - **Change Data Key**: change the passphrase used to generate the encryption key that is used to encrypt sensitive data. If you select this option, a new random passphrase is generated and the current one is replaced.
   - **Change Transport Key**: generate a new pair of RSA-2048 encryption keys that is used for encrypting data for transport between the server and workstations.

Warning: Your system must be at the Database level to change any key, and changing the database key will rebuild the database.

When performing key rotation, Database Manager unloads and reloads the entire database and re-encrypts all historical data. This operation may take several hours.

---

3. Click **Change Encryption Keys** to change the selected keys.

Changing User Passwords

1. Make sure you have sufficient privileges for changing passwords. To configure these privileges in POS Configurator, select the **Employees** tab, click **Employee Classes**, select the **Privileges** tab, and then select the **Privilege Options** tab.
2. Launch the Database Manager and click **Users\Passwords**.
3. To change the password for an existing user:
   a. Select **Change Users Password**.
   b. Select the **User Name** from the drop-down list.
   c. Enter the new password and click **Change Password**.
4. To add a new user account:
   a. Select **Create New User**.
   b. Enter a user name and password, and then click **Change Password**.

Oracle Hospitality RES 3700 does not include any additional applications or databases that require the account and password criteria from the above 11 requirements.

PA-DSS 3.2: Control access, via unique username and PCI DSS-compliant complex passwords, to any PCs or servers with payment applications and to databases storing cardholder data.

Properly Train and Monitor Admin Personnel

It is your responsibility to institute proper personnel management techniques for allowing admin user access to cardholder data, site data, etc. In most systems, a security breach is the result of unethical personnel. Pay special attention to whom you trust into your admin site and who you allow to view full decrypted and unmasked payment information.

Log Settings must be Compliant (PA-DSS 4.1.b and 4.4.b)

4.1.b: Oracle Hospitality RES 3700 has PA-DSS compliant logging enabled by default. This logging is not configurable and may not be disabled. Disabling or subverting the logging function of Oracle Hospitality RES 3700 in any way will result in non-compliance with PCI DSS. This logging is integrated with the Microsoft® Event Viewer and is created in a custom log named MICROS Security Log. It is accessed and managed using the same mechanism as the standard Microsoft® Event logs.

Implement automated assessment trails for all system components to reconstruct the following events:

10.2.1 All individual user accesses to cardholder data from the application

10.2.2 All actions taken by any individual with administrative privileges in the application

10.2.3 Access to application audit trails managed by or within the application

10.2.4 Invalid logical access attempts

10.2.5 Use of the application's identification and authentication mechanisms (including but not limited to creation of new accounts, elevation of privileges, etc.) and all changes, additions, deletions to application accounts with root or administrative privileges

10.2.6 Initialization, stopping, or pausing of the application audit logs

10.2.7 Creation and deletion of system-level objects within or by the application

Record at least the following assessment trail entries for all system components for each event from 10.2.x above:

10.3.1 User identification

10.3.2 Type of event

10.3.3 Date and time

10.3.4 Success or failure indication

10.3.5 Origination of event

10.3.6 Identity or name of affected data, system component, or resource.

Disabling or subverting the logging function of Oracle Hospitality RES 3700 in any way will result in non-compliance with PCI DSS.

4.4.b: Oracle Hospitality RES 3700 facilitates centralized logging by using industry standard logging based on Microsoft Windows Event Logging.

3 PCI-Compliant Wireless Settings (PA-DSS 6.1.a and 6.2.b)

Oracle Hospitality RES 3700 does not support wireless technologies and the following guidelines for secure wireless settings must be followed per PCI Data Security Standard 1.2.3, 2.1.1 and 4.1.1:

1.2.3: Perimeter firewalls must be installed between any wireless networks and systems that store cardholder data, and these firewalls must deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.

2.1.1: Change wireless vendor defaults per the following 5 points:

1. Encryption keys must be changed from default at installation, and must be changed anytime anyone with knowledge of the keys leaves the company or changes positions.
2. Default SNMP community strings on wireless devices must be changed.
3. Default passwords/passphrases on access points must be changed.
4. Firmware on wireless devices must be updated to support strong encryption for authentication and transmission over wireless networks.
5. Other security-related wireless vendor defaults, if applicable, must be changed.

1.2.3: Perimeter firewalls must be installed between any wireless networks and systems that store cardholder data, and these firewalls must deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.

4.1.1: Industry best practices (for example, IEEE 802.11.i) must be used to implement strong encryption for authentication and transmission of cardholder data.

Note: The use of WEP as a security control was prohibited as of June 30, 2010.

4 Services and Protocols (PA-DSS 8.2.c)

Oracle Hospitality RES 3700 does not require the use of any insecure services or protocols. Oracle Hospitality RES 3700 requires the following:

- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper
- World Wide Web Publishing Service

RES 3700 also uses the TCP protocol for internal (LAN) communication.

Never Store Cardholder Data on Internet-Accessible Systems (PA-DSS 9.1.c)

Never store cardholder data on Internet-accessible systems (e.g., web server and database server must not be on same server.)

PCI-Compliant Remote Access (PA-DSS 10.1)

The PCI standard requires that if employees, administrators, or vendors are granted remote access to the payment processing environment; access should be authenticated using a two-factor authentication mechanism. The means two of the following three authentication methods must be used:

1. Something you know, such as a password or passphrase
2. Something you have, such as a token device or smart card
3. Something you are, such as a biometric

PCI-Compliant Delivery of Updates (PA-DSS 7.2.3, 10.2.1.a)

Oracle Hospitality RES 3700 delivers patches and updates in a secure manner:

- **How you communicate the availability of new patches and updates to customers.**

  Normally, email notification is sent to the customer.

- **Timely development and deployment of patches and updates.**
  Starting in January 2011, Critical Patch Updates (CPU) are released on the Tuesdays closest to the 17th of the months of January, April, July, and October. The Critical Patch Updates and Security Alerts page on Oracle's web site always list the dates of release for the next four Critical Patch Updates, thus effectively providing a one-year notice to customers.

  On the Thursday before the release of each CPU, a PreRelease Advisory is published by Oracle. Both the PreRelease Advisory and the CPU Release Documentation are posted on the Critical Patch Updates and Security Alerts page on Oracle's web site located at
  http://www.oracle.com/technetwork/topics/security/alerts086861.html.

- **Software patches and updates are delivered from the My Oracle Support webpage.**

  As outlined in the *Oracle Customer Support Security Practices* document:

My Oracle Support is the key website service for providing interactions with Global Customer Support (GCS) for Oracle programs and hardware, including (Service Request) SR access, knowledge search / browse, support communities and technical forums.

My Oracle Support employs the following security controls:

- My Oracle Support is an HTTPS extranet website service using TLS 1.2 encryption for data transmitted over the Internet
- Your registration on My Oracle Support uses a unique Customer Support Identifier (CSI) linked to your Support contract(s)
- Each CSI has at least one customer-designated My Oracle Support Customer User Administrator. Your Customer User Administrators approve / reject requests from users for new accounts and CSI associations to existing accounts; you are responsible for provisioning and de-provisioning your users on a timely basis.
- Your Customer User Administrator can control which features your users may access on My Oracle Support (for example, write access to SRs can be enabled or disabled for a given user)
- Your Customer User Administrator can view users associated with its CSIs, and has the ability to remove access privileges for users
- My Oracle Support SR Attachments (documents uploaded as part of the My Oracle Support SR create / update process) are saved into a dedicated GCS repository. Your communications with this repository are secured using Hypertext Transfer Protocol over Secure Socket Layer (https).

- **Delivery in a manner that maintains the integrity of the deliverable.**

  When a patch is downloaded from My Oracle Support's Automated Release Updates (ARU) page, the patch's digital signature should be verified. This is a relatively simple manual process.

  There are several free file integrity validation tools available on the web that can verify the Message Digest 5 (MD5) or Secure Hash Algorithm (SHA-1) checksum for the downloaded patch file. You can use a tool like the Microsoft File Checksum Integrity Verifier, or a similar MD5 and SHA-1 checksum utility.

  Choose and download the validation tool that you want to use. Once a patch has been downloaded, run your file integrity validation tool against it and compare the hash value generated by the validation tool to the hash value that corresponds to the patch on the ARU page. Both hash values should exactly match each other to confirm the file's integrity. Once you have validated the patch file's integrity, deploy the patch at a time of your choosing.

PCI-Compliant Remote Access (PA-DSS 10.3.2.a)

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

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

As outlined in *Oracle Global Customer Support Security Practices*, Oracle Global Customer Support (GCS) uses two main collaboration tools to review issues reported to Oracle: Oracle Web Conferencing (OWC) for programs and Oracle Shared Shell for hardware. Both tools share the following common features:

- You control and participate actively in all sessions. You control the session, what navigation is undertaken, what data is displayed and what commands are issued. You also have the ability to shut down the session at any time for any reason.
- Secure Socket Layer (SSL) encryption is provided for data transmitted over the Internet.

Additional details about OWC and Shared Shell:

If users and hosts within the payment application environment may need to use third-party remote access software such as Oracle Web Conferencing (OWC), Oracle Shared Cell, to access other hosts within the payment processing environment, special care must be taken.

In order 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).

When requesting support from a vendor, reseller, or integrator, customers are advised to take the following precautions:

- Change default settings (such as usernames and passwords) on remote access software (e.g. VNC).
- Allow connections only from specific IP and/or MAC addresses.
- Use strong authentication and complex passwords for logins according to PA-DSS 3.1.1 – 3.1.10 and PCI DSS 8.1, 8.3, and 8.5.8-8.5.15.
- Enable encrypted data transmission according to PA-DSS 12.1 and PCI DSS 4.1.
- Enable account lockouts after a certain number of failed login attempts according to PA-DSS 3.1.8 and PCI DSS 8.5.13.
- Require that remote access take place over a VPN via a firewall as opposed to allowing connections directly from the internet.
- Enable logging for auditing purposes.
- Restrict access to customer passwords to authorized reseller/integrator personnel.
- Establish customer passwords according to PA-DSS 3.1.1 – 3.1.10 and PCI DSS Requirements 8.1, 8.2, 8.4, and 8.5.

Data Transport Encryption (PA-DSS 11.1.b)

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

PCI DSS requirement 4.1: Use strong cryptography and security protocols such as transport layer security (TLS 1.1/TLS 1.2) and Internet protocol security (IPSEC) to safeguard sensitive cardholder data during transmission over open, public networks.

Examples of open, public networks that are in scope of the PCI DSS are:

- The Internet
- Wireless technologies
- Global System for Mobile Communications (GSM)
- General Packet Radio Service (GPRS)

Refer to the Dataflow diagram for an understanding of the flow of encrypted data associated with Oracle Hospitality RES 3700

PCI-Compliant Use of End User Messaging Technologies (PA-DSS 11.2.b)

Oracle Hospitality RES 3700 does not allow or facilitate the sending of PANs via any end user messaging technology (for example, e-mail, instant messaging, and chat).

Non-Console Administration and Multi-Factor Authentication (PA-DSS 12.1, 12.2)

Oracle Hospitality RES 3700 does not implement non-console administration.

If non-console administration is used in your environment you must follow the same rules as for remote access.

- Encrypt all access connections
- Use multi-factor authentication

Network Segmentation

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

Refer to the standardized Network diagram for an understanding of the flow of encrypted data associated with Oracle Hospitality RES 3700.

Maintain an Information Security Program

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

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

- Read the PCI DSS in full and perform a security gap analysis. Identify any gaps between existing practices in your organization and those outlined by the PCI requirements.
- Once the gaps are identified, determine the steps to close the gaps and protect cardholder data. Changes could mean adding new technologies to shore up firewall

and perimeter controls, or increasing the logging and archiving procedures associated with transaction data.

- Create an action plan for on-going compliance and assessment.
- Implement, monitor and maintain the plan. Compliance is not a one-time event. Regardless of merchant or service provider level, all entities should complete annual self-assessments using the PCI Self-Assessment Questionnaire.
- Call in outside experts as needed.

Application System Configuration

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

- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2008 R2
- Microsoft Windows 10
- Microsoft Windows 8.1
- Microsoft Windows 7 SP1
- Microsoft Windows CE 6
- Microsoft Windows Embedded Compact 7
- Microsoft POSReady 2009
- Microsoft POSReady 7

Appendix A Inadvertent Capture of PAN

This appendix provides instructions for addressing the inadvertent capture of PAN on the following supported operating systems:

- Microsoft Windows 8
- Microsoft Windows 7

Microsoft Windows 8

Disable System Restore

1. Right-click **Computer** and select **Properties**.
2. On the System dialog box, click **Advanced system settings**.
3. On the **System Protection** tab, click **Configure**.
4. Select **Turn off system protection**, click **Apply**, and then click **OK** until you return to the System dialog box.
5. Restart the computer.

Encrypt PageFile.sys

Your hard disk must be formatted using NTFS to perform this operation.

1. Click the **Start** button and enter `cmd`.
2. Right-click **Command Prompt** and select **Run as Administrator**.
3. Enter the command: `fsutil behavior set EncryptPagingFile 1`
   To disable encryption, enter 0 instead of 1.
4. Enter the command: `fsutil behavior query EncryptPagingFile`
5. Verify that the command prompt returns: `EncryptPagingFile = 1`

Clear the System PageFile.sys on Shutdown

You can enable the option to clear PageFile.sys on system shutdown to purge temporary data. This ensures that information such as system and application passwords and cardholder data are not inadvertently kept in the temporary files. Enabling this feature may increase the time it takes for system shutdown.

1. Click the **Start** button and enter `regedit`.
2. Right-click Registry Editor and select **Run as Administrator**.
3. Navigate to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\
4. Right-click ClearPageFileAtShutdown and select **Modify**.
   If ClearPageFileAtShutdown does not exist, right-click the Memory Management folder, select **New**, and select **DWORD (32-bit) Value**.
5. Set the **Value data** field to 1 and click **OK**.

Disable System Management of PageFile.sys

1. Right-click **Computer** and select **Properties**.
2. On the System dialog box, click **Advanced system settings**.
3. On the **Advanced** tab, click **Settings** for Performance.
4. On the **Advanced** tab, click **Change**.
5. Deselect **Automatically manage page file size for all drives**, select **Custom size**, and set the following fields:
    a. Initial Size: the amount of Random Access Memory (RAM) available.
    b. Maximum Size: 2x the amount of RAM.
6. Click **OK** until you return to the System dialog box.
7. Restart the computer.

Disable Error Reporting

1. Click the **Start** button and enter `Control Panel`.
2. Click **Control Panel**, then click **Action Center**.
3. Click **Change Action Center settings**, then click **Problem reporting settings**.
4. Select **Never check for solutions**, then click **OK**.

Microsoft Windows 7

Disable System Restore

1. Right-click **Computer** and select **Properties**.
2. On the System dialog box, click **Advanced system settings**.
3. On the **System Protection** tab, click **Configure**.
4. Select **Turn off system protection**, click **Apply**, and then click **OK** until you return to the System dialog box.
5. Restart the computer.

Encrypt PageFile.sys

Your hard disk must be formatted using NTFS to perform this operation.

1. Click the **Start** button and enter `cmd` in the search field.
2. Right-click cmd.exe and select **Run as Administrator**.
3. Enter the command: `fsutil behavior set EncryptPagingFile 1`
   To disable encryption, enter 0 instead of 1.
4. Enter the command: `fsutil behavior query EncryptPagingFile`
5. Verify that the command prompt returns: `EncryptPagingFile = 1`

Clear the System PageFile.sys on Shutdown

You can enable the option to clear PageFile.sys on system shutdown to purge temporary data. This ensures that information such as system and application passwords and

cardholder data are not inadvertently kept in the temporary files. Enabling this feature may increase the time it takes for system shutdown.

1. Click the **Start** button and enter `regedit` in the search field.
2. Right-click regedit.exe and select **Run as Administrator**.
3. Navigate to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\
4. Right-click ClearPageFileAtShutdown and select **Modify**.
   If ClearPageFileAtShutdown does not exist, right-click the Memory Management folder, select **New**, and select **DWORD (32-bit) Value**.
5. Set the **Value data** field to 1 and click **OK**.

Disable System Management of PageFile.sys

1. Right-click **Computer** and select **Properties**.
2. On the System dialog box, click **Advanced system settings**.
3. On the **Advanced** tab, click **Settings** for Performance.
4. On the **Advanced** tab, click **Change**.
5. Deselect **Automatically manage page file size for all drives**, select **Custom size**, and set the following fields:
   a. Initial Size: the amount of Random Access Memory (RAM) available.
   b. Maximum Size: 2x the amount of RAM.
6. Click **OK** until you return to the System dialog box.
7. Restart the computer.

Disable Error Reporting

1. Click the **Start** button, select **Control Panel**, and then click **Action Center**.
2. Click **Change Action Center settings**, then click **Problem reporting settings**.
3. Select **Never check for solutions**, then click **OK**.

Appendix B Stored Cardholder Data

Database

Data	Table	Column	State
Account Number	cc_auth_dtl	cc_acct_num	Truncated to last 4 digits
Account Number	cc_batch_xfer_item_status	cc_acct_num	Truncated to last 4 digits
Account Number	cc_item_dtl_temp	cc_acct_num	Truncated to last 4 digits
Account Number	cc_vchr_dtl	cc_acct_num	Truncated to last 4 digits
Account Number	ref_dtl	ref	Truncated to last 4 digits
Account Number	tmed_dtl	cc_acct_num	Truncated to last 4 digits
Account Number	trans_archive_dtl	P_cc_acct_num	Truncated to last 4 digits
Account Number	trans_archive_dtl	R_ref	Truncated to last 4 digits
Account Number	cc_auth_dtl	cc_acct_num_ex	Truncated to first 6 and last 4/Blank
Account Number	cc_batch_item_dtl	cc_acct_num	Truncated to first 6 and last 4/last 4
Account Number	encrypt_cc_value_dtl	hashcode	Hashed Value
Account Number	encrypt_cc_value_dtl	cc_acct_num	Encrypted
Account Number	encrypt_cc_value_dtl	track_data (contains PAN and Exp Date ONLY)	Encrypted
Card Holder Name	cc_auth_dtl	customer_name	Clear text
Card Holder Name	cc_batch_item_dtl	customer_name	Clear text
Card Holder Name	encrypt_cc_value_dtl	customer_name	Encrypted
Expiration Date	cc_auth_dtl	expiration_date	Masked/Clear text
Expiration Date	cc_batch_item_dtl	expiration_date	Masked/Clear text
Expiration Date	cc_batch_xfer_item_status	expiration_date	Masked/Clear text
Expiration Date	cc_item_dtl_temp	expiration_date	Masked/Clear text
Expiration Date	cc_vchr_dtl	expiration_date	Masked/Clear text
Expiration Date	tmed_dtl	expiration_date	Masked/Clear text
Expiration Date	encrypt_cc_value_dtl	exp_date	Encrypted
Expiration Date	encrypt_cc_value_dtl	track_data (contains PAN and Exp Date ONLY)	Encrypted
Track 1 EMSR	encrypt_cc_value_dtl	emsr_track_1	Encrypted
Track 2 EMSR	encrypt_cc_value_dtl	emsr_track_2	Encrypted

Unused Database

This schema exists solely for legacy reasons. Track 1/2 data is absolutely never stored.

Data	Table	Column	State
Track 1	cc_auth_dtl	track_1_data	Not Used
Track 1	cc_batch_item_dtl	track_1_data	Not Used
Track 2	cc_auth_dtl	track_2_data	Not Used
Track 2	cc_auth_dtl	etrack2	Not Used
Track 2	cc_batch_item_dtl	track_2_data	Not Used
Track 2	cc_batch_item_dtl	etrack2	Not Used
Track 2	cc_item_dtl_temp	track2_data	Not Used

Files: Backup Server Mode

Data	File Location	State
Account Number	Micros\Res\Pos\Etc\BackupDB\Current\Dtl-(Check sequence number).bin	Truncated to last 4 digits
Account Number	Micros\Res\Pos\Etc\BackupDB\Current\Dtl-(Check sequence number).bin	Truncated to first 6 and last 4
Account Number	Micros\Res\Pos\Etc\BackupDB\Current\Dtl-(Check sequence number).bin	Encrypted
Card Holder Name	Micros\Res\Pos\Etc\BackupDB\Current\Dtl-(Check sequence number).bin	Blank/Clear text
Expiration Date	Micros\Res\Pos\Etc\BackupDB\Current\Dtl-(Check sequence number).bin	Masked
Expiration Date	Micros\Res\Pos\Etc\BackupDB\Current\Dtl-(Check sequence number).bin	Encrypted
Track 1 EMSR	Micros\Res\Pos\Etc\BackupDB\Current\Dtl-(Check sequence number).bin	Encrypted
Track 2 EMSR	Micros\Res\Pos\Etc\BackupDB\Current\Dtl-(Check sequence number).bin	Encrypted

Files: Standalone Mode

Data	File Location	State
Account Number	Micros\Res\Pos\Etc\LocalDB\Current\Checks\Dtl-(Check sequence number).bin	Truncated to last 4 digits
Account Number	Micros\Res\Pos\Etc\LocalDB\Current\Checks\Dtl-(Check sequence number).bin	Truncated to first 6 and last 4
Account Number	Micros\Res\Pos\Etc\LocalDB\Current\Checks\Dtl-(Check sequence number).bin	Encrypted
Card Holder Name	Micros\Res\Pos\Etc\LocalDB\Current\Checks\Dtl-(Check sequence number).bin	Blank/Clear text
Expiration Date	Micros\Res\Pos\Etc\LocalDB\Current\Checks\Dtl-(Check sequence number).bin	Masked
Expiration Date	Micros\Res\Pos\Etc\LocalDB\Current\Checks\Dtl-(Check sequence number).bin	Encrypted
Track 1 EMSR	Micros\Res\Pos\Etc\LocalDB\Current\Checks\Dtl-(Check sequence number).bin	Encrypted
Track 2 EMSR	Micros\Res\Pos\Etc\LocalDB\Current\Checks\Dtl-(Check sequence number).bin	Encrypted

Appendix C Components of the Payment Application

File Name	Description
3700d.exe	System management and status
3700dPS.dll	COM proxy stub for RES logging
AccuClt.dll	Order confirmation board utility
AlertViewerPlugIn.dll	Alert viewer utility
Analyzer.exe	An application to review transaction activity
AppStarter.exe	An application for the client that allows a configurable set of applications to be started
AutoSeqExec.exe	Application to run autosequences and reports
AutoSeqServ.exe	Service for auto sequences and reports
AutoSeqServPS.dll	COM proxy stub for the auto sequence service
autosequence.dll	Utility for auto sequences and reports
BSMdump.exe	Test utility for backup server mode
CaAdapter.dll	credit card authorization utility
CaClient.dll	Client credit card authorizations
cademo.dll	Test driver for credit card transactions
caedc.dll	credit card settlement utility
CALSrv.exe	Client application loader server
CALUWSDiscovery.dll	Network discovery utility for CALSrv.exe
CaTVCa.dll	Trans Vault credit card authorization driver
CaTVCS.dll	Trans Vault credit card settlement driver
CCS.exe	Credit card processing server
CCSPS.dll	COM proxy stub for the credit card server
ci_drv.dll	Caller ID utility
CIServ.dll	Caller ID utility
CIService.exe	Caller ID service
CLControl.exe	Command line interface for Control Panel
CMAutoCloseTill.exe	Cash management close till application
CMBO.exe	Cash management back office application
CMC.dll	Cash management utility
CMS.exe	Cash management service
CMSC.exe	Cash management COM service
CMSCProxy.dll	Cash management utility
CommonUtils.dll	Common utilities
CommonUtils.dll	Common utilities
ComScheduler.exe	Labor Matrix COM scheduler
control.dll	System management and status

File Name	Description
CopyFile.exe	File copy utility
CPanel.exe	Control panel application
CreditCards.exe	Credit card settlement application
CRUFLccy.dll	Currency utility
CRUMCCS.dll	Create settings for the card server
CRUMIFS.dll	Load settings for the interface server
CRUMILDS.dll	Load settings for the ILDS server
CRUMKDS.dll	Load settings for the KDS server
CRUMMAL.dll	Load settings for major account licensing
CRUMMDS.dll	Create the MDS host XML file
CRUMNALDS.dll	Load settings for the NALDS
CRUMOPS.dll	Load settings for Ops
CrumPINpad.dll	Load settings for pinpad devices
CrumPrinters.dll	Create the printer host XML file
CTUtil.exe	Utility to enter and verify the client trust passphrase
DBInterface.dll	Database utility
dbmsConsole.exe	Application starts the dbms console
dbsecurity.dll	Database security
DBSecurity2.dll	Database security and encryption
DbUpdateServer.exe	Service that handles database updates
DbUpdt.exe	Application used to apply updates securely to the database
DeliveryConfig.exe	Application to configure the delivery dispatch screens
DeliveryDispatch.dll	Delivery dispatch utility
DesktopBtnControl.ocx	Micros desktop utility
DM.exe	Database management application
drawengine.dll	Drawing utility
DSM.exe	Distributed services management service
DSMAdapter.dll	Distributed services utility
DSMinterface.dll	Distributed services utility
EJPrint.exe	Electronic journal printing application
EventAdjustmentEngine.dll	Forecasting utility
ExecKDSCmd.exe	Command line interface for KDS
ExportUtility.exe	Data export application
FlushRegistry.exe	WinCE application to clear registry values
Fm.exe	Financial management application
ForecastCfg.exe	Forecast editor application
Forecasting.exe	Forecast generation application
FpRecEng.dll	Finger print recognition and enrollment
GSS.exe	Guest services application

File Name	Description
GSSDataService.exe	Guest services service
gssdb.dll	Guest services utility
gssmsg.dll	Guest services utility
gssops.dll	Guest services utility
HHTHardware.dll	Handheld workstation hardware utility
HRWizards.dll	Human resources utility
HumanResources.exe	Human resources application
Ifs.exe	Interface server service
IfsPS.dll	COM proxy stub for interface server
ilds.exe	International liquor dispenser service
IMicrosPlugin.exe	Micros desktop utility
INQ2GSS.exe	Application to convert touch screen SIM/PMS keys to GSS function keys
Interop.MICROSHWSCRIPTERLib.dll	Hardware interface
Interop.MicrosSecurityLog.dll	Utility to write security events to the event log
InvoicePrint.exe	Application to print invoices
KDSController.exe	Kitchen Display control service
KdsDAI.dll	Kitchen Display utility
KDSDisplay.exe	Kitchen Display Application
KdsSysIntfc.dll	Kitchen Display utility
KdsToPosServ.dll	Kitchen Display utility
LangTransCom.dll	Language translation
LanguagePlugIn.dll	Language utility
lcpanel.exe	Control panel utility
LDSRpt.dll	Liquor dispensing report utility
LicManager.exe	License manager application
LM.exe	Labor Management application
LogAdapter.dll	Logging utility
LogAdapterps.dll	COM proxy stub for log adapter
LogMan.exe	Log Manager application
LogonPlugIn.dll	Logon utility
LogonUI.dll	Dialog to login and change password
LogViewer.exe	Log Viewer application
ManagerProcs.dll	Manager procedures utility
ManProcsGrid.ocx	Display grid used by manager procedures
mBrowser.exe	Manager procedures utility
MBViewer.exe	Menu Board application
McrsCALConfig.dll	CAL utility
McrsCALNet.dll	CAL utility
McrsCALReg.dll	CAL utility

File Name	Description
McrsCALUtils.dll	CAL utility
mcrsMessages.dll	Defines micros messages
McrsOpenSSLHelper.dll	Network communication utility
McrsPlatform.dll	Hardware platform library
McrsRF.dll	Wireless workstation support utility
McrsSendWakeup.exe	Network wakeup utility
MDS3700d.dll	Distributed services processing
MDS3700dAdapter.dll	Distributed services processing
MDS3700dProxy.dll	Distributed services processing
MDSASEQ.dll	Distributed services processing
MDSASEQADAPTER.dll	Distributed services processing
MDSBroker.dll	Distributed services processing
MDSCa.dll	Distributed services processing
MDSCAResponse.dll	Distributed services processing
MDSCaXML.dll	Distributed services processing
MDSClientLicense.dll	Distributed services processing
MDSCM.dll	Distributed services processing
MDSCMAdapter.dll	Distributed services processing
MDSDATATYPES.dll	Distributed services processing
MDSDispatcher.dll	Distributed services processing
MDSHTTPService.exe	Distributed services processing
MDSHTTPTransport.dll	Distributed services processing
MDSIFS.dll	Distributed services processing
MDSIFSADAPTER.dll	Distributed services processing
MDSKds.dll	Distributed services processing
MDSPrinting.dll	Distributed services processing
MDSPrintingProxy.dll	Distributed services processing
MDSRecordSetProxy.dll	Distributed services processing
MDSResDbs.dll	Distributed services processing
MdsResDbsAdapter.dll	Distributed services processing
MdsResDbsProxy.dll	Distributed services processing
MDSSERVICE_PRINTING.dll	Distributed services processing
MDSServices.dll	Distributed services processing
MDSSysUtils.dll	Distributed services processing
MDSSysUtilsCOM.dll	Distributed services processing
MDSSysUtilsProxy.dll	Distributed services processing
MDSUpdateNotify.dll	Distributed services processing
MDSXMLDirectory.dll	Distributed services processing
MenuItemInfo.dll	Menu item information display utility
MessageHelper.dll	Wrapper for Microsoft MSMQ

File Name	Description
MicrosAccess.dll	Logon utility
MicrosCfdTest.exe	System testing utility
MicrosCompress.dll	File compression utility
microsDbms.dll	Module contains routines callable from Sybase SQL
MicrosDesktop.exe	Micros Desktop application
MicrosDevices.dll	WinCE Hardware interface
MicrosExportUtility.dll	Data export utility
MicrosHWScripter.dll	Hardware interface
MicrosHWSWrapper.dll	Hardware interface
MicrosIcons.dll	Icon storage
MicrosRemotingPlugIn.dll	.Net interface utility
MicrosRemotingService.exe	.Net interface
MicrosSequenceGen.dll	String mapping utility
mmx.dll	Micros message exchange - communication for distributed applications
MMX_IP.dll	KDS - Micros message exchange - communication for distributed applications
Nalds.dll	Liquor dispensing utility
OCB.exe	Order confirmation board application
OCB32.exe	Order confirmation board application
OCB32Stop.exe	Order confirmation board application
OCBClient.dll	Order confirmation board utility
ops.exe	Main POS application
OrderingModule.dll	Ordering module utility
PayrollPre.exe	Payroll preprocessing application
pcd.dll	Price confirmation display interface
pcontrol.exe	Print controller server
pcontrolps.dll	COM proxy stub for print controller
pcprint.dll	Printing utility
Periphs.exe	Hardware interface
periphsdll.dll	Hardware interface
Periphsps.dll	COM proxy stub for periphs.exe
PeripsDllmTablet.dll	Hardware interface
PeripsDllWS4.dll	Hardware interface
PinPad.dll	Hardware interface
PM.exe	Product management (inventory) application
pmanager.dll	Printing utility
PMCloseCheck.exe	Product management utility
PMPPC.exe	Product management utility
PMProcedures.exe	Product management utility

File Name	Description
poscfg.exe	POS configuration application
PosToKds.dll	Assembles messages to be sent to the KDS controller
PrintAdapter.exe	Printing utility
PrintAdapterps.dll	COM proxy stub for print adapter
PrintControllerCE.dll	Printing utility
PrintingPlugIn.dll	Printing utility
Printmanager.dll	Printing utility
Procedures.exe	Manager procedures application
RecipeViewer.exe	Displays recipe and prep information
RecipeViewerPlugIn.dll	Displays recipe and prep information
RegMDS.exe	Registry utility
RemoteReboot.exe	Reboot utility
ReportPlugIn.dll	Report utility
ReportPlugInAdapter.dll	Report utility
RESAlertViewer.exe	Displays RES alerts
RESAudioIntegration.dll	Audio utility
resbsm.exe	Backup server service
resbsmPS.dll	COM proxy stub for backup server
resdbs.exe	Database server service
resdbsPS.dll	COM proxy stub for database server
ResPosApi.dll	API interface
ResPrintApi.dll	API printing interface
ResSIMDB.exe	SIM database server interface
ResSIMDBPS.dll	COM proxy stub for ResSIMDB
rotatelog.exe	Logging utility
RptCtrl.dll	Report utility
RptExpl.exe	Report explorer application
rundbms.exe	Database utility
rundbmsdll.dll	Database utility
RvcChkCntImport.dll	Labor management utility
RvcCvrCntImport.dll	Labor management utility
RvcFamGrpCntImport.dll	Labor management utility
RvcFamGrpImport.dll	Labor management utility
RvcMjrGrpImport.dll	Labor management utility
RvcSalesImport.dll	Labor management utility
RvcTblCntImport.dll	Labor management utility
SARreport.dll	Standalone mode reporting
ScaleAPI.dll	Utility for scales
SchedulerStatus.exe	Auto sequence schedule status
Scheduling.exe	Employee scheduling utility

File Name	Description
SetPath.exe	Utility to set the current path
settle.exe	Command line credit card settlement
spexport.exe	Command line export utility
SwitchTo.exe	Application switching utility
SysAvgChkSlsImport.dll	Labor management utility
SysChkCntImport.dll	Labor management utility
SysCvrCntImport.dll	Labor management utility
SysFamGrpCntImport.dll	Labor management utility
SysFamGrpImport.dll	Labor management utility
SysMjrGrpCntImport.dll	Labor management utility
SysMjrGrpImport.dll	Labor management utility
SysSlsByOTImport.dll	Labor management utility
SysSlsImport.dll	Labor management utility
SysTblCntImport.dll	Labor management utility
TMS_RES.dll	Table management
TMSInterface.exe	Table management
TMSService.exe	Table management service
Translate.exe	Language translation test application
Translator.exe	Language translation
UI_Utils.dll	User interface utility
UpdateAdapter.dll	Database update utility
VersionInfo.exe	Version information
VideoPlayerInterop.dll	Video player utility for RecipeViewer.exe
WaitForHostsFile.exe	Application that verifies the local MDSHosts.xml file
WS4BeepDotNet.dll	KDS beep utility
XMLUtils.dll	Helper utility for forming XML