



RSA Secured Implementation Guide

Last Modified: August 29, 2008

Partner Information

Product Information	
Partner Name	Oracle Corp.
Web Site	http://www.oracle.com/retail
Product Name	Oracle Retail Point-of-Service, Oracle Retail Back Office and Oracle Retail Central Office
Version & Platform	13.0
Product Description	<p>Oracle Retail In-Store Operations solutions enable true multi-channel retailing by delivering a consistent shopping experience across all retail channels—in your stores, on your Web site, and through your catalog or call center. Key business functions include point of sale, store labor management, customer order management, and store inventory management.</p> <p>Oracle Retail Point-of-Service provides the flexibility, responsiveness, and scalability to meet even the largest retailer's point-of-sale requirements, leading to improved customer service and higher sales. Access to real-time customer, product, and market information means more opportunities to turn occasional shoppers into lifetime customers. In addition, Oracle Retail Point-of-Service offers next-generation features that improve customer service and reduce costs, including the ability to process returns for items purchased on the Web, access retail Web sites, fulfill Web-generated orders, and look up cross-store inventory.</p> <p>Oracle Retail Back Office offers a flexible and efficient way to manage critical store operations, while improving customer service and enhancing profits. Store management and reporting functionality are accessible from various devices throughout the store, from front registers to back-office PCs. Real-time access to accurate information across stores, coupled with the ability to analyze in-store data, enables managers to react quickly to business needs and trends and to more effectively meet customer demands.</p> <p>Oracle Retail Central Office is a scalable all-in-one application that enables you to effectively oversee operations and better manage stores to ensure excellent customer service. Based on industry standards, this flexible solution provides the ability to manage data movement and access real-time information and reports across channels. Key features include parameter management to improve store policy consistency, sophisticated data management capabilities to leverage built-in workflow technologies, and the ability to manage cross-channel transactions and access electronic journal details, including customer signatures for audit and loss-prevention activities.</p>
Product Category	e-Commerce / e-Business





Solution Summary

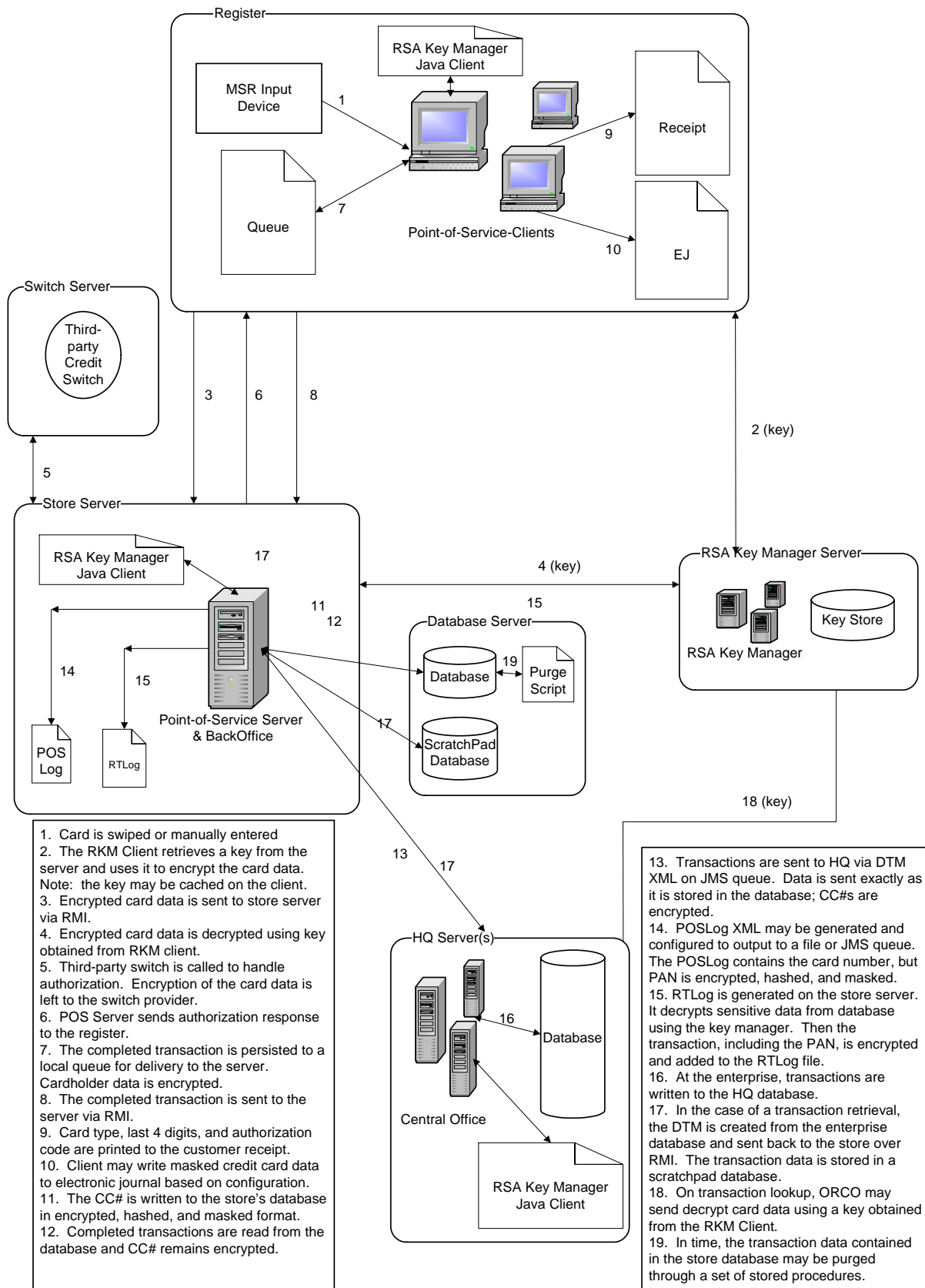
Oracle Retail In-Store Operations integrates with RSA Key Manager to provide the encryption and key management that protects customer cardholder data. Oracle Retail Point-of-Service, Oracle Retail Back Office, and Oracle Retail Central Office encrypt cardholder data as soon as it is read into memory, and only decrypt the data when necessary. The applications use RSA Key Manager (RKM) for all encryption and decryption services, as well as key management such as generation and rotation.

An instance of RKM Server runs at the enterprise level. It provides services for Oracle Retail Central Office, which also runs at the enterprise, as well as Oracle Retail Back Office and Oracle Retail Point-of-Service, which typically run in a merchant's stores. The Oracle applications communicate with the RKM Java Client through the Simple API.

Oracle Retail Point-of-Service is a client/server Point-of-Service application. Both the client, which is usually a cash register device, and the server, which is a server machine usually located within the store, are Java applications. Both the client and the server communicate with their own instances of the RKM Java Client. The RKM Java Client caching capability enables the register and store server to obtain services when they are unable to contact the RKM Server.

Oracle Retail Back Office and Oracle Retail Central Office are web-based applications. Oracle Retail Back Office runs within the store and shares a database with Oracle Retail Point-of-Service. Oracle Retail Central Office runs at the enterprise and communicates with the stores both synchronously and asynchronously. Both web applications communicate with the RKM Java Client through the J2EE Connector Architecture (JCA), a standard for integrating enterprise applications. The RKM Java Client is wrapped and deployed to the JCA container as a Resource Adapter Archive, or a .RAR file.

The diagram below shows where the RKM Java Clients are deployed, as well as the connections to the RKM Server.





Product Configuration for Interoperability

RSA Key Manager Configuration

- Install and configure the RSA Key Manager Server
 - Various stacks are supported by RSA, but the required elements are a database, an application server and an HTTP server.
 - Oracle Retail has established the RSA Key Manager Server running on:
 - Oracle Enterprise Linux
 - Apache HTTP Server
 - IBM WebSphere Application Server
 - Oracle 10g Database
- For instructions on setting up RSA Key Manager, see the RSA Key Manager Server Installation Guide
- Ensure that the key class used by the application is created on the Key Manager Server Administration Console, as shown in Figure F-1.

Key Manager Administration Console

Logged in as: kmsadmin [Log Out](#)

Identity Groups | Identities | Crypto Policies | **Key Classes** | Security Classes

Key Classes

[Create](#)

Pages: [1]

Key Class	Identity Group	Cipher			Key Life	View Keys	Generate Key
		Algorithm	Key Size	Mode			
KeyClasses1	Group01	HMAC SHA1	80	-	30 Days		
SamKeyClass_AES_CBC_192	Group01	AES	192	CBC	1 Year		
SampleKey_RC2_40_CBC	Group01	RC2	40	CBC	1 Year		
Sample_HMAC_MD5	Group01	HMAC MD5	64	-	1 Year		
Sample_RC2_64_CFB	Group01	RC2	64	CFB	1 Year		
Sample_RC4_40	Group01	RC4	40	-	1 Year		
Sample_hmac_sha1	Group01	HMAC SHA1	80	-	1 Year		
SamplekeyClass_AES_CBC_192	Group01	AES	192	CBC	1 Year		
Samples_RC4_40	Group01	RC4	40	-	1 Year		

Pages: [1]

[Create](#)

Figure F-1 RSA Key Manager Server Administration Console



Oracle Retail Configuration

- Set the RSA config.properties file
 - Set the address of the server host and port number.
 - Set the client keystore file and the server keystore file.
 - Set other properties that affect retries, caching, etc.
- To configure Oracle Retail Point-of-Service:
 - Modify posenv.bat to include kmsclient.jar in the Java classpath.
 - Set the encryption service to “RSAKeyStoreEncryptionService” in ServiceContext.xml.
 - Ensure the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy is installed in the JRE used by Oracle Retail Point-of-Service.
 - Ensure the RSAKeyStoreEncryptionService class is included in the Java classpath. This is the adapter that directs encryption and decryption requests to the RKM API.
- To configure the Java EE applications, Oracle Retail Back Office and Oracle Retail Central Office, running on Oracle Application Server (OAS):
 - Copy the kmsclient.jar file to the <OAS_HOME>\j2ee\home\lib folder.
 - Modify spring.properties to set the encryption providerName property to “RSA”
 - Ensure the JCE Unlimited Strength Jurisdiction Policy is installed in the JRE used by the application server
 - Ensure the RSAKeyStoreEncryptionService class is included in the deployed keystoreconnector-rar.rar file

Certification Checklist for 3rd Party Applications

Date Tested: 08/29/2008

Product	Operating System	Tested Version
Key Manager Server	Oracle Enterprise Linux	2.1.3
Key Manager Client	Java on Windows XP	2.1.3.1
Oracle Retail Point-of-Service	Java on Windows XP	13.0
Oracle Retail Back Office	Oracle Enterprise Linux	13.0
Oracle Retail Central Office	Oracle Enterprise Linux	13.0

RSA Key Manager Client	Result
Partner Product Functionality	
Partner product successfully encrypts data utilizing key material from RKM	✓
Partner product successfully decrypts data utilizing key material from RKM	✓
RSA Key Manager / Partner Product API Functionality	
Key archival	N/A
Key retrieval by key class	N/A
Key retrieval by key ID	N/A
Encrypt data	✓
Decrypt data	✓

JGS / PAR

✓ = Pass ✗ = Fail N/A = Non-Available Function



Appendix

J2EE Connector Architecture (JCA) - defines a standard architecture for connecting the J2EE platform to heterogeneous enterprise information systems.

JRE – Java Runtime Environment – allows end-users to run Java applications

RTLog – A representation of an ORPOS retail transaction that can be interpreted by OReSA, an Oracle Retail application for Sales Auditing