

RSA® Key Manager with Application Encryption

Quickly achieve regulatory compliance by encrypting sensitive data within applications at the point of creation.

At a Glance

- Lower the overall total cost of ownership associated with encryption with enterprise key management
- Key management to solve a wide array of encryption and data protection needs – hosts, databases, SAN switches, tape libraries, tokenization, etc.
- Broad platform support, including Windows®, UNIX, Linux and mainframe
- Operates using RSA BSAFE® technology, one of the industry's most widely deployed encryption tools

Executive Summary

RSA® Key Manager with Application Encryption helps achieve compliance with regulations related to PCI and PII (personally identifiable information) by quickly embedding the encryption of sensitive data into enterprise applications; it also helps prevent the loss of sensitive data. It works at the point of creation, ensuring that the data stays encrypted as it is transmitted and stored. Built-in integration with the RSA® Key Manager Server, available in both software and hardware, simplifies provisioning, distribution and management of keys and speeds up the deployment and administration of encryption-enabled applications.

The Importance of Designing for Security

New regulatory pressures and demands from customers and partners to better protect sensitive information are elevating the importance of designing for security and not just for functionality. Designing for security requires building secure applications. Improperly secured applications greatly increase the risk of unsecured data making its way into unauthorized and unsecured locations. Increasingly, application security for the successful mitigation of risk are becoming just as important as functional needs.

The RSA® Key Manager with Application Encryption is designed specifically to address the needs of security teams and application owners. It has been used in many diverse, business-critical applications, including point-of-sale, business intelligence, transaction processing and web applications for regulatory as well as internal security policy encryption requirements. Its simple, straightforward programming interfaces do not require prior security knowledge to use effectively. Also, by encrypting data right inside the applications that create it, you ensure that it is protected regardless of where it goes in its lifecycle. Since it comes pre-built with the RSA® Key Manager Server for performing key generation, distribution, storage and management functions, it greatly simplifies the deployment and administration of encryption-enabled applications.



Realize the Benefits of Enterprise Key Management

A 2007 Forrester Research study of 199 IT decision makers responsible for security revealed that administrative overhead and the ROI burden remain a significant challenge when sustained with traditional approaches to encryption key management. This is because too many customers rely on the simplest mechanism for key management when implementing their encryption projects. Taking this approach may seem like an easy solution at first, but it leads to a number of problems. First, key management is an important part of meeting compliance standards and with native solutions it is difficult for administrators to ensure that keys are handled in the proper manner. Second, when keys are managed in silos it limits the ability to share data across applications. Lastly, the lack of an enterprise key manager creates the possibility of compromised or lost keys.

RSA Key Manager with Application Encryption combines industry-leading encryption capability with enterprise key management, reducing administrative overhead and improving ROI. According to a 2008 report by Aberdeen Research, organizations that deploy enterprise key managers are able to support encryption in 40% more applications and are able to manage 11.5 times more encryption keys. In addition, these organizations are able to do so at a significantly lower cost, up to 92% less in terms of average cost per key!*

RSA Key Manager with Application Encryption can enable consistent key policies and allow organizations to leverage one key manager for a variety of encryption devices. This increases security, simplifies operations and lowers the total cost of ownership.

Capabilities

Easy-to-use client and server tools – Key Manager has simple client commands like “encrypt” or “decrypt”. This keeps development simple and shortens the learning curve for developers not familiar with encryption. Key Manager also has advanced server GUIs to manage keys for the long term. This vastly reduces operational overhead and lowers costs.

Central control over client permissions – Key Manager can define encryption key policies, like which clients have permission to generate/rotate/delete keys, centrally.

Support for custom object metadata – Key Manager provides for storage of custom attributes with encryption keys to provide more detailed tracking of key usage. This information is also easily searched upon, which helps meet audit requirements.

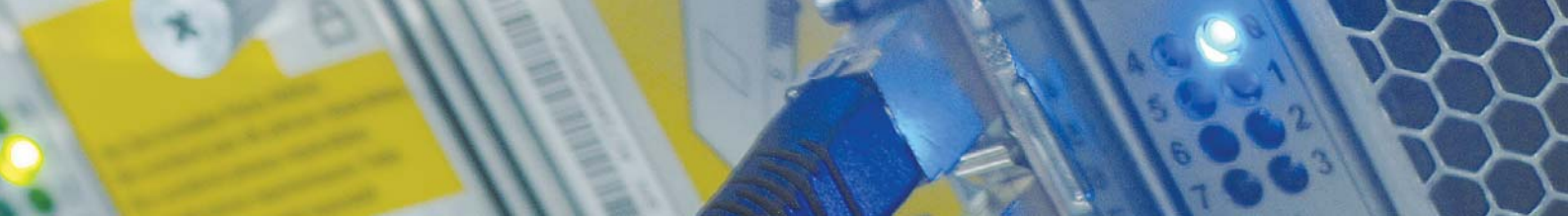
Increased client and server security – Key Manager allows administrators control over client commands, so keys can be expired or rotated by admins from the server. Key Manager also has built-in disaster recovery and fail-over to ensure proper protection of the keys.

Support for a common key management infrastructure – Key Manager is integrated with the leading encryption devices with Key Manager for the Datacenter, which allows customers to use the same key manager for all types of encryption, including applications, databases, tape and disk media.

RSA Services for RSA Key Manager with Application Encryption

RSA Key Manager with Application Encryption has been widely adopted by many well known large enterprise customers that needed to comply with regulations such as PCI and PII. The product is supported by RSA's professional services and technical support organizations that have years of experience deploying encryption solutions in very complex IT environments. Our professional services organization can help you customize the RSA Key Manager with Application Encryption to suit your business needs and your IT infrastructure needs.

* Aberdeen Group, *Managing Encryption*, October 2008



Supported Platforms for RSA Key Manager Encryption C Client

Platform	Operating System	CPU Architecture	Compiler Version
Microsoft®	Windows® XP SP2 Windows 2000 SP4	x86 (32-bit) ¹	Microsoft C/C++ Optimizing Compiler v12.00.8168 for 80x86 (Visual Studio 6)
			Microsoft C/C++ Optimizing Compiler v14.00.50727.762 for 80x86 (Visual Studio 2005 SP 1)
	Windows 2003 Server SP1	x86 (32-bit) ¹	Microsoft C/C++ Optimizing Compiler v12.00.8168 for 80x86 (Visual Studio 6)
			Microsoft C/C++ Optimizing Compiler v14.00.50727.762 for 80x86 (Visual Studio 2005 SP 1)
		Intel® x86 (64-bit)	Microsoft C/C++ Optimizing Compiler v14.00.50727.762 for x64 (Visual Studio 2005 SP 1)
	Windows Server 2008	x86 (32-bit) ¹	Microsoft C/C++ Optimizing Compiler v12.00.8168 for 80x86 (Visual Studio 6)
			Microsoft C/C++ Optimizing Compiler v14.00.50727.762 for 80x86 (Visual Studio 2005 SP 1)
		Intel® x86 (64-bit)	Microsoft C/C++ Optimizing Compiler v12.00.8168 for 80x86 (Visual Studio 6) Microsoft C/C++ Optimizing Compiler v14.00.50727.762 for 80x86 (Visual Studio 2005 SP 1)
Sun™	Solaris 9 Solaris 10	UltraSparc v8+(32-bit)	Sun 5.3
		UltraSparc v9 (64-bit)	Sun 5.3
Red Hat®	Enterprise Linux® AS 3.0	x86 (32-bit) ¹	gcc 3.4.3 20041212
	Enterprise Linux AS 4.0	AMD x86 (64-bit)	gcc 3.3.3
Novell®	SUSE® Linux Enterprise Server 9	AMD x86 (64-bit)	gcc 3.3.3
		AMD x86 (32-bit)	gcc 4.12
	SUSE® Linux Enterprise Server 10	AMD x86 (64-bit)	gcc 4.12
HP	HP-UX 11.x	PA RISC (32-bit)	HP ANSI-C 11.02
		PA RISC (64-bit)	HP ANSI-C 11.02
	HP-UX 11.x	Itanium 2 (64-bit)	HP aC++/ANSI-C B3910B A.06.50
IBM®	AIX 5L™ 5.2	Power PC® (32-bit)	VisualAge C++ Professional V6.0 for AIX
		Power PC (64-bit)	VisualAge C++ Professional V6.0 for AIX

Supported Platforms for RSA Key Manager Encryption Mainframe Client

Platform	Operating System	CPU Architecture	Environment	Compiler Version
IBM® Mainframe	z/OS V1R7 ²	z/Architecture (64 bit)	CICS	V1R7 XL C/C++ with TARGET(zOSV1R4) directive
	z/OS V1R7 ²	z/Architecture (64 bit)	COBOL	V1R7 XL C/C++ with TARGET(zOSV1R4) directive
	z/OS V1R7 ²	z/Architecture (64 bit)	C/C++	V1R7 XL C/C++ with TARGET(zOSV1R4) directive
	i5/OS V5R3	Power5 (64 bit)	C/C++	ILE C/C++ with TGTRLS(V5R2M0) directive

¹ Tested against Intel x86 (32-bit).

² Compatible with V1R4 and above

Supported Platforms for RSA Key Manager Encryption JAVA Client

Platform	Operating System	CPU Architecture	JDK
Microsoft	Windows 2000 Professional SP4	Intel® x86 (32-bit)	Sun JDK 1.4.2, 5.0, 6.0; IBM JDK 1.4.2, 5.0
	Windows XP SP2	Intel x86 (32-bit)	Sun JDK 1.4.2, 5.0, 6.0; IBM JDK 1.4.2, 5.0; JRockit 5.0, 6.0
	Windows XP Professional x64 Ed.	Intel x86 (64-bit)	Sun JDK 5.0, 6.0
	Windows 2003 Server	Intel x86 (32-bit)	Sun JDK 1.4.2, 5.0, 6.0; IBM JDK 1.4.2, 5.0; JRockit 5.0, 6.0
		Intel x86 (64-bit)	Sun JDK 5.0, 6.0; JRockit 5.0, 6.0
	Windows Vista® Enterprise	Intel x86 (32-bit)	Sun JDK 1.4.2, 5.0, 6.0; IBM JDK 1.4.2, 5.0; JRockit 5.0, 6.0
Intel x86 (64-bit)		Sun JDK 5.0, 6.0; JRockit 5.0, 6.0	
Sun™	Solaris™ 9	UltraSparc® (32-bit)	Sun JDK 1.4.2, 5.0, 6.0
		UltraSparc (64-bit)	Sun JDK 5.0, 6.0
	Solaris 10	UltraSparc (32-bit)	Sun JDK 1.4.2, 5.0, 6.0
		UltraSparc (64-bit)	Sun JDK 1.4.2, 5.0, 6.0; IBM JDK 5.0; JRockit 5.0
		Intel x86 (64-bit)	Sun JDK 5.0, 6.0
Red Hat®	Enterprise Linux Adv. Server 4.0	Intel x86 (32-bit)	Sun JDK 1.4.2, 5.0, 6.0; IBM JDK 5.0; JRockit 5.0, 6.0
		Intel x86 (64-bit)	Sun JDK 5.0, 6.0; JRockit 5.0, 6.0
	Enterprise Linux Advanced Server 5.0	Intel x86 (32-bit)	Sun JDK 1.4.2, 5.0, 6.0; IBM JDK 5.0; JRockit 5.0, 6.0
		Intel x86 (64-bit)	Sun JDK 5.0, 6.0; JRockit 5.0, 6.0
Novell®	SUSE® Linux Enterprise Server 9.0	Intel x86 (32-bit)	Sun JDK 1.4.2, 5.0, 6.0
		Intel x86 (64-bit)	Sun JDK 5.0, 6.0
HP	HP-UX 11.23	Itanium 2 (32-bit)	HP JDK 1.4.2
		Itanium2 (64-bit)	HP JDK 1.4.2, 5.0
	HP-UX 11.31	Itanium2 (32-bit)	HP JDK 5.0
		Itanium2 (64-bit)	HP JDK 5.0
IBM®	AIX® 5L v5.3	Power PC (32-bit)	IBM JDK 1.4.2, 5.0
		Power PC (64-bit)	IBM JDK 5.0

This release of the Java Client is compatible with the RSA Key Manager Server 2.1.3 or higher.

Why RSA?

RSA Key Manager with Application Encryption is a core component of the RSA Encryption and Key Management Suite, a collection of integrated products and services for managing encryption and key management across the enterprise. The Suite is part of the RSA Data Security System, a unique and comprehensive framework to discover and monitor sensitive information, apply the appropriate enforcement mechanisms and report and audit on security events to ensure compliance with policy. This system leverages RSA's more-than 25 years of experience solving data security problems. Implementing this system will help to protect your organization against major threats to data.



RSA Security Inc.
 RSA Security Ireland Limited
www.rsa.com

The Security Division of EMC

©2008-2009 RSA Security Inc. RSA, the RSA logo, SecurID and BSAFE are registered trademarks or trademarks of RSA Security Inc. in the U.S. and/or other countries. EMC, PowerPath and Symmetrix are trademarks or registered trademarks of EMC Corporation. All other trademarks mentioned herein are the properties of their respective owners.

RKMAE DS 0509