

# RSA® Key Manager

## At a Glance

- Scalable, centralized lifecycle management for encryption keys and other enterprise security objects
- Integrates with existing business applications and storage infrastructure
- Provides robust separation of duties to ensure security objects are protected throughout their life
- Fault tolerance and redundancy ensure continuous security and access to your data

Regulatory guidelines, internal policies and increasing risk of public exposure continue to motivate companies to develop and adopt enterprise-wide security strategies to encrypt their most sensitive data. However, as a recent survey commissioned by RSA and conducted by Forrester Research shows, most companies are still relying on manual processes and a disjointed collection of point encryption tools to address the challenge. Organizations often make the mistake of managing each of these tools separately, which results in policy misalignment, high management costs and a lack of business process continuity. Attempting to do this using manual processes and existing tools has also proven to be a huge resource drain. To avoid these problems, companies must manage their security control mechanisms centrally. RSA® Key Manager addresses these issues by providing a centralized system to provision, administer and manage all security objects throughout your enterprise.

RSA Key Manager enables you to configure and manage encryption usage through policies – ensuring that configurations are aligned with business' underlying security policies. It facilitates the sharing of encrypted data between applications, groups or infrastructures by:

- Eliminating the need to decrypt data before sending it from one point to another and re-encrypting on the other end,
- Distributing keys to applications on an as-needed basis versus the riskier practice of needing to transport the keys with the data and
- Limiting the risk of breaking established processes such as replication or other forms of data sharing.

RSA Key Manager provides a complete, enterprise-wide approach to securing the entire data lifecycle, ensuring that you meet both regulatory and internal policy requirements consistently regardless of how data is accessed, used or distributed.

## Part of RSA's Solution for Securing Enterprise Data

RSA Key Manager is a core component of the RSA Encryption Suite, a collection of integrated products and services for managing encryption across the enterprise. The Encryption Suite is part of the RSA Data Security System, a comprehensive framework for enforcing data security policy through a combination of enforcement, management and auditing controls. The System leverages RSA's 25-plus years of experience solving data security problems. Implementing this system can help enable you to protect your organization against major threats to your data such as breaches by privileged users, lost or stolen media and lapses or failures of defined security processes.

## Capabilities

**Lifecycle management for security objects** — Key Manager helps enable secure generation, distribution, storage and management of symmetric encryption keys. It also supports secure distribution, storage, and management of other types of security objects including RSA Keys, PGP Keys, certificates, and others. The system provides interfaces for integrating with existing encryption systems. It supports retrieval, caching, archival, restoration, expiration and rollover for all of these objects. It also supports generation and provisioning of symmetric keys.





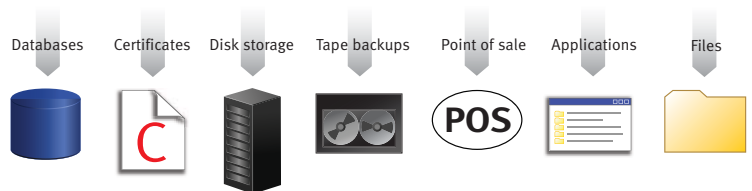
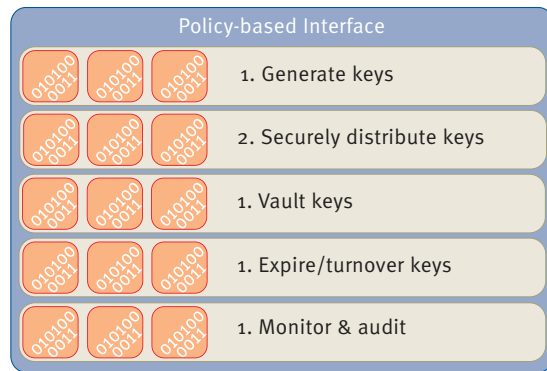
**Support for custom object metadata** — Key Manager helps enable storage of custom metadata elements with security objects to enable more detailed tracking, usage and other information managed along with the security object to improve auditing and ongoing system management.

**Integration with existing user access management systems** provides interfaces to integrate systems such as Microsoft® Active Directory to enable inheritance of existing defined administrative roles.

**Secure and scalable architecture** helps allow centralized management across multiple locations and end-points. It also includes fail-over and high-availability features, such as unattended restart and replication, to help ensure maximum uptime for mission critical applications that require access to security objects.

**Built using industry proven technologies**, Key Manager employs a robust and open architecture that leverages proven RSA BSAFE® FIPS-140 validated cryptographic toolkits and is built using industry-standards. The product also integrates with other RSA technologies including RSA SecurID® authentication for additional security.

### RSA Key Manager



### Platform Support Matrix

Base Operating System	Web Server	Application Server	Database Server	RSA® Access Manager (formerly ClearTrust®)	Hardware Security Module	Java Virtual Machine
Microsoft Windows® 2003 Server RC2 (Intel® x86 32-bit)	Microsoft IIS 6.0	Apache® Tomcat 5.5.17	Microsoft SQL Server 2000/2005	Access Manager Server 6.0; Agent 4.7	nCipher™ netHSM™ – Firmware 2.18.13 – CipherTools 1.0.0.8 – Support Utilities 10.15	Sun JRE™ 1.5
Red Hat® Enterprise Linux® AS 4.0 (Intel® x86 32-bit)	Apache HTTP Server 2.0.40	BEA® WebLogic™ 9.0*	Oracle® 10GR, Release 2RAC			IBM JRE 1.4
Sun™ Solaris™ 9 or 10 (UltraSparc v9 32-bit)	Apache HTTP Server 2.0.59	IBM WebSphere® 6.0**				Sun JRE 1.5
		BEA® WebLogic™ 9.0.1				

\* BEA Weblogic software requires patch number CR238704

\*\* IBM Websphere software requires patches up to 6.0.2.15



RSA Security Inc.  
RSA Security Ireland Limited  
[www.rsa.com](http://www.rsa.com)

The Security Division of EMC

©2006-2007 RSA Security Inc. All Rights Reserved.  
BSAFE, RSA, SecurID and the RSA logo are either registered trademarks or trademarks of RSA Security Inc. in the United States and/or other countries. EMC is a registered trademark of EMC Corporation. All other products and services mentioned are trademarks of their respective companies.