



The Security Division of EMC

RSA Solution Brief

# RSA® Key Manager for PCI Compliance



A core pillar of the Payment Card Industry (PCI) Data Security Standard – detailed in Requirements 3 and 4 – is securing any cardholder data, regardless its location. Alongside these protection mandates come detailed and prescriptive requirements for key management. Embedding encryption capabilities into applications with RSA® Key Manager with Application Encryption helps organizations address PCI's data protection and key management requirements. By working at the point of creation, RSA Key Manager with Application Encryption ensures that cardholder data stays encrypted as it is transmitted and stored. Integration with the RSA® Key Management Server simplifies provisioning, distribution and management of keys while speeding up deployment and easing the administration of encryption-enabled applications.

The purpose of this document is to explain how the RSA Key Manager with Application Encryption provides the necessary functionality to satisfy PCI requirements 3.4, 3.5, 3.6 and 4.1.

### **3.4** *Render PAN (primary account number) unreadable anywhere it is stored*

RSA Key Manager's application encryption client can be used to extend encryption capabilities – 192-bit 3DES or 128-bit, 192-bit or 256-bit AES encryption – to a variety of applications, including point-of-sale (POS) devices. By encrypting the cardholder data at the point of creation, the data remains encrypted both as it travels and in storage.

In addition to the application layer, cardholder data can be encrypted while stored in files, databases and storage media. The RSA Key Management Server integrates with a variety of these solutions to ease the challenges of enterprise key management and address the key management-focused PCI requirements.

### **3.5** *Protect keys used for encryption of cardholder data against both disclosure and misuse.*

RSA Key Manager provides strong vaulting of encryption keys within a FIPS 140-2 Level 1 or Level 3 boundary. Keys are distributed via mutually authenticated SSL so that they cannot be intercepted in transit.

#### **3.5.1** *Restrict key access to the fewest number of custodians necessary*

RSA Key Manager helps ensure that administrators are both authenticated and authorized to perform RSA Key Manager operations. It provides the option to utilize RSA® Access Manager for the validation of administrators.

To protect encryption keys from unauthorized disclosure and misuse, an RSA Key Manager deployment provides administration facilities that enforce separation of duties.\*

The Key Management Server supports two administrator roles:

#### **1. Key Administrators**

Key administrators manage manual key generation and the assignment of client applications to application groups.

#### **2. User Administrators**

User administrators create, delete and modify Key Management Server administrator user accounts, and grant key administrators the rights to manage application groups.

#### **3.5.2** *Store keys securely in the fewest possible locations and forms*

RSA Key Manager contains a centralized, secure vault for encryption keys. This single vault is utilized by all end points for the generation of and access to keys within a PCI infrastructure.

- Multiple RSA Key Manager instances utilize the same technology and separation of duties to ensure that policy is distributed uniformly across the enterprise.
- Designed as an enterprise system, RSA Key Manager can be configured to enable access from any encryption end point.

---

\*NIST defines separation of duties as a fundamental security principle that requires system administrators to "... divide critical functions among different staff members ... to ensure that no one individual has enough information or access privilege to perpetrate damaging fraud."

## By working at the point of creation, Key Manager helps ensure that cardholder data stays encrypted as it is transmitted and stored.

### 3.6.1 Generation of strong keys

RSA Key Manager generates keys suitable for use with the algorithms seen in the table. These keys can be used to encrypt and decrypt data or to generate message authentication code.

### 3.6.2 Secure key distribution

RSA Key Manager uses the same secure communications channel set up between the Key Manager client and the Key Management Server, which is used for the original key request, to return key material to the Key Manager clients. This secure communication channel is implemented using SSLv3/TLSv1. The Key Management Server rejects all key requests received over an insecure communication channel.

To ensure that keys are only distributed to trusted identities, the RSA Key Management Server uses the public key certificate supplied by the Key Manager client to establish a secure communications channel, which is used to provide the appropriate authentication. The Key Management Server compares the issuer and serial number of the public key certificate supplied by the client against the list of identities defined on the Server. Key requests from clients that cannot be authenticated are rejected.

### 3.6.3 Secure key storage

After creation, keys are concatenated with a SHA-256 digest of the data, encrypted and then stored in the RSA Key Management Server database. The encryption uses a key encryption key, which is stored either protected in memory (level 0 security), or on a dedicated hardware security module (level 1 security). For more information on security levels, please see the solution for requirement 3.5.2.

Algorithm	Key length (bits)	Mode
AES	128, 192, and 256	CBC, ECB, CTR, CFB, OFB
DES3	112 and 168	CBC, CFB, ECB, OFB
RC2	40, 64, and 128	CBC, ECB, CFB, OFB
RC4	40, 64, 128, and 256	
RC5	128, 192, and 256	CBC, ECB, CFB, OFB
HMAC MD5	64	
HMAC SHA224	112, 168, and 224	
HMAC SHA256	128, 192, and 256	
HMAC SHA384	192, 288, and 384	
HMAC SHA512	256, 384, and 512	

### 3.6.4 Periodic changing of keys as deemed necessary and recommended by the associated application (for example, re-keying); preferably automatically, at least annually.

RSA Key Manager provides the following options related to duration of keys:

1. **Active Encryption Key Rotation based on Corporate Policy.** Each key has a set lifetime. At the end of that lifetime the key is no longer active for encryption operations, only for decryption operations. This is commonly used for POS solutions where a new key might be used each day for all credit card numbers accepted at a given store on that day.
2. **Unique Key Operations.** When dealing with data at rest in the form of tapes or similar discrete elements, RKM provides the functionality to generate a new key for each component.

### 3.6.5 Destruction of old keys

RSA Key Manager's keys are assigned NIST standard states. These states include

1. **Activated.** A key is active and available for use.
2. **Deactivated.** A key can be utilized to decrypt data, but not encrypt new data.
3. **Destroyed.** The key is no longer in existence. For auditing purposes, the meta data associated with the key is retained.
4. **Compromised.** The key has been exposed and needs to be clearly marked as a risk for audit and remediation purposes.

### 3.6.7 Prevention of unauthorized substitution of keys

By using Mutually Authenticated SSL for key distribution, RSA Key Manager prevents unauthorized key substitution. In addition, the cryptography within the RKM Application Encryption Clients are all FIPS 140-2 level 1 validated to prevent misuse.

### 3.6.8 & 3.6.9

*Replacement of known or suspected compromised keys; revocation of old or invalid keys*

See Destruction of old keys (3.6.5) above.

- 4.1 *Use strong cryptography and security protocols such as secure sockets layer (SSL)/transport layer security (TLS) 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, WiFi (IEEE 802.11x), global system for mobile communications (GSM), and general packet radio service (GPRS).*

RSA Key Manager's application encryption client can be used to extend encryption capabilities, – 192-bit 3DES or 128-bit, 192-bit, or 256-bit AES – encryption to a variety of applications. This enables the credit card data to be encrypted *at the application*, including point of sale, prior to traversing a network.

RSA Key Manager with Application Encryption is used by many well known large enterprise customers to comply with the data protection and key management aspects of PCI. To learn about these organizations, or for more information on RSA solutions to help customers address PCI DSS compliance, visit [www.RSA.com/PCI](http://www.RSA.com/PCI).

### About RSA

RSA, the Security Division of EMC, is the expert in information-centric security, enabling the protection of information throughout its lifecycle. RSA enables customers to cost-effectively secure critical information assets and online identities wherever they live and at every step of the way, and manage security information and events to ease the burden of compliance.

RSA offers industry-leading solutions in identity assurance & access control, encryption & key management, compliance & security information management and fraud protection. These solutions bring trust to millions of user identities, the transactions that they perform, and the data that is generated. For more information, please visit [www.RSA.com](http://www.RSA.com) and [www.EMC.com](http://www.EMC.com).



The Security Division of EMC

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

©2008 RSA Security Inc. All Rights Reserved.

RSA, RSA Security 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.

PCIKM SB 0608