



The Security Division of EMC

STORAGE AREA NETWORK

RSA Key Management with EMC Connectrix B-Series Encryption Solutions

EMC offers a highly integrated encryption solution that works non-disruptively with existing storage and servers. Combining RSA® Key Manager for the Datacenter with EMC® Connectrix® encryption devices creates an industry-leading solution for encrypting data-at-rest.

CONTENTS

Contents.....	2
Introduction.....	3
Connectrix B-Series Encryption with RKM.....	3
Encrypting Symmetrix Storage with Connectrix Encryption and RKM.....	5
Setting up Connectrix Encryption with RKM.....	9
Conclusion.....	11

INTRODUCTION

Most encryption experts agree that the most difficult aspect of encrypting data-at-rest is managing the Data Encryption Keys (DEKs). EMC offers a cost-effective key management solution with hardware-based encryption. The Connectrix B-Series encryption device combines 96 gigabits per second (Gbps) of encryption processing performance with the RSA Key Manager for the Datacenter (RKM) solution. RKM enables policy-driven key management for the broadest range of encryption solutions, establishing true enterprise key management. The power of the encryption hardware combined with a flexible key management system helps organizations deploy enterprise-wide solutions for securing their data.

NOTE: The term “Connectrix encryption device” is used in this paper to reference both the Connectrix ES-5832B Encryption Switch and the PB-DCX-16EB Encryption Blade for the DCX family of directors.

EMC designed an encryption solution to succeed in advanced storage environments, by integrating Connectrix encryption devices with the RKM solution. EMC understands that organizations must comply with government regulations and offers services to help customers meet the stringent requirements of state and federal mandates. Corporations have entrusted EMC with their most valuable data for over a decade and now these same corporations can encrypt their data with EMC products.

The symmetric keys used in fabric-based encryption for disk and tape are the most essential and sensitive piece of information in the solution. Not only do the keys need to be protected so that the data encrypted with these keys cannot be decrypted by unauthorized users, but they also must be preserved for as long as the encrypted data is preserved. If not, the encrypted data cannot be decrypted and will therefore be unrecoverable when the key is no longer available.

The Connectrix encryption devices are responsible for generating keys and wrapping those keys to ensure their integrity and security. Once generated, the keys are then vaulted to RKM, to ensure that the keys are available for decryption when and where needed.

RKM provides a highly available and resilient environment for long-term storage of encryption keys across a broad range of encryption environments. RKM ensures that keys are preserved in an environment that can support large numbers of keys, across geographic and organizational boundaries, without risk of key loss or compromise. It distributes encryption keys when and where they are needed, protecting them in transit and ensuring they are provided only to authenticated and authorized entities. Through its enterprise-grade capabilities, RKM complements the capabilities of Connectrix encryption to provide the industry-leading solution for securing data on disk.

CONNECTRIX B-SERIES ENCRYPTION WITH RKM

The key management requirements associated with enterprise-wide deployment of encryption have a great impact on both the effectiveness of encryption and on total cost of ownership for encryption solutions.

There are three major impacts of enterprise-wide decryption deployments related to key management:

1. The more that key management is split across different encryption environments, the more difficult it is to align the configuration and operation of encryption in these environments with the security policies for the business. Enterprise key management alleviates these issues. A central, unified definition of key management makes it simpler to establish and maintain consistent control of keys across all environments in which encryption is performed, including how and where keys are used.

2. When key management is split across environments, a larger number of individuals is required to manage keys. Often the management cost is further increased by the multiplication of key management tools, making it difficult to share expertise and resources across these environments. In addition, without enterprise key management, expensive manual processes must be put in place to propagate keys when encrypted data is shared with partners or backup sites, so that business processes are not broken.
3. When encrypted data needs to be shared among applications, groups, or infrastructure, lack of centralized management for key sharing often means that data needs to be decrypted before sending it from one point to another and then re-encrypted at the destination. This increases both the cost of data sharing and the vulnerability of the data.

Using RKM to establish an enterprise key management environment, as shown in the Figure 1, addresses these issues to ensure both the cost effectiveness and the strength of encryption solutions.

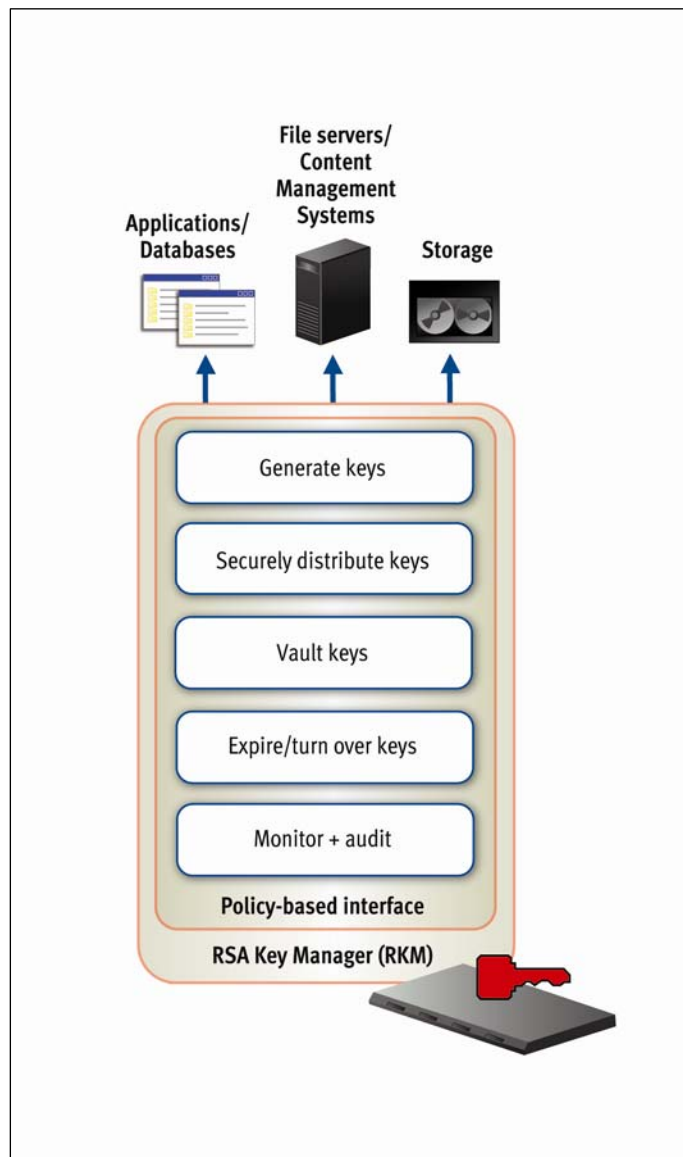


Figure 1. RSA Key Manager for the Datacenter

Establishing effective data protection is possible only if enterprise control mechanisms participate in well understood security policies that reflect an accurate understanding of the enterprise's data, threats and risk model. Using an enterprise key management system that participates in centralized policy administration ensures that localized data protection enforcement is aligned with data protection policies. RKM can provide this alignment of encryption with enterprise security policy, helping to address the challenge of achieving effective and auditable security, while optimizing accessibility to information and minimizing cost of operations.

The integration of RKM with Connectrix fabric-based encryption provides three major capabilities:

- Centralized vaulting, protection, and recoverability of keys
- Policy-based security
- Comprehensive audit capabilities

RKM provides centralized vaulting of the encryption keys for Connectrix disk encryption. Encryption keys are generated in the Connectrix encryption device and vaulted in RKM. Those keys can then be retrieved by the Connectrix encryption device when keys need to be restored to the disk encryption environment. This enables encryption deployments to scale while minimizing administrative costs and ensuring separation of duties.

The policy-based security in RKM ensures effective control of encryption. RKM controls how long a key is available and where it is distributed, ensuring that policies for data availability are effectively and consistently enforced. It enforces authentication and authorization of entities vaulting and requesting keys, to ensure that even an organization that has inappropriately acquired an encrypted tape will not be able to acquire the key to decrypt it. RKM security policies also control administrative access to keys, establishing separation of duties between policy management and key use essential to effective control of security.

Auditing of all encryption key activity enables organizations to ensure that key-related security policies are being followed to meet compliance requirements. Vaulting of keys, restoring keys to the Connectrix encryption environment, expiration or revocation of keys and distribution of keys across the enterprise can all be tracked in a secure log. This provides both the operational control and compliance visibility to ensure that encryption is being used effectively and according to defined security policies.

ENCRYPTING SYMMETRIX STORAGE WITH CONNECTRIX ENCRYPTION AND RKM

Encrypting existing EMC storage, including an EMC Symmetrix® and EMC CLARiiON® product lines, is a key aspect of the solutions offered by EMC. Existing EMC storage can be converted to encrypted data selectively at the Logical Unit Number (LUN) level, so that only select LUNs are encrypted. While some LUNs remain stored in plaintext, the user-specified LUNs are encrypted at up to 96 Gbps per encryption device. Within minutes of committing the configuration, the data is encrypted according to IEEE 1619 standards for data at rest.

The basic configuration of the encryption solution is shown in Figure 2. EMC recommends deploying encryption with redundant encryption devices and redundant RKM systems. The basic configuration of the solution includes:

- An initiator to read and write the data
- A Symmetrix storage device
- A Fibre Channel fabric that consists of two Connectrix ES-5832B encryption switches in this example. However, it could also be two PB-DCX-16EB Encryption Blades in a Connectrix DCX Backbone chassis.
- Redundant RKM system to manage the Data Encryption Keys on separate servers
- Connectrix Manager Data Center Edition (CMDCE) to manage the fabric and encryption

- A management Local Area Network (LAN) to connect the RKM server, the management station, fabric devices (including the Connectrix encryption devices), and other equipment
- A cluster LAN of Gigabit Ethernet links between the Connectrix encryption devices for exchanging DEKs

In this example, LUN A of the Symmetrix is defined to be encrypted. When the encryption configuration is committed, the Connectrix encryption device creates a random 256-bit DEK that is used to encrypt data. After the key has securely been stored in RKM, the encryption device creates a virtual target and initiator as shown in Figure 1. The virtual initiator reads the LUN in 256kB blocks, encrypts the data using AES256-XTS encryption algorithm, and writes it back to the same location as shown in data exchange 1 (blue). With up to 96 Gbps of encryption processing power, terabytes of data can be encrypted in a matter of minutes.

When the configured host writes data to the LUN, the host sends the request to the virtual target as shown in data flow 2 (green) of Figure 2. The data is encrypted by the Connectrix encryption device and sent from the virtual initiator to the target as shown in data flow 3 (also green). The virtual target and initiator have their own Fibre Channel address and are instantiated in the redundant Connectrix encryption device if the current encryption device fails. The virtualization of the host and target enable transparent migration between the encryption devices. Every host needs to be configured for the encryption procedure to ensure that all data that is written to the LUN is encrypted.

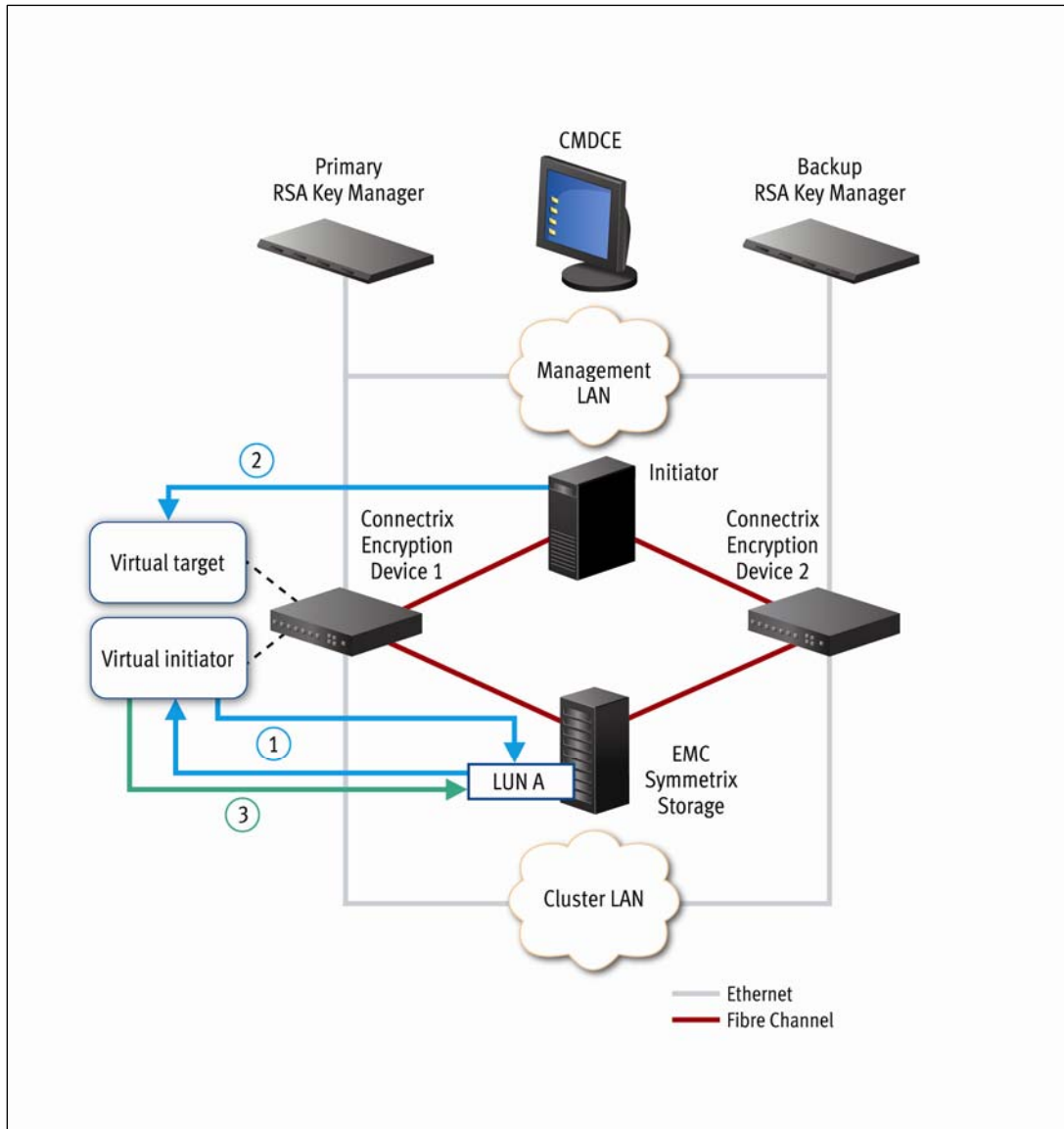


Figure 2. Encrypting disk data

Looking at the Connectrix encryption device in more detail, Figure 3 shows how traffic is routed to the virtual initiators and targets with the encryption engine between them. The cleartext (unencrypted data) is sent to the encryption engine that resides inside the Federal Information Processing Standard 140-2 (FIPS 140-2 Level 3) security boundary (red dashed line). Within the boundary, the encryption engine combines the DEK with the cleartext to create the ciphertext. The security boundary ensures the integrity of the DEKs and the encryption process. The DEKs are always encrypted when they leave the FIPS security boundary and when they are stored in RKM. The ciphertext is placed in Fibre Channel frames and sent from the virtual initiator to the target. Many encryption engines work in parallel to support 96 Gbps of encryption processing power.

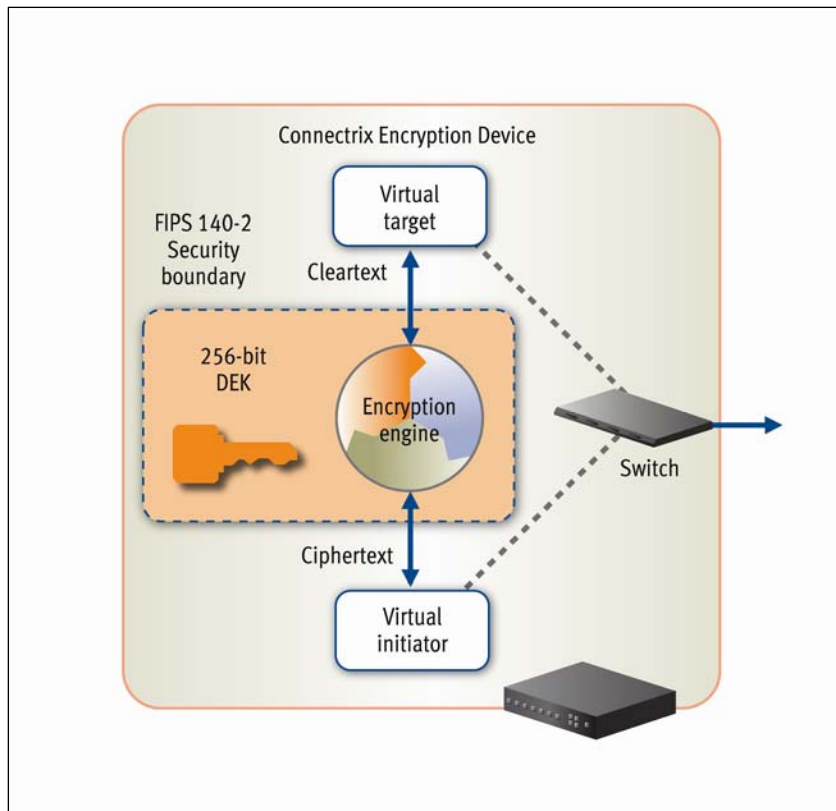


Figure 3. Connectrix encryption device internals

SETTING UP CONNECTRIX ENCRYPTION WITH RKM

Because RKM takes advantage of the enterprise key management interface provided by Connectrix encryption, deploying RKM with Connectrix encryption is simple to set up. The Connectrix encryption switches vaulting keys to RKM or requesting archived keys from RKM are configured to communicate with an RKM, as shown in Figure 8.

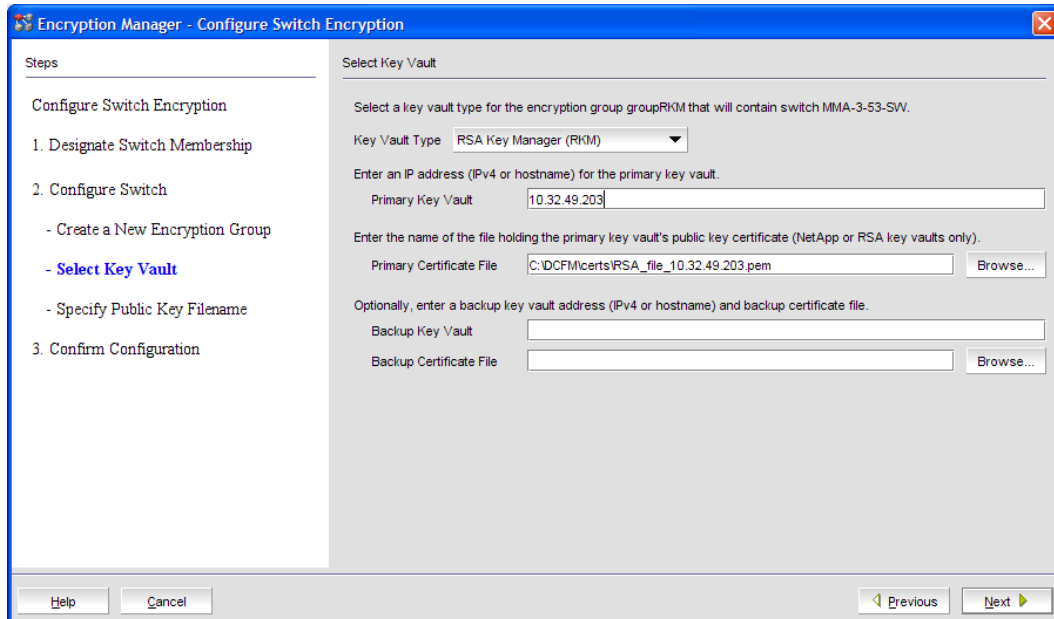


Figure 8. Configuring Connectrix encryption to use RKM

A backup or secondary RKM is defined for recovery purposes. Alternatively, highly available environments can be configured as shown in Figure 9. In that case, the IP address for the load-balanced RKM servers is specified at a given site, relying on the replication between RKM servers to synchronize keys across sites.

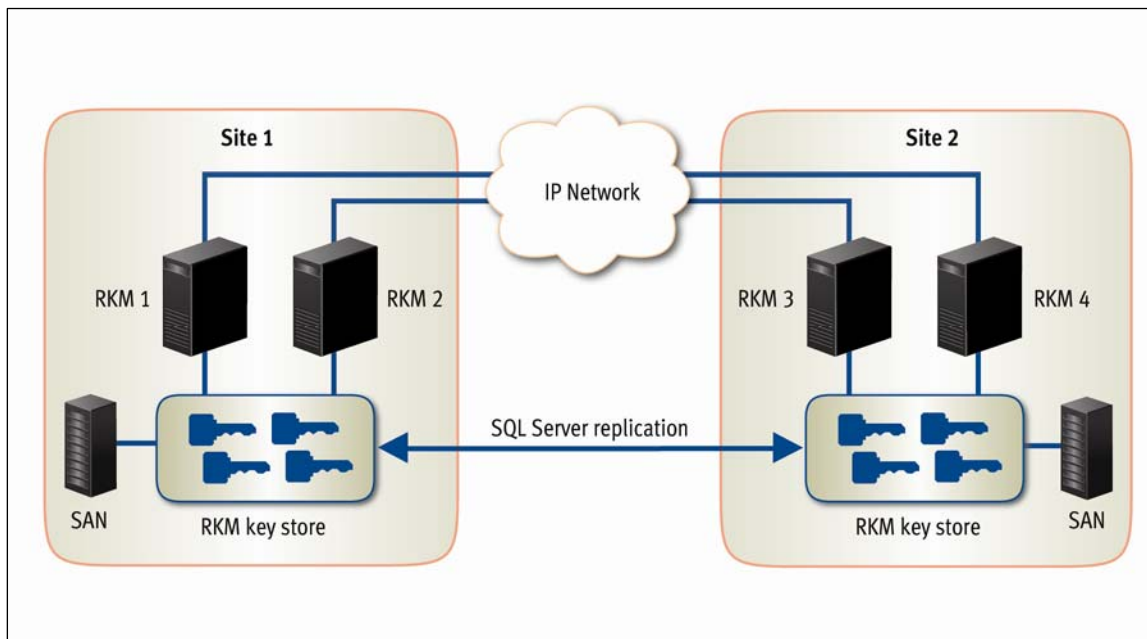


Figure 9. Connectrix encryption and RKM

Additional information about RKM is required during setup, as the Connectrix encryption device needs to know how to access RKM. The additional information is the IP Address of the RKM Server, the TCP port to access the services on the RKM (usually 443), and the Public Key Infrastructure (PKI)-based credentials used to gain access to RKM. Use of these credentials by Connectrix encryption devices and RKM ensures that attacks, such as man-in-the-middle and injection, are prevented.

Once the setup is completed, communication between the Connectrix encryption environment and RKM is transparent. When a Connectrix encryption device creates an encryption key for disk encryption or tape backup, the key is wrapped with the key encryption key for that Connectrix encryption device. The wrapped key is then immediately vaulted to RSA to ensure its availability for subsequent use, as shown in Figure 10.

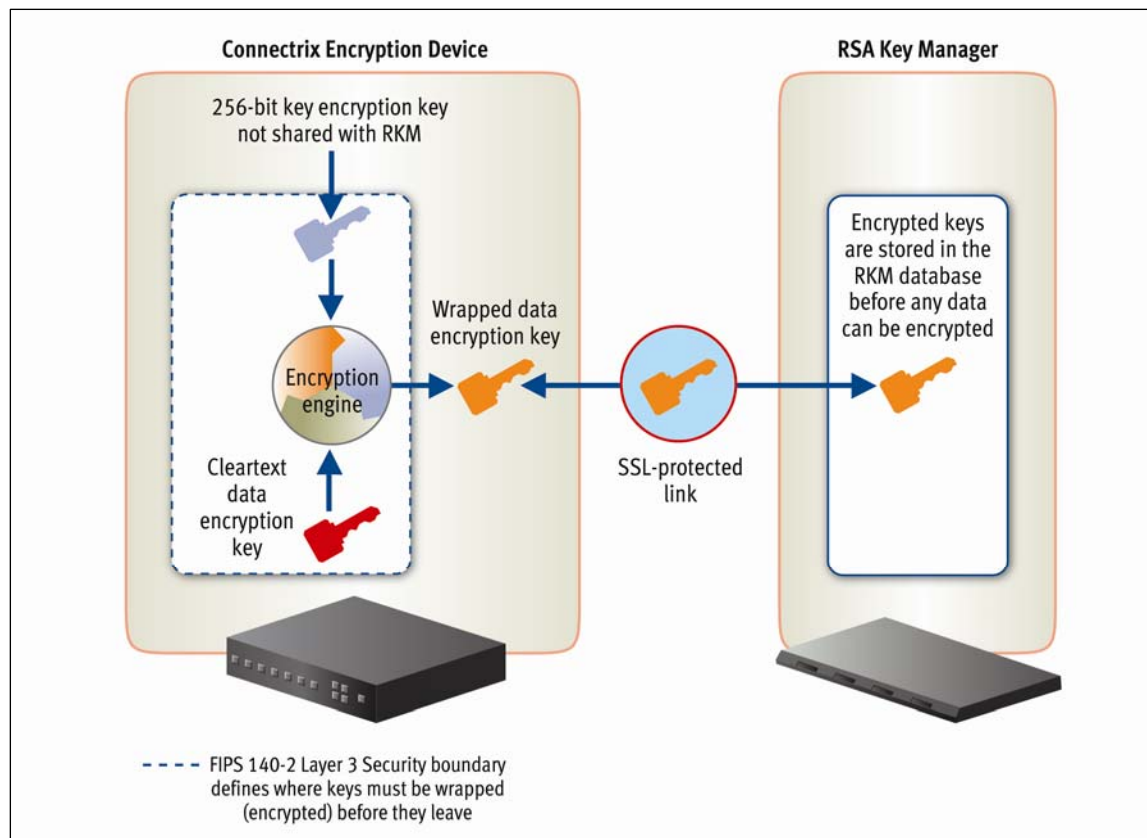


Figure 10. Vaulting keys to RKM for the Datacenter

RKM writes additional audit information to its own log file, in addition to that provided by Connectrix encryption. Information written to the log file includes:

- DEK-related events, such as generation of a DEK, generation of a new DEK, or location of a requested DEK.
- Key distribution events, such as a request, are received for a new DEK or a DEK is sent to a client.
- Administrator events, such as initiation or termination of access to RKM, creation of a new key class, creation of a new key policy, or creation of a new client entity.

In addition to this RKM server log, additional auditing information is provided by log files managed by related components, such as the database manager for the RKM repository. Combined with the Connectrix log files, the RKM audit capabilities provide a comprehensive view of key management activity in the Connectrix encryption environment.

CONCLUSION

EMC offers secure encryption solutions for the highest-performing data center applications in the world. At 96 Gbps of encryption processing power per Connectrix encryption device, customers can easily deploy this powerful solution for multiple applications. With RKM providing cost-effective, policy-based key management, the needs of multiple organizations can be addressed with one application. Together, the Connectrix encryption device and RSA Key Manager for the Datacenter form an unmatched solution for securing large amounts of customer data.

The service divisions of both EMC and RSA can provide needed assistance in deploying encryption solutions. From evaluating what data should be encrypted to meet government regulations to configuring key policies, the experts in both companies can lead customers to a safe and secure encryption solution. The complex nature of securing sensitive information is made much easier when Connectrix and RSA become part of the solution.

EMC², EMC, CLARiiON, Connectrix, Symmetrix, and where information lives are registered trademarks or trademarks of EMC Corporation in the United States and other countries. RSA is a registered trademark or trademark of RSA Security Inc. All other trademarks used herein are the property of their respective owners. © Copyright 2009 EMC Corporation. All rights reserved. Published in the USA. 7/09 White Paper GA-TB-131-00 (CSG7381)

