



The Security Division of EMC

RSA Technology Solution Brief

## PowerPath® Encryption with RSA

The EMC Solution for Securing Data in Enterprise Storage

PowerPath Encryption with RSA is a powerful tool for ensuring the confidentiality of critical information in the enterprise. Leveraging the unique position that PowerPath has in the I/O stack – below the application level, database level and file system level but above the HBA and I/O drivers – PowerPath Encryption with RSA enhances the scalability and heterogeneous support of storage arrays that PowerPath provides with security capabilities that are unique in the industry.

PowerPath® Encryption with RSA is a host-based solution which uses strong encryption to safeguard and prevent unauthorized access to sensitive data on disk devices. It also incorporates RSA® Key Manager for the Datacenter for centralized, enterprise-level key management. PowerPath Encryption encrypts a single device, a range of devices, or an entire storage array. The storage array can be an EMC® Symmetrix® or EMC CLARiiON® storage array. The device can reside on direct-attached storage, on network-attached storage, or on a storage area network.

The most important features of PowerPath Encryption with RSA include:

- Transparent data encryption. PowerPath virtual logical devices are implemented as pseudo devices below the file system and logical volume level and above the physical device level. Therefore, no application changes are needed to use PowerPath Encryption with RSA to encrypt data written to a disk device and decrypt data read from it.
- Comprehensive security services provided by RSA Key Manager for the Datacenter. PowerPath Encryption with RSA leverages the RSA Key Manager to implement strong encryption to protect data on disk devices. RSA Key Manager provides centralized key management and automatic provisioning of encryption keys.
- Data migration capabilities. PowerPath Encryption with RSA leverages host copy services to migrate plain text data on unencrypted disk devices to ciphertext data on encrypted disk devices.
- Multi-pathing, load balancing and fail-over. PowerPath Encryption with RSA can leverage PowerPath software (separately licensable) to provide Multi-pathing, load balancing, and fail-over for encrypted disk devices.
- Replication support. PowerPath Encryption with RSA works with EMC array-based replication products, such as EMC SRDF®. No additional steps need to be added to existing replication procedures to use PowerPath Encryption with RSA with replicas.
- Protection of existing storage infrastructure investment. PowerPath Encryption with RSA works with EMC Symmetrix and EMC CLARiiON storage arrays.

PowerPath Encryption with RSA encrypts and decrypts all user data on a virtualized logical unit. It does not encrypt PowerPath meta data or operating system meta data accessed below PowerPath. It also does not encrypt meta data that is not accessible to PowerPath, such as on internal devices. Further, PowerPath does not encrypt devices that are needed by the operating system during boot sequence before PowerPath is loaded, such as boot devices, swap devices and dump devices.

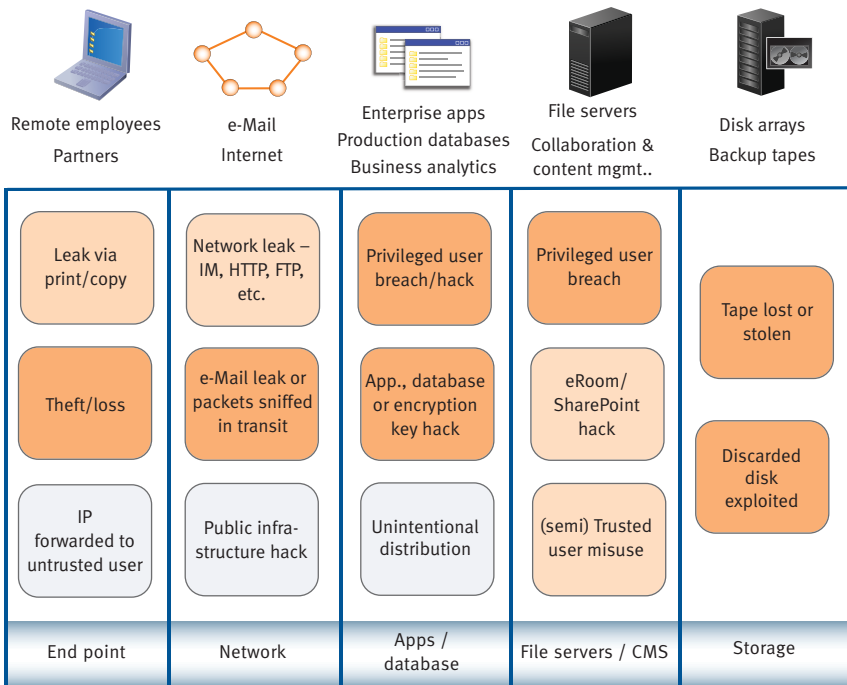


Figure 1. Data Locations and Threats

- High risk incident
- Medium risk incident
- Low risk incident

## Securing Data at Rest with PowerPath Encryption with RSA

In many enterprises, the most difficult problem in security today is securing sensitive data. Increasing regulatory and legislative demands and the constantly changing threat landscape have brought data security to the forefront of IT issues.

Enterprises face many threats to the security of their data. Backup tapes may be stolen or lost. Privileged users may obtain unauthorized access to data. Data may be inadvertently leaked outside the enterprise in email messages or attachments. Trojan viruses and other malware attacks may provide hackers and criminals with access to corporate systems.

As shown in Figure 1, several of the most important threats are directly related to protection of the storage environment, in particular the threats related to re-purposed or discarded media.

PowerPath Encryption with RSA protects data confidentiality by adding encryption functionality to a

PowerPath pseudo device. The encryption-enabled pseudo device is called a virtual logical unit, which shares the name space as a PowerPath pseudo device. A virtual logical unit sits beneath the application, file system, and Logical Volume Manager level and above the physical device level. As shown in Figure 2, when an application or file system writes data to a virtual logical unit, the PowerPath Encryption manager encrypts that data before writing it to a physical storage device. Conversely, when an application or file system reads data from a virtual logical unit, the PowerPath Encryption manager decrypts the data before passing it back to the application or file.

From the point of view of applications, data remains unencrypted, which means that applications are unaffected by enabling PowerPath Encryption with RSA. Similarly, upstream de-duplication devices are not impacted because they continue to see unencrypted data. By using PowerPath Encryption with RSA with array-based replication at production and recovery sites, data security can be integrated immediately into business continuity operations without disruption or increased administration.

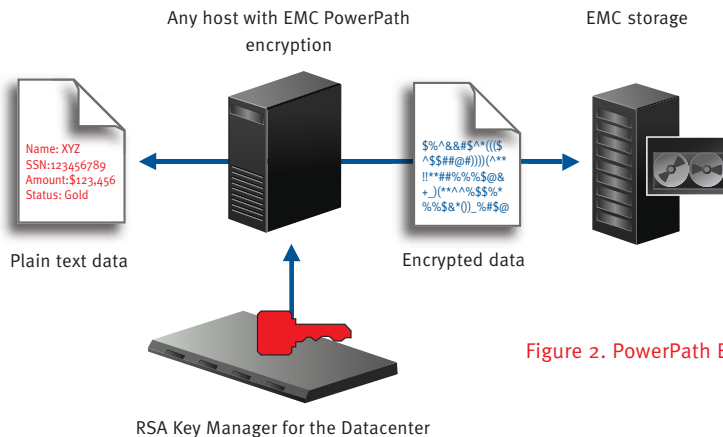


Figure 2. PowerPath Encryption with RSA

### Solution Use Cases for PowerPath Encryption with RSA

PowerPath Encryption with RSA addresses four primary use cases related to data security:

- It helps address compliance and industry regulations such as PCI, SOX, SB 1386, UK DPA act, European directive 95/46/EC, as well as internal security requirements for securing information.
- It limits exposure to security breaches, such that even if someone is able to access the storage media through an alternate path, the data is still protected to prevent unauthorized access to sensitive information.
- It secures data moving through the storage area network, from host to SAN switch to array.
- It enables infrastructure compartmentalization, such as to support multi-divisional enterprises and information service providers.

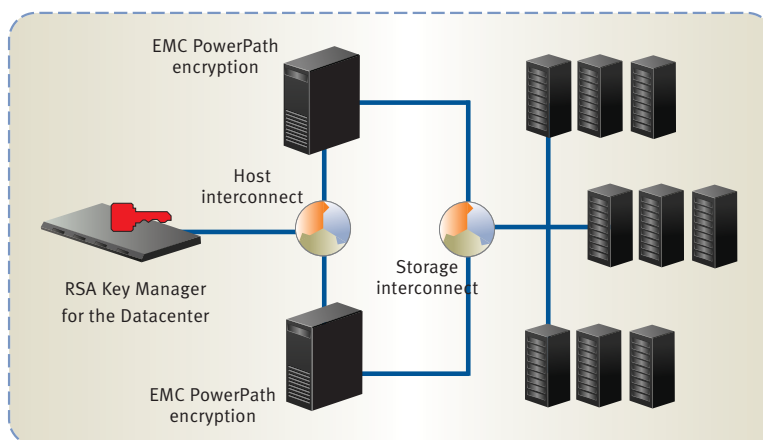
In a recent Enterprise Strategy Group survey, 72% of respondents found government regulations and compliance the biggest motivators for protecting confidential data. For example, California Senate Bill 1386 (now CA 1798) mandated that, as of July 1, 2003, state government agencies as well as companies and nonprofit organizations, regardless of geographic location, must notify California customers if personal information maintained in computerized

data files have been compromised by unauthorized access. U.S. federal legislation such as the Gramm-Leach-Bliley Act, Sarbanes-Oxley Act, HIPAA and national data privacy laws, as well as industry initiatives such as PCL Data Security Standard, have recommended or mandated encryption as a core mechanism for securing data. As a result, encryption is typically a critical part of enterprise data security and privacy strategies for many companies.

By securing data on enterprise storage, PowerPath Encryption with RSA ensures that the potential exposure of sensitive data on discarded, re-used or stolen media is reduced or eliminated. As long as the key used to encrypt the data is secured, encrypted data cannot be read; this is the reason, for example, why data encryption establishes a “safe harbor” for PCL-compliant enterprises. In addition to protecting against threats related to physical removal of media, this also means that media can readily be re-purposed by destroying the encryption key used for securing the data previously stored on that media. In this way, disk rotation, migration and upgrade are secured, without changes to operational procedures.

Replication and back-up capabilities that are downstream from PowerPath Encryption with RSA, such as EMC SRDF, see encrypted rather than

Figure 3. Secured Area



plaintext data. This means that the data is secured in these cases not only at rest but also in transit, whenever the data is being written to or read from the storage via PowerPath. Threats such as internal and external tapping into the data stream are addressed through this non-disruptive application of encryption to existing business continuity strategies.

PowerPath Encryption with RSA provides significant benefits to shared service providers with consolidated storage, such as multi-tenant data centers. These companies must secure not only their own data, but also that of their customers. By controlling access to data at the storage level, and thereby ensuring confidentiality, PowerPath Encryption with RSA provides a layer of security that complements the authorization capabilities provided by other infrastructure components and applications used by service providers. This same capability is also important as a way to reduce the risk of insider attacks in general, and to support such requirements as enforcing compartmentalization of legal entities within a single enterprise.

#### PowerPath Encryption with RSA Architecture

The primary purpose of encrypting data is to control how data is accessed.

PowerPath Encryption with RSA prevents access to data when it is removed from a secured area, as shown in Figure 3.

The configuration shown in Figure 3 represents a secured area within a data center that is secured both physically, such as by requiring key-card access to the computer room, and electronically, such as by firewalls and other perimeter security devices. Components within the secure area are typically trusted, though access control mechanisms are also implemented within the secure area to prevent insider attacks.

One or more PowerPath Encryption hosts are established in this secure area. The PowerPath hosts have either SAN (for Fibre Channel) or IP (for iSCSI) connectivity to the storage within the secure area. All components of PowerPath Encryption with RSA, with the exception of the RSA® Key Manager for the Datacenter server, reside on these hosts. These components include the following RSA Key Manager-related components:

- PowerPath driver (kernel space) and associated user-space software.
- RSA BSAFE® cryptographic libraries that encrypt and decrypt data, running in the PowerPath kernel.
- RSA® Key Manager client libraries that handle communication with the RSA Key Manager for the Datacenter server and provide local caching for encryption keys.
- RSA Key Manager client configuration files that establish such parameters as the RSA Key Manager for the Datacenter server to which to connect.
- An encrypted file, referred to as the Lockbox, used to securely store passwords and a master key for protecting configurations. Storing the secrets in the lockbox enables the secrets to be maintained across system reboots.

RSA Key Manager for the Datacenter, discussed in detail later in this paper, provides encryption key management capabilities for all PowerPath Encryption hosts, including secure key generation, storage, distribution and audit. As an enterprise-level capability, it also provides key management for many other encryption capabilities in the enterprise, such

as RSA Key Manager with Application Encryption, EMC Connectrix® MDS Storage Media Encryption and Oracle 11g Transparent Data Encryption.

## Enterprise Key Management for PowerPath Encryption with RSA

Because encryption offers protection for the data itself, rather than for a device or a host, it is a powerful tool for enforcing your security policies. The data security provided by encryption is only as good as the generation, protection and management of the keys used in the encryption process—the importance of which is increased by the growing pervasiveness of encryption throughout the enterprise. Encryption keys must be available when they are needed, but at the same time access to keys must be tightly controlled so that they are provided only to authorized entities. The keys themselves, as well as the information required to enable the use of the key during decryption activities, must be preserved for the lifetime of the data. This is especially important for enterprise storage environments where encrypted data is kept for many years.

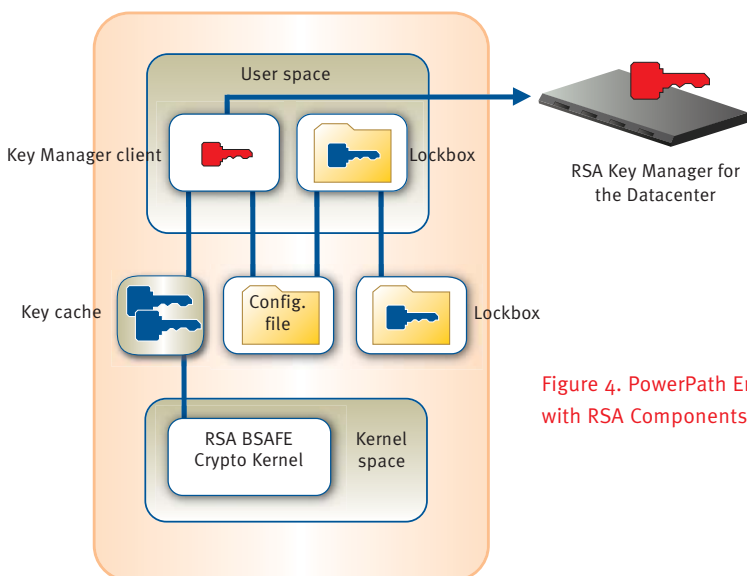


Figure 4. PowerPath Encryption with RSA Components

Because of the critical importance of key management in encryption solutions, PowerPath Encryption was designed from the ground up to be integrated with RSA Key Manager for the Datacenter (RSA Key Manager or RSA Key Manager). All instances of PowerPath Encryption are sold with RSA Key Manager, completing the PowerPath Encryption with RSA solution. As shown in Figure 5, RSA Key Manager provides enterprise key management for a broad range of encryption environments, establishing a pervasive and secure infrastructure for this essential component of data security.

All key generation, distribution and management capabilities required for PowerPath Encryption are provided by RSA Key Manager for the Datacenter, according to the best practices defined by industry standards such as NIST 800-57 and ISO 11770. These best practices include:

- Central management of encryption key policy, including algorithms supported, key length and key lifetime.
- Central management of encryption key operations, including generation, integrity checking, distribution, backup and audit.
- Secure, durable storage of keys.
- Secured access to keys, both administratively and programmatically.
- Support for high-availability and disaster recovery.

RSA Key Manager consists of two primary components:

RSA Key Manager for the Datacenter running on a system separate from PowerPath, generates, manages and audits encryption keys.

RSA Key Manager client libraries, integrated into PowerPath, provide local key caching and handle all communication between the PowerPath Encryption host and the RSA Key Manager for the Datacenter server.

All communications between the RSA Key Manager client and the RSA Key Manager server are encrypted using Secure Sockets Layer (SSL) to protect against insertion, man-in-the-middle and sniffer attacks. The RSA Key Manager client and server are mutually authenticated, to protect against spoofing attacks by unauthorized clients and servers. In addition, the RSA Key Manager server checks the client identity against its authorization rules, to be sure that an encryption key requested by a particular PowerPath host can be sent to that host. This minimizes the risk of Trojan viruses or other malware acquiring keys that can be used to decrypt sensitive data.

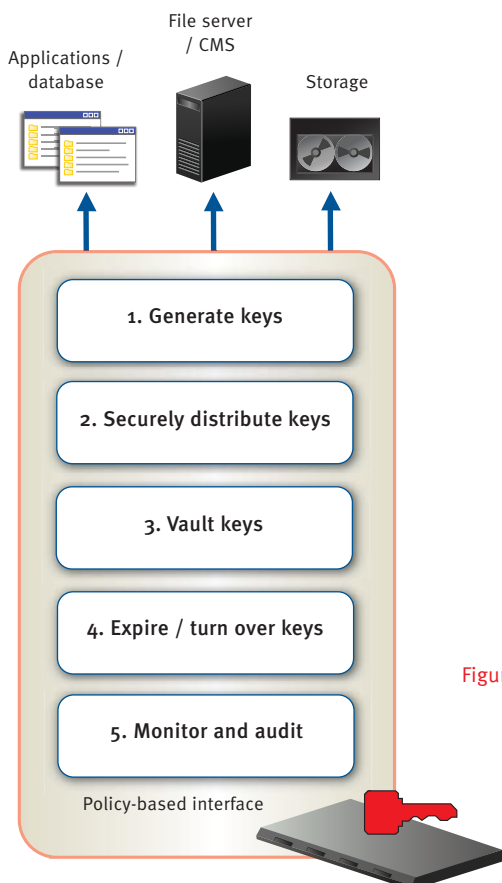


Figure 5. RSA Key Manager Ecosystem

---

## PowerPath Encryption with RSA Capabilities

---

Setting up and using PowerPath Encryption with RSA are straightforward operational processes. This section describes these primary use cases for PowerPath Encryption with RSA.

### Setting up Encryption

There are two administrative roles required for setting up PowerPath Encryption with RSA:

- RSA Key Manager for the Datacenter Security Administrator
- PowerPath System Administrator

The RSA Key Manager Security Administrator is responsible for the system on which the RSA Key Manager server software is running. Responsibilities for this individual include initializing RSA Key Manager, setting up identity groups and creating credentials and certificates required for RSA Key Manager client and server authentication. Once setup is complete, this individual performs the ongoing administrative tasks for RSA Key Manager, such as monitoring RSA Key Manager logs.

In order to set up RSA Key Manager to handle encryption keys for PowerPath, the RSA Key Manager Security Administrator begins by setting up the authentication credentials for trusted communication between the RSA Key Manager server and the RSA Key Manager client. Since RSA Key Manager authentication is based on PKI certificates, this entails creating certificates for the client and server, by obtaining them either from a public certificate authority or from a certificate authority set up in the enterprise where PowerPath encryption is deployed. The certificates that will be issued to PowerPath instances are then deployed on the PowerPath host and also defined as identities in RSA Key Manager. Once the authentication environment is set up, the RSA Key Manager Security Administrator creates the encryption key policies that will be applied to keys

created for PowerPath instances, including the algorithm to be used for PowerPath Encryption, the key lengths and the key life times.

PowerPath Encryption with RSA supports the AES (Advanced Encryption Standard) algorithm in either of two modes: CBC (Cipher Block Chaining) or XTS (Xor-Encrypt-Xor-based Tweaked CodeBook with CipherText Stealing). Since performance is generally better with XTS mode in PowerPath Encryption, this mode is recommended. For either mode, 256-bit encryption (for XTS, two 128-bit keys) should be used.

The PowerPath System Administrator is responsible for the host on which PowerPath is running. This individual must have root privilege on the host in order to perform such tasks as enabling PowerPath Encryption and turning encryption on and off for specific logical units. Other responsibilities include migrating data from unencrypted to encrypted LUNs, managing lockbox passwords and updating the RSA Key Manager-related configuration information for PowerPath Encryption with RSA.

In order to set up PowerPath Encryption on the host, the PowerPath System Administrator also begins by setting up the authentication environment for PowerPath communication with RSA Key Manager. This is done by saving the trusted PKI root certificate and host credential files in the root directory on the host system. The PowerPath System Administrator then completes the set up by creating a configuration file from the template provided and running a configuration script that enable PowerPath Encryption.

### Reading and Writing Encrypted Data

An administrator using the PowerPath commands can turn encryption on for a particular logical unit. This operation is destructive – any data on the logical unit is no longer accessible. Turning encryption on involves provisioning a new data encryption key for that logical unit. At the time that this command is run, a unique identifier is stored in PowerPath meta data on the logical unit. This identifier can be used to

retrieve the data encryption key for the logical unit. At the same time, the data encryption key is stored in non-pageable kernel memory for use in reading data from and writing data to the logical unit.

Reading and writing encrypted data is transparent to applications. As shown in Figure 6, PowerPath resides below volume management, file system and applications, providing access to data through virtual logical units used by applications as they would any other logical device.

When an application, DBMS or file system performs a write operation, the PowerPath filter driver in kernel space receives the plaintext data. It uses the previously-stored key for the virtual logical unit to encrypt the data and send it to the storage device. Similarly on a read operation, the kernel space PowerPath filter driver receives the encrypted data and uses the previously stored key to decrypt the data before sending it to the application, database or file system.

### High-Availability PowerPath Encryption with RSA

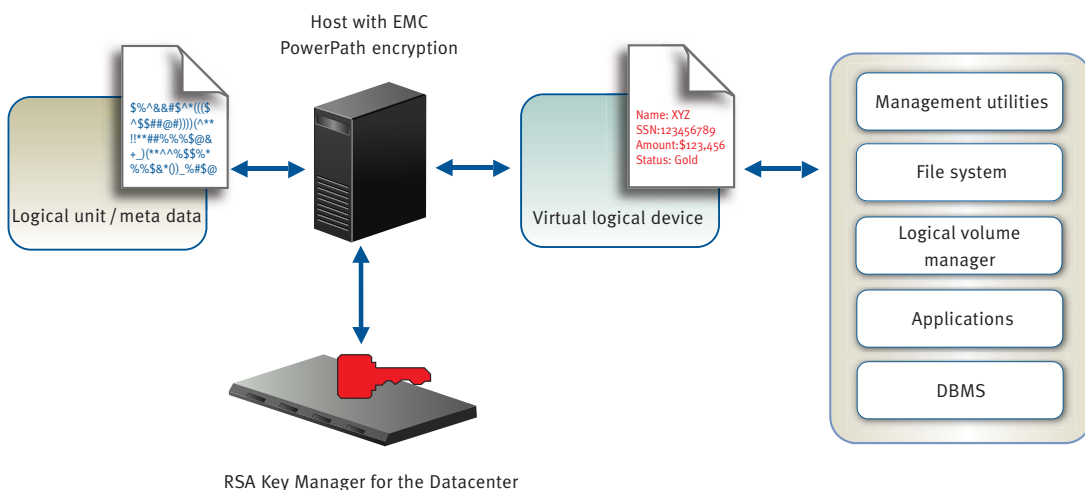
PowerPath Multi-pathing provides several important features to ensure high availability of data:

- **Unattended operations.** PowerPath Encryption with RSA does not require operator intervention in order to be started or restarted.

- **Automatic path fail-over.** PowerPath increases server access to data on EMC Symmetrix, EMC CLARiiON, and non-EMC arrays. It moves I/O workloads across multiple paths to ensure the fastest possible I/O speed.
- **Automatic detection and restore of failed components.** PowerPath Auto Detect automatically detects a path failure, then re-routes all existing I/O in transit on that path to another active path, maintaining application availability and continuous data access. Once the failed path has been restored, PowerPath Auto Restore automatically re-establishes access to the first path, permitting data flow down it again.
- **Dynamic load balancing.** PowerPath evenly distributes I/O among all available paths via a comprehensive set of sophisticated load-balancing policies, which results in more efficient data access and increased availability.

Once configured, PowerPath Encryption with RSA operates in unattended mode, where various system parameters are used to retrieve items from the Lockbox as needed. Unattended operations, such as starting or restarting PowerPath Encryption with RSA, are illustrated in Figure 7.

Figure 6: Reading and Writing Encrypted Data



On startup or reboot of a PowerPath host, data encryption keys previously used by the host are available in the local persistent key cache, secured by being themselves encrypted. At host startup, PowerPath code in the kernel requests the daemon (service) to lookup a key for each encrypted device. The daemon uses the RSA Key Manager client code to retrieve the key and provide it to the PowerPath kernel component which stores it in non-pageable, kernel memory within PowerPath. Note that the data encryption key is decrypted by the RSA Key Manager client code prior to providing it to the daemon. The unencrypted data encryption key stored in the kernel is then used by PowerPath to call RSA BSAFE cryptographic code to perform the encryption and decryption for that specific device.

If an encrypted device has never been configured to the host, then the RSA Key Manager client code will retrieve the data encryption key from the RSA Key Manager server over the network, as the key will not be in the persistent cache. Once retrieved, it is written into the cache as well as being provided to the daemon to provide to the PowerPath kernel. This

happens whether the not-yet-configured device is encountered at start-up or is configured after the host starts up.

PowerPath acts as a filter driver within the I/O stack of the operating system. It intercepts I/O requests to a device, allocating them across the available functioning paths, reducing bottlenecks, managing availability and improving performance. Figure 8 shows this architecture, with PowerPath using multiple paths to optimize the queue depth on all paths.

Because the Channel Directors or Storage Processors are reading from and writing to cache and not from and to disks, any Channel Director/Storage Processor can handle any request. This allows PowerPath to constantly tune the host I/O to adjust to changing loads from the applications running on the server and to ensure on-going operations despite loss of components in the I/O path.

PowerPath allows the administrator to set up various fail-over policies, such as round-robin versus path fail-over only. All PowerPath high-availability options are supported by PowerPath Encryption with RSA.

The accessibility of encryption keys is also a critical factor in high-availability. RSA Key Manager addresses this in two ways. First, as described earlier, keys are cached locally in each PowerPath instance, so that the need to connect to the RSA Key Manager for the Datacenter server is minimized in normal operations. Second, the RSA Key Manager for the Datacenter server supports both local high-availability and disaster recovery configurations, such as the one shown in Figure 9.

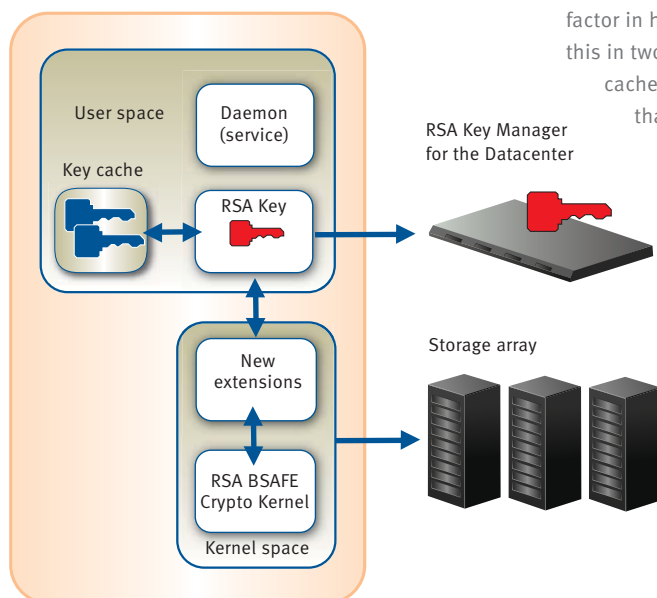


Figure 7. Unattended Operations

Figure 8: PowerPath Multi-channel Support

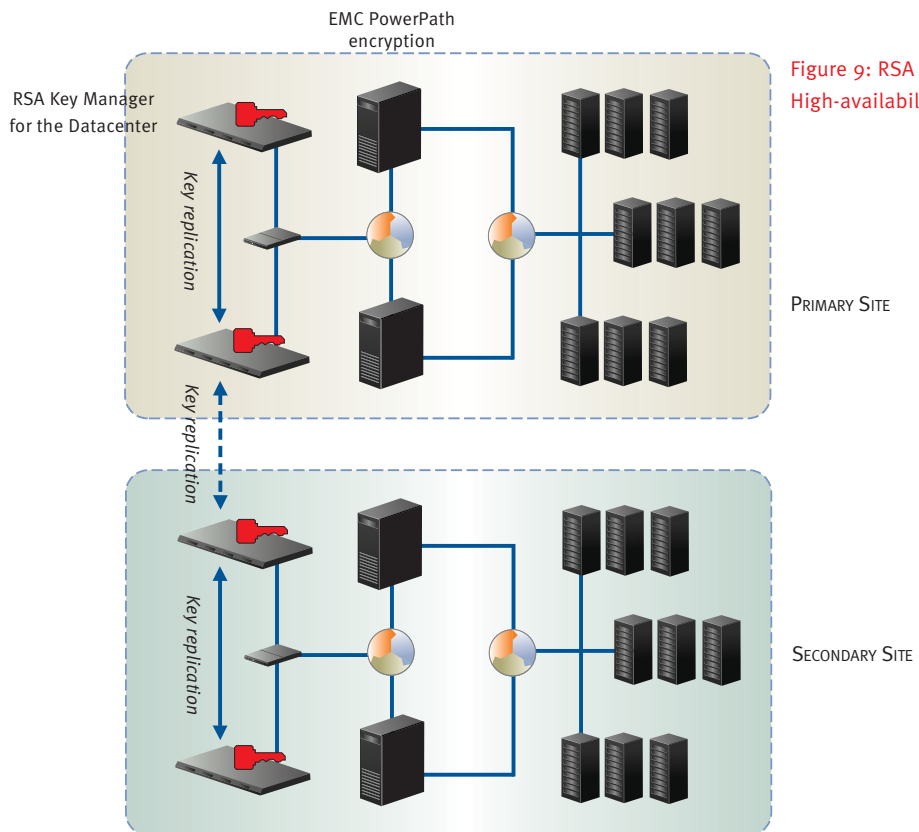
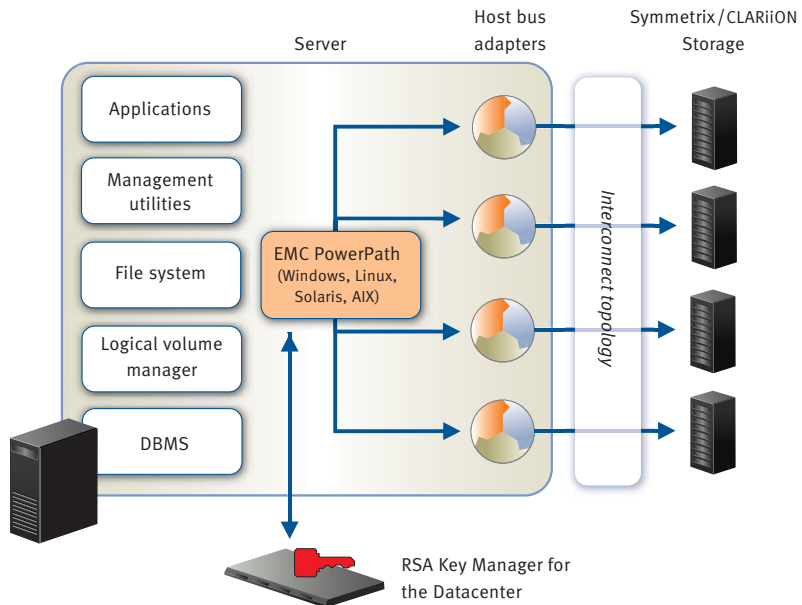


Figure 9: RSA Key Manager High-availability

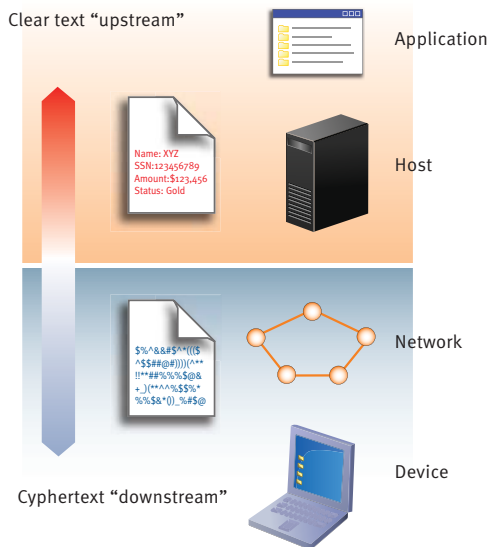


Figure 10: Upstream and Downstream Operations

In this configuration, redundant RSA Key Manager for the Datacenter appliances are deployed in each location, with encryption keys securely propagated between these appliances and between the sites. Communication between the PowerPath hosts and the RSA Key Manager appliances is mediated by re-directors that handle both load-balancing and fail-over.

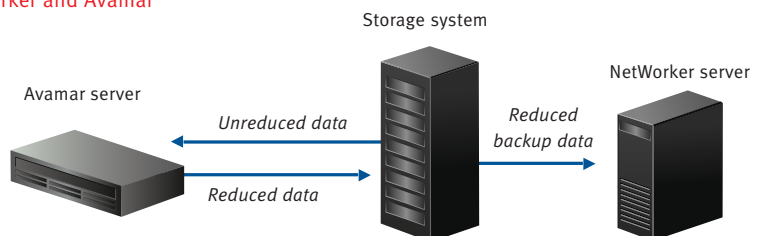
### Backing up Encrypted Data

Backup operations, in general, continue to work without change when using PowerPath Encryption with RSA. However, as shown in Figure 10, whether the data is backed up in plaintext or in encrypted form depends on whether the backup operation happens “upstream” or “downstream” of PowerPath Encryption.

When the backup application operates on data upstream of PowerPath Encryption, as is the case with EMC NetWorker® with EMC Avamar®, the data is read by the backup application as clear text. This is shown in Figure 11.

In this case, NetWorker walks the file system of the PowerPath-protected system and does the indexing of the material to be backed up. NetWorker then sends the data to Avamar via an Application-Specific Module (ASM) to be de-duplicated. Avamar returns the reduced data (as hashes) to NetWorker, which completes the back-up of the reduced data.

Figure 11: Upstream Backup with NetWorker and Avamar



When the backup application operates on data downstream of PowerPath Encryption, then the data is backed up as ciphertext, that is, in encrypted form. This occurs with physical backups performed by NetWorker, for example. In this case, the restore operation will return encrypted data to the target PowerPath environment, which must have access to an instance of RSA Key Manager for the Datacenter containing the keys for that data in order for the data to be decrypted.

### Enabling Replication

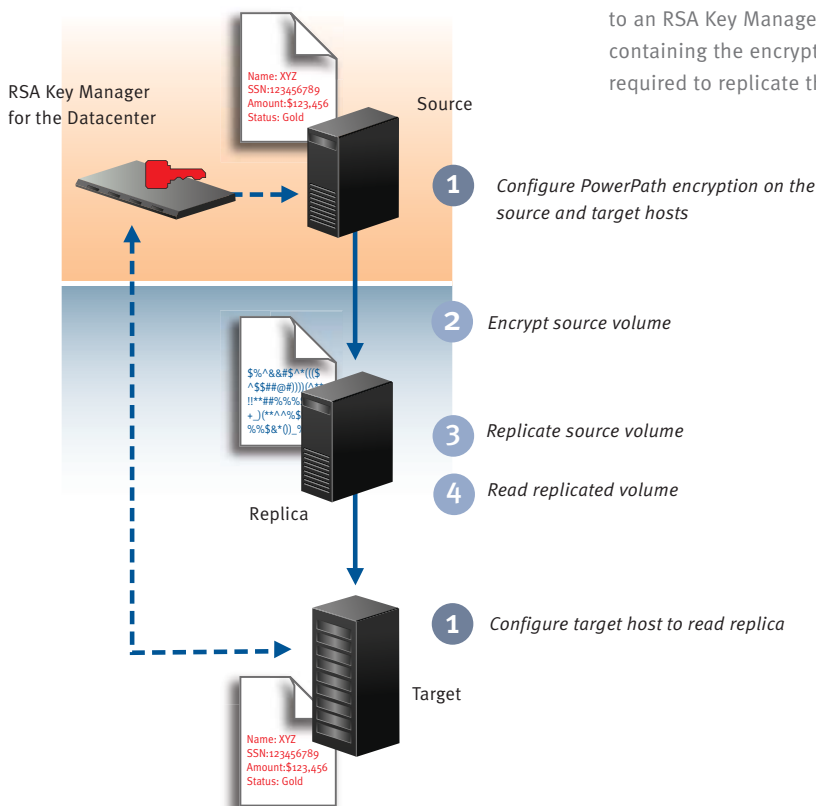
Replication products can also operate on either upstream or downstream data. As with backup, upstream applications on PowerPath Encryption hosts continue to operate normally because data is not encrypted.

For replication products that operate downstream, data security is integrated into business continuity operations by using PowerPath Encryption with RSA with array-based replication at the source and target sites. This approach is shown in Figure 12.

As shown in this diagram, the first step is to install PowerPath Encryption with RSA on the source and target hosts and configure them to access RSA Key Manager for the Datacenter. The source volume is then encrypted by migrating the unencrypted data to encrypted data, as discussed below. Next, the encrypted volume is replicated to the target array. The target host is then configured to access the replica. Since it has access to the encryption key to decrypt the volume, it can then access the encrypted data.

The meta data stored by PowerPath Encryption in the encrypted LUN provides enough ID information (but not the key itself) to get the key from RSA Key Manager for the Datacenter for any PowerPath host where encryption has been enabled. Other than making sure the source and target hosts have access to an RSA Key Manager for the Datacenter server containing the encryption key, nothing else is required to replicate the encrypted data.

**Figure 12: PowerPath Encryption with RSA and Downstream Replication**



## De-duplication and Compression

Whether backup or replication tools operate on upstream or downstream data affects both compression and de-duplication. As shown in Figure 13, for upstream applications such as NetWorker with Avamar, capacity optimization such as compression and de-duplication can be performed, as these applications see the plaintext version of the data.

Similarly, de-duplication can be performed upstream of PowerPath Encryption, such as with EMC Avamar.

Replication and backup performed downstream of PowerPath Encryption benefit from the protection that encryption provides for the data as it moves across the network. At the same time, however, neither compression nor de-duplication are effective downstream of PowerPath Encryption. Encrypted data is typically not compressible because encryption

transforms spaces and character repetition in a data object, making them opaque to compression engines. The same plain-text data at different block locations on a LUN encrypts to different cipher-text, so it cannot be de-duplicated.

This means that the de-duplication and compression capabilities in RecoverPoint and asynchronous SRDF, for example, will not provide benefits in terms of reducing network traffic when replicating storage encrypted with PowerPath Encryption with RSA. However, both RecoverPoint and SRDF can benefit from the security benefits and encryption provides for data in flight.

## Migration of Encrypted Devices

PowerPath Migration Enabler Host Copy, which is included with PowerPath Encryption with RSA, supports a number of critical encryption-related operations for data migration:

- Migration of unencrypted data onto encrypted devices (that is, unencrypted to encrypted data migration).
- Migration of encrypted data off encrypted devices to unencrypted devices (that is, encrypted to unencrypted data migration).
- Re-keying of encrypted data (that is, encrypted to encrypted data migration).

The first step is to ensure that the target device has sufficient space for the encrypted data, as it must be large enough to accommodate the encryption meta data. Once you use the `powervt` command to turn encryption on for the target device, use the `format` command to read the label to ensure that it is the same size or larger than the source device for the migration. Then follow the usual steps for a PowerPath Migration Enabler migration, using the `powermig` command line interface (CLI). If the target device is not large enough, the `powermig` setup command will fail.

During the migration, prior to commit (i.e., during the `targetSelected` state in PowerPath Migration Enabler), the results can be checked to ensure that all the data was migrated successfully. When the migration is completed, the target device will be exactly the same size as the source device, from an operating system point of view. If there is unused space, the `powervt`

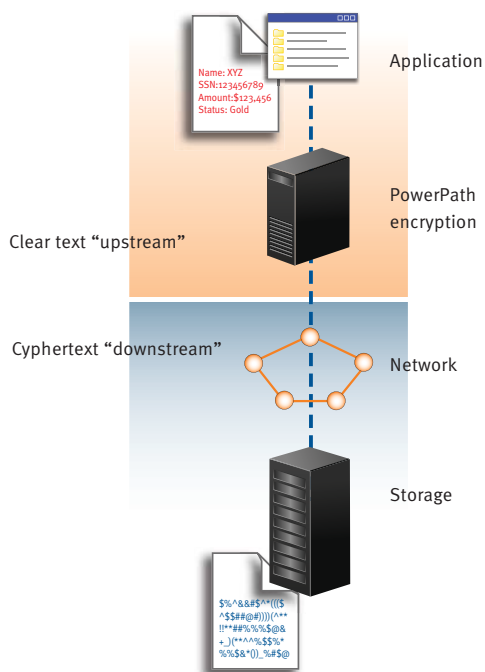


Figure 13: Upstream Compression with PowerPath Encryption with RSA





## RSA is your trusted partner

RSA, the Security Division of EMC, is the premier provider of security solutions for business acceleration, helping the world's leading organizations succeed by solving their most complex and sensitive security challenges. RSA's information-centric approach to security guards the integrity and confidentiality of information throughout its lifecycle – no matter where it moves, who accesses it or how it is used.

RSA offers industry-leading solutions in identity assurance & access control, data loss prevention & encryption, 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).

©2008 RSA Security Inc. All Rights Reserved. RSA, RSA Security, BSAFE and the RSA logo are either registered trademarks or trademarks of RSA Security Inc. in the United States and/or other countries. EMC, EMC<sup>2</sup>, Avamar, CLARiiON, Connectrix, NetWorker, PowerPath, SRDF, Symmetrix, and *where information lives* are registered trademarks of EMC Corporation. All other products and services mentioned are trademarks of their respective companies.

RKMPP SB 0808

**EMC<sup>2</sup>**  
where information lives<sup>®</sup>



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

The Security Division of EMC