EMC Symmetrix Data at Rest Encryption

Detailed Review

Abstract
This white paper provides a detailed description of EMC® Symmetrix® Data at Rest Encryption features and operations.
Table of Contents

Executive summary ........................................................................................................... 4
  Audience .......................................................................................................................... 4
  Terminology .................................................................................................................... 4

Data at Rest Encryption .................................................................................................. 5
  Key management ............................................................................................................ 7
    RSA Embedded Key Manager components ................................................................. 7
    DEK protection ............................................................................................................. 7
    Data integrity ................................................................................................................. 7
  Operational examples ................................................................................................... 8
    Installation of a Symmetrix system ............................................................................. 8
    Replacement of a drive .............................................................................................. 8
    Decommissioning of a Symmetrix system ................................................................. 9

Data at Rest Encryption options ...................................................................................... 9

Conclusion ...................................................................................................................... 9
Executive summary

Securing sensitive data is one of the greatest challenges faced by many enterprises. Increasing regulatory and legislative demands and the constantly changing threat landscape have brought data security to the forefront of IT issues. Several of the most important data security threats are related to protection of the storage environment. Drive loss and theft are primary risk factors. EMC® Symmetrix® Data at Rest Encryption protects data confidentiality by adding back-end encryption to the entire array.

Audience

The audience for this white paper includes:

- Customers, including IT planners, storage architects, and administrators involved in evaluating, acquiring, managing, operating, or designing security for an EMC networked storage environment.
- EMC staff and partners, for guidance and development of proposals.

Terminology

**Table 1. Symmetrix system terms**

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enginuity</td>
<td>EMC Symmetrix systems run the Enginuity™ operating environment.</td>
</tr>
<tr>
<td>Symmetrix Audit Logs</td>
<td>An immutable (not changeable) audit log that tracks security events on a Symmetrix system. The audit log allows administrators to identify any breaches in the system and prove compliance with data protection policies.</td>
</tr>
<tr>
<td>Symmetrix Service Processor</td>
<td>A component that monitors the system environment, provides remote notification and remote support capabilities, and allows EMC personnel to access the system locally or remotely.</td>
</tr>
<tr>
<td>SymmWin Application</td>
<td>A graphics-based tool for configuring and monitoring a Symmetrix system.</td>
</tr>
</tbody>
</table>

**Table 2. Encryption terms**

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>XTS-AES Algorithm</td>
<td>An XEX-based Tweaked Codebook (TCB) mode with Cipher Text Stealing (CTS) disk encryption used for the encryption of sector-based storage devices.</td>
</tr>
<tr>
<td>Data Encryption Key (DEK)</td>
<td>Uses key algorithms to encrypt and decrypt data and apply confidentiality protection to information.</td>
</tr>
<tr>
<td>Key Encryption Key (KEK)</td>
<td>Keeps DEKs secure during storage and transmission. The approved technique to protect DEKs is to use KEKs along with the AES Key Wrap algorithm.</td>
</tr>
<tr>
<td>Key Tag</td>
<td>A value that is permanently attached to an encryption key. Key tag verification in controller-based encryption guarantees reliable encryption without any potential loss or corruption of data.</td>
</tr>
</tbody>
</table>
Data at Rest Encryption

Data at Rest Encryption provides hardware-based, on-array, back-end encryption for Symmetrix systems. Back-end encryption protects your information from unauthorized access when drives are removed from the system. Data at Rest Encryption provides encryption on the back end using Fibre Channel I/O modules that incorporate XTS-AES 256-bit data-at-rest encryption. These modules encrypt and decrypt data as it is being written to or read from a drive. All configured drives are encrypted, including data drives, spares, and drives with no provisioned volumes. In addition, all array data is encrypted, including Symmetrix File System and PowerVault contents.

Data at Rest Encryption incorporates RSA® Embedded Key Manager for key management. With Data at Rest Encryption, keys are self-managed, and there is no need to replicate keys across volume snapshots or remote sites. RSA Embedded Key Manager provides a separate, unique DEK for each drive in the array, including spare drives.

By securing data on enterprise storage, Data at Rest Encryption ensures that the potential exposure of sensitive data on discarded, misplaced, or stolen media is reduced or eliminated. As long as the key used to encrypt the data is secured, encrypted data cannot be read. In addition to protecting against threats related to physical removal of media, this also means that media can readily be repurposed by destroying the encryption key used for securing the data previously stored on that media.

Data at Rest Encryption is compatible with all Symmetrix system features, allows for encryption of any supported local drive types or volume emulations, and delivers powerful encryption without performance degradation or disruption to existing applications or infrastructure.
The following illustration shows a high-level overview of the Data at Rest Encryption architecture:

Figure 1. Data at Rest Encryption architecture
Key management

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. However, the data security provided by encryption is only as good as the generation, protection, and management of the keys used in the encryption process. Encryption keys must be available when they are needed, but at the same time access to keys must be tightly controlled. 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.

Because of the critical importance of key management in encryption solutions, Data at Rest Encryption was designed to be integrated with RSA Embedded Key Manager. RSA Embedded 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 Data at Rest Encryption are provided by RSA Embedded Key Manager, according to the best practices defined by industry standards such as NIST 800-57 and ISO 11770.

The accessibility of encryption keys is a critical factor in high availability. Data at Rest Encryption addresses this by caching the keys locally so that the need to connect to RSA Embedded Key Manager is limited to maintenance operations such as the initial installation of the Symmetrix system, the replacement of a drive, or drive upgrades.

Key management events such as key creation, key deletion, and Key Manager recovery are reported in the Symmetrix Audit Log.

RSA Embedded Key Manager components

Data at Rest Encryption utilizes the following RSA software, which is compiled into the SymmWin application on the Symmetrix Service Processor:

- RSA Embedded Key Manager Server — an embedded version of RSA Key Manager Enterprise Server, which provides encryption key management capabilities such as secure key generation, storage, distribution, and audit.
- RSA Key Manager client — handles communication with the RSA Embedded Key Manager Server.
- RSA BSAFE® cryptographic libraries — provide foundational security functionality for RSA Embedded Key Manager Server and the RSA Key Manager client.
- RSA Lockbox — a hardware-and software-specific encrypted repository that securely stores passwords and other sensitive key manager configuration information.

DEK protection

The following features ensure the protection of the DEKs:

- The RSA Embedded Key Manager Server repository is encrypted with 256-bit AES using an RSA-generated random password, which is saved in the RSA Lockbox.
- All persistent key storage locations either contain wrapped or encrypted keys, or unwrapped keys that are protected from access by hardware. DEKs are wrapped by encrypting the key data using a standard AES keywrap operation that utilizes a KEK that is unique to each array.
- There are no backdoor keys or passwords to bypass security.

Data integrity

The following features allow Data at Rest Encryption to ensure that the correct key is used with the correct drive:

- DEKs stored in the RSA Embedded Key Manager include a unique key tag along with the key metadata, which is included with the key material while wrapping (encrypting) the DEK for use in the array.
During encryption I/O, the expected key tag associated with the drive is separately supplied along with the wrapped key.

During key unwrap (prior to starting an I/O) the encryption hardware checks that the key unwrapped properly and that it matches the supplied key tag.

Arrays with data encryption enabled have a special Physical Information Block (PHIB) located in reserved space at the beginning of each drive. Before the drive is made available for normal I/O operation, the PHIB contents are used to validate that the key used to encrypt the drive data matches the key in use by the array.

To prevent silent data corruption due to encryption hardware datapath failures, the hardware performs self-tests during initialization to ensure that the encryption/decryption logic is intact.

Operational examples
This section describes how Data at Rest Encryption works during several common operations.

Installation of a Symmetrix system
When an EMC Customer Engineer installs a Symmetrix system:
1. The EMC Customer Engineer enables Data at Rest Encryption by setting the DARE flag in the initial configuration file for the Symmetrix system.
2. The Symmetrix system installation script automatically installs the RSA software on the Service Processor during the installation process.
3. The RSA Embedded Key Manager Server generates DEKs for each drive in the array and a KEK that is unique to the array.
4. Enginuity generates Symmetrix Audit Logs for every key generation event.
5. The RSA Embedded Key Manager Server encrypts the keys and stores them in the local key repository file as non-volatile copies.
6. The RSA Embedded Key Manager Server wraps each DEK with the KEK, and Enginuity stores all of the keys on the array as encrypted, persistent backup copies.

   The KEK is programmed into write-only, non-volatile memory in the encryption hardware, which cannot be retrieved back from the hardware.

7. Enginuity initializes volumes using the DEKs and writes any incoming host data to the drives as encrypted data.

Replacement of a drive
When a customer or EMC Customer Engineer removes a drive from an array:
1. The RSA Embedded Key Manager Server securely deletes the key associated with the removed drive from the key repository on the Service Processor.
2. After the customer or EMC Customer Engineer installs the new drive and Enginuity verifies that it is working, the RSA Embedded Key Manager Server generates a new DEK for the drive and wraps the DEK using the KEK.
3. Enginuity generates Symmetrix Audit Log entries for the deletion of the old DEK and the creation of the new DEK.
4. Enginuity caches the new DEK, which replaces the previous drive's DEK.
5. Enginuity validates the contents of the drive and rebuilds the data using the new DEK.
Decommissioning of a Symmetrix system
When an EMC Customer Engineer decommissions a Symmetrix system:

1. The RSA Embedded Key Manager Server securely deletes all persistent copies of the keys in the key repository.
2. Enginuity zeroizes the cached keys stored within the array. The Symmetrix Audit Log becomes irretrievable from the array due to the key destruction.
3. A certificate file detailing the status of the keys involved in the array decommissioning operation is produced.

**Data at Rest Encryption options**
The following options apply to Data at Rest Encryption:

- Data at Rest Encryption is an install-time option only. If Data at Rest Encryption is not enabled during installation, it cannot be enabled at a later time. Conversely, if Data at Rest Encryption is enabled during installation, it cannot be disabled.
- All disk groups are encrypted. Mixing encrypted and unencrypted data within the array is not supported.

**Conclusion**
Data at Rest Encryption is an easy-to-use, minimal-maintenance solution for data-at-rest encryption. Data at Rest Encryption keeps information safe from drive theft or loss by providing back-end encryption for the entire array. By utilizing RSA Embedded Key Manager, Data at Rest Encryption is able to self-manage encryption keys, so manual key management is not required.

The following table describes the capabilities and benefits of Data at Rest Encryption as compared to other data-at-rest security products on the market:

### Table 3. Competitive comparison

<table>
<thead>
<tr>
<th>Capability/Benefit</th>
<th>EMC</th>
<th>Hitachi/HP</th>
<th>IBM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage physical protection</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Drive segregation</td>
<td>Yes: one key per drive.</td>
<td>Limited: one key per parity group with a maximum of 32 keys per array.</td>
<td>Yes: one key per drive.</td>
</tr>
<tr>
<td>Multi-layered protection and availability</td>
<td>Yes: redundant internal key backup.</td>
<td>No: requires manual key backup management.</td>
<td>No: arrays require access to one of multiple Tivoli Key Lifecycle Manager servers to boot successfully.</td>
</tr>
<tr>
<td>Operates without manual key management by users</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Compatible with all array capabilities</td>
<td>Yes</td>
<td>Yes</td>
<td>No: FDE is only available on FC drives and eliminates the use of Easy Tier.</td>
</tr>
</tbody>
</table>