

**WHITE PAPER**

**Encryption Best Practices:  
Protecting Backed Up Data**



# Encryption Best Practices

## CONTENTS

- Executive Summary . . . . . 3
- Encryption Best Practices Overview . . . . . 4
- People . . . . . 4
- Processes . . . . . 5
- Users and Secret Identifiers . . . . . 7
- Examples of Best Practices . . . . . 8
  - Example: Low Security Site . . . . . 8
  - Example: Medium Security Site . . . . . 9
  - Example: High Security Site . . . . . 10
  - Example Tracking Sheet . . . . . 11
- Conclusion . . . . . 12

SabreDisk, SabreMedia, and RXT are trademarks, and BlueScale, Spectra, Spectra Logic, and the Spectra Logic Logo are registered trademarks of Spectra Logic Corporation. All rights reserved worldwide. All other trademarks and registered trademarks are the property of their respective owners. All library features and specifications listed in this white paper are subject to change at any time without notice. Copyright © 2006 by Spectra Logic Corporation. All rights reserved.

## Executive Summary

Encrypting backed up data is increasingly becoming a priority, and developing procedures to easily manage encryption helps reinforce your data's security. The encryption types most commonly used, for example to secure commercial transactions over the Internet, are handled without requiring the user to know the encryption key. This kind of encryption, asymmetric encryption that uses a public key authority, is the most commonly used in protecting data.

To protect data you have backed up, symmetric encryption is preferable because the key is created, stored, and deleted locally, so the user backing up the data has control over the key. The fewer people that have access to the key, the more secure the encrypted data. A public key encryption method trusts the key value to an outside party; symmetric encryption protects the key with even greater security—local control. Along with control comes extra steps to protect the key. That means your site needs to put procedures in place so you protect the key, and at the same time, can quickly identify and retrieve the key when you need to decrypt the data.

As with most IT procedures, encryption best practices are simply a well thought-out series of standard tasks. Assuming that the encryption solution you are using enforces strong encryption, such as AES-256 (the federally approved encryption algorithm considered to be unbreakable), then the rest of the encryption best practices are simply a codification of common sense that includes:

- ♦ Having an overall security plan that includes the encryption of backed up data and defines the sets of data to be encrypted
- ♦ Identifying who can access encryption features and encrypted data
- ♦ Protecting key access with passwords and key nicknames (monikers) to shield the key so that the real key (that is, the numerical string) is never displayed as cleartext (that is, human readable text)
- ♦ Making backup copies of encryption keys
- ♦ Identifying how to track keys, passwords, and encrypted data

With Spectra® BlueScale™ Encryption, you can easily create and implement encryption best practices that keep your backed up data secure.

## Encryption Best Practices Overview

Symmetric encryption is used to encrypt backed up data, and differs from most digital security methods because it requires you to create and use an encryption key, which you track over the life of the stored data. Asymmetric encryption, which network and Internet encryption primarily rely on, automatically creates and deletes keys with a public key/private key method that requires no action on your part.

For backed up data, symmetric encryption is the best choice, because no external (public key) authority is involved. Your encryption solutions let you create, track, and, when appropriate, delete your own keys. Protecting encryption keys therefore is a new component of an overall organizational security strategy—and fortunately, one that's straightforward to implement.

Most of the best practices for encryption involve keeping encryption keys safe. With a few standard procedures in place and a complete, easy-to-use key management system, such as the Endura™ key management system for BlueScale Encryption, encryption best practices can be effortlessly implemented.

To summarize, encryption best practices involve three main categories: people, processes, and passwords.

### People

Identify the people on your site who are to be responsible for encrypting backed up data written to tape and to other portable media, such as mobile RXT™ SabreMedia disk packs. In any encryption system, multiple layers of security protect access to encryption, and people must supply the right passwords to access encryption features. BlueScale Encryption passwords are alphanumeric character strings.

For example, to access BlueScale Encryption, someone needs to:

- ♦ Log in with superuser privileges on the Spectra Logic library with BlueScale encryption
- ♦ Log in and enter the encryption password that lets you access encryption features

Identify and document the users who are to have responsibilities that involve encryption. It may be wise to have more than a single user familiar with passwords, depending on the size of your organization, so that if one person is not available, another can take over. Make sure that only authorized users know the encryption passwords, and that the passwords themselves are secure. See

*Users and Secret Identifiers* on page 7 for more information on selecting passwords and monikers.

## Processes

On an organizational level, you need to identify the level of security your site requires, and the data to be encrypted—for example, all data, or any combination of financial, email, intellectual property, identity-related information, and strategic data. These two decisions govern all processes that involve encryption. Further, make sure that you implement the strongest available security—BlueScale Encryption supports the strongest version of encryption available: federally approved AES-256, using 256-bit keys. Because this is implemented in hardware, the encryption is fast and the implementation of encryption (using hardware-based random key generation, which is a necessary step in creating an encryption key) is more secure.

Here is a brief description of some issues to consider when establishing encryption procedures:

- ♦ **Identify the level of security your site needs.**

BlueScale Encryption provides the same strong AES-256 encryption in both the Standard and Professional Editions. The Professional Edition supplies additional features and flexibility, and some extra layers of user authentication and additional security options. Both editions let you create partitions—that is, parts of the library that will each be seen as an individual library to the backup or networked environment.

Both editions permit a standard mode and a security initialization mode. In standard mode, when the library is powered on, all encryption partitions are enabled. In secure initialization mode, encryption partitions are not available on power up. These encryption partitions are only available following the login of both the superuser and the encryption user.

- ♦ **Identify any data sets that must be isolated from other encrypted data sets.**

Define partitions as necessary to handle the data. For example, if all of the site's data is to be encrypted on backup, then the single partition used by all Spectra Logic libraries by default should be sufficient. If, however, you are backing up some data without encryption, create a partition dedicated to encrypting data, and another for non-encrypted data.

- ♦ **Identify how you will protect, or escrow, keys.**

AES-256 encryption, a symmetric encryption method, is a private key method. Users must track each key, which BlueScale Encryption identifies only by a nickname, or moniker. The key itself is never displayed in clear text, and

is encrypted before a copy is made that can be exported and stored outside the library.

- ◆ **Identify the number of copies of each key to export and store, and the stored key's locations.**

Consider storing multiple copies of every key that you export (that is, copy it so that it is stored outside the library). You need to track each exported key copy. To help with this, you may want to investigate the use of an escrow company—a trusted private firm that keeps copies of your keys for you, so that the keys are off-site in case of disaster and separate from the data they encrypted, further securing your backed up data. It is important to make sure that at least one copy of each key is secure and readable (that is, uncorrupted), which ensures that you can restore your data. This is important because once keys are deleted, they are *not* recoverable. Once the key is gone, the data is inaccessible, and is considered deleted for most legal and all practical purposes.

- ◆ **Identify the key rotation plan—how often to create and use new keys.**

BlueScale Encryption Standard Edition stores one key in the library at a time. Professional Edition permits multiple keys per library, with a single key dedicated to each encryption partition. Often, organizations define a schedule associated with changing keys. For sites simply requiring protection for stored data, this may be a simple schedule such as changing keys once every six months, and destroying the keys only after the last set of data encrypted using that key is overwritten or destroyed.

- ◆ **Identify methods of tracking user logins, passwords, and monikers.**

Make sure you track the data required to access and identify keys, along with the location of stored data. Make sure this data is not stored with the encrypted data. Keep it on a system or in an archive that is not available on a network, and optionally one that uses encryption.

- ◆ **Optionally, identify a primary and secondary team.**

You may want to assign multiple encryption teams so that you have redundancy in your encryption processes. Although this means the information required to decrypt data is spread across more people, it also means that restoration of encrypted data may be much easier, and you may ultimately have more data protection given the extra layer of coverage. If a user leaves, you aren't in a position to lose data. This returns to the initial decision: how tightly to enforce security for your site.

- ◆ **Run drills.**

Run data recovery drills to confirm that your data is being encrypted properly, that keys are stored properly, and that you can recover your data efficiently. Make sure that these drills are part of your overall organizational security policy and strategy.

- ♦ **Outline the procedure to follow if keys are compromised.**

Create a procedure to follow if an unauthorized person may have had access to one or more keys. Make sure you can identify the data associated with the compromised key or keys, then re-key it, minimizing the potential for unauthorized data access.

## Users and Secret Identifiers

Defining access by role is standard user security, where the user has a password—a private character string—that only authorized users have access to. Spectra Logic BlueScale Encryption supports four categories of access:

- ♦ Superuser: all administrative privileges except encryption privileges
- ♦ Administrator: all superuser privileges except authorizing other users
- ♦ Operator: basic library maintenance tasks, such as media import and export
- ♦ Encryption user: password access lets superusers access encryption privileges

Monikers are the name or other alphanumeric identifier referring to the never-revealed true key value, which is a 256-bit key.

Best practices dictate that you should create standards that apply to creating password and key nicknames (that is, creating a moniker for a key). These standards should be based on your site's security requirements. For example, your site may require a high level of security for access to encryption partitions, in which case you may require some combination of the following:

- ♦ Long passwords
- ♦ Password combinations requiring alphabetic *and* numeric characters
- ♦ Passwords that do *not* correspond to dictionary entries
- ♦ Passwords are reset on predefined schedules

### References

Barker, Elaine, W. Barker, W. Burr, W. Polk, and M. Smid. *Recommendation for Key Management Part 1: General*. NIST Publication 800-57, 2005, p. 25

Guel Michele D. *A Short Primer for Developing Security Policies*, The SANS Institute, 2001.

M-Tech Information Technology, Inc. *Password Management Best Practices*, 2006.

Storage Networking Industry Association (SNIA), <http://snia.org/education>.

## Examples of Best Practices

### Example: Low Security Site

Description of organization: Small company with 75 employees.

Security Considerations	Processes
Security goals	Protecting company from legal liability associated with unauthorized access to data stored on tape, both onsite and offsite, including transport to the offsite location.
Encryption principals	IT administrator, company president, corporate legal counsel.
Data to encrypt	Financial and consumer identity data.
Level of security to implement	BlueScale Standard Edition: single key per library is sufficient. Standard initialization mode: encryption partitions are enabled at all times.
Data sets requiring isolation from other encrypted data	None: a single partition for encrypted data is sufficient.
Key escrow method	Staff at company will escrow keys at a site remote from the data storage location.
Number of copies of each key to store, and the stored keys' locations	Keep three copies of each: one with the senior IT administrator, one with the company president, and one in a corporate safety deposit box.
Key rotation plan	Create a new key every six months.
Tracking key monikers and passwords	On a non-networked computer that supports encryption, create one or more charts or lists with this data, including key moniker, dates used, encryption password and superuser password, and password used to encrypt exported key. Because BlueScale Endura software prompts for the required encryption key moniker when you are restoring encrypted data, the company does not have to track monikers and their relationship to tape cartridges or disk packs.
Multiple encryption teams (optional)	Deemed unnecessary given the users already identified as those responsible for encryption.
Schedule and run drills	Formalized approach deemed unnecessary; instead, incorporate review of data decryption into standard six-month check to make sure that backups and restores are working properly; this now includes a test involving data decryption.
Passwords	<ul style="list-style-type: none"> <li>• Password to access encryption features: minimum of 12 characters, including at least one number and one letter.</li> <li>• Password to export and import encryption keys: minimum of 30 characters including at least one number and one letter.</li> </ul>
Monikers	Minimum of 8 characters with the space between words indicated by the underscore character.

## Example: Medium Security Site

Description of organization: Medium-sized organization with 250 employees.

Medium Security Site	Processes
Security goals	Protecting company from legal liability associated with unauthorized access to data stored on tape, both onsite and offsite, including transport to the off-site location.
Encryption principals	IT senior staff, chief operating officer (COO).
Data to encrypt	Intellectual property, financial, customer, and inventory data.
Level of security to implement	<ul style="list-style-type: none"> <li>• BlueScale Professional Edition, with multiple keys.</li> <li>• Standard initialization mode: encryption partitions enabled at start-up.</li> <li>• Multi-user mode, with three encryption passwords.</li> </ul>
Data sets requiring isolation from other encrypted data	Separate partitions and keys for these data sets: financial data, inventory data, customer data, and intellectual property data. With this requirement, the site must accommodate a minimum of four encryption-enabled partitions, along with one or more partitions for non-encrypted data.
Key escrow method	Key copies stored with corporate legal counsel and a paid, trusted, third-party escrow service.
Number of copies of each key to store, and locations	Keep three copies of each key: one with corporate legal counsel, two with a key escrow service.
Key rotation plan	Create a new key every quarter for every partition dedicated to encryption.
Tracking key monikers, exported key passwords and password to permit access to encryption features	Send to key escrow service an encrypted document that includes the password used to access encryption features, superuser password, and all passwords necessary to import encryption keys. This file cannot be created or stored on networked computer. Delete the file from the computer once the document or file is transmitted securely to the key escrow service. Store the key to decrypt the document as you store any key (see above).
Multiple encryption teams (optional)	Three IT administrators, along with the senior IT admin, and the COO.
Schedule and run drills	Annual evaluation and review, along with a wider corporate security plan.
Passwords	<ul style="list-style-type: none"> <li>• Passwords to access encryption features: minimum of 12 characters, including at least one number and one letter.</li> <li>• Password to export and import encryption keys: minimum of 30 characters, including at least one number and one letter.</li> </ul>
Monikers	Minimum of 12 characters including at least one number and one letter.

## Example: High Security Site

Description of organization: Enterprise organization with more than 250 employees

High Security Site	Processes
Security goals	Protecting all stored data.
Encryption principals	IT senior staff, COO, chief security officer (CSO), chief technology officer (CTO).
Data to encrypt	All.
Level of security to implement	<ul style="list-style-type: none"> <li>• BlueScale Professional Edition, with multiple keys.</li> <li>• Secure Initialization Mode: After library power is turned on, encryption user must enter password to enable partitions dedicated to encryption.</li> <li>• Multi-user mode, with three encryption passwords.</li> </ul>
Data sets requiring isolation from other encrypted data	Each data set is separately keyed, as defined by the department generating data.
Key escrow method	Key copies stored with two remote corporate legal counsel offices and also by a paid, trusted, third-party escrow service.
Number of copies of each key to store, and the stored keys' locations	Keep three copies of each: one to the main office of corporate legal counsel, two to a key escrow service.
Key rotation plan	Create a new key every month for every partition dedicated to encryption.
Tracking key monikers and passwords	Send to key escrow service an encrypted document that shows encryption access password and superuser password. Send to corporate legal office a list of passwords used to export keys. Files with this data cannot be created or stored on networked computer; delete file or files from computer once data is transmitted securely.
Multiple encryption teams (optional)	The senior IT admin, COO, CSO, and CTO.
Schedule and run drills	Quarterly evaluation and review, in conjunction with wider corporate security plan.
Passwords	<ul style="list-style-type: none"> <li>• Passwords to access encryption features: minimum of 15 characters, including at least one number and one letter.</li> <li>• Password to export and import encryption keys: minimum of 40 characters, including at least one number and one letter.</li> </ul>
Monikers	Minimum of 15 characters, including at least one number and one letter.

## Example Tracking Sheet

For example, you may want to track this information about every key you create.

<b>Key Moniker:</b> <hr/>	<b>Detailed Information</b>
Number and location of each copy of the key:	
Password(s) associated with exported copy of the moniker:	
Superuser and encryption passwords associated with this moniker:	
Location of data (stored on tapes or other mobile media, such as RXT SabreMedia) encrypted using this moniker:	
Dates of moniker creation and proposed expiration:	

## Conclusion

Once you have selected a strong encryption method, such as BlueScale Encryption, you can easily implement a robust security practice by making sure that the people who access encryption on your site are trustworthy, that procedures are in place to make sure that encryption keys are copied and stored safely, and that passwords and monikers are thoughtfully applied.

Of course, additional layers of procedure and security are often available through your encryption system. For example, you can set up the Professional Edition of BlueScale Encryption to require multiple users to copy a stored key back onto a library. These and other options let you customize security to the right degree for your site, in conjunction with your organization's security strategy.

These best practices let easily manage your encrypted data, and keep encryption keys safe and still accessible when you need to recover data. BlueScale Encryption provides a key management system that's easy to use, keeping your data, and your keys, secure.



Spectra Logic Corporation  
1700 N 55th Street  
Boulder Colorado 80303 USA  
800.833.1132  
303.449.6400

Spectra Logic Europe Limited  
Magdalen Centre  
Robert Robinson Avenue  
Oxford Science Park  
Oxford UK OX4 4GA  
+44 (0) 870.112.2150