WHITE PAPER

Complete Encryption: LTO and Spectra Key Management

MARCH 2013: VER. B

Encryption: Managing Keys and Data

CONTENTS

Executive Summary

LTO tape drives offer half of what it takes to encrypt data during backup. As noted in a Spectra® White Paper dated 2005, however, implementing hardware encryption is only part of the solution.

> "With the advances in technology and cryptography, it turns out that encryption itself isn't hard—for example, the AES-256 encryption algorithm has already been implemented in hardware and put into wide use. Instead, the difficult aspects of stored data encryption involve key management: creating keys, protecting keys, and linking keys to encrypted data all while maintaining security."

Accessing and using LTO encryption is exactly what Spectra BlueScale Encryption Key Management lets you do.

AES-256 hardware-based encryption, the method used by LTO tape drives beginning with LTO-4 —and used within all Spectra Logic libraries—depends on encryption keys. These keys are at the heart of using and managing encryption processes.

Spectra Logic libraries provide complete encryption key management for drive-based encryption. With LTO-4 and later generation tape drives, your T50e, T120, T200, T380, T680, T950, and T-Finity libraries can take advantage of the drive's encryption capabilities. Spectra began providing encryption capabilities in August 2007 when Spectra delivered the only LTO key management option that was, and still is, integrated within the library itself, without requiring additional applications or hardware.

Spectra Logic's BlueScale Encryption Key Management provides an easy-to-use interface that lets customers start taking advantage of encryption quickly while providing additional options to increase security levels. Much of the key protection is automatically handled in multiple software layers, as well, so it is not apparent to the user.

BlueScale Encryption Key Management lets you access LTO tape drive encryption while keeping the encryption process simple.

Encryption Key Management Basics

LTO tape drives use AES-256-bit encryption keys generated within BlueScale to encrypt data. This data can't be read until it is decrypted, which requires the use of the same key that was used during data encryption. If you don't have the key, you can't read the data. Managing keys is central to taking advantage of LTO tape drive encryption.

This kind of encryption requires creation, tracking, and protection of the encryption keys. The life cycle of a BlueSCale encryption key includes these stages:

- Encryption User Definition
- Key Creation / Deletion
- Key Escrow
- Key Use in Data Encryption / Decryption

A key management system, central to any encryption system, needs to handle every phase of the key's lifecycle. The Spectra BlueScale Encryption Key Management system handles these requirements for LTO tape drive encryption. Key management is easily handled using the library's graphical interface, available on the library front panel or from anywhere using a Web browser. It does not require additional interfaces, software, or hardware.

Regardless of where the data is encrypted—the LTO drive and the Spectra library's BlueScale interface make it easy to manage encryption keys.

Authorizing an Administrator to Manage Encryption

Once you have an LTO drive (Generation 4 or later) installed, you need to access its encryption functionality. This functionality is accessible through BlueScale Encryption Key Management. BlueScale Encryption Key Management not only makes LTO encryption usable; it also helps protect the key.

To configure the library to use drive-based encryption, follow the few simple steps that are outlined next.

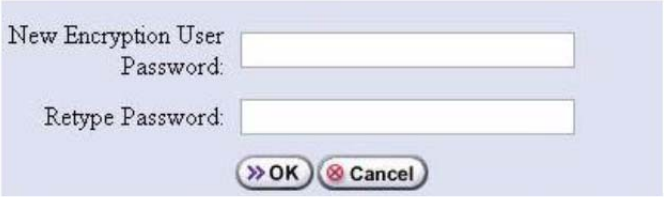
The first task in using encryption is also part of the key protection strategy: define library users who have encryption privileges. This limits the number of people who can access keys and therefore access encrypted data.

Spectra BlueScale Encryption Key Management provides an added layer of administrative security: a superuser *must* log in before the encryption password can even be entered. That means that users with fewer privileges, such as administrators and operators, can't even see the BlueScale Encryption icon (below), which lets users access encryption features.

Creating the password for the encryption user first requires:

- superuser (su) login to BlueScale
- selection of the encryption icon

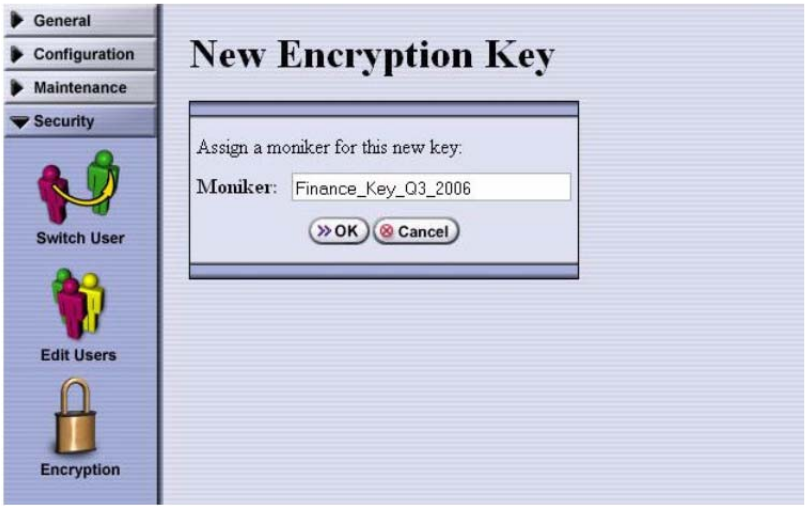
Once the Super User is logged in, then simply create the encryption password:


New Encryption User Password:

Retype Password:

Creating an Encryption Key

Now that the encryption features are available, you can create a key. The key must be easily identified *and* its true value must be hidden. Both of these are handled easily with BlueScale Encryption Key Management, simply by assigning a nickname, or moniker, to each key:



New Encryption Key

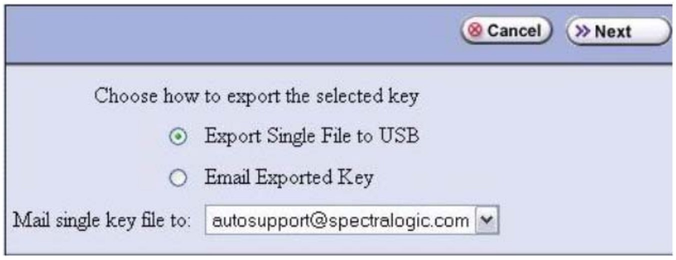
Assign a moniker for this new key:

Moniker: Finance_Key_Q3_2006

The moniker is always used. The real key value (256 bits in length) is never displayed, nor is it stored statically in clear text.

Protecting Encryption Keys

As soon as you create a key, BlueScale prompts you to make a copy of the key for safe storage outside the library. This step is critically important: without the key, you can't access encrypted data. Storing a copy of the encryption key outside of the library helps ensure the key's availability in the event of a disaster.



Choose how to export the selected key

● Export Single File to USB

○ Email Exported Key

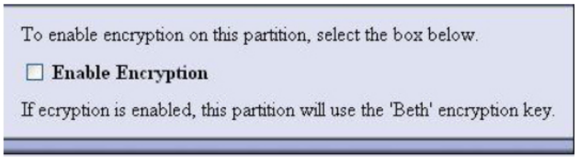
Mail single key file to: autosupport@spectralogic.com

All you need to do then is to enter the password that is used to encrypt the key prior to exporting it.

Encrypting Data

To give you flexibility in encrypting data, encryption is set up per partition—that is, per logical library within the physical library. This lets you store both encrypted and unencrypted data in a single, physical library. If you don't need to group data separately, then simply use one partition and encrypt all data.

To define partitions through which data is encrypted and decrypted, simply select the Enable Encryption option:



To enable encryption on this partition, select the box below.

☐ **Enable Encryption**

If ecryption is enabled, this partition will use the 'Beth' encryption key.

Use your backup software to make sure that data to be encrypted is sent to the appropriate partition. From then on, that data is encrypted during backup. It really is that easy.

Decrypting Data

Data decryption and recovery depends on pulling together the right tapes, the right key or keys, and the right hardware to support the decryption.

BlueScale Encryption helps you identify the key required to decrypt data by writing the encryption moniker (the nickname, not the key's 256-bit value) to the tape cartridge's memory. When a tape with encrypted data is then loaded into a library, the BlueScale software determines what key was used with the LTO tape. It checks the library to identify keys stored on the library. If the matching key—revealed only by its moniker—is available on the library, the data is automatically decrypted.

If the key is not available, the encryption software tells you the moniker of the key that is required to decrypt the data. You can then import the key. (To import the key, enter the same password you used when you exported the key—one more layer of data protection.)

Deleting Keys

Encrypted data is considered deleted and unrecoverable once all copies of its key are destroyed. The key management software needs to provide a feature that deletes specific encryption keys. Note that data deletion may be mandated by law, such as with HIPAA, and that this method of data deletion is by far the simplest and most cost-effective method of deleting data.

The role of the administrator in this process is to make sure every copy of a key is identified, and if necessary, destroyed.

It's easy to delete keys using BlueScale Encryption Key Management. If the key is on the library, delete it using the key management software. If the key is on a USB device, delete the key from the device. Even though data encrypted using the key may still be stored, the data is inaccessible.

Restoring Data Using a Command Line Utility

In the event of a crisis or disaster, you may need an alternative method of recovering your encrypted data. For example, your usual Information Technology (IT) infrastructure may be unavailable.

Spectra Logic has command-line utility software, Endura Decryption Utility (EDU), that lets you restore data with a minimum of hardware, and without requiring any Spectra equipment. You can use it on a host that is running Linux (RedHat) and has one or more tape drives connected and online. The EDU utility decrypts the data stored on tape and writes it to the same or a different tape. You can then restore the data with the backup software used to back up the data.

Conclusion

With the LTO drive-based encryption, access to data encryption appears easy. What is not obvious is that it's easy to encrypt data. Tracking and managing the keys used to encrypt and decrypt data is the real challenge. The Spectra Logic BlueScale Encryption Key Management solution provides key management features which you must have to take advantage of LTO encryption. The taxonomy presented in this white paper applies particularly to systems encrypting secondary storage, where keys may need to be retained for long periods of time.

Managing a key across its life cycle requires a balance between security and ease of data decryption and restoration. You'll have to identify the right level of security for your data and your site. Regardless, the key management system needs to let you easily create and use keys, escrow keys, access keys when you need to decrypt data, and destroy keys at the end of the data lifecycle.

The BlueScale system protects keys in multiple layers. First—and foremost from a user perspective—the system lets the key creator assign a key nickname or moniker. Users always reference the key's moniker, rather than the key's real value (the 256-bit key). Second, the key's value is encrypted for remote escrow. Decrypting the key from this state, then, requires an authorized user and a key-specific pass-phrase. (Some systems store keys in clear text in databases, or give users the option of not encrypting the key. This weakens the encryption implementation altogether.)

LTO-4 and later generation drives support strong encryption. The next step is taking advantage of that LTO encryption. BlueScale Encryption Key Management on Spectra T50e, T120, T200, T380, T680, T950, and T-Finity libraries is the only library integrated encryption key management solution on the market today that lets you take advantage of LTO drive-based encryption.

References

Denning, Dorothy E. and Dennis K. Branstad. “A Taxonomy for Key Escrow Encryption Systems,” *Communications of the ACM*, Vol. 39, No. 3, March 1996.

Seleborg, Svante. “About AES—Advanced Encryption Standard: A Short Introduction,” Axantum Software AB, 10-26-2004.

www.SpectraLogic.com

Spectra Logic Corporation
6285 Lookout Road
Boulder Colorado 80301 USA
800.833.1132
303.449.6400

Spectra Logic Europe Limited
Venture House
Arlington Square, Downshire Way
Bracknell, RG12 1WA
United Kingdom
+44 (0) 870 112 2150