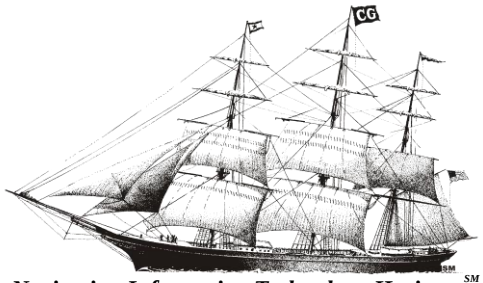
THE CLIPPER GROUP
Navigator™



Navigating Information Technology Horizons℠

Published Since 1993 Report #TCG2012025 October 30, 2012

Spectra Implements New Data Protection Management Facility for Encrypted Data

Analyst: David Reine

Management Summary

Have you ever picked up a newspaper and seen your bank or other financial institution trying to explain how they lost backup tapes with the personal data of numerous customers? Have you checked your mail recently to find a letter from one of these institutions apologizing for having potentially exposed your own data? They try to appease us by explaining that these unusual circumstances probably did not result in any identity theft, but, just in case, they have enrolled each of us in a credit monitoring service. I am only too familiar with this exercise as my personal data has now been exposed twice, once by the local newspaper and again by my bank. I am sure that the businesses involved regret their inaction in better protecting this data, especially when they have to pay the bill for the notification, enrollment, and public embarrassment. I am sure that they regret not encrypting that data before sending it out the data center door.

In other cases, protecting our identity is our own responsibility. In fact, we are all very familiar with protecting our own personal info; we protect it by putting passwords on all of our Internet accounts. If you follow best practices, you will use a different password for each site. Some of us, however, are not so good at remembering a myriad of different passwords, so we use the same password for each and every website that we visit – not a good idea. Some of us who do use different passwords frequently make note of them on little yellow Post-It notes and stick them on the monitor. Again, not the best way to manage your own security! Managing these passwords is our responsibility just as encrypting data and managing the encryption keys is the clear responsibility of each and every business with whom we interact.

With enterprise data doubling every 12-to-18 months, the requirement to protect that data becomes more urgent, and more difficult, with every passing day. Many enterprises have responded to this crisis with the implementation of encryption techniques at various levels within the data center – in the hardware, within an application, or in transit through the network. This has resulted in the creation of islands of encryption with a fragmented approach to the management of the encryption keys. In fact, many applications, each possibly using a different encryption technique, add to the chore of managing the keys. A well-managed yet simplified process to implement and deploy a secure method to manage these encryption keys is essential. That is where Spectra Logic has stepped up to the challenge for enterprise data centers.

Spectra Logic has always had a strategic encryption process for their tape libraries through their *BlueScale* Encryption Key Management software. Now Spectra Logic has complemented that security with *Spectra TKLM*, key management to include multi-vendor and multi-site support, as well as a variety of new features. To learn more about Spectra TKLM please read on.

IN THIS ISSUE

Data Security in the Enterprise

No one will argue the point that enterprise data is expanding at an unprecedented rate. For many, it is doubling every 12-to-18 months. In addition, no one will argue that the enterprise must be protected from the loss of any of that data or the breach of the enterprise firewall, allowing personal or corporate data to leak out. Any time that a tape cartridge is removed from the library system to be transported within the data center or offsite, that risk grows higher.

The damage to the business's reputation, as well as the economic cost to rectify the loss, is very expensive. All enterprise data needs to be secure, within the data center as well as outside of the control of the IT staff, but especially for financial institutions and those in the healthcare industry. One way to do that is with encryption. If encrypted data is lost or stolen, it is useless to the thief. Unfortunately, if the encryption key is lost, the data itself is useless to the enterprise that created it.

Encryption is not only a best practice for every data center, but in many cases, it is mandated by law or industry best practices. The emphasis to encrypt is a direct result of new regulations and laws requiring encryption to protect personal, financial, and sensitive corporate data. **Because of the multitude of encryption strategies being implemented, even within a single data center, the requirement to simplify, centralize, and automate the encryption key management process is of major concern.** Some enterprises do not encrypt data at rest, only in motion. Every data center needs to improve data security and do everything they can to facilitate compliance management to meet all regulations and standards. This also includes, but is not limited to, enterprises in industries such as insurance, retail and consumer, manufacturing, and media and entertainment. In order to do this, the Organization for the Advancement of Structured Information Standards (OASIS) has established a new encryption key management standard. **As more and more data centers are encrypting data at rest, the need to centralize key management to get a simplified, consistent approach to encryption has never been greater.** It makes sense for every enterprise to meet these new standards.

One way to accomplish this is to deploy a single encryption management solution that safeguards data from breach or loss. This includes environments that already may not have deployed an encryption solution or those that deployed a solution that is no longer being supported. Furthermore, this solution must meet all compliance requirements to safeguard the encryption keys, automate key management, and to scale that key management across multiple environments. Hopefully, the enterprise can deploy a solution that minimizes management overhead and enables the data center to control costs. One company, Spectra Logic, has already developed an encryption key management for an integrated library server, and now is making available a standalone server to mange encryption keys across multiple, heterogeneous environments across the enterprise.

Spectra Logic BlueScale Encryption

Spectra Logic has offered an integrated encryption key management system for quite some time. The latest version, *BlueScale 12*[1], completely integrates library administration with encryption key management. Version 12 complemented the previous version, BlueScale 11.3[2], introduced earlier in 2011 to provide data integrity assurance, delivering *Data Integrity Verification* to the data center. BlueScale key management is secure and easy to use, providing the IT staff with powerful key management features for encryption and decryption, including restoration of data without a Spectra Library.

However, BlueScale Encryption is aimed at supporting the SMB or enterprise department that deploys a single library with LTO drives, employs a small number of keys, and needs to satisfy basic security requirements, such as AES-256 bit encryption. BlueScale 12 provides an integrated key management facility for encryption-capable LTO drives, with a web-based *Remote Library Controller* (*RLC*) enabling the staff to manage data encryption safely, from anywhere, with a secured web connection. BlueScale fits nicely into an open systems environment with a vendor-agnostic architecture and compatibility with major backup, archive, and tiered storage applications. In addition to a free standard edition, BlueScale comes in an advanced, professional package, supporting such features as multiple keys and M-of-N key support. **For organizations with more data, more keys, and more complex requirements,**

[1] See **The Clipper Group Navigator** dated November 14, 2011, entitled *Spectra Raises the Ceiling on Archiving - Lowering TCO for Their Tape Libraries*, available at http://www.clipper.com/research/TCG2011036.pdf.

[2] See **The Clipper Group Navigator** dated March 21, 2011, entitled *Spectra Raises BlueScale 11 Delivers Data Integrity Verification to SME, Mid-Range and Enterprise Users*, available at http://www.clipper.com/research/TCG2011011.pdf.

Exhibit 1 – Comparison of BlueScale to TKLM

Spectra offers two types of encryption to address diverse customer requirements. TKLM is a stand-alone, centralized key manager while BlueScale is integrated within, and specific to, each library. The following table shows the encryption features and functionality provided by BlueScale and Spectra TKLM encryption key management offerings, respectively.

Feature	BlueScale Encryption Key Management	Spectra TKLM Encryption Key Management
Library Integrated Server	X	
Stand-alone Server		X
Supports T50e, T120, T200, T380, T680, T950, T-Finity	X	X
Multi-vendor Library Support (dual vendor shops)		X
Secure Initialization Mode	X	
Graphical User Interface	X	X
Command Line Interface		X
LTO4 Drive Support	X	
LTO5 Drive Support	X	X
TS1140 Technology Drive Support (T-Finity only)		X
Multi-library / Multi-site Support		X
AES-256 Bit Encryption	X	X
Key Max: 30	X	
Key Max: 1,000,000+		X
Key per Tape		X
M-of-N Key Shares	X	
Symmetric Keys	X	X
Asymmetric Keys		X
Role-based Access Control	X	X
Key Grouping		X
Device Grouping		X
Key Group Policies		X
Key Rotation Policies		X
Key Lifecycle Status		X
Audit Verified Key Deletion		X
Certificates of Authority		X
Audit Trail		X
FIPS Certification		X
KMIP Compliance		X
IKEv2-SCSI Compliance		X
Configuration, Policies, & Keystore Backup		X
LDAP Support		X

Source: Spectra Logic

Spectra now offers *Spectra TKLM* as a more robust encryption key manager.

Spectra TKLM

Where BlueScale is aimed at the SMB or enterprise department, Spectra TKLM is geared more toward the larger enterprise data center and can be deployed in those environments that require a superset of the functionality provided by BlueScale. **Spectra TKLM scales key management across multiple, heterogeneous environments, safeguarding the keys used in encryption operations.** It simplifies and automates key management, relieving a variety of IT teams

of a manual role that is wide open for the potential loss of encryption keys. This fragmented approach to key management can only lead to a loss, or breach, of mission-critical enterprise data. With this integrated, standalone solution, the data center can control management overhead and costs.

Typically, the more encryption that the data center deploys, the more keys the IT staff has to manage. Encryption keys have their own lifecycle, in addition to the lifecycle of the data that they are protecting. TKLM gives the IT staff the tools that they need to simplify, centralize, and automate the key management processes and help to reduce operational costs. With support for the new OASIS KMIP standard[3], TKLM provides a simplified management of encryption keys for the entire enterprise.

Spectra TKLM is a standalone server designed to enable the data center to deploy a simple solution for a very complex problem: encryption key management and security. TKLM enables the data center to manage encryption keys across multiple libraries and data center sites from a centrally controlled workstation. It enables strong authentication and security, providing the flexibility to meet the unique requirements of each data center. It simplifies both configuration and management tasks for keys and certificates of authority, and facilitates security audits and tracks key lifecycle, from cradle to grave. TKLM licensing starts at an MSRP of $8,750 for a Spectra Logic *T950* or *T-Finity* library. Pricing for smaller libraries starts at $4,250.

Like BlueScale, TKLM has implemented government-approved standards, such as FIPS 140-2 for compliant tape drives and encryption key manager, using the AES-256 bit standard. However, unlike BlueScale, **TKLM provides multi-vendor, multi-library, multi-site library support along with the capability to manage both LTO and TS1140 enterprise drives from IBM.** While BlueScale is limited to a maximum of 30 keys, TKLM can support more than one million keys, including a unique key for each tape. For a complete list of the functional differences between BlueScale and TKLM, please see Exhibit 1 on the previous page.

Conclusion

Spectra Logic has supplemented its BlueScale encryption offering with the availability of Spectra TKLM, extending the simplified management of encryption keys to a multi-vendor, multi-library, multi-site library environment. Spectra TKLM provides a unified key management strategy to enable the data center to streamline the implementation of encrypted data throughout the enterprise. This enables the IT staff to improve the security of critical data throughout the enterprise. Developed with open standards, TKLM enables the flexibility and vendor interoperability that the enterprise demands.

If you are looking to deploy encryption for the first time or simply looking to replace a legacy encryption package that may no longer be supported, Spectra Logic can provide an encryption solution tailored to the needs of your data center.

[3] See http://docs.oasis-open.org/kmip/spec/v1.0/os/kmip-spec-1.0-os.pdf.

About The Clipper Group, Inc.

The Clipper Group, Inc., now in its twentieth year, is an independent publishing and consulting firm specializing in acquisition decisions and strategic advice regarding complex, enterprise-class information technologies. Our team of industry professionals averages more than 25 years of real-world experience. A team of staff consultants augments our capabilities, with significant experience across a broad spectrum of applications and environments.

- ***The Clipper Group can be reached at 781-235-0085 and found on the web at www.clipper.com.***

About the Author

David Reine **is a Senior Contributing Analyst for The Clipper Group.** Mr. Reine specializes in enterprise servers, storage, and software, strategic business solutions, and trends in open systems architectures. In 2002, he joined The Clipper Group after three decades in server and storage product marketing and program management for Groupe Bull, Zenith Data Systems, and Honeywell Information Systems. Mr. Reine earned a Bachelor of Arts degree from Tufts University, and an MBA from Northeastern University.

- ***Reach David Reine via e-mail at dave.reine@clipper.com or at 781-235-0085 Ext. 123. (Please dial "123" when you hear the automated attendant.)***

Regarding Trademarks and Service Marks

The Clipper Group Navigator, **The Clipper Group Explorer**, **The Clipper Group Observer**, **The Clipper Group** *Captain's Log*, **The Clipper Group Voyager**, **Clipper Notes**, and *"clipper.com"* are trademarks of The Clipper Group, Inc., and the clipper ship drawings, *"Navigating Information Technology Horizons"*, and *"teraproductivity"* are service marks of The Clipper Group, Inc. The Clipper Group, Inc., reserves all rights regarding its trademarks and service marks. All other trademarks, etc., belong to their respective owners.

Disclosures

Officers and/or employees of The Clipper Group may own as individuals, directly or indirectly, shares in one or more companies discussed in this bulletin. Company policy prohibits any officer or employee from holding more than one percent of the outstanding shares of any company covered by The Clipper Group. The Clipper Group, Inc., has no such equity holdings.

After publication of a bulletin on *clipper.com*, The Clipper Group offers all vendors and users the opportunity to license its publications for a fee, since linking to Clipper's web pages, posting of Clipper documents on other's websites, and printing of hard-copy reprints is not allowed without payment of related fee(s). Less than half of our publications are licensed in this way. In addition, analysts regularly receive briefings from many vendors. Occasionally, Clipper analysts' travel and/or lodging expenses and/or conference fees have been subsidized by a vendor, in order to participate in briefings. The Clipper Group does not charge any professional fees to participate in these information-gathering events. In addition, some vendors sometime provide binders, USB drives containing presentations, and other conference-related paraphernalia to Clipper's analysts.

Regarding the Information in this Issue

The Clipper Group believes the information included in this report to be accurate. Data has been received from a variety of sources, which we believe to be reliable, including manufacturers, distributors, or users of the products discussed herein. The Clipper Group, Inc., cannot be held responsible for any consequential damages resulting from the application of information or opinions contained in this report.