

Tape Encryption: A Must in Today's World

IBM and Sun Square Off

Summary

Vastly different solutions from IBM and Sun force a user to make a strategic bet. IBM appears to be the best bet.

Introduction

Unencrypted tape is a huge security risk today. Fortunately, new tape drives from IBM and Sun address the problem. For maximum scalability, encryption of data at rest is best done at the tape-drive level and these drives are aimed there. Both vendors offer strong encryption for tape. After that their solutions differ substantially, particularly in encryption key management.

In the ideal world, key management and storage encryption should be ubiquitous and transparent, but the market has been held back by the lack of enterprise-wide encryption key management standards. So, we must examine these two vendors' tape encryption key management offerings in detail along with their drive specifications.

Both vendors' offerings help customers comply with current standards, rules and regulations, but are priced quite differently and offer significantly different key management. It is also important to note that ultimately the cost of compliance certification far outweighs the difference in cost of the tape drives.

Keys and Key Management

IBM

IBM's encryption and key management approach, which supports dynamic keys today, is more elegant and flexible than Sun's. For high-end tape drives, IBM's TS1120 drive stores the tape data key on tape. That data key is itself encrypted using Public-Key Cryptography Standards (PKCS) also known as asymmetric keys. The data key can then only be accessed with either of two private keys.

This makes it easy to share tape data with a trusted partner. Just give the partner the tape cartridge that contains the data key securely wrapped with the partner's public key. The partner – and only the partner - can decrypt with their private key. This can greatly simplify the encrypted cartridge sharing process and can eliminate the need to transmit secret keys. An auditor or Chief Security Officer must approve the plan and supervise only once. The same applies for sharing tapes among multiple data centers or disaster recovery sites.

This key management solution for tape encryption is similar to the industry standard SSL (Secure Sockets Layer) for securely transmitting data over the internet.

Today, IBM supports encryption at the volume level where all the datasets residing on one tape are protected by one set of keys. However, IBM's architecture supports the ability to have multiple key sets per cartridge and as application requirements evolve to support this, we expect dataset level encryption to become available. This is where IBM's dynamic key management will excel.

IBM's key management offering is called the Encryption Key Manager (EKM). Java-based, it runs on many platforms including mainframes, uses standard Java features, and can integrate with many configurations. It is also included free of charge and has flexible deployment options.

With IBM, there are three ways available to deploy key management, two using EKM and even one without EKM. The EKM uses secure, encrypted communications over any IP network or in some cases FICON:

- System-Managed

For open system environments, the tape drive device driver controls whether data is encrypted. Key management is via EKM. Encryption management is by drive rather than by cartridge. This method transparently supports a large number of libraries including some non-IBM libraries.

Points to Remember

- Key management and storage encryption should be ubiquitous and transparent.
- Tape data encryption is best done at the device level for scalability.
- Both IBM and Sun offer strong encryption.
- After that their solutions differ vastly.
- Key management flexibility should be a key factor in your decision.
- Both vendors can help you comply with high-end tape drives, but IBM's flexible key management, tape drive attributes and lower pricing win the race.
- Only IBM provides both high-end tape and LTO-4 encryption managed with one key manager.
- End-to-end, enterprise-wide storage encryption does not exist today, but IBM is a clear leader and is best positioned to get there before Sun.

For IBM mainframes and z/OS, system-managed encryption leverages the full suite of security features available there including ICSF, RACF and DFSMS. IBM leverages the proven encryption technologies of the IBM mainframe. Mainframe centralized key management provides a single point of control for the tape encryption keys, with high security and availability, long-term key management, and proven disaster recovery capabilities. System z servers also use tamper-resistant hardware features, Crypto Express2, for further protection of the keys. This tamper-resistant feature is a strong differentiator for enterprises who need to address more stringent compliance requirements.

When only mainframes are involved, all traffic runs over FICON. If a tape library is being shared with non-mainframes, key management is still performed by ICSF, but an IP network connection is used to send an encrypted data key to the library, which passes it on to the drive.

- Application-Managed

This approach does not use EKM. Instead it leverages IBM's Tivoli Storage Manager (TSM) which has had embedded support for encrypted tape for quite a while.

- Library-Managed

The tape library controls whether a specific cartridge is encrypted. This approach also uses EKM and is the most transparent because storage applications (i.e., TSM) and device drivers might not need updates, but new library firmware is required.

Overall, IBM's tape encryption solution(s) are more open than Sun's. There is comprehensive documentation that is open to all and IBM uses standard Java security protocols. No dedicated appliance is required to run EKM and IBM is helping to drive standards at many levels including featured membership in OATH (initiative for open authentication).

IBM's solution also makes encrypted data more easily available. The tape itself has the encrypted (wrapped) data key making the management and sharing of encrypted cartridges with a third party more fully automated and easier.

To address hardware, software or data center outages, any other EKM can authorize decryption if it has the proper private key to decrypt the public-wrapped data key. In addition, the user can have several EKMs running that can be accessed by drives in the event one of the EKMs is not accessible. The key store can also be copied to any number of other EKMs for failover capability.

IBM's EKM also supports LTO-4 as well. LTO-4 is the first of the LTO family to support tape encryption. LTO-4 uses a different key scheme than does the TS1120. That is, the data key is not stored on the tape itself. Instead, symmetric/private keys are kept in the key store in the EKM. A data key identifier is stored on the tape and is used to request the data key from the EKM.

Today, IBM has no native key life-cycle management, but a user can achieve that functionality with products from nCipher.

What's more, we believe IBM senior management is committed to end-to-end storage security. So, we expect IBM to set the pace for others to follow.

Sun

In contrast to IBM, along with its T10000 (T10K) tape drives, Sun requires a user to deploy an appliance-based Key Management Station (KMS) that runs only on Sun Solaris and costs \$45,000 including mandatory professional services. Sun's encryption-enabled drives are also priced 20-24% higher than IBM's depending on the configuration. In addition, once a T10K's encryption is turned on, it cannot be turned off unless sent back to the factory.

Another big difference is that the private/symmetric tape data key is not stored on the tape. Instead, the key is stored in the KMS and transmitted to the drives via a physical token. Under operator control, static, manually provisioned and encrypted keys are loaded into the tokens by the KMS. Holding as many as 60,000 keys, each token must then be made accessible to a pre-selected set of tape drives/libraries. Data key generation is strongly tied to those tape drives and the KMS. That access can be manual or networked.

Originally, Sun only supported the manual approach, where the tokens are manually carried from the KMS token bay to tape library. An auditor's presence is recommended by Sun each time the drives are provisioned this way. This design is intended to satisfy users whose data centers are not considered secure enough, so the KMS and its token bay are kept in a more secure location.

The other approach, where the data center is considered sufficiently secure, simply networks one token bay among the KMS and the tape drives on a private LAN. The KMS loads the tokens over this LAN and then the drives read the keys from the tokens in the same token bay. Key provisioning is still manual, but an auditor may not be needed once the system is set up. This approach works, but only in one local data center.

However, with either of Sun's approaches, there are many more limitations than with IBM. Each tape drive can hold only 32 data keys (1 read/write and 31 read keys). Therefore the user must ensure media is mounted in the correct drive. Key policies are also limited, e.g., retention periods vs. frequency of key changes. Moreover, compromised keys would require each cartridge to be rewritten. Thus, Sun recommends users use one key for the entire data center.

Sun has told users that it intends to provide dynamic keys (more like IBM's approach), key life-cycle management, and LTO-4 support in the future, but there are no firm dates yet. In addition, we believe Sun has been in discussions with other security vendors regarding key management. Given Sun's public declaration of its commitment to open source, Sun should be more open about its storage encryption strategy and solutions, but we remain skeptical that these will come to fruition anytime soon.

All these limitations prompt us to believe that the T10K tape drive was ready, but time to market issues and acquisition turmoil forced an inferior, albeit compliant key

management solution. This creates the potential for wasted time and investment as the user would have to re-certify compliance when dynamic keys become available.

The Drives and Media

See Table 1 at the end of this report for a comparison of features. We see the key differences as:

IBM Drives:

- Dual mode – encryption and/or no encryption
- Standard on new drives
- Field upgrade on existing installations
- Priced below Sun
- Supports Fibre Channel, FICON and ESCON
- Compatible with 3592 media (one generation)
- Two independent sources for media (Fuji and IBM)

Sun Drives:

- Single mode operation – encryption or not
- Sun recommends not mixing modes in the same tape library
- Priced higher than IBM
- No ESCON; No 4-Gbit FICON
- No support for mainframe z/OS encryption management features
- Not backward compatible with previous media
- Media is only available through Sun, albeit from two sources

Bottom Line

If keys are to be changed infrequently, both vendors' solutions are viable for the short term, but IBM's key management is vastly superior today. In our opinion, IBM is farther ahead and more openly committed to end-to-end storage security.

Nick Allen, Founder
Publish Date, July 2007

Regarding the information in this report:

The Tod Point 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 Tod Point Group cannot be held responsible for any consequential damages resulting from the application of information or opinions contained in this report.

This report was developed by The Tod Point Group with IBM and funding. This report may utilize information including publicly available data, provided by various companies and sources, including IBM. The opinions are those of the report's author, and do not necessarily represent IBM's position on these issues.

Table 1. Tape Drive Comparison

Feature	IBM TS1120	Sun T10000	IBM Score*	Sun Score*
Maximum Native Cartridge Capacity **	700 GB	500 GB	1	
Native Data Rate	104 MB/s	120 MB/s		1
Typical Compression Ratio – Open systems/System z	2:1/3:1	2:1/3:1		
General Availability	4Q05	1H06	1	
System z Attachment	4Gbps FICON/ ESCON	2 Gbps FICON only	1	
Open Systems Attachment	4-Gbps Fibre	2-Gbps Fibre, 4-Gbps Fibre		
Virtual Back Hitch	Yes	No	1	
Tape Drive Buffer	512 MB	256 MB	1	
Speed Matching Capability	6 speeds	2 speeds	1	
Load Thread Time	13 seconds	16 seconds	1	
Average File Access Time (500GB cartridge) (Includes Load/Thread Time)	46 sec	62 seconds	1	
Maximum Rewind Time (500GB cartridge)	66 sec	91 seconds	1	
Encryption Strength	AES-256	AES-256		
Encryption Availability	2H06	2H06		
Selectable Encryption	Yes	No	1	
Data Encryption Key	Private wrapped in PKCS/ Asymmetric and stored on cartridge	Private/ Symmetric	1	
Power Consumption	65 W/307 BTU/hour	90 W/420 BTU/hour	1	
Price*** for Fibre Channel Drive	\$35,500	\$37,000	1	
Price for FICON drive	\$35,500 w/o ctrl. \$40,300 with ctrl.	\$44,000	1	
Price for Encryption Feature	None	\$5000	1	
Price to Upgrade Existing drive for Encryption	\$5,000	n/a	1	
Price for Key Management	No Charge	\$45,000	1	
Recommended Maximum number of Full File Tape Media Passes	300	350		1
Media Price	Street is \$189 each in 10-pack	Street is \$149 each in 10-pack		1
Street Cost per Raw GB	27 cents	30 cents	1	
Score Totals			18	3

* This score is a simple binary -- which vendor has better specifications

** Depends on media length – longest used

*** All prices are the manufacturer's list price in U.S. dollars except as noted

Sources: IBM, Sun, and Google