



LTO4 with encryption on iSeries

Why it might not be what you expect

A whitepaper from DISUK Limited

By Paul Howard

LTO4 with encryption on iSeries *Why it might not be what you expect*

Executive Summary

It is clear that with the very large number of confidential records being compromised every month, companies need to treat the need to encrypt backups as a “must do now” project. The announcement from IBM that they would be the first-to-market embedded encryption in their new LTO4 tape drive appeared at first sight to offer the solution in dealing with this continued loss of private and confidential data. This article looks at the possible issues of using this approach and offers some alternative options. For iSeries users the IBM offering would appear to be a straightforward solution but when looking at this in detail several issues arise.

Interface

The first surprise is that the LTO4 with encryption is not available with the SCSI interface for the iSeries. This forces users to add a fiber channel IOP if they do not already have one. Even if there is already an existing fiber IOP the advice from IBM is that the drive should have its own dedicated IOP. This means the system must be brought down in order to install and configure the new hardware which will likely require an IBM SE. In addition, if there is not room to add the fiber card and IOP, an expensive expansion tower/drawer will have to be purchased. This may cause some users the headache of getting staff to work outside normal hours to allow this to be done when least disruptive to the business.

Library

LTO4 encryption for iSeries is only supported with library based units; stand-alone drives are not supported. This clearly increases the cost and complexity of an installation. It may require more physical space which needs to be considered. In addition, a library might require expensive electrical additions to the data center.

Media

The next surprise to many industry insiders was the fact that the encryption will only work when using LTO4 media. This brings two issues, first, the extra cost associated with buying a complete new set of media and second, what happens to the existing media pool. The LTO4 media lists at \$160 each and although the capacity of the new tape is twice that of the previous iteration of LTO media, most companies can't take advantage of this.

LTO4 with encryption on iSeries *Why it might not be what you expect*

Configuration and control

The next item of interest is how this encryption is configured and controlled. Using encryption with the LTO4 on the iSeries also requires the use of Backup Recovery Media Services (BRMS). Not all iSeries customers are using this package as part of their backup procedures today. This means replacing the package currently in use, purchasing BRMS (5722-BR1) and learning how to work with it. Even for those customers who are using BRMS, the backup and recovery procedures will need to be changed to utilize encryption. The learning aspect of this is certainly something that needs to be carefully considered.

Archive

Most businesses will have a pool of data on existing media; the question will be just what to do with it. The data on these tapes need to be retained for a given period but it is essential to ensure the data on it is secured. To copy all these tapes on new LTO4 media using some duplication method such as DUPTAP will be both time consuming and will affect system resources. Once this is completed the old media then needs to be destroyed as it cannot be rewritten in encrypted mode. This is again another expense that needs to be considered.

Key Management

The Java based Encryption Key Management (EKM) package for the LTO4 encryption requires a separate server or partition (LPAR) to run. This software itself may provide potential security flaws dependant on how it is implemented because anywhere the security keys can be accessed outside of the server is a possible weakness. IBM recommends that two EKM's be used for fault tolerance, without the EKM tapes cannot be read. Of course, these servers need to be backed up.

Restore Considerations

With the IBM solution, the iSeries needs to be operational with the OS loaded, and the key management server needs to be up and running before restoring any encrypted data. This leads to a complex restore procedure. Because this is a fiber channel interfaced unit, the system cannot IPL from this LTO4 drive, unlike a SCSI drive that is used as an alternate IPL device.

LTO4 with encryption on iSeries *Why it might not be what you expect*

Interoperability

Most companies send data from time-to-time to other companies, the LTO4 can only write to LTO3 or LTO4; therefore, for the supplier / customer to be able to read these tapes they will need at least an LTO3 drive. And since the LTO4 is so new, the most common drive in the market today is the LTO2.

Speed

There is often a misunderstanding over the throughput of tape drives. Many people are under the impression that the tape drive is the slowest item, but frequently the tape drive sits idle while the system retrieves the data. Therefore a faster drive does not always mean faster backup. Retrieving data from a large capacity tape like the LTO4 may also be slower as the data needed may be near the end of the tape.

Conclusions

Although it appears at first that going with an IBM solution is the save, simple and sensible way to go this will not be true for many organizations. IBM seems to think that all organizations have their own dedicated disaster recovery facility where there is not need to consider the time and complexity involved in configuring the systems before commencing a system restore. In the real world this approach may mean that it will be impossible to meet the requirements of existing SLAs using the LTO4 approach. Adding to this the fact that it is not common across all platforms and has no uniqueness beyond the keys may mean that people will look towards the established encryption appliance that has been in use across the iSeries community for over 12 years.



DISUK Limited

Silverstone Innovation Centre
Silverstone Circuit
Silverstone
Northants, NN12 8GX,
United Kingdom

Phone: 01327 856070

Fax: 01327 856071

E-mail: sales@disuk.com

[About the Author](#)

Paul Howard is joint founder and managing director of DISUK Limited. Mr. Howard was trained in the Royal Air Force where he specialized in cryptography. During his time with the RAF, Mr. Howard served both in Europe and the Middle East as well as a tour at HQ Strike Command. After leaving the RAF, Mr. Howard played key roles within major UK Electronics Groups. Founded in 2004, DISUK Limited is a British company specialising in design and manufacture of electronic data storage encryption systems.

Copyright © 2008 DISUK Ltd. All rights reserved.

The trademarks, logos and service marks ("Marks") displayed herein are the property of DISUK or other third parties. You are not permitted to use these Marks without the prior written consent of DISUK or such appropriate third party. All other trademarks mentioned in this document are the property of their respective owners.