



Points to consider when looking at V6R1 for Tape Encryption

A whitepaper from DISUK Limited

By Paul Howard

Points to consider when looking at V6R1 for Tape Encryption

Executive Summary

There are many changes in V6R1 from V5R4 and it will take time to get to fully comprehend and understand the implications of them all but some initial thoughts following reading available information, the briefing by IBM in February/March and the Common presentations by IBM April 2008.

IBM has clearly understood that drive based encryption is not suitable for all users and that the complexity and needs for multiple EKM servers cost did not match the customer site profile for a large number of their users. The pressure now being put on organisations to secure all sensitive data, and particularly the requirements to meet PCI DSS, meant that IBM looked for other ways to help users meet their needs.

V6R1 is the first release of i5OS to offer built in software tape encryption and many people have understandably held off from making a decision of how to encrypt their sensitive data being written to tape until the implications of V6R1 were known.

V6R1 also offers file level encryption on the disk storage and this may well give many people the belief that this is the "total solution" they are looking for.

A recent Ponemon Institute survey of 9,000 people found that 12% of respondents had been notified of a data breach or loss by a company with which they did business. Of those affected, 20% said they immediately stopped doing business with the companies that couldn't keep their data secure. Can you afford to lose 20% of your customers?

Throughput

As with all software based encryption throughput always need consideration. Firstly it should be understood that the system processor is not specifically designed to run encryption algorithms and these by their very nature are complex and processor intensive operations. In their presentations IBM are quoting a maximum of 75 Mb/sec on a P5 processor and 130 Mb/sec or less on the P6 processor. The encryption algorithms available are AES 128, AES 196 or AES 265 but IBM did not make it clear which of these the figures pertain to but if these were with AES 128 you could sensible expect them to halve running AES256. In any case this was presumably with no other system processes being run at the same time.

IBM also pointed out that because the encrypted data will not be compressible on the drive because of the very random data patterns therefore the drives will only run at their native throughput. IBM gave the examples of 40Mb/sec on a 3592 Model 01A and 80 Mb/sec on the 3580 model 003 but of course this is simply the max true drive speed and even that does not take into account command overheads and similar issues that will further slow the throughput.

Points to consider when looking at V6R1 for Tape Encryption

IBM also gave examples of the impact of their software encryption with different file types with little or no impact on a 1Gb source file which is already very slow but also showed around a fifty percent slowdown doing a 64Gb and 320 Gb large file. Unfortunately they did not share with the audience which encryption method they tested with so care should be taken in case this was done with AES 128.

When asked about restore times there were unable to give an informative response and indicated they had no test figures to share with us. It is normally assumed that a restore will be slower than the save so you might expect this to also be true with the encrypted data being decrypted during a restore.

Complexity

One of the often heard comments about the LTO-4 tape encryption was that it was difficult to configure and even more difficult to understand, so how does the V6R1 tape encryption option stack up in this area? Well the good news is that it is both easier to configure and to understand. but the bad news is that it is still not simple and straightforward.

To use V6R1 tape encryption users will need a tape Management Application and IBM are recommending BRMS with the advanced option. They must also purchase the Encryption Enablement Option. If you are already a confident BRMS user then adding the encryption will not be the steep learning curve as those users who don't have a background in BRMS.

The V6R1 tape encryption option cannot encrypt everything to tape and specifically excludes *SAVSYS, *SAVSECDTA, *SAVCFG, *IBM, and libraries starting with a Q. Remember that user objects are in QGPL and QUSRSYS. This means that restores of a complete system really do have to be done in a very controlled and structured way to ensure everything runs as planned.

Key Management is via multiple layers of protection. The key store file is protected by the Master Key which is protected by the Save / Restore key. The keys stores need to be backed up separately to ensure the restore is possible. IBM points out that if the key store file is lost then the data is unrecoverable which is quite clear but users need to ensure they understand this and the importance of having good backups of the key store file.

Points to consider when looking at V6R1 for Tape Encryption

Capacity

As stated earlier IBM are warning users that the tape drives will not compress the encrypted data so this will slow down the maximum drive speeds to their native throughputs but this will also mean the amount of tape being used will increase.

For many users this increase in tape utilisation will have no discernable impact; however users with lower capacity drives such as the 3590E might need to consider what impact it may have on them. For some people already spanning across say eight tapes a thirty percent increase in tape utilisation might tape them over the number of tapes contained in their auto-loader and mean a rethink of their previously unattended overnight backup.

Other new features

Under V6R1 IBM has introduced the ability to use a Fibre Channel connected tape to do an alternate IPL whilst previously this was only available with SCSI tapes. This would appear to be restricted to the new 5749 and 5774 fibre channel feature cards initially but this will perhaps also be available on other FC cards. This means a full system restore can now be done quickly and efficiently from FC tape but unfortunately not from an encrypted tape! Because of the previously mentioned restrictions on the ability to run certain backup procedures, specifically a *SAVSYS, these cannot be used to IPL from.

IBM has also added the ability to encrypt each file using a different key. Exactly why this was considered as something that users might want was not made clear. What was made clear was this would have a considerable impact on save times so you should consider the use of this option very carefully.

Disaster Recovery

In a true DR situation the system is first be restored on the DR server and all the non encrypted files restored. Once this has been done the BRMS can be configured and set up with the correct key database and then the user can start to begin their restore of their encrypted data from tape. Clearly all companies should be running regular DR exercises to test and hone their DR policy but these needs to be given greater emphasis regarding V6R1 tape encryption configurations. This will also be the time to check the impact on restore times and ensure these still meet the SLAs in place. When using an external DR company it is suggested they are included in the discussions to ensure they have the correct levels of extra hardware to meet the needs.

Points to consider when looking at V6R1 for Tape Encryption

Costs

Users will need to consider the extra costs of BRMS when budgeting for using tape encryption and they need to have the Advanced Option on top of the BASE version of BRMS. You should also look at you existing tape utilisation and taking into account the loss of drive compression look at whether or not you need to plan extra tapes as part of the implementation. For those companies not already using BRMS it is suggested that you include some training in BRMS for those members of staff entrusted in implementing the encryption.

Conclusions

Tape encryption under V6R1 is a big improvement as compared with the LTO-4 or TS1120 drives and EKM as far as complexity and ease of understanding but has all the standard problems and disadvantages as any other software solution. The major issues are the speed and that it is still quite complex along with the extra complications of the restrictions that you cannot use it for *SAVSYS, *SAVSECDTA, *SAVCFG, *IBM, or to backup libraries starting with a Q.

[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 keys 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.

DISUK Limited
Silverstone Innovation Centre
Silverstone
Northamptonshire
NN12 8GX
United Kingdom

Tel: +44 (0) 1327 856070
Fax: +44 (0) 1327 856071

Web: www.disuk.com
Email: Sales@disuk.com

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.