

white paper

MCP Library Maintenance Tape Encryption

By: Alan Fritchhoff, Manager, Computer Systems Architecture Group

security

You've seen it in the news. Another financial institution, company or government agency has lost or had stolen the private and perhaps financial data about its customers or employees. In several of the better known cases, it's been the loss of backup tapes on their way into storage.

But how do news organizations learn about these incidents? Easily. Among the growing list of U.S. state regulations is one that requires an enterprise to make disclosure of such lost or compromised data.

What happens next? First, there's the financial and productivity costs of alerting the individuals and entities affected. Even greater costs can arise out of damage to the company's brand. One other cost is incalculable... the harm done to a company's image.

Fortunately, more and more states are also citing types of incidents wherein disclosure isn't required. For example, when misuse of the data is not reasonably possible, such as when the lost or stolen data was encrypted.

And that's what you'll learn about in this paper. The Unisys ClearPath MCP tape encryption solution is an optional software product that can further protect your critical information. One that also addresses issues you should consider when developing your backup processes. You'll also find information about encryption key management and methods for sharing encrypted data with your partners.

Table of Contents

The Need to Secure Removable Data	4
Encryption Performance Considerations	5
Business Process Considerations	6
Create Tape Encryption Keys	7
Back Up Tape Encryption Keys	10
Share Encrypted Tapes	12
Tape Encryption Algorithms	14
Library Maintenance Tape Encryption	14
Checklist	16
Restrictions	16
Future Directions	17
Biography	18

The Need to Secure Removable Data

In a consumer survey conducted by the Council of Better Business Bureaus in the U.S., results showed that identity theft cost consumers and businesses \$54.4 billion in 2005. And it rose another four percent in 2006. Most recently, consumers shouldered about 10 percent or about \$5 billion a year in costs associated with identity theft. Businesses, including lenders and credit card companies, bore the remaining billions in costs.

There's been an increase in the amount of pending and passing legislation in the U.S., at both the federal and state level. Much of this legislation has been aimed at providing consumers the tools they need to help prevent and combat identity theft and deal with its aftermath. Most of it would require that consumers be notified of breaches that allowed unauthorized access to nonpublic personal information that could lead to identity theft.

Should you ever lose any employee or customer data, complying with disclosure regulations would have both an immediate and long-term monetary impact on your business. There's the immediate expense of notifying each customer or employee whose data has been compromised. Then there's the long-term impact to your company's reputation; consumers may well take their business to your competitors... ones that can demonstrate stronger security measures.

A growing number of U.S. states are following the State of California's 2003 law addressing unauthorized access to personal information. More than 20 states introduced a total of 42 bills in 2005 that were modeled after the California law. At the time of publication, 23 states had enacted this or a similar type of legislation.

The California law requires notice to customers of potential unauthorized access to their personal information. In that legislation, personal information is defined as an individual's first name or first initial and last name in combination with their Social Security number; driver's license or ID card number; account, credit or debit card number, in combination with a required security code, access code or password that would permit access to an individual's financial account. The California law states that disclosure of this breach must be made whenever the information isn't encrypted.

The State of New Jersey enacted a similar law in 2006 that says: "Disclosure of a breach of security to a customer shall not be required under this section if the business or public entity establishes that the misuse of the information is not reasonably possible. Any determination shall be documented in writing and retained for five years." One could interpret this as saying, "The misuse of encrypted data is not reasonably possible."

The situation is a growing concern not only in the U.S., but also worldwide. While the EU Data Protection Directive doesn't specify the encryption of data as one of their standards, international organizations are increasingly turning to encryption as a prudent practice.

To help you address both U.S. and international regulations and data privacy concerns, we offer an optional, separately priced Tape Encryption software product. This software adds tape encryption and decryption capabilities to the Library Maintenance facility delivered with MCP, DMSII (as of MCP 11.1), and the MCP TapeStack solution*. Library Maintenance encryption can be used when writing data to tape or CD. MCP TapeStack is another optional, separately priced software product that offers both software and services for taking advantage of new high-density tape technologies to consolidate tapes and simplify tape management.

* While Unisys is providing this separately priced encryption facility, Unisys customers have the responsibility to determine whether to use this encryption facility and whether any notices would be required if the encryption option is used and the encrypted data is lost or stolen.

Encryption Performance Considerations

The Library Maintenance facility (part of the MCP operating system) and the tape encryption product work together to encrypt tapes using software-based encryption that affects both the total time to transfer data to tape and results in increased processor utilization. We strongly recommend that you first conduct your own tests with Library Maintenance tape encryption in your production environment to assess its impact on your system's operations.

Another approach you might consider is breaking a large encrypted backup into two small encrypted backups, then running both at the same time. During our testing, we measured as much as 30 percent improvement in elapsed time to encrypt data through breaking up a large encrypted backup into two smaller encrypted backups and running them at the same time.

The actual encryption is performed on ClearPath Cryptographic Co-processors on native systems such as the Libra Models 680 and 690 and the FS1800 server. Encryption is performed on the Windows side of MCPvm-based systems such as the Libra Model 300 and the FS1300 server.

We've found that performance is affected by tape drive throughput, the performance level of your MCP system, the performance level of the hardware actually doing the encryption and any competing workloads. While we provide (in the paragraphs below) the performance results of measuring our systems, you will need to do your own performance analysis with your own hardware and software configuration. You may find that your performance characteristics are significantly different than those related to our system measurements.

Normal, unencrypted copies of files to tape made by the Library Maintenance facility incur very little system overhead. Basically, data is read from disk into the same buffer that is used to write to tape. A minimal number of processor cycles are utilized, therefore there's little or no effect on performance. When the Tape Encryption software is used, the Library Maintenance facility and the infrastructure involved will inherently use more processor cycles, thus there's some amount of impact on the performance of running workloads.

Below is a table that demonstrates different potential impacts to encryption performance. While we provide you examples of the impact to elapsed time and processor utilization when using the Library Maintenance facility to write encrypted tapes, we highly recommend that you conduct your own performance tests to determine the resulting effects in your production environment.

The Libra Model 300 server we reference is a single-CPM system running at 1500 RPM. The Libra Model 595 server is a single-processor system running 12,150 RPM, then reconfigured to run at 4860 RPM. The amount of data encrypted was contained in a single 2 GB file. Our test was performed on an LTO-2 tape drive on both systems, then on a DDS5 tape drive (slower performance than LTO-2) on the Libra Model 300 server.

Copying 2 GB File Elapsed-Processor Time Comparison With and Without Encryption

System	Tape Drive	Non-Encrypt Elapsed Time	Encrypt Elapsed Time	Elapsed Time Difference	Non-Encrypt Processor Time	Encrypt Processor Time
Libra 595 12,150 RPM	LTO-2	112 s	296 s	264%	3 s	89 s
Libra 595 4860 RPM	LTO-2	111 s	457 s	411%	7 s	239 s
Libra 300 1500 RPM	LTO-2	136 s	393 s	288%	12 s	142 s
Libra 300 1500 RPM	DDS5	344 s	921 s	266%	12 s	131 s

Business Process Considerations

Library Maintenance Tape Encryption impacts the time taken to copy data to tape or CD and results in greater processor utilization. We cannot emphasize enough that you need to test tape encryption in your production environment to first determine the best way to integrate tape encryption with your regular backup process. Since encryption naturally takes extra time and consumes more processor cycles, you may want to restrict Library Maintenance Tape Encryption to only those backup tapes that contain sensitive data that may be at risk if lost or stolen in transit to your disaster recovery facility.

If you were to temporarily stop your business while backing up (and encrypting) your data, could you afford to have your business down for a somewhat longer period of time? You may want to consider a two-step backup process such as first copying your data to disk and then encrypting the disk copy to tape. This can reduce the amount of business downtime, assuming that your disk throughput is faster than your tape throughput.

Another consideration for the above-mentioned process is the reliability of your tape drives. We recommend that you do regular general maintenance on your tape drives since hardware errors that occur during encryption/decryption are much more critical.

In addition to testing tape encryption before you implement it, you should also test tape decryption before you completely convert to encrypted backup tapes. First be sure you understand the process required to restore data and the amount of time involved. You don't want to have your first experience with this process under the pressure of having to restore your system.

If your encrypted tapes are going to be shared with partners or sent to a disaster backup facility, that process should be tested as well before completely converting to data encryption. Encryption key management and methods for sharing encryption keys are explained later in this paper. Note that sharing Library Maintenance encrypted tapes requires that your partner or disaster backup facility also have available to them a ClearPath system running MCP and the Library Maintenance facility software. Tapes encrypted by Library Maintenance are not interchangeable with other non-MCP operating systems.

While Library Maintenance tape encryption supports COPY&VERIFY and COPY&COMPARE, you should be aware that these options will further impact elapsed time and processing usage.

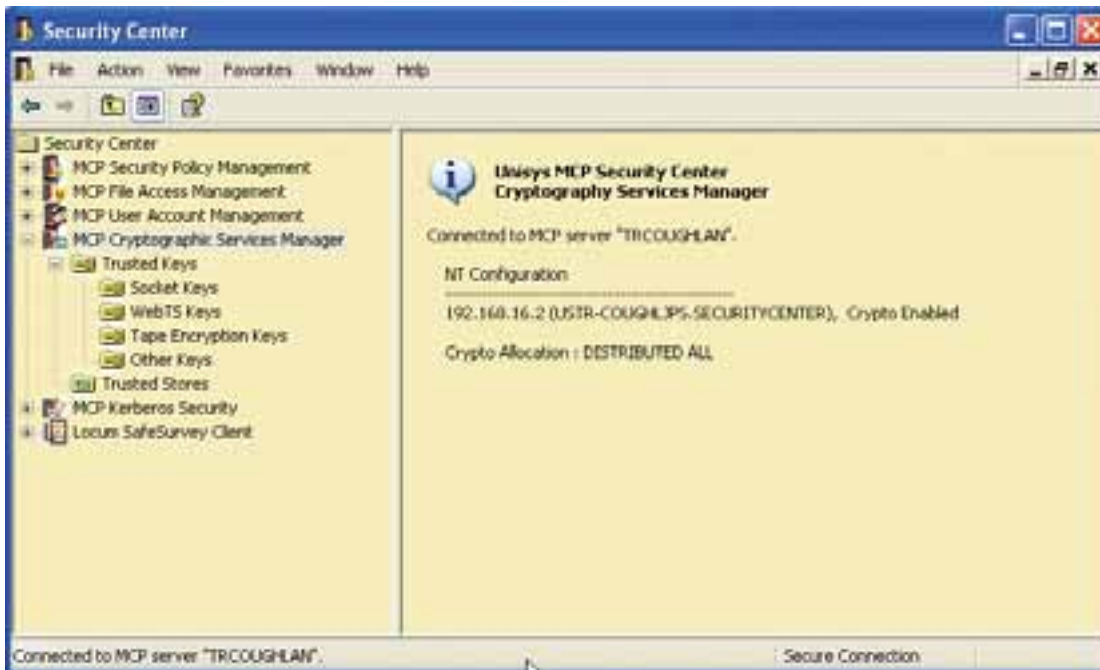
Create Tape Encryption Keys

Before you can use Library Maintenance Tape Encryption, your security administrator must first establish machine encryption keys. This is accomplished by using the Security Center MMC snap-in that runs on the security administrator's workstation. This could be a separate Windows based computer or, on the MCPvm systems, the Windows side of the ClearPath system. (Note that Security Center refers to these keys as tape encryption keys.) Your security administrator follows these steps to create machine encryption keys:

1. Initiates the Security Center MMC snap-in, via Start / Programs / Unisys MCP, and then clicks on Security Center.
2. Fills in the hostname of the MCP environment that you want to connect to, i.e. the MCP system for which you want to create the tape encryption keys, in the dialog box presented.
3. Logs on to the MCP environment, using the security administrator's usercode / password, in the dialog box.

If the Security Center database is not already initialized, this may cause the Security Center database initialization wizard to activate on the first valid connection. The database must be initialized successfully in order to create tape encryption machine keys.

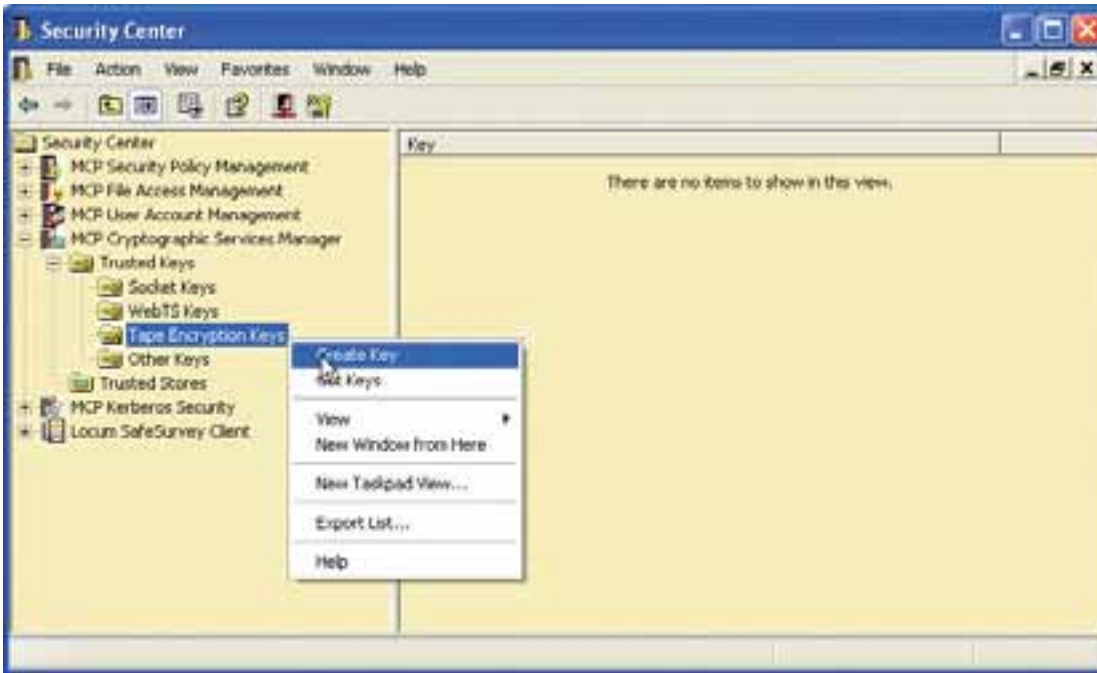
A successful logon results in the presentation of this Security Center window:



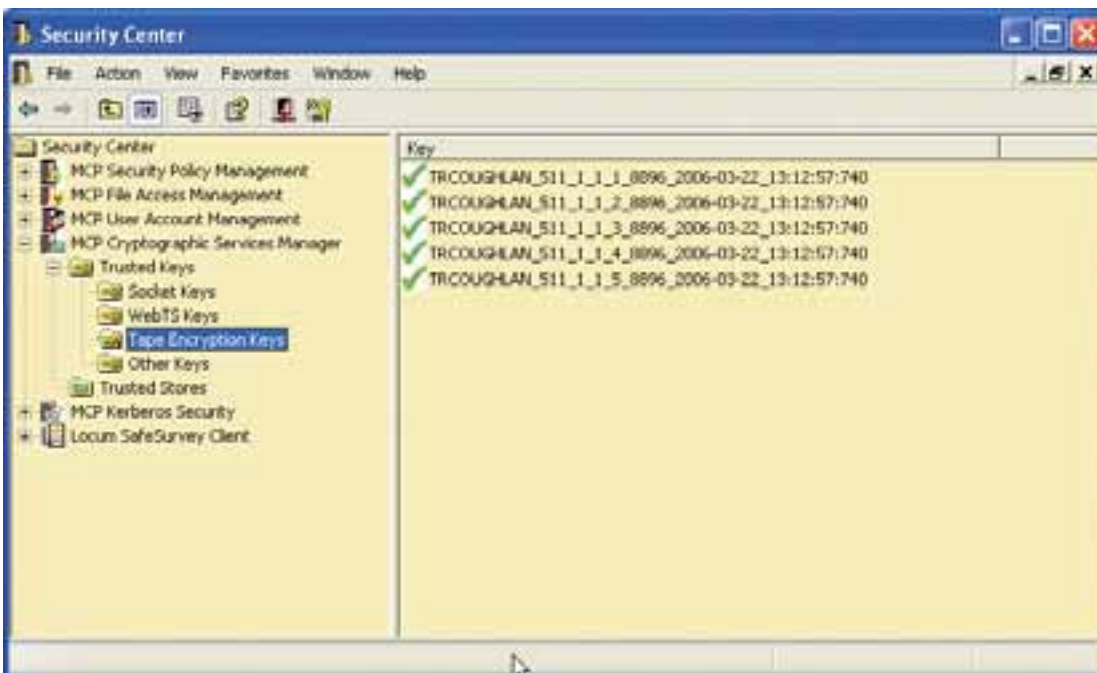
4. Next, your security administrator clicks on Cryptography Services Manager to expand this node, and then clicks on Trusted Keys.

5. And then right clicks on Tape Encryption Keys and chooses Create.

Then this window appears:



As shown below, a set of five (5) tape encryption keys now appears in the right-hand pane, for this hostname and SSR level of the currently running MCP.



Note that tape encryption keys are specific to an MCP release. If the MCP on your ClearPath system is upgraded to a new release (such as MCP 11.0), the security administrator needs to create a new set of tape encryption keys.

The created machine encryption keys are stored in the Security Center Database, which is a guardfile-protected DMSII database on your MCP host. These keys are “pushed down” into the Microsoft Windows based cryptography environments (the Intel / Windows side of an MCPvm-based system or a Cryptographic Co-processor) by Security Center.

The DMSII on the host is the DMSII runtime-only version that’s packaged with Security Center. This version can be used only by Security Center. (No DMSII runtime key is required.) With the Unisys Cryptographic Co-processor, the machine encryption keys are stored in protected storage that isn’t directly accessible to other programs.

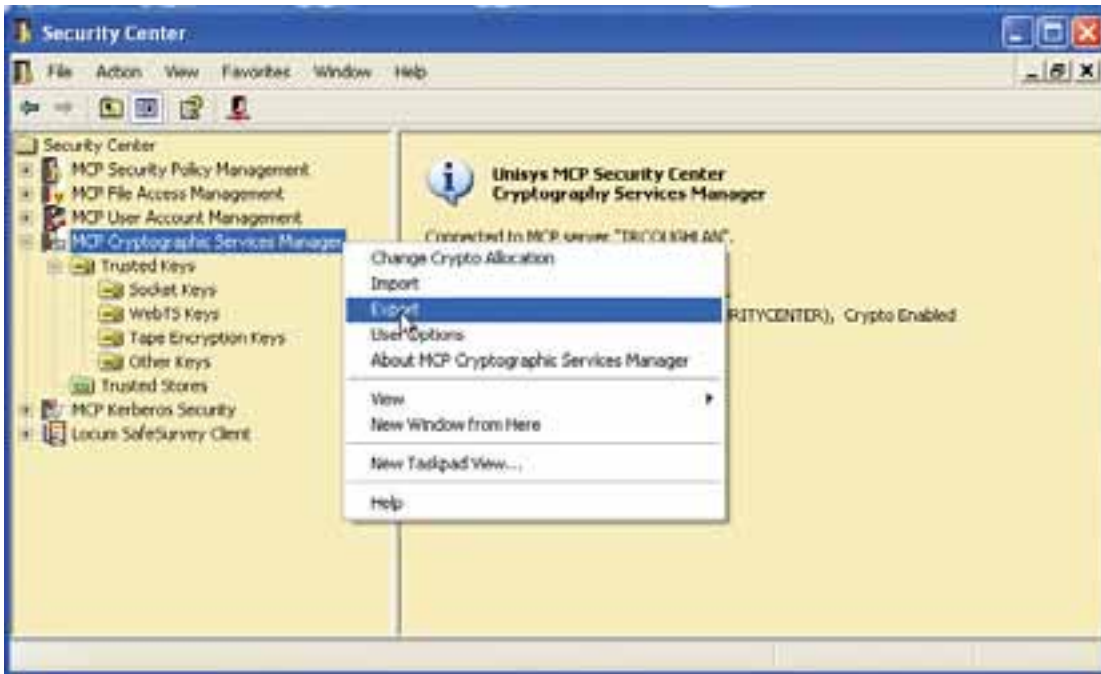
Back Up Tape Encryption Keys

Immediately upon having created tape encryption keys, it is very important to also create a backup copy of those tape encryption keys. Let us repeat this. Immediately backing up your keys is very important. If you were to lose these encryption keys, Unisys will be unable to help you decrypt your tapes.

You'll also need to back up or make a copy of these tape encryption keys in order to share the encrypted tapes and make it possible to decrypt them on other systems, such as those at your partners sites, your own disaster recovery facility or one belonging to a company providing you disaster recovery services.

Here is the process for backing up your encryption keys:

1. Right click on MCP Cryptographic Services Manager, then choose Export.

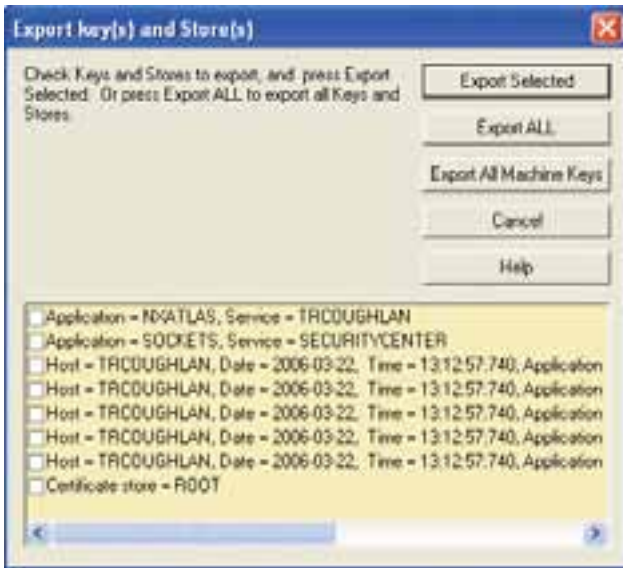


2. On the dialog box that's presented, select Export All or Export All Machine Keys, depending on your preference.

Note that this will back up all keys, not just the tape encryption keys.

Alternately, you can select the tape encryption keys by clicking on the selection boxes in front of them, and then clicking Export.

The tape encryption keys start with: <Hostname>_<MCP Level>_1.



3. A Save File dialog box will appear. Fill in the name of the file you want to create, and then click Save.

4. Either Save this file directly onto some portable media or Copy it to a portable media and store that media in a secure location.

For more information, please refer to the Security Center Readme and Help files on the Windows system where Security Center is installed.

Share Encrypted Tapes

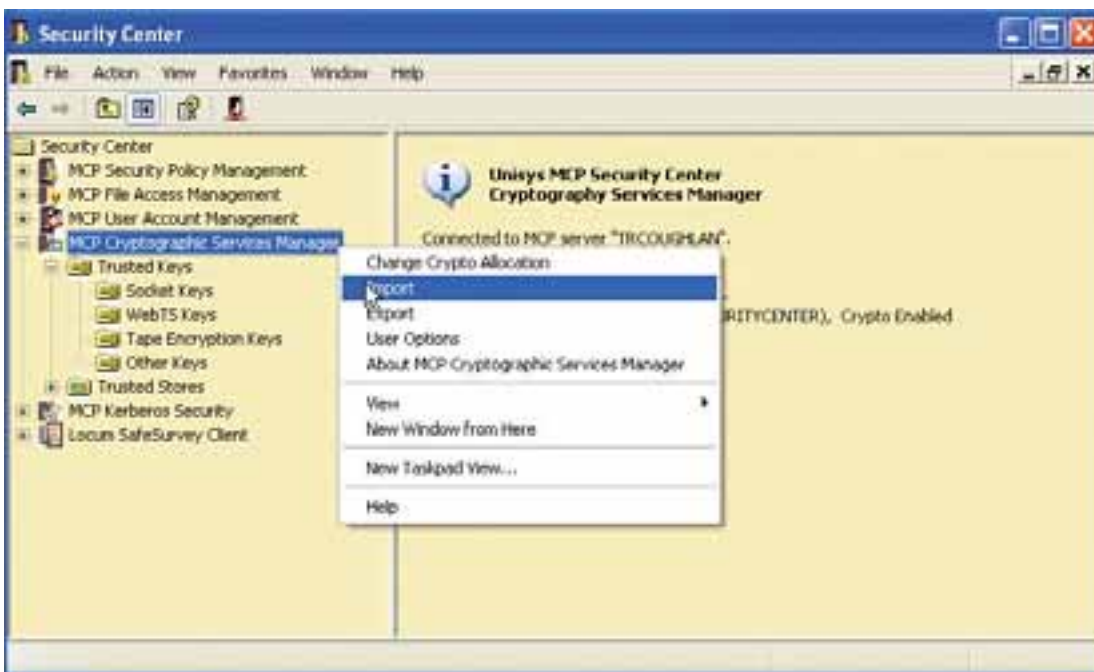
As long as you are decrypting tapes on the system used to encrypt them, no further action is required. Tapes are automatically decrypted on the system they were encrypted on.

However, you may need to share your tapes with a partner, such as a bank that shares customer information with a credit bureau. Or you may have an outside company providing disaster recovery for your operation. To decrypt a tape on a destination system other than the local system, the security administrator must first export the tape encryption keys from the local system and then import them on the destination system. If you are sending these keys offsite, it is essential to transport the tape encryption keys in a secure manner since access to these keys allows access to all the tapes encrypted by those keys. We strongly recommend using separate shipments to send encrypted tapes and encryption keys.

The first step to sharing keys is to export the tape encryption keys from the local system. Refer to the section Backing Up Tape Encryption Keys above for instructions on how to obtain a backup of the keys suitable for sharing with others.

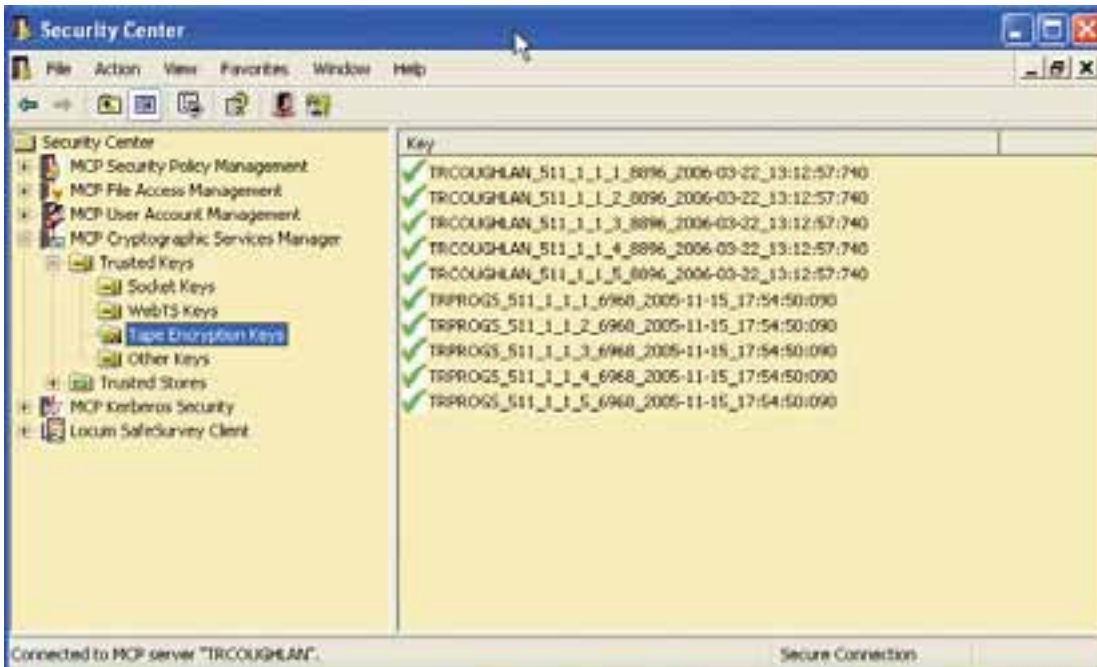
After transporting the media with the tape encryption keys to the destination system, your partner's or disaster recovery vendor's security administrator uses the Security Center MMC snap-in to:

1. Initiate the Security Center snap-in, connect and log on as we've described above.
2. Right click on MCP Cryptographic Services Manager and choose Import.



3. Enter the name of the file (and select the drive that the file is on) containing the tape encryption keys from the source system.
4. Click on Open.

The tape encryption keys from your source system have now been installed and appear in the right-hand pane when Tape Encryption Keys are selected. The example below indicates that tapes on this system will make use of the TRCOUGHLAN encryption keys. In addition, this system will be able to decrypt tapes from TRPROGS.



Encrypted tapes from your system (the source system) can now be decrypted on the destination system by just using a simple COPY command. Library Maintenance will have enough information to determine what original key was used to encrypt the tape, search for it among the installed tape encryption keys and then use it to decrypt the tape. It is not a problem to import keys from multiple systems if your requirement is to read or decrypt tapes from multiple systems.

Note that you can only encrypt tapes with the tape encryption keys that were created for your local system. Imported keys cannot be used to encrypt a tape. Your partner or disaster recovery vendor will not be able to create encrypted tapes with your encryption keys. If they intend to create encrypted tapes to be shared with you, they will have to go through the same encryption key backup and encryption key sharing process described above. Likewise, you will need to then import their tape encryption keys onto your system following the encryption-key-sharing process described above.

Tape Encryption Algorithms

The Library Maintenance facility supports two different encryption algorithms:

- Advanced Encryption Standard (AES, also known as AES256)
- A variant of the Data Encryption Standard (DES) known as Triple DES (3DES or TDES)

When using the AES encryption algorithm, you'll need the support of hardware running Microsoft Windows Server 2003 or Windows XP for encrypting tapes on systems such as the ClearPath Plus Libra Model 300 or Libra Model 595 servers. ClearPath Cryptographic Co-processors running on these systems support the AES encryption algorithm.

Only the Triple DES tape encryption algorithm is supported on hardware running Microsoft Windows 2000, a possibility with some configurations of ClearPath Plus Libra Model 180, Libra Model 520, CS7201 and LX7100 systems.

Library Maintenance Tape Encryption

When Library Maintenance software is used to encrypt a tape, two levels of automatically-generated encryption keys are used. As we previously explained in our step-by-step example, Security Center generates five machine keys. When the Library Maintenance facility encrypts a tape, it requests a new randomly-generated data encryption key and one of the five machine keys. The data encryption key itself is encrypted by the machine key and written to the tape, along with information that the Library Maintenance facility can use (when decrypting) to determine which machine encryption key was used to encrypt the data encryption key. Files are then written to tape using the data encryption key.

Tape encryption can be requested in two different ways. The SYSOPS option is provided to establish your system's default when you use Library Maintenance to copy data to tape.

The SYSOPS LMENCRYPT has three available values:

- NO (the default)
- TDES (3DES)
- AES256

This option establishes the default that Library Maintenance software is to use when copying files to tape. In this way, a local system administrator can set the system-wide tape encryption default for Library Maintenance. Setting this option is helpful when you are making use of WFL jobs to write your data to tape because it allows non-modified WFL jobs to write encrypted tapes. Care must be taken when applying the SYSOPS global encryption option on a system where multiple departments that may have conflicting encryption requirements are using the same system.

Tape encryption can also be requested with the Library Maintenance facility's COPY syntax, making use of the ENCRYPT attribute with the same three values (NO, TDES, and AES256). When you specify an ENCRYPT value in a COPY statement, it overrides any value that's been specified by SYSOPS LMENCRYPT.

Here are some examples:

`COPY <files> TO T (SERIALNO=55555);`
defers to the SYSOPS LMENCRYPT setting.

If SYSOPS LMENCRYPT is NO, the data written by the Library Maintenance facility to destination tape T will not be encrypted.

If SYSOPS LMENCRYPT is TDES or AES256, the data written by Library Maintenance to destination tape T will be encrypted accordingly.

`COPY <files> TO T (SERIALNO=55555, ENCRYPT = NO);`
Library Maintenance writes unencrypted data to destination tape T, regardless of the setting of SYSOPS LMENCRYPT.

`COPY <files> TO T (SERIALNO=55555, ENCRYPT = TDES);`
Library Maintenance writes encrypted data to tape using the 3DES algorithm, regardless of the setting of SYSOPS LMENCRYPT.

Checklist

Now that you're familiar with the major aspects of using the ClearPath Tape Encryption solution used in combination with the MCP Library Maintenance facility, you may find this checklist useful in deciding if you're prepared to get started.

- Install Security Center (if necessary)
- Verify that the latest IC levels for MCP, SECURITY and SECURE-TRANSPORT are installed
- Initialize database (if necessary)
- Create machine keys
- Back up machine keys (very important)
- Test encryption
- Test decryption
- Test backup/restore process (using encrypted data)
- Test sharing keys and encrypted data (if encrypted tapes are to be shared)

Restrictions

Please be sure that you are aware of these restrictions before getting started with the Library Maintenance Tape Encryption solution:

- The Library Maintenance facility can't encrypt data being copied to disk or CD. Library Maintenance can only be used to encrypt data being written to tape or CD.
- Earlier versions of Library Maintenance did not support using ENCRYPT with & VERIFY. This restriction has been removed with later versions of Library Maintenance (MCP 11.0 IC26, MCP 10.0 IC98, and MCP 9.0 IC149).
- The LOADER can't load files stored on encrypted Library Maintenance tapes.
- You can only use AES256 encryption on ClearPath systems that have Microsoft Windows Server 2003 or Windows XP on the MCPvm system (such as an FS1400 or Libra Model 300 server) or on an attached Intel processor running Windows for native MCP systems (such as a Libra Model 680 or Libra Model 690 server). [On ClearPath systems that have only Windows 2000 available (possible for some configurations of the CS7201, Libra Model 180 and Libra Model 520 servers and the LX7100), you can use the Triple DES (3DES) algorithm to encrypt tapes.]

- You can't decrypt a tape encrypted using the AES256 algorithm on an MCP ClearPath system running Windows 2000 in the Windows environment. [If there is a possibility that an encrypted tape might have to be decrypted on an MCP ClearPath system running Windows 2000 on its Windows environment, then you must encrypt the tape using the 3DES algorithm.
- You can't encrypt a tape using the MCP Library Maintenance facility, then decrypt it on an OS 2200 based ClearPath system.
- You can't use MCP Library Maintenance to decrypt a tape that was created on an OS 2200-based ClearPath system or one that was created by any third-party product.

Future Directions

Note that as of the MCP 11.1 release, the Tape Encryption product now supports encrypting data when creating DMSII Backup or DMSII Audit tapes. For earlier releases, refer to FAQ 10029953 for using a combination of MCP DMUTILITY Dump, Enterprise Database server for ClearPath Quiesce, and Library Maintenance to backup and encrypt DMSII data and audit files from disk to tape, and to decrypt the files from tape to disk for recovery operations. We are investigating more secure methods of sharing encryption keys with partners and disaster recovery facilities. We are also examining hardware-based tape encryption options such as co-processors and tape drives that encrypt and decrypt at the drive level.

There's an emerging industry standard being defined for tape encryption: the IEEE P1619 Standard Architecture for Encrypted Shared Storage Media. Unisys Library Maintenance Tape Encryption is to be evaluated against that standard when it's available to determine what, if any, changes might be appropriate.

Hardware tape peripheral development in the industry is clearly heading toward more native support for encryption within the tape drive itself. Unisys will continue to monitor and evaluate hardware advances to determine appropriate tape drives to add to our list of qualified and supported peripherals.

Biography

Author

Alan Fritchoff is a manager for the ClearPath MCP platform's Computer Systems Architecture Group. Alan has more than 26 years of experience with the MCP software environment and has served as a Unisys manager for a variety of ClearPath products and projects.

His current management responsibility covers an array of MCP components and utilities that include security and data encryption. Alan holds a Bachelors degree in Mathematics from the University of California at Santa Barbara.

Notes:

For more information, contact your Unisys representative.

Or call:

1-800-874-8647, ext. 776 (U.S and Canada)

00-1-595-742-6780, ext. 776 (other countries)

In a hurry to learn more? Visit:

<http://unisys.com/cp/libra>

For even more details, visit:

<http://unisys.com/cp/community>

This document is not a contract and does not create any binding representations or warranties by Unisys. All representations are contained only in the applicable agreement signed by the parties.

The information contained herein is subject to change without notice.

© 2007 Unisys Corporation. All rights reserved.

Unisys is a registered trademark of Unisys Corporation. All other brands and products referenced in this document are acknowledged to be the trademarks or registered trademarks of their respective holders.

