CA Tape Encryption

Best Practices Guide

Release 14.5.00

CA Technologies Product References

This document references the following CA Technologies products:

- CA 1® Tape Management (CA 1)
- CA Tape Encryption
- CA TLMS® Tape Management (CA TLMS)

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Provide Feedback

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

If you would like to provide feedback about CA Technologies product documentation, complete our short customer survey, which is available on the CA Support website at http://ca.com/docs.

Best Practices Guide Process

These best practices represent years of product experience, much of which is based on customer experience reported through interviews with development, technical support, and technical services. Therefore, many of these best practices are truly a collaborative effort stemming from customer feedback.

To continue and build on this process, we encourage users to share common themes of product use that might benefit other users. Please consider sharing your best practices with us.

To share your best practices, contact us at techpubs@ca.com and preface your email subject line with "Best Practices for *product name*" so that we can easily identify and categorize them.

Contents

Chapter 1: Introduction 7

Purpose of this Guide 7
Audience 7
Mainframe 2.0 Overview 7
Mainframe 2.0 Features 8

Chapter 2: CA Tape Encryption Installation and Configuration Best Practices 11

Installation Considerations 11
Configuration for Optimal Performance 11
- Disaster Recovery Plan 12
- Database Selection 13
- Pass Phrase Protection 14
- Dual Pass Phrases 14
- Multi-System Environment Considerations 15
- zIIP Processor 15
- Encryption Algorithm Selection 16
- Compression 17
- Key Life Cycle Management 18
- CA Tape Encryption Health Checker 19
- Use the Graphical Management Interface (GMI) 20

Index 23

Chapter 1: Introduction

This section contains the following topics:

Purpose of this Guide (see page 7)
Audience (see page 7)
Mainframe 2.0 Overview (see page 7)
Mainframe 2.0 Features (see page 8)

Purpose of this Guide

The guide provides a brief introduction to CA's Mainframe 2.0 strategy and features, and describes the best practices for installing and configuring CA Tape Encryption.

Audience

The intended audience of this guide is systems programmers and administrators who install, configure, deploy, and maintain CA Tape Encryption.

Mainframe 2.0 Overview

Mainframe 2.0 is our strategy for providing leadership in the mainframe operating environment. We intend to lead the mainframe marketplace for customer experience, Out-Tasking solutions, and solution innovation. After listening to customer needs and requirements to keep the mainframe operating environment viable and cost-effective, we are providing new tools to simplify usage and to energize this operating environment for years to come.

CA Mainframe Software Manager™ (CA MSM) is an important step in realizing the Mainframe 2.0 strategy. CA MSM simplifies and standardizes the delivery, installation, and maintenance of mainframe products on z/OS systems. CA MSM has a browser-based user interface (UI) with a modern look and feel for managing those solutions. As products adopt Mainframe 2.0 features and CA MSM services, you can acquire, install, and manage your software in a common way.

CA MSM provides software acquisition and installation that make it easier for you to obtain and install CA mainframe products, and apply the recommended maintenance. The services within CA MSM enable you to manage your software easily based on industry accepted best practices. The common browser-based UI makes the look and feel of the environment friendly and familiar.

We follow the IBM z/OS packaging standards using SMP/E, with some additional CA qualities of service added, to make installation simple and consistent. Additionally, through the synchronization of product releases and the use of common test environments, we will declare a yearly mainframe software stack that includes many new releases with enhanced functionality. This stack is certified for interoperability across the CA mainframe product portfolio and the base IBM z/OS product stack.

Mainframe 2.0 Features

Mainframe 2.0 has the following main features:

CA Mainframe Software Manager (CA MSM)

Delivers simplified acquisition, installation, and deployment capabilities using a common z/OS-based web application delivered through a browser-based UI. CA MSM includes the following services:

Product Acquisition Service (PAS)

Facilitates the acquisition of our mainframe products and services, including product base installation packages and program temporary fixes (PTFs). This service integrates the inventory of products available on your system with CA Support, providing a seamless environment for managing and downloading software and fixes onto your system.

Software Installation Service (SIS)

Facilitates the installation and maintenance of our mainframe products in the software inventory of the driving system. This service enables you to browse and manage the software inventory using a web interface, and automates tasks for products that use SMP/E to manage installation. You can browse downloaded software packages, and browse and manage one or more consolidated software inventories (CSIs) on the driving system.

Software Deployment Service (SDS)

Facilitates the deployment of CA Technologies mainframe products from the software inventory of the driving system. This service enables you to deploy installed products that are policy driven with a set of appropriate transport mechanisms across a known topology. The enterprise system topology can include shared DASD environments, networked environments, and z/OS systems. Policies represent a combination of metadata input that identifies the component parts of a product and user-supplied input that identifies the deployment criteria, such as where it will go and what will it be called.

Electronic Software Delivery (ESD)

Enables you to get our products from an FTP server. We have improved this process so that you no longer need to build a tape to install the product.

Best Practices Management

Integrates with IBM Health Checker for z/OS to verify that deployed software follows our best practices. The health checks continually monitor the system and software to provide feedback on whether the software continues to be configured optimally.

Best Practices Guide

Provides best practices for product installation and configuration.

Note: For additional information about the CA Mainframe 2.0 initiative, see http://ca.com//mainframe2.

Chapter 2: CA Tape Encryption Installation and Configuration Best Practices

This section contains the following topics:

Installation Considerations (see page 11)
Configuration for Optimal Performance (see page 11)

Installation Considerations

Use CA Mainframe Software Manager to acquire, install, and maintain your product.

Business Value:

CA Mainframe Software Manager provides a web interface, which works with ESD and standardized installation, to provide a common way to manage CA mainframe products. You can use it to download and install CA Tape Encryption.

CA Mainframe Software Manager lets you download product and maintenance releases over the Internet directly to your system from the CA Support website. After you use CA Mainframe Software Manager to download your product or maintenance, you use the same interface to install the downloaded software packages using SMP/E.

Additional Considerations:

After you install the product, use the *Configuration Guide* to set it up. CA Mainframe Software Manager can continue to help you maintain your product.

More Information:

For more information about CA Mainframe Software Manager, see the *CA Mainframe Software Manager Guide*. For more information about product setup, see the *Installation Guide*.

Configuration for Optimal Performance

The following section explains the best practices for configuring CA Tape Encryption for optimal performance.

Disaster Recovery Plan

Create a plan that includes all of the environments where CA Tape Encryption will run before commencing installation.

Business Value:

Planning ahead to identify the z/OS system and cryptographic components available at your disaster recovery (DR) site ensures that CA Tape Encryption can initialize and run smoothly at DR. This avoids any problems with not having the required cryptographic components available at DR. For example, if your production site runs a z9 with CPACF enabled and your DR site runs a z890, the CPACF processor may not be enabled at the DR site. This would require you to use slow software-based algorithms rather than the fast hardware-based implementations of the algorithms

Additional Considerations:

If a third party hosts your disaster recovery processing, contact them to identify the cryptographic capabilities of the systems at DR.

More Information:

For information on identifying cryptographic capabilities, see the *Installation Guide*.

Database Selection

Use the CA Tape Encryption database (BES database) as your key repository unless your company has specific security and cryptography requirements.

Business Value:

CA Tape Encryption with a BES database key repository is faster and easier to recover at DR than CA Tape Encryption with a Cryptographic Key Data Set (CKDS) key repository. Choosing the BES database saves your business time and money because you can start application processing at DR more quickly.

Additional Considerations:

Symmetric keys generated by CA Tape Encryption are saved in *one* of the following:

- The BES database
- The CKDS database

The parmlib attribute KeysDatabase= specifies the database used.

If you choose to save keys in the CKDS database:

- The keys are prevented from leaving the secure hardware environment provided by a FIPS 140-2 certified IBM PCI cryptographic coprocessor card.
- The ICSF component must be installed and configured to allow CA Tape Encryption to request that ICSF create keys in the trusted hardware.
- You must recover the ICSF application and the CKDS using the utilities and procedures provided by IBM to run your applications at DR.
- You must recover the BES database to run at DR.

More Information:

For information on secure key processing requirements, see the *Administration Guide*.

Pass Phrase Protection

Update your DR procedures to make sure that you have the pass phrase (or dual pass phrases) used to protect the BES database before leaving your home site.

Business Value:

Having the BES database pass phrase (or dual pass phrases) with you at DR insures that you are able to recover CA Tape Encryption quickly on a new CPU.

Additional Considerations:

You are prompted for the pass phrase when:

- Starting the BES task on a new CPU
- You use the RELOAD=PASSPHRASE command to change the pass phrase

Until you provide the correct pass phrase (or dual pass phrases) you cannot access your encrypted tape data. If you upgrade CPUs at your home site you should also be prepared to provide the pass phrase (or dual pass phrases) when starting CA Tape Encryption on any new CPUs.

Dual Pass Phrases

Use the dual pass phrase feature to provide optimal protection of the BES database.

Business Value:

The use of dual pass phrases insures that no individual can gain access to the BES database that contains the crypto-keys used by CA Tape Encryption. This provides increased protection for this critical resource.

Additional Considerations:

The master BES pass phrases are the cryptographic pass phrases used to securely encrypt sensitive data in the BES database.

Use the PassPhraseCount= attribute in the PARMLIB Startup member to specify either a single or dual pass phrase.

Use PassPhraseID1= and PassPhraseID2= attributes in the Startup member to customize the messages issued at startup that request the two parts of the pass phrase. The messages can be used to specify names or groups that are meaningful for your company to identify the individuals owning the two parts of the pass phrase.

Multi-System Environment Considerations

Use a single PARMLIB in shared multi-system environments.

Business Value:

A single PARMLIB simplifies maintenance and control of the system options.

Additional Considerations:

If you are sharing the BES database and mirror database among multiple systems, consider the following:

- The CA Tape Encryption installation libraries can be shared or cloned.
- The CA Tape Encryption maintenance levels of sharing systems do not need to be the same, but new features or enhancements might be usable only when supported by all systems.
- The sharing systems do not need to belong to the same SYSPLEX and do not have to be at the same MVS level.
- Keep production and test BES systems separate. Have a test “sandbox” system with a different BES database and mirror and a separate tape management system catalog.

zIIP Processor

Use the IBM System z Integrated Information Processors (zIIPs) if they are available.

Business Value:

Off-loading encryption and compression processing from the main processor to the zIIP:

- Saves billable CPU time by reducing the execution time on the normal central processing unit (CPU).
- Frees up processing cycles from the CPU to other work.

Additional Considerations:

To direct encryption and compression processing to the zIIP:

- Specify zIIPExploitation=Y in the StartupOptions member.
- Update the PercentRunOnzIIP= attribute with a value greater than 0 in the DynamicOptions member.

Use of the zIIP processor is monitored through the IBM Resource Management Facility (RMF) Service Class (WLMGL) report using SMF Record Types 72 (RMF Workload Activity and Storage Data) and 79 (RMF Monitor II Activity).

Encryption Algorithm Selection

Select the strongest hardware-based algorithm available on your system.

Business Value:

Selecting a strong algorithm implemented in hardware with a larger key gives you the best combination of faster processing while securing the encrypted data for a longer period of time.

Additional Considerations:

CA Tape Encryption supports the DES, triple DES, and AES algorithms:

- DES64
- 3DES128
- 3DES192
- AES128
- AES192
- AES256

Hardware algorithms perform quicker than their software equivalents. With the exception of DES64, these algorithms are all FIPS-compliant. The DES and triple DES algorithms are implemented in hardware in CCF and CPACF, and AES128 is implemented in hardware on the z9. The z10 provides hardware implementations of AES192 and AES256.

Consider your DR processing when selecting the algorithm. CA Tape Encryption provides software versions of the AES128, AES192, and AES256 algorithms that can be used to recover tapes at a DR site if the algorithms are not available in hardware.

Compression

Enable the CA Tape Encryption compression feature.

Business Value:

Enabling CA Tape Encryption compression and selecting the best compression method for your site reduces the number of tapes required for your business.

Additional Considerations:

The IDRC compression provided in most tape hardware is rendered ineffective by encryption. Tape files that used to fit on one tape cartridge might expand to a second or third cartridge. The built-in compression processing in CA Tape Encryption, includes:

- Nine software compression algorithms (S0-S8)
- Five hardware compression algorithms (H1-H5)
- A utility that evaluates the effectiveness of the different compression algorithms on your data

To activate compression, specify the Compress= parameter in either the Dynamic Options member or in specific symmetric key definitions. Use the MinimumCompressionRate = parameter to turn off compression if the desired rate of compression is not met.

Use the S0 compression algorithm if you do not have the time to research the best compression algorithm. S0 is a standard Run Length Encoding (RLE) algorithm primarily used for files that contain redundant alphanumeric data such as blanks, zeros, and asterisks. The S0 algorithm generally produces the best results with fewer CPU cycles.

If CPU resources are available, the S8 algorithm might result in better compression. The S8 algorithm is an adaptive Ziv-Lempel algorithm commonly referred to as LZ78, but the data is first compressed using the S0 method (RLE) to reduce the amount of data that must be processed by LZ78.

Key Life Cycle Management

Use CA Tape Encryption automated key life cycle management.

Business Value:

The CA Tape Encryption key life cycle management feature reduces business costs by allowing you to control the expiration of your tape files from the tape management system. Keys that are known to no longer be used are available for deletion.

Additional Considerations:

CA Tape Encryption integrates with the CA 1, CA TLMS, and IBM DFSMSrmm tape management systems to control the life-cycle management of keys used to encrypt tape files managed by these products.

CA Tape Encryption assigns a unique identifier for each symmetric key known as the BES Key Index (BESKEY). The BESKEY is saved in:

- The tape management catalog. This allows you to identify what files are encrypted and what key was used to encrypt the data.
- The User Header Labels (UHL) and User Trailer Labels (UTL) on the tape and in the CA Tape Encryption database.

CA Tape Encryption provides a job to read each tape management system's catalog to identify all BESKEYs retained in the catalog to ensure that the keys are retained. To automatically remove keys, set the PARMLIB attribute AutomaticallyRemoveKeys=Y. CA Tape Encryption puts the keys no longer defined to the tape management system catalog on a 90 day deletion queue. If a key is used to decrypt a tape it is automatically removed from the queue.

CA Tape Encryption Health Checker

Monitor the CA Tape Encryption Health Checker messages to:

- Alert you to conditions that can prevent CA Tape Encryption from running properly.
- Guide you in how to address any problems.
- Provide best practices for running CA Tape Encryption.

Business Value:

The Health Checker helps you configure CA Tape Encryption for optimum performance.

Additional Considerations:

The following checks are provided for CA Tape Encryption:

TE_BEST_PRACTICE_ALOGRITHMS@BESn

Monitors your use of control parameters that cause encryption to be performed outside of the CPACF processor.

TE_CHECK_BES_KEYS_AVAIL@BESn

Monitors the number of unique BES key index values in use by this BES.

TE_VRFY_DB_PLACEMENT@BESn

Ensures the BES primary and mirror databases are not on the same volume.

TE_VRFY_DB_SPACE@BESn

Monitors the amount of space available for encryption key storage in the database used by this BES.

TE_VRFY_ICSF_CHECKAUTH@BESn

Ensures your ICSF system is operating with CHECKAUTH(NO) specified.

TE_VRFY_KEYS_DB@BESn

Ensures your KeysDatabase StartUp attribute correctly identifies the keys database.

TE_VRFY_LPA_MODULES@BESn

Ensures the LPA modules in use by this BES are not back-leveled by another BES.

TE_VRFY_ZIIP_ATTRS@BESn

Ensures the zIIPExploitation and the PercentRunOnzIIP attributes are consistent.

TE_VRFY_ZIIP_ENVIRON@BESn

Ensures zIIP resources are being used when they are available in the system.

Use the Graphical Management Interface (GMI)

Use the CA Graphical Management Interface (CA GMI) to view and monitor CA Tape Encryption activity.

Business Value:

CA GMI is CA's graphical management interface product that allows you to view and manage CA Tape Encryption activity from a Windows PC. CA GMI's structure is object oriented and provides a common layout consisting of an object tree, and consistent menu options and icons. This common layout makes it easy to remember how to navigate and use features. It also supports having multiple windows open at the same time (not hierarchical like the 3270), which allows you to view and compare information simultaneously.

This point-and-click interface provides a common and consistent method for viewing and managing multiple CA products, which can save considerable cost and time on training and learning.

Additional Considerations:

CA GMI consists of PC clients which interface with a z/OS server component to allow access to basic z/OS server functions.

The following are the available PC clients:

Windows-based Client

This client provides full functionality. That is, you can manually perform view and analysis functions, filter and sort desired entries, zoom (drill-down) to related objects, and take actions upon selected entries. You can create customized colored reports in different formats, for example, tables and graphs. These reports can be printed and exported to your PC directory, servers, intranet, and so on. You can create, manage, and view Summary objects. This client also provides designer wizards to create scripts to monitor and respond to any condition, exceptional or routine, in automatic ways. These automation services let you replace many if not all of the manual processes of managing your system.

Web-based Client

This client can be used from any PC with internet access to the CA GMI application server. The current version of the Web-based Client provides the user-driven functionality of view and analysis, filtering and sorting, zooming, and the ability to take actions on selected entries. You can create customized colored reports in different formats, for example, tables and graphs, and you can also view Summary objects.

CA GMI is included free of charge with many CA products, including CA Tape Encryption.

More Information:

For more information about CA GMI for CA Tape Encryption, see the *CA Tape Encryption CA GMI Guide*.

More Information:

For more information about GMI for CA Tape Encryption, see the *Audit Guide*.

Index

A

algorithms, compression • 17
algorithms, encryption • 16
AutomaticallyRemoveKeys attribute • 18

B

BES database • 13

C

CA Mainframe Software Manager • 7, 11
CA Tape Encryption Health Checker • 19
compression • 17
contacting technical support • 3
Cryptographic Key Data Set • 13

D

disaster recovery • 12
dual pass phrases • 14

E

Electronic Software Delivery • 8
encryption algorithm • 16

G

GMI (Graphical Management Interface) • 20

I

IBM Health Checker • 8

K

key life cycle management • 18

M

Mainframe 2.0 • 7
multi-system environments • 15

P

pass phrases • 14
pass phrases, dual • 14
PassPhraseID1 attribute • 14
PassPhraseID2 attribute • 14
PercentRunOnzIIP attribute • 15
Product Acquisition Service • 8

S

Software Installation Service • 8
support, contacting • 3

Z

zIIP processor • 15