

CA Encryption Key Manager r14.5

CA Encryption Key Manager is a z/OS-based, software cryptographic solution that helps ensure the highest availability of encryption keys and encrypted data enterprise-wide. It centralizes and automates key lifecycle processes to reduce the possibility of downtime resulting from the inability to access encrypted data. It provides centralized encryption key management for any combination of IBM TS1120 (3592-E05) and IBM TS1130 tape encryption devices, as well as CA Tape Encryption subsystems. It can also automatically and transparently replicate and share encryption keys across a secure internal network within the enterprise and secure external network connections with business partners.

Business Value

CA Encryption Key Manager helps ensure compliance with data security regulations and laws by delivering automated, centralized management for encryption keys from different cryptographic solutions. It enables higher availability of encrypted data in your enterprise, and reduces any delay accessing encrypted data during disaster recovery, hardware errors or system outages. By reducing the complexity and time to manage local or remote systems, novice and experienced staff can easily manage cryptography and compliance. Plus, since it is vendor-neutral, you avoid being locked into costly stand-alone hardware or software purchases that could introduce single points of failure, or are not designed to share keys across the network nor designed for business continuance.

Product Overview

CA Encryption Key Manager lets you monitor, track, audit, manage, and protect multiple vendor's encryption keys from a single location to ensure their highest availability, recoverability and portability. It helps facilitate FIPS 140-2 compliance and supports NIST 800-57 key standards. Users of IBM TS1120 and TS1130 tape encryption devices, as well as users of CA Tape Encryption, can save time and reduce complexity by using a single centralized interface to manage multiple hardware or software instances. In addition these users can automatically share, replicate and exchange encryption keys, including Business-to-Business (B2B) decryption keys, without manual intervention or interaction—making encrypted data always available across the enterprise and to authorized business partners without being limited by geography or hardware configuration.

Delivery Approach

CA Services provides a portfolio of mainframe services delivered through CA internal staff and a network of established partners chosen to help you achieve a successful deployment and get the desired business results as quickly as possible. Our standard service offerings are designed to speed deployment and accelerate the learning curve for your staff. CA's field-proven mainframe best practices and training help you lower risk, improve use/adoption and ultimately align the product configuration to your business requirements.

Features

Mainframe 2.0

CA Encryption Key Manager has adopted key Mainframe 2.0 features designed to simplify your use of CA Encryption Key Manager and enable your staff to install, configure and maintain it more effectively and quickly.

- **CA Mainframe Software Manager:** The CA Mainframe Software Manager automates CA Encryption Key Manager installation and maintenance and removes SMP/E complexities.
 - > The **Product Acquisition Service** enables you to easily move product installation packages and maintenance from CA Support Online directly to your mainframe environment and prepare them for installation.
 - > The **Software Installation Service** standardizes CA Encryption Key Manager installation, which includes a new, streamlined Electronic Software Delivery (ESD) method that allows CA Encryption Key Manager to be installed using standard utilities. This service also provides standardized SMP/E product installation and maintenance via APARs and PTFs, and simplifies SMP/E processing through an intuitive graphical user interface and an intelligent Installation Wizard.
 - > The **Software Deployment Service** enables you to easily deploy CA Encryption Key Manager in your mainframe environment.
 - > **CA MSM Consolidated Software Inventory (CSI)** updates and infrastructure improvements add flexibility to CA MSM processing of CSIs and enable CA MSM to more effectively utilize CPU and system memory.
- **Installation Verification Program (IVP) and Execution Verification Program (EVP):** As part of qualification for inclusion in the set of CA mainframe products released every May, CA Encryption Key Manager has passed stringent tests performed through the IVP and EVP to find and resolve interoperability problems prior to release. These programs are an extension of CA's ongoing interoperability certification initiative launched in May 2009
- **Best Practices Guide:** This guide provides information on CA Encryption Key Manager installation, initial configuration and deployment to shorten the learning curve for staff responsible for the installation and management of this product.
- **Health Checker:** The Mainframe 2.0 Health Checker provides CA Encryption Key Manager Health Checks that execute under the IBM Health Checker for z/OS.
 - > CA Encryption Key Manager provides 5 health checks to inspect parameter settings and to monitor active encryption processing for possible problems. When problems are found the checks provide detailed recommendations on how to correct the problem. The CA Encryption Key Manager Health Checks also make "best practice" recommendations for using the products, telling the user how to implement the best practice. Examples of CA Encryption Key Manager Health Checks include:
 - Checks to monitor the availability of space in the database for key generation and key lifecycle tracking
 - Monitoring the maintenance levels of the active CA Encryption Key Manager tasks on the system to help make sure that shared modules are current and to warn if product load libraries are found to be back-level.

Other Key Features

- **Centralized Multi-Vendor Management of Encryption Keys:** Centralized multi-vendor key management enables efficient compliance and administration of the entire encryption infrastructure. The status of managed encryption keys for different encryption devices and systems across multiple CPUs and multiple sites can be seen at a glance.



- **Automated Key Replication and Failover Support:** Encryption keys are automatically replicated over a cluster of local and geographically dispersed hosts making each participant a potential failover system and a source to recover encryption keys in case of a disaster, hardware errors or system outage.
- **Automated Full Lifecycle Encryption Key Management:** CA Encryption Key Manager features full lifecycle key management that goes beyond just the central creation and storage of keys. Rather, it includes creation, monitoring, tracking, auditing, backup and recovery, and the automated expiration and removal of expired keys.
- **Automatic Synchronization with External Security Systems:** CA Encryption Key Manager interfaces with all z/OS external security systems like CA ACF2™ for z/OS, CA TopSecret® for z/OS and IBM RACF for Public/Private keys and digital certificates storage. When CA Encryption Key Manager is started in a multi-system or disaster recovery environment, the external security system key store is monitored and digital certificates automatically re-imported if they are not found. This provides for fast and automated recovery of encrypted data.
- **Digital Certificate Protection:** Every digital certificate created by CA Encryption Key Manager is also saved in the product key store, providing additional protection of this critical resource. In addition each product key store can be replicated over key stores owned by a cluster of local and geographically dispersed hosts.
- **RSA Key Pairs for the Enterprise:** Ability to create and exchange/export RSA Keys (public private key pairs) in digital certificates with any application that supports digital certificates adhering to the X.509 standard.
- **Automated Tape Key Generation and Key Change Policy Enforcement:** Supports dynamic, automated change of encryption keys and digital certificates used to protect data to reduce risk and manual intervention.
- **NIST 800-57 Key Standards:** Helps ensure compliance and fully supports the National Institute of Standards and Technology; document NIST 800-57, Recommendation for Key Management.
- **Tape Management System Support:** Integration of CA Encryption Key Manager into CA's z/OS tape management systems, CA 1® Tape Management and CA TLMS® Tape Management, as well as IBM's DFSMSrmm provides simplified and integrated full lifecycle key management and tape data protection.
- **Option for Networked Key Management:** This optional feature helps increase encrypted data availability, accessibility and instant encryption key recoverability for IBM TS1120 and TS1130 tape encryption devices, as well as CA Tape Encryption subsystems throughout any Sysplex, LPAR and site within the enterprise. It offers:
 - > An interconnected network of encryption keys and encrypted data for enterprise-wide high availability
 - > Automated encryption key replication that helps reduce single points of failure through real-time key store synchronization and change propagation over SSL TCP/IP connections
 - > Flexible, centralized control that gives users the ability to manage and operate all hosts in the Enterprise from a single LPAR
 - > Transparent B2B encryption key exchange by automatically obtaining and sharing symmetric decryption keys
- **Integrates with Web-based and Windows-based CA Graphical Management Interface (CA GMI):** This no-cost feature brings a common user interface, either web-based or Windows-based, to the power of CA Encryption Key Manager. This interface provides access to the keys and policies in use and details on each symmetric and RSA key (digital certificate) created, as well as the CA Encryption Key Manager subsystem and configuration settings. In addition, CA GMI allows many of the capabilities and value of CA Vantage™ Storage Resource Manager to be at the fingertips of CA Encryption Key Manager users.



UNIFY AND SIMPLIFY ENCRYPTION KEY MANAGEMENT OPERATIONS

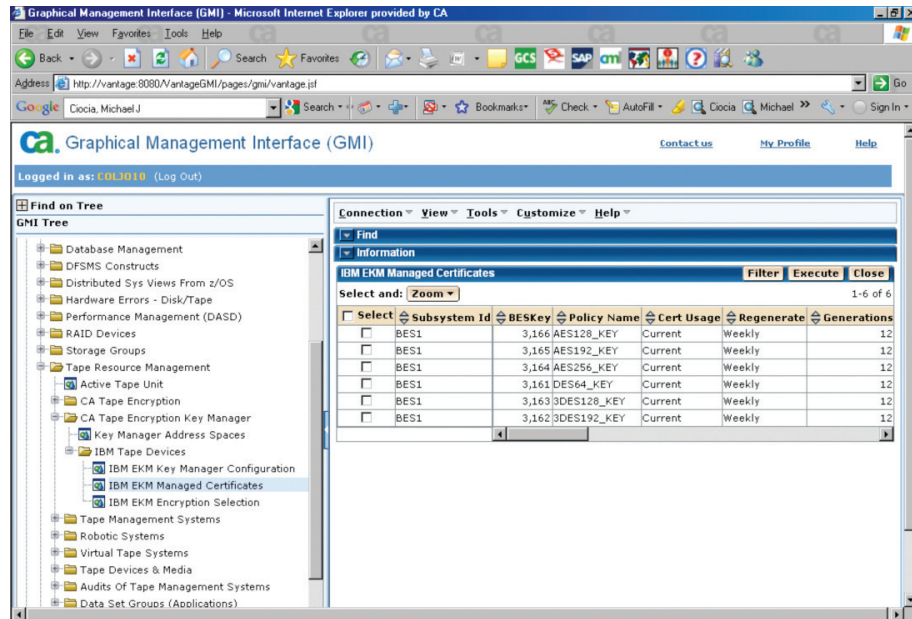


FIGURE A: The Web-based CA GMI includes an object tree that interfaces with CA Encryption Key Manager.

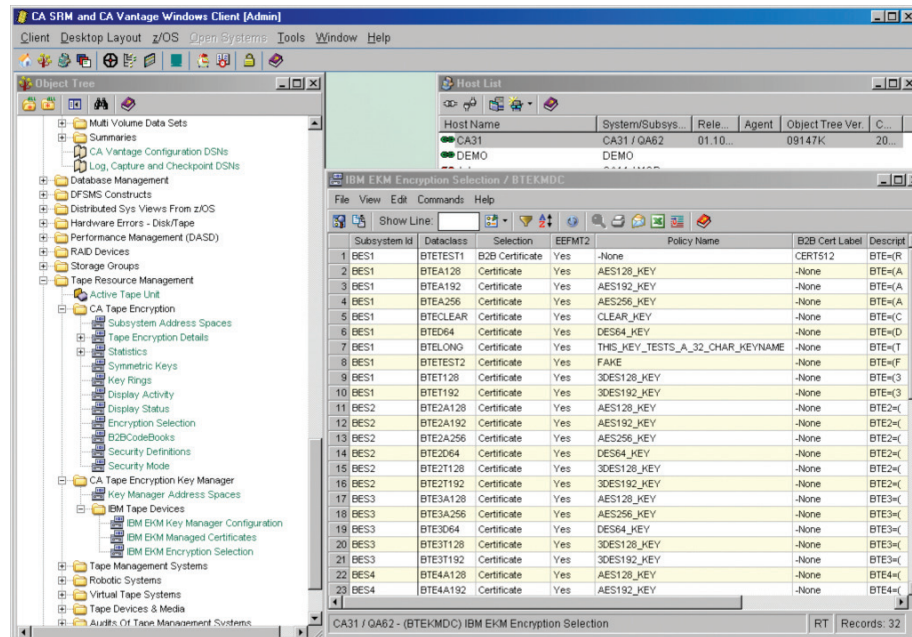


FIGURE B: The Windows-based CA GMI includes an object tree that interfaces with CA Encryption Key Manager.



CA Encryption Key Manager Options

All CA Encryption Key Manager Options are activated via license keys for specific functions. They ensure encrypted data and cryptographic components remain available.

- **Option for IBM:** Ability to manage tape encryption keys, for z/OS and distributed environments, when attached to an IBM TS1120 (3592-E05) or IBM TS1130 tape device
 - > Cross-platform key management and protection across multiple tape storage vendors using a single point of control
 - > The status of keys and media across the enterprise can be visualized and audited at a glance, including “in-transit” and offsite locations

Benefits

CA Encryption Key Manager helps ensure compliance with data security regulations and laws by delivering automated, centralized management for encryption keys from different cryptographic solutions. Implementing the CA Encryption Key Manager enables centralized management of multi-vendor encryption keys and higher encrypted data availability across the enterprise, reducing any delay accessing encrypted data during disaster recovery, hardware errors or system outage. Temporary or permanent loss of encryption keys and therefore access to encrypted data can lead to potential financial impact resulting from application outages, negative publicity and other downtime costs. By reducing the complexity and time to manage local or remote systems, novice and experienced staff can easily manage cryptography and compliance.

Why CA

A key component of both CA's Mainframe 2.0 initiative, CA Encryption Key Manager expands on CA's thirty-plus years of mainframe management leadership, offering tight integration with CA's z/OS Storage Management Solutions and unifying with CA's powerful CA Graphical Management Interface (CA GMI).

Copyright © 2010 CA. All rights reserved. IBM, z/OS and RACF are trademarks of International Business Machines Corporation in the United States, other countries, or both. All trademarks, trade names, service marks and logos referenced herein belong to their respective companies. This document is for your informational purposes only. CA assumes no responsibility for the accuracy or completeness of the information. To the extent permitted by applicable law, CA provides this document “as is” without warranty of any kind, including, without limitation, any implied warranties of merchantability, fitness for a particular purpose, or noninfringement. In no event will CA be liable for any loss or damage, direct or indirect, from the use of this document, including, without limitation, lost profits, business interruption, goodwill or lost data, even if CA is expressly advised in advance of the possibility of such damages.

1848_0410

