

PCI DSS REQUIREMENTS AND CA PRODUCTS:

CA Tape Encryption

CA Tape Encryption is employed to dynamically encrypt and decrypt mainframe and distributed application data as it is being written to standard label z/OS tapes. It also automates the protection, availability and auditability of encryption keys.

PCI Requirement 3

Protect stored cardholder data.

Protection methods such as encryption, truncation, masking, and hashing are critical components of cardholder data protection. If an intruder circumvents other network security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. Other effective methods of protecting stored data should be considered as potential risk mitigation opportunities.

PCI Requirement 3.5 Protect cryptographic keys used for encryption of cardholder data against both disclosure and misuse

PCI Requirement 3.6 Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data including the following:

3.6.1 Generation of strong cryptographic keys

3.6.3 Secure cryptographic key storage

3.6.4 Periodic cryptographic key changes

How CA Tape Encryption Addresses this Requirement:

Transparent Data Encryption & Decryption

CA Tape Encryption encrypts and decrypts data as it is written to or read from z/OS tapes. This helps protect data from being exposed even if the tape falls into the wrong hands. CA Tape Encryption provides support for symmetric cryptography using Advanced Encryption Standard (AES) with Key strengths of 128, 192 and 256 bits. Data Encryption Standard (DES) and Triple Data Encryption (3DES/TDES) algorithms.

3.5 CA Tape Encryption stores keys used to encrypt data in an encrypted proprietary data base.

3.6 The Key Management facility of CA Tape Encryption can be used to manage the entire Key Management life process.

3.6.1 The Key Management facility of CA Tape Encryption creates strong cryptographic keys

3.6.3 CA Tape Encryption keys are stored in an encrypted proprietary database.

3.6.4 CA Tape Encryption keys can be set up to expire, thus enabling the requirement to change keys periodically.

Additional Considerations

PCI DSS REQUIREMENT NUMBER	PCI DSS REQUIREMENT AREA	SUPPORT BY CA TAPE ENCRYPTION
9.9	Strict control of storage and accessibility of media	CA Tape Encryption integrates with z/OS tape management systems to provide control for the encrypted tapes.

The Process

Users have a choice of utilizing DFSMS-based selection, a supported z/OS security system of their choice (see specifications below), or a combination of both DFSMS and their security system. Tape data is encrypted only when needed, using the user selected encryption method. During decryption, CA Tape Encryption automatically identifies encrypted tapes it owns and dynamically invokes the appropriate decryption routine.

CA provides decryption utilities for any Business to Business (B2B) partner at no charge to whom users wish to send encrypted tapes, which include a mainframe decryption module as well as Java-based Multiplatform Decryption Utilities for the Windows, UNIX and Solaris platforms. Integration with leading external security systems such as CA ACF2™ for z/OS, CA Top Secret® for z/OS or IBM RACF® helps facilitate the secure exchange of public/private key pairs.

Integration with CA's z/OS tape management systems (CA 1® Tape Management and CA TLMS® Tape Management) offers out-of-the box encryption key life cycle management. This unique automated process is designed to secure control for the entire life cycle of the keys used for encrypting tapes. It will manage the creation, monitoring, tracking, auditing, backup and recovery, and expiration and removal of expired keys. Batch reports, custom reporting and online interface can provide detailed history and status of encryption and decryption activity.

CA Tape Encryption exploits IBM's System z Integrated Information Processor (zIIP) to offload encryption and compression processing from the mainframe's general-purpose processors. This unique integration enables users to better protect growing volumes of business critical data by unifying on the zIIP processor to reduce Million Service Units (MSU) requirements and tape storage management costs.

Specifications

Support for z/OS Tape Management Systems

- CA1 Tape Management® and CA TLMS Tape Management®
- IBM DFSMSrmm

Support for z/OS External Security Systems

- CA ACF2™ for z/OS
- CA Top Secret® for z/OS
- IBM RACF®

Support for z/OS Virtual Tape Systems

- CA Vtape™ Virtual Tape System
- IBM TotalStorage® Virtual Tape Server (VTS)
- Sun StorageTek Virtual Storage Manager™ (VSM)

Source Document

The source for this document is the PCI DSS version 1.2, published in October 2008, as this was the current standard at the time of this writing. A free copy may be obtained at the PCI Security Standards Council ([HTTPS://WWW.PCISECURITYSTANDARDS.ORG/](https://www.pcisecuritystandards.org/)).

Legal

Copyright © 2008 CA. All rights reserved. IBM, DFSMS, DFSMSrmm, TotalStorage, RACF, System z and z/OS are trademarks of International Business Machines Corporation in the United States, other countries, or both. Sun, Solaris, StorageTek, and Virtual Storage Manager are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries. UNIX is a registered trademark of The Open Group. Windows is a registered trademark or trademark of Microsoft Corporation in the United States and other countries. All trademarks, trade names, service marks and logos referenced herein belong to their respective companies. THIS DOCUMENT IS FOR YOUR INFORMATIONAL PURPOSES ONLY. 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 NON-INFRINGEMENT. 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, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED OF SUCH DAMAGES. Notwithstanding anything in this publication to the contrary, this publication shall not: (i) constitute product documentation or specifications under any existing or future written license agreement or services agreement relating to any CA software product, or be subject to any warranty set forth in any such written agreement; or (ii) serve to affect the rights and/or obligations of CA or its licensees under any existing or future written license agreement or services agreement.

