z/OS 3.2 IBM Education Assistant

Solution Name: z/OS DFSMS Tape Data Set Access Method Encryption

Solution Element: DFSMSdfp

July 2025

Agenda

- Trademarks
- Objectives
- Overview
- Usage & Invocation
- Interactions & Dependencies
- Upgrade & Coexistence Considerations
- Installation & Configuration
- Summary
- Appendix

Trademarks

- See url http://www.ibm.com/legal/copytrade.shtml for a list of trademarks.
- Additional Trademarks:
  - None

Objectives

Clients have a requirement to protect their petabytes of tape data. Support of access method tape encryption continues the pervasive encryption strategy to Encrypt Everything by satisfying an additional data set type on the data set encryption roadmap.

- PCI-DSS V4.0 indicates that hardware encryption is not sufficient. Host based encryption is needed to satisfy this regulation, which went into effect April 2025.

Tape data set encryption is designed to provide the same client value and user experience as the other supported data set types for data set encryption.

- No application changes required when using standard BSAM/QSAM APIs
- Data set level granularity. Key labels are assigned to tape data sets.
- Supports separation of access control for data set and encryption key label. SAF authority to the key label required to access data in the clear.
- Enabled through RACF and / or SMS policy. Source of key label.
- Audit readiness. System level services to display encryption status.

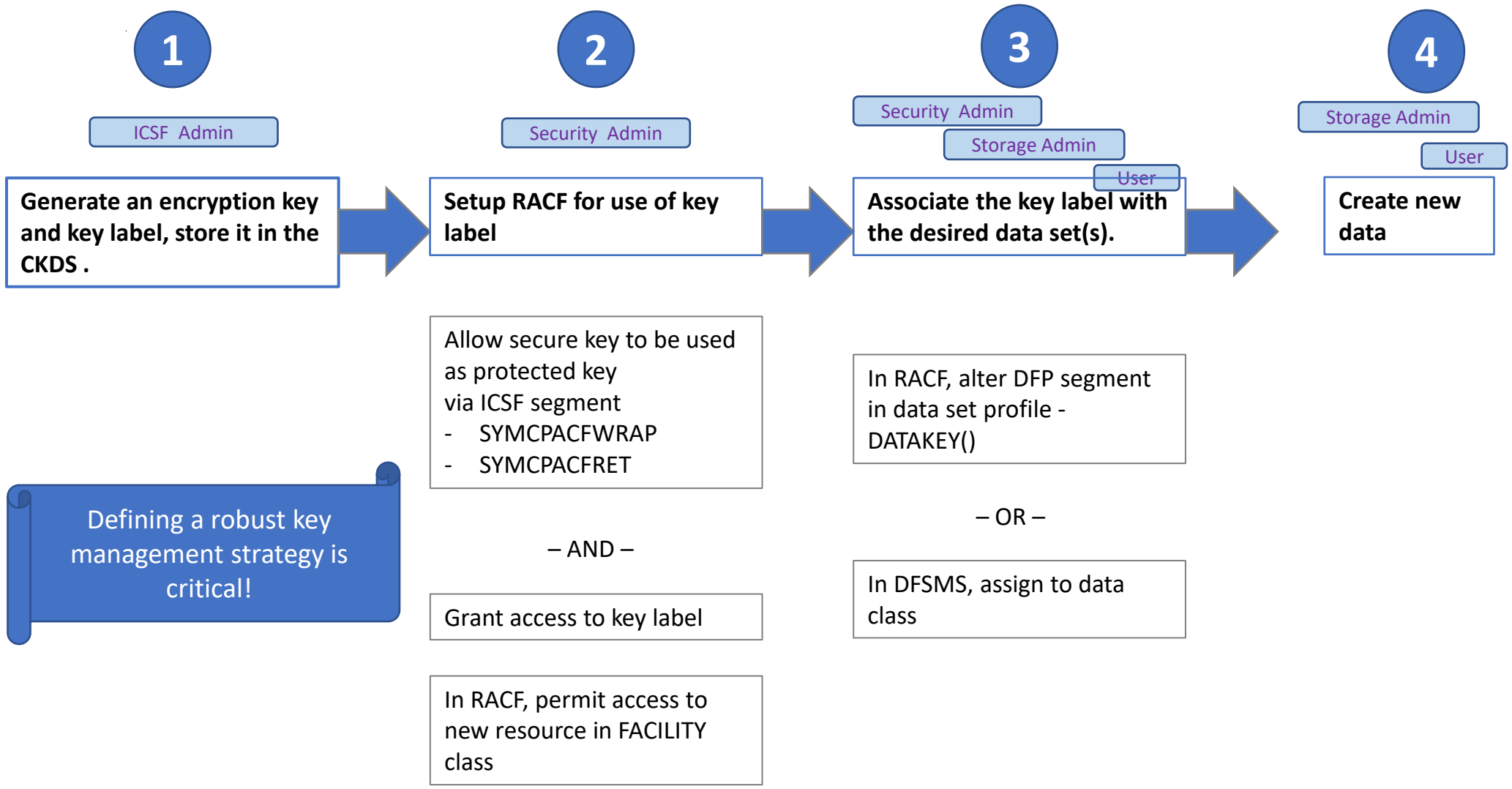
Overview

- Who (Audience)
  - Security Architect; Security Administrator
- What (Solution)
  - Encryption of tape data sets with no (or minimal) application changes when using standard BSAM/QSAM APIs
- Wow (Benefit / Value, Need Addressed)
  - Ability to implement the Quantum-safe encryption techniques and best practices as part of an overall security strategy to ensure sensitive data is protected from unauthorized access, while also meeting regulatory and compliance requirements.

Usage & Invocation

Implementation high level steps

Similar user experience for all supported data set types for data set level encryption



Supported data set type for data set encryption

To allow the system to treat ***tape data sets*** as a supported data set type for encryption

- System level
  - New FACILITY class resource: STGADMIN.SMS.ALLOW.DATASET.TAPE.ENCRYPT
    - Tells the system to honor key label if supplied for a tape data set

- Data set level – Allows for a granular approach to encrypt data sets
  - New keywords on RACF DATASET profile DFP Segment: ***ENCRYPTTYPES(INTAPE|EXTAPE|NOTAPE)***
    - **INTAPE -** Tape data sets covered by this profile are eligible for data set encryption**.**
    - **EXTAPE -** Tape data sets covered by this profile are excluded from data set encryption.
    - **NOTAPE -** SMS to use the FACILITY class resource to determine if data sets covered by this profile are eligible for data set encryption.

The System level FACILITY class resource is not needed when using the Data set level support.

Encryption key label

For tape data set encryption, the key label can be obtained from sources supported for DASD data set encryption.

Fields used today with existing hardware encryption will be unchanged. New fields to be added for access method tape encryption.

Security policy

DFP segment in RACF data set profile

- DATAKEY

NEW: SMS to capture key label from DATASET profile DFP segment for tape data set. (Only key label will be taken from DFP segment.)

Explicitly

JCL, Dynamic allocation, TSO Allocate

- JCL DSKEYLBL, Dynalloc DALDKYL

NOTE: JCL Key label keywords KEYLABL1 and KEYLABL2 only for tape hardware encryption

SMS policy

Data class

- Data Set Key Label

NOTE: Key labels in tape management section only for tape hardware encryption

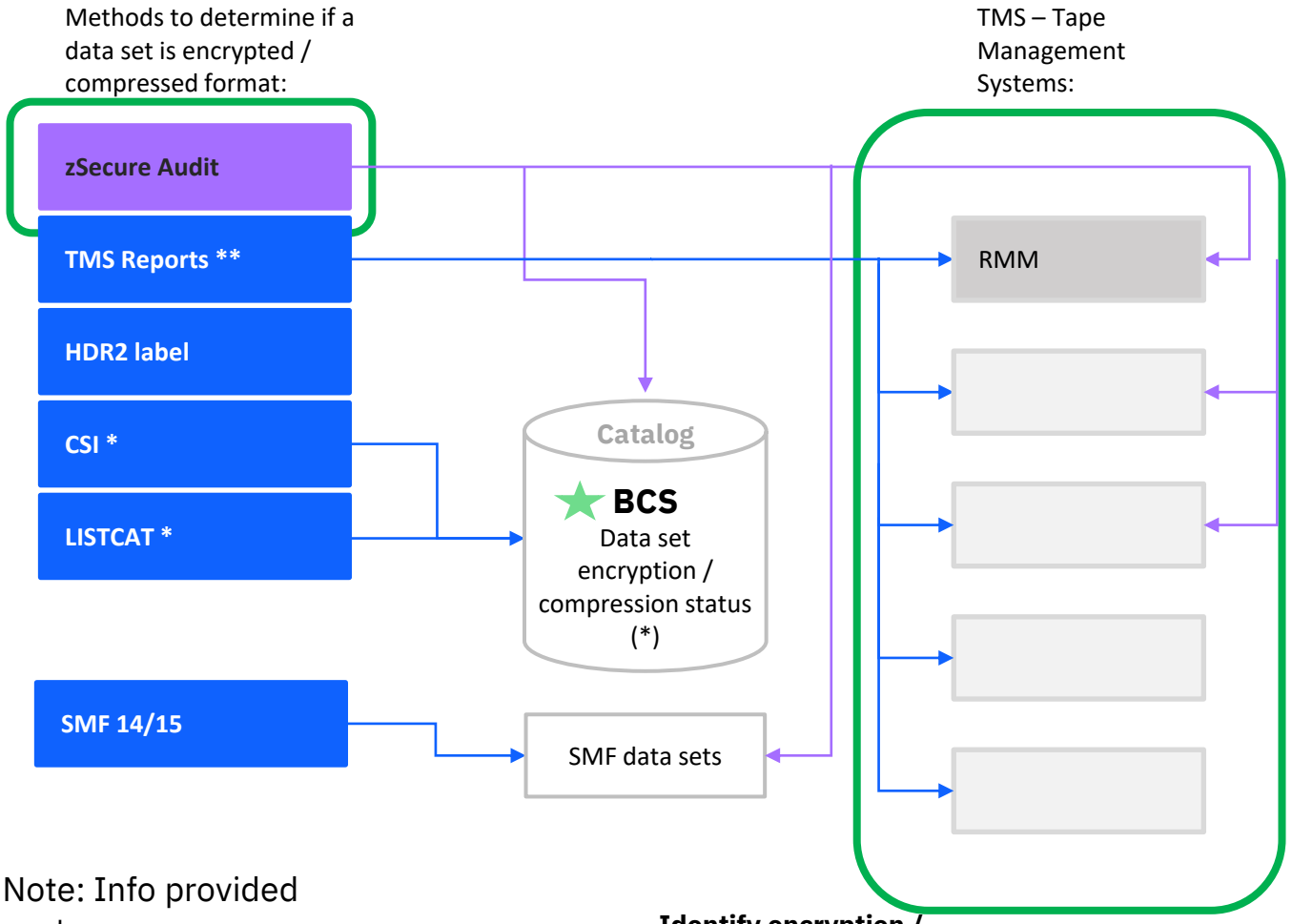
Tape encryption – Length restrictions

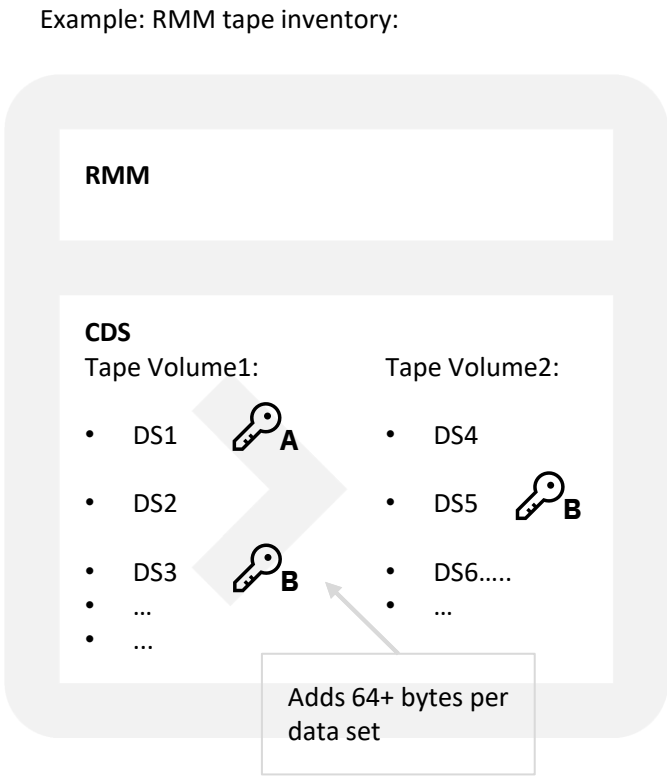
Length restrictions due to the 16-byte minimum data length for encryption.

- For an encrypted (non-compressed format) tape data set
  - For RECFM=F(B(S)), the minimum BLKSIZE is 16 bytes
  - For RECFM=FB(S), the minimum LRECL is 2 bytes

Open fails with Abend 613-A8 if the minimum is not met.

Reporting tape data set encryption / compression





(*) If data set catalogued
(**) If maintained by TMS. Note: Info provided to other TMSs for their support.

Data set create message

IEC205I message issued at close processing for a tape data set. New text to identify data set encryption and compression status.

```
IEC205I ddname,jobname,stepname,FILESEQ = nnn, COMPLETE VOLUME LIST |
EXTEND VOLUME LIST, [DSN=dsn,] VOLS=volser, [number ADDITIONAL VOLS,]
[LISTED VOL(S) HAVE BEEN DATA ENCRYPTED.KL1CD:L|H KL2CD:L|H,
KL1=keylabe11,KL2=keylabel2, [TOTALBLOCKS=mmm,] [3490 EMULATION VOLUMES
EXTENDED CAPACITY MODE|3490 EMULATION VOLUMES EXTENDED CAPACITY USED,]
[PERFORMANCE SEGMENTED | PERFORMANCE SCALED,]
[DATA SET  ENCRYPTION DSKEYLBL=DATASET.APP1.V001,]
[DATA SET COMPRESSION FORM=BASIC]
```

Catalog reporting

LISTCAT

```
ENCRYPTIONDATA
  DATA SET ENCRYPTION----
(YES)
```

[Note: Will not display DATA SET KEY LABEL, since not stored in the catalog]

..

..

```
ATTRIBUTES
    COMP-FORMT
```

CSI (Catalog Search Interface)

```
COMPIND - Compression & misc
indicators

    8 bits

    .1.. …. ds is extended format

    ..1. …. ds is compressible
```

[*existing flag* also to be returned for compressed format tape]

```
    .... 1... ds is encrypted
```

[*new flag* to be returned for encrypted dasd and tape data sets]

Note: IGGCSIF updated to include mapping for COMPIND

SMF record Type 14 and 15

Enhanced to provide information for tape data set encryption and compression

***NEW* TAPE Data Set Extended Information Section (Type 10)**

- Encryption indicator
- Key label
- Encryption type
- Encryption mode
- Encryption ICV value
- Compression indicator
- User bytes read/written
- Compressed bytes read/written

Fields used today with existing hardware encryption (Tape Encryption Data Section - Type 7) and DASD compression (Compressed format data set section - Type 1) will be unchanged.

New fields to be added for access method tape encryption and compression.

The TAPE Data Set Extended Information Section (Type 10)

Offset	Name	Len	Format	Description
...				
4(4)	SMF14TEncCmpFlg	1	binary	Tape AM Encryption / Compression indicator
	SMF14TDSEnc			Tape AM encryption
	SMF14TDSCmp			Tape AM compression
5(5)	SMF14TFLG	1	binary	Flag byte Bit (Name) 0 (SMF14TDSENCARCHKEY) The encrypted data set is being accessed with an archived key that only supports decryption operations. 1 (SMF14TENCRYPTOK) If on, the application program is enabled for tape ds encryption with EXCP. The application coded DSENCRYPT=OK on the DCBE macro. 2 (SMF14TCOMPRESSOK) If on, the application program is enabled for tape ds compression with EXCP. The application coded DSENCRYPT=OK on the DCBE macro.

The TAPE Data Set Extended Information Section (Type 10) continued

				macro.
6(6)	SMF14TEncType	2	binary	Encryption type. The first byte is X'01' to signify AES. The second byte is X'00' to signify 256 bits.
8(8)	SMF14TEncMode	1	binary	Encryption mode. 0 signifies XTS mode
		3		Reserved
12(C)	SMF14TEncKeyLabel	64	EBCDIC	Encryption key label
76(4C)	SMF14TEncICV	8	binary	Encryption ICV value
84(54)	SMF14TEncVerify	16	binary	Encryption verification bytes
100(64)	SMF14TUserBlksRW	8	binary	Number of user blocks read/written during this open
108(6C)	SMF14TPhysBlksRW	8	binary	Number of physical blocks read/written during this open
116(74)	SMF14TUserBytesRW	8	binary	User bytes read/written
124(7C)	SMF14TCmpBytesRW	8	binary	Compressed bytes read/written

Interactions & Dependencies

- Software Dependencies
  - None
- Hardware Dependencies
  - None
  - Note:
    - This tape access method encryption support can coexist with existing tape hardware encryption support.
- Exploiters
  - DFSMS OAM, DFSMSrmm, DFSMSdss
  - Note:
    - Support is transparent to OAM’s object support
    - DFSMShsm will not support the tape ML2 or backup data sets to be defined as encrypted with this support. HSM will fail if it encounters the ML2 or backup data set defined as an access method encrypted tape data set.
    - DFSMShsm ABARs will not support access method encrypted tape data sets.

Upgrade & Coexistence Considerations

- To exploit this solution, all systems in the Plex must be at the new z/OS level: Yes

- List any toleration/coexistence APARs/PTFs. - None
- List anything that doesn't work the same anymore. – N/A
- Upgrade involves only those actions required to make the new system behave as the old one did.- N/A
- Coexistence applies to lower level systems which coexist (share resources) with latest z/OS systems.
  - APARs available for lower level systems: OA66326, which will bring in all requisite support.

Installation & Configuration

- List anything that a client needs to be aware of during installation
  - N/A

- To enable the system to treat a tape data set as a supported data set type, the system must be configured to enable tape data sets to be eligible via the system level or the data set level. Refer to chart 8 Supported data set type for data set encryption.

Summary

Tape data set encryption is designed to provide the same client value and user experience as the other supported data set types for data set encryption.

This solution includes support to

- Identify that tape data sets should be supported at the system level or data set level
- Ability to assign a key label from various sources
- Ability to create an encrypted data set without requiring change to applications using standard BSAM/QSAM APIs.
- Ability to display reporting via various system utilities.

This solution also includes exploitation by DFSMS OAM and DFSMSrmm.

Appendix (1)

Publications

- z/OS DFSMS Using New Functions
- z/OS DFSMS Using Data Sets
- z/OS DFSMS Macro Instruction for Data Sets
- z/OS DFSMSdfp Storage Administration
- z/OS MVS Initialization and Tuning Reference
- z/OS DFSMSdfp Advanced Services
- z/OS MVS System Messages, Vol 8 (IEF-IGD)
- z/OS MVS System Messages, Vol 7 (IEB-IEE)
- z/OS MVS System Management Facilities (SMF)
- z/OS DFSMS OAM Planning, Installation, and Storage Administration Guide for Object Support
- z/OS DFSMS OAM Planning, Installation, and Storage Administration Guide for Tape Libraries
- z/OS DFSMSrmm Implementation and Customization Guide
- z/OS DFSMSrmm Managing and Using Removable Media

Appendix (2)

Data Set Encryption Resources

- **Redbook:** Getting Started with z/OS Data Set Encryption Redbook http://www.redbooks.ibm.com/redpieces/abstracts/sg248410.html?Open

- IBM Z Content Solution pervasive encryption technical landing page https://www.ibm.com/support/z-content-solutions/pervasive-encryption/

- IBM Crypto Education page: https://community.ibm.com/community/user/ibmz-and-linuxone/groups/community-home?communitykey=6593e27b-caf6-4f6c-a8a8-10b62a02509c&tab=groupdetails