z/OS 2.4 IBM Education Assistant (IEA)

Solution (Epic) Name: PDSE Encryption
Element(s)/Component(s): z/OS DFSMS

Agenda

- Trademarks
- Session Objectives
- Overview
- Usage & Invocation
- Interactions & Dependencies
- Migration & Coexistence Considerations
- Installation
- Session Summary
- Appendix

Trademarks

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

Overview

- Who (Audience)
  - z/OS Security administrators
- What (Solution)
  - Can protect sensitive data in SMS-managed PDSEs by requesting data set level encryption via security policy
- Wow (Benefit / Value, Need Addressed)
  - Allows applications to encrypt partitioned data securely using BSAM, BPAM and QSAM APIs with no changes

High Level Function / Solution Description

- Enable SMS-managed PDSEs as an additional supported data set type for Data Set Encryption
  - Allows access via BSAM, BPAM and QSAM
  - Allows for creation using key label
  - The user must have SAF authority to both the data set and the key label.
  - The data will remain encrypted during backup, migration and replication.

High Level Function / Solution Description, Cont.

- For applications using standard BSAM, BPAM and QSAM APIs, no application changes are required
  - Applications which set DCBE BYPASS_AUTH=YES may wish to perform a SAF check for key label access

Usage - Creating encrypted data sets (today)

- A data set is defined as an encrypted data set when a **key label** is supplied on *data set create of a **supported data set type** for data set encryption*
- A **key label** can be supplied in any of the following sources (*in order of precedence as follows*):
  - **Security policy:** RACF data set profile DFP segment
  - **Explicity:** JCL, Dynamic Allocation, TSO Allocate, IDCAMS DEFINE
  - **SMS policy:** Data class
    - To allocate via ISPF 3.2, can specify a data class with key label

Usage - Preparing system for new encryption data set types

When a key label is specified during data set create

- To allow the system to treat ***PDSEs*** as a supported data set type, the following new ***discrete*** resource profile in the FACILITY class must be **defined:**

  STGADMIN.SMS.ALLOW.PDSE.ENCRYPT

  - Users are not required to have access to this resource to encrypt PDSEs.

For supported data set type,

- To allow the system to create encrypted data sets when the key label is specified via a method *outside of the DFP segment in the RACF data set profile*, the user must have at least **READ authority** to the following new resource in the FACILITY class.

  STGADMIN.SMS.ALLOW.DATASET.ENCRYPT

For unsupported data set type,

Restrictions

- Similar to extended format encryption
  - System data sets (such as Catalogs, SHCDS, HSM data sets) must not be encrypted, unless otherwise specified
  - Data sets used before ICSF is started must not be encrypted
- PDSE-specific restrictions
  - Program objects cannot be encrypted
    - Operation will fail when attempting to write a program object to an encrypted PDSE
  - Requires PDSE version 2
    - If Version 1 is specified for an encrypted PDSE, it will be changed to Version 2

How to detect that support is installed

- New DFA bit indicating ‘PDSE encryption’ support installed.
  - DFAPDSEENCRYPT

81 (51)	BITSTRING	1	DFAFEAT10	Features Byte 10
	…. ..1.		DFAPDSEENCRYPT	PDSE Encryption Support

Interactions & Dependencies

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

- Software Dependencies
  - ICSF installed and configured with a CKDS
  - AES master key loaded in Crypto Express
- Hardware Dependencies
  - Crypto Express3 Coprocessor or later
  - Feature 3863, CP Assist for Cryptographic Functions (CPACF)
- Exploiters
  - NONE

Installation

- Provided with based z/OS V2R4
- V2R2 and V2R3 support will be provided at V2R4 GA with main APAR OA56324

How to detect that support is installed

- New DFA bit indicating ‘PDSE encryption’ support installed.
  - DFAPDSEENCRYPT

81 (51)	BITSTRING	1	DFAFEAT10	Features Byte 10
	…. ..1.		DFAPDSEENCRYPT	PDSE Encryption Support

Session Summary

- Version 2 PDSEs can be enabled as a supported data set type for data set encryption in z/OS V2R4
- Support should not require any application changes
- Supported only on V2R4 in ESP timeframe
- Support will enabled on V2R2 and V2R3 at V2R4 GA

Appendix

- Publications
  - z/OS DFSMSdss Administration
  - z/OS MVS System Messages, Vol 1

  - z/OS DFSMShsm Implementation and Customization
  - z/OS DFSMShsm Storage Administration
  - z/OS DFSMShsm Managing Your Own Data
  - z/OS DFSMShsm Diagnosis
  - z/OS DFSMShsm Data Areas
  - z/OS DFSMS Installation Exits
  - z/OS MVS System Messages, Vol 2