z/OS 3.1 IBM Education Assistant

Solution Name: Master key entry key part ownership

Solution Element(s): ICSF

July 2023

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:
  - If you need to list any that aren't included on the website above, please do so here. If not, remove the text in this bullet and just say “None”.

Objectives

- Describe the changes to the ICSF Master Key Entry Utility to support ownership of key parts

Overview

- Who (Audience)
  - ICSF administrators who load clear master key parts using the ICSF Master Key Entry ISPF utility
- What (Solution)
  - The Master Key Entry utility doesn’t restrict who can entry specific key parts (first, middle, last)
  - Access to the utility allows the user to load any key part.
  - New optional control to restrict user to one key part.
  - Optional control uses SAF to enable the function and to restrict users
- Wow (Benefit / Value, Need Addressed)
  - Customer satisfaction (RFE: 141030, 132591)

Usage & Invocation

- Master Key Entry utility allows users to load clear master key parts into the new master key register of the selected coprocessors
- The utility is controlled by the CSFSERV SAF class resource CSFDKCS.
  - Users needs READ access to the resource. The default behavior when no covering profile exists is to permit the use of the utility.
- New Key part ownership control will restrict which users can load FIRST, MIDDLE, and LAST parts and RESET the new master key registers
- Key part ownership control is enabled by the XFACILIT class discrete profile CSF.MASTER.KEY.ENTRY.BY.PART
  - When the XFACILIT profile exists, the control is enabled and all key parts loaded are subject to SAF authority checks
  - Message CSFM732I is issued at initialization and whenever the state of the function changes

Usage & Invocation

- Key part profiles
  - The load key part profiles are XFACILIT class profiles. The users must have READ access to the profile. If no profile exists, the request fails.
  - CSF.MKE.LOAD.FIRST.PART
  - CSF.MKE.LOAD.MIDDLE.PART
  - CSF.MKE.LOAD.FINAL.PART
  - CSF.MKE.RESET.NMK
- Pass Phrase Initialization utility is affected when the Key part ownership control is enabled.
  - A user of the Pass Phrase Initialization utility must be authorized to load FIRST and FINAL key parts and to RESET the master key registers.
  - If the user isn’t authorized, the Pass Phrase Initialization utility will fail.

Usage & Invocation

CSFM732I MASTER KEY ENTRY UTILITY KEY OWNERSHIP CONTROL IS state.

Explanation

The Master Key Entry utility key ownership control is currently in the specific state. The state may be ENABLED or DISABLED. The profile that activates the Master Key Entry utility key ownership control is the CSF.MASTER.KEY.ENTRY.BY.PART resource in the XFACILIT class. RACF commands can be used to define, change, list, or delete the profiles that cover these resources in the XFACILIT class. This message may be issued during ICSF initialization and when ICSF detects that the key store policy is changed.

System action

Processing continues.

Operator response

None.

System programmer response

None.

Usage & Invocation

- State of control displayed using CSFIQF service, rule array keyword ICSFST2

Element number	Name	Description
13	ICSF Status Field 5 continued	Key Store Policy status continued from element 7. The first character in this string indicates if the Archived Key for Data Decryption Use control has been enabled. The numbers that can appear in the first character of this string are: Number Meaning 0 Archived Key for Data Decryption Use control is disabled. 1 Archived Key for Data Decryption Use control is enabled. Miscellaneous controls The second character in this string indicates the state of the CSFKEYS PKA ECD private-key name checking (XFACILIT profile CSF.CSFKEYS.ECC.PRIVATEKEYNAME.ENABLE). Number Meaning 0 PKA ECC private-key name SAF checking is not enabled. 1 PKA ECC private-key name SAF checking is enabled. The third character in this string indicates the state of the Clear Master Key Entry utility key part ownership control. (XFACILIT profile CSF.MASTER.KEY.ENTRY.BY.PART) Number Meaning 0 Clear Master Key Entry utility key part ownership control is not enabled. 1 Clear Master Key Entry utility key part ownership control is enabled.

Interactions & Dependencies

- Software Dependencies
  - None
- Hardware Dependencies
  - None
- Exploiters
  - None

Upgrade & Coexistence Considerations

- To exploit this solution, all systems in the Plex must be at the new z/OS level: No
- There are no coexistence or migration considerations

Installation & Configuration

- None

Summary

- New optional control to allow ICSF administrators to control which user can entry clear master key parts into the Master Key Entry utility

Appendix

- Publications
  - ICSF Administrator’s Guide
  - ICSF Application Programmer’s Guide
  - ICSF Messages