

z/OS V2.5 IBM Education Assistant

Solution Name: Change Master Key Audit Part 2

Solution Element(s): ICSF (FMID HCR77D2)



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

- Need Addressed :
 - Give ICSF system administrators a way to display the date/time of a master key change using the ICSF display command
- Solution:
 - Save the timestamp of the SMF master key promotion event that occurs during a change master key and display the time stamp in the output of the D ICSF command.
- Benefit / Value:
 - Administrator's can display the date/time a master key was changed as part of maintaining and demonstrating (to security auditors) their master key rotation policy.
 - Administrators know the date and time of the existing SMF generated records for master key promotion.

Overview

- Who (Audience)
 - System Administrators and System Programmers
- What (Solution)
 - Supply a way to display the date/time a master key was changed as part of maintaining and demonstrating (to security auditors) their master key rotation policy.
- Wow (Benefit / Value, Need Addressed)
 - Simplifies maintaining and demonstrating (to security auditors) a master key rotation policy.

Usage & Invocation

- D ICSF,KDS

CSFM668I 18.18.12 ICSF KDS 119

CKDS ISFTTEST.CLC.CKDSVAR

FORMAT=KDSR COMM LVL=3 SYSPLEX=Y MKVPs=DES AES

DES MKVP date=2020-05-13 22:09:56

AES MKVP date=2020-05-13 22:09:56

PKDS ISFTTEST.CLC.PKDSR.NEW

FORMAT=KDSR COMM LVL=3 SYSPLEX=Y MKVPs=RSA ECC

RSA MKVP date=Unknown

ECC=2020-03-03 18:02:47

TKDS ISFTTEST.CLC.TKDSRNEW

FORMAT=VARIABLE COMM LVL=3 SYSPLEX=Y MKVPs=P11

P11 MKVP date=2020-05-01 14:21:10

Usage & Invocation

- D ICSF,MKVPS

CSFM668I 18.14.04 ICSF KDS

CKDS ISFTEST.CLC.CKDSVAR

AES MKVP Date=2020-04-20 17:25:27

DES MKVP Date=2020-05-13 22:09:56

| | ID | AES | DES |
|----------|------|--------|--------|
| KDSMKVPS | | 2058C8 | CA6B40 |
| SY1 | 6C02 | 2058C8 | CA6B40 |

PKDS ISFTEST.CLC.PKDSR

ECC MKVP Date=2020-03-03 18:02:47

RSA MKVP Date=Unknown

| | ID | ECC | RSA |
|----------|------|--------|--------|
| KDSMKVPS | | 78D81A | E83F15 |
| SY1 | 6C02 | 78D81A | E83F15 |

No TKDS defined or no EP11 adapters online

Usage & Invocation

- z/OS ICSF System Programmer's Guide : Examples linking D ICSF output date to SMF records. For example, a coordinated change master key for RSA: the D ICSF,MKVPS command shows

```
PKDS  ISFTTEST.CLC.PKDSR.NEW
ECC MKVP Date=2020-08-04 18:18:16
RSA MKVP Date=2020-08-05 20:40:41
      ID      ECC      RSA
KDSMKVPS  ....  78D81A  EF4C65
SY1       5C03  78D81A  EF4C65
SY1       5C09  78D81A  EF4C65
```

The corresponding SMF record for the promotion of the RSA new master key shows

Subtype=0031 Master Key Event

Written when a Master Key is set or changed

5 Aug 2020 16:40:42.21

TME... 005B9DFD DTE... 0120218F SID... SP21 SSI... 00000000 STY... 0031

SYSNME SY1 ...

MKVP.. 0320EF4C65754B5088C22D03480BC7B952B2

03----- RSA

TOD... 2020-08-05 20:40:41 <- new formatting by CSFSMFR

...

Usage & Invocation

- Not every SMF subtype 31 record TOD matches the D ICSF output date
 - A NMK can be promoted because when NMK MKVP matches the KDS existing MKVP but it is not always the case of KDS initialization/update at the same time. These master key promotions can happen at
 - ICSF Initialization without KDS MKVP update
 - ICSF SET MK panels
 - Refresh and activate master keys via ICSF panels
 - ICSF config runs
- There is an existing related SMF record record 82 Subtype 14 for Cryptographic coprocessor master key entry
- D ICSF,KDS and D ICSF,MKVPS **allow the SYSPLEX=YES option**

Usage and Innovation

- ICSF Samplib CSFSMFR SMF formatter record 82(x52) updates
 - Subtype 49(x31) updated TOD formatting to match the format of the D ICSF command output

Subtype=0031 Master Key Event

Written when a Master Key is set or changed

5 Aug 2020 16:40:42.21

TME... 005B9DFD DTE... 0120218F SID... SP21 SSI... 00000000 STY... 0031

SYSNME SY1

MKFLGS C0

80 This system initiated a coordinated change master key

40 A change master key occurred on this system

KDSN.. ISFTEST.CLC.PKDSR.NEW

...

TOD... 2020-08-05 20:40:41 (old format TOD... 07/31/2019 18:29:08.533149)

...

Usage and Innovation

- ICSF Samplib CSFMKVPR – new samplib member created to clear the MKVP in the KDS header
 - Not created specifically for this line item
 - This sample is used to remove the verification pattern, for a master key that is no longer being used, from a KDS header
 - The sample is part of a process which is :
 - Use the sample to generate a sequential dataset (also known as a 'flatfile') with the MKVP, MKVP date, and MKVP date flags removed
 - VSAM REPRO the output sequential dataset into a VSAM KDS dataset
 - Make the VSAM KDS dataset the active KDS

Usage and Innovation

- ... ICSF Samplib CSFMKVPR (cont)
 - Invocation parms
 - Arg1 – the single MKVP to delete
 - Arg2 – pre-allocated sequential output KDS
 - Arg3 – optional VSAM KDS source dataset
 - If specified, Arg3 is REPROed to Arg2
 - See the sample prologue for more information
 - Error checking (MKVP not present, keys encrypted under master key in KDS)
 - Invocation examples

EX 'SYS1.SAMPLIB(CSFMKVPR)' 'RSA CSF.PKDS.FLATFILE CSF.PKDS'
will REPRO from CSF.PKDS to CSF.PKDS.FLATFILE and then
remove the RSA MKVP from CSF.PKDS.FLATFILE

Usage and Innovation

- CSFMKVPR – new samplib member created to clear the MKVP in the KDS header
 - Not created specifically for this line item
 - This sample is used to remove the verification pattern, for a master key that is no longer being used, from a KDS header
 - The sample is part of a process which is :
 - Use the sample to generate a sequential dataset (also known as a ‘flatfile’) with the MKVP, MKVP date, and MKVP date flags removed
 - VSAM REPRO the output sequential dataset into a VSAM KDS dataset
 - Make the VSAM KDS dataset the active KDS

Interactions & Dependencies

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

Upgrade & Coexistence Considerations

- To exploit this solution, all systems in the Sysplex must be at the new z/OS level:
NO
- No
 - toleration/coexistence APARs/PTFs.
 - changes to previous function

Installation & Configuration

- None

Summary

- Gave ICSF system administrators a way to display the date/time of a master key change using the ICSF display command
- Save the timestamp of the SMF master key promotion event that occurs during a change master key and display the time stamp in the output of the D ICSF command.
- Administrator's can display the date/time a master key was changed as part of maintaining and demonstrating (to security auditors) their master key rotation policy.
- Administrators know the date and time of the SMF records generated when the new master key was promoted as part of change master key.

Appendix

- z/OS ICSF System Programmer's Guide ,Chapter 4, ICSF Commands
 - Appendix A. Diagnosis reference information
 - Cryptographic Key Data Set Header Record Format for each KDS
 - Appendix B. ICSF SMF Records
 - Describes Subtype 49 – things like key type, coprocessor serial number etc. included in the record written when a new master key is promoted to current in a coprocessor
 - Subtype 49 updated for SMF82_TAG_TOD – describes connection to D ICSF command output with examples
- z/OS ICSF Messages
 - CSFM668I D ICSF command output
- z/OS ICSF Administrator's Guide
 - Text pointing to D ICSF command output where KDS initialization and change master key are discussed

Appendix

- Sample JCL for saving particular SMF types to a DS specific to that type:
<https://community.ibm.com/community/user/ibmz-and-linuxone/blogs/eysha-shirriner-powers2/2020/03/25/sample-jcl-to-show-how-to-save-a-particular-event-record-using-smf-dump-job?CommunityKey=6593e27b-caf6-4f6c-a8a8-10b62a02509c&Tab=groupdetails>