z/OS 3.2 IBM Education Assistant

Solution Name: MK Query Updates

Solution Element(s): ICSF

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

- Review MK Query Update enhancement

Overview

- Who (Audience)

  - Application programmers

- What (Solution)

  - Provide support for the STATICSB rule which is needed to programmatically obtain master key verification patterns for all CCA master keys using all methods that have been supported.

- Wow (Benefit / Value, Need Addressed)

  - Previously, only some of the MKVP methods were supported making determination of the correct MKVPs impossible.

Usage & Invocation

- Callable service ICSF Query Facility (CSFIQF and CSFIQF6) will now accept a new rule "STATICSB" which will return all master key register statuses and all supported MKVP formats.

- Sample results (after parsing):

```
card_serial   = 93ZZ1234
DES_NMK_state = 1         (empty register)
DES_CMK_state = 2         (full register)
DES_OMK_state = 2         (full register)
RSA_NMK_state = 1         (empty register)
RSA_CMK_state = 2         (full register)
RSA_OMK_state = 2         (full register)
AES_NMK_state = 1         (empty register)
AES_CMK_state = 2         (full register)
AES_OMK_state = 2         (full register)
ECC_NMK_state = 1         (empty register)
ECC_CMK_state = 2         (full register)
ECC_OMK_state = 2         (full register)
DES_OMK_MDC4  = 2B0C723D1AB9C948E9C9E32E7FF3B7F4
DES_CMK_MDC4  = DF3A50AE3546612396EF557E8BD074C1
DES_NMK_MDC4  = 00000000000000000000000000000000
RSA_OMK_HP    = EF4C65754B5088C22D03480BC7B952B2
RSA_CMK_HP    = E83F158521FEEA23986CC9483DAFD711
RSA_NMK_HP    = 00000000000000000000000000000000
DES_OMK_VP    = 1D08F1C67A1B709A
DES_CMK_VP    = CA6B408A02371B1D
DES_NMK_VP    = 0000000000000000
DES_NMK_MKAP  = 0000000000000000
AES_OMK_VP    = BF494FF74B86343F
AES_CMK_VP    = 2058C870E9D3194F
AES_NMK_VP    = 0000000000000000
ECC_OMK_VP    = E2FDFFDC8FA7A6CA
ECC_CMK_VP    = 78D81AC6C9610A2C
ECC_NMK_VP    = 0000000000000000
```

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 is no need for toleration/coexistence APARs/PTFs.

Installation & Configuration

- No special installation or configuration actions are needed

Summary

- Callable service ICSF Query Facility (CSFIQF and CSFIQF6) will now accept a new rule "STATICSB" which will return all master key register statuses and all supported MKVP formats.

Appendix

- References
  - Integrated Cryptographic Service Facility Application Programmer's Guide