z/OS 3.1 IBM Education Assistant

Solution Name: AES CIPHER and HMAC key panels

Solution Element(s): ICSF

July 2023

Agenda

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

© 2023 IBM Corporation

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”.

© 2023 IBM Corporation

Objectives

- New ICSF panels to simplify key generation of AES CIPHER keys and key generation and import of HMAC keys.

© 2023 IBM Corporation

Overview

- Who (Audience)
  - ICSF administrators that need to generate new CCA keys for use with z/OS Data set encryption or RACF enhanced PassTickets
- What (Solution)
  - New ICSF panel to allow key generation of AES CIPHER keys
  - New ICSF panel to allow key generation and import of HMAC keys
- Wow (Benefit / Value, Need Addressed)
  - Quick generation of AES Cipher keys for use with z/OS Data set encryption
  - Quick generation and import of HMAC keys for use with RACF enhanced PassTickets

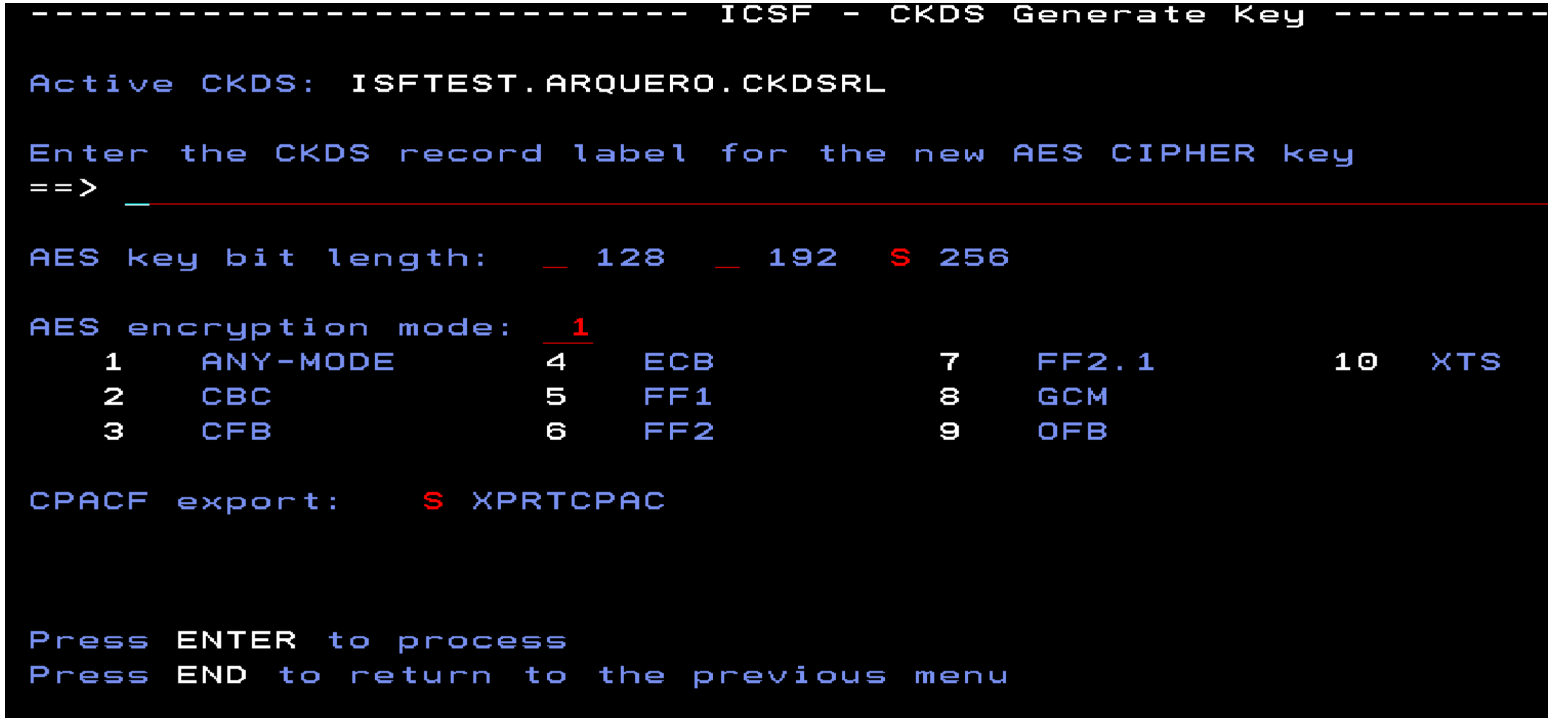
© 2023 IBM Corporation

Usage & Invocation – AES CIPHER panel

- Enter key label for new AES key.

- Select bit length, encryption mode, and CPACF export settings.

- By default, settings are selected best suited for z/OS Data Set Encryption.



```
--------------------------- ICSF - CKDS Generate Key ---------

Active CKDS:  ISFTEST.ARQUERO.CKDSRL

Enter the CKDS record label for the new AES CIPHER key
==> _

AES key bit length:   _  128   _  192   S  256

AES encryption mode:   1
   1    ANY-MODE          4    ECB           7    FF2.1         10   XTS
   2    CBC               5    FF1           8    GCM
   3    CFB               6    FF2           9    OFB

CPACF export:     S  XPRTCPAC



Press ENTER to process
Press END to return to the previous menu
```

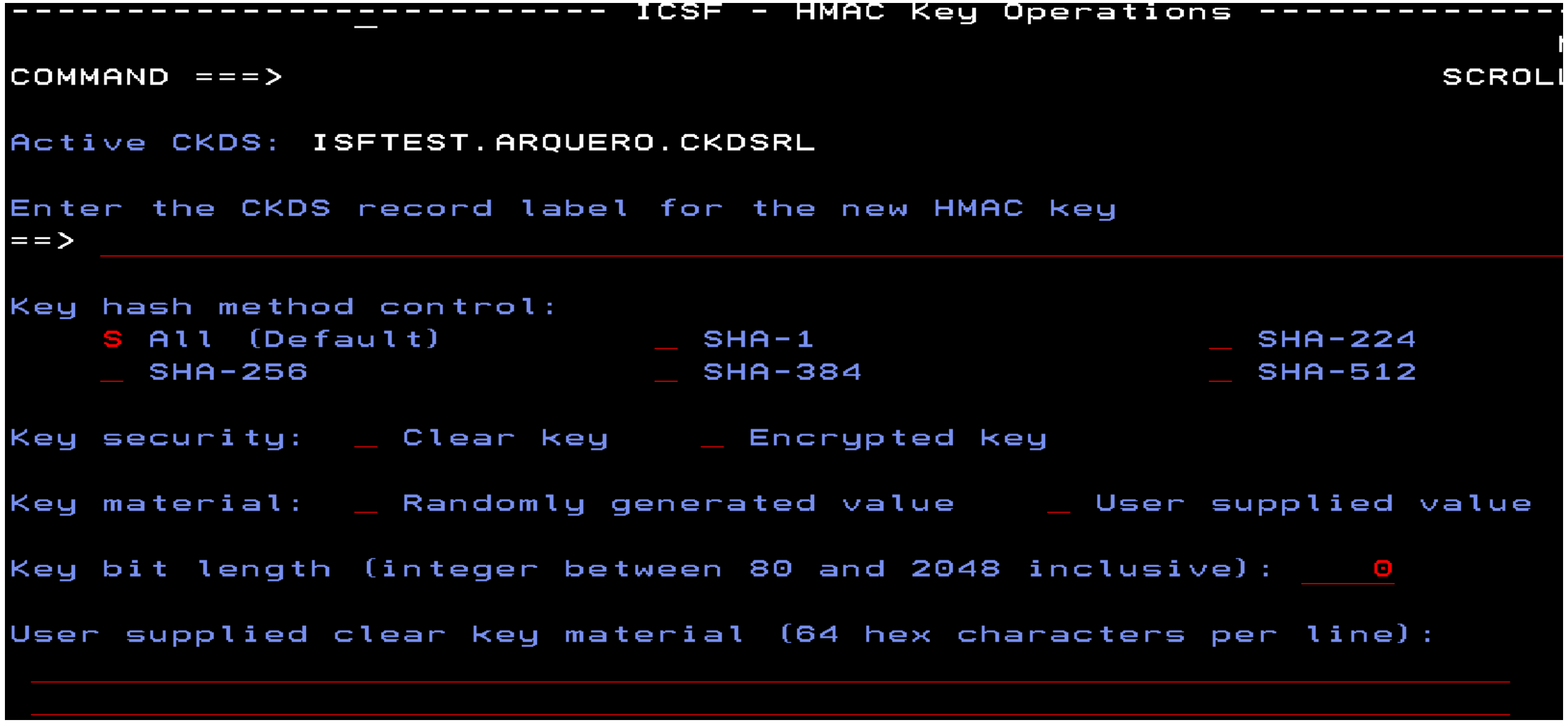
© 2023 IBM Corporation

Usage & Invocation – HMAC panel

- Enter key label for new HMAC key.

- Select hash method control, key security, and whether a new random key will be generated or imported.

- You can optionally import a clear key value by entering the clear key material onto the panel



```
------------------------------- ICSF - HMAC Key Operations -------------
                                                                       M
COMMAND ===>                                                      SCROLL

Active CKDS:  ISFTEST.ARQUERO.CKDSRL

Enter the CKDS record label for the new HMAC key
==> ____________________________________________________________________

Key hash method control:
    S All (Default)           _ SHA-1                   _ SHA-224
    _ SHA-256                 _ SHA-384                 _ SHA-512

Key security:   _ Clear key    _ Encrypted key

Key material:   _ Randomly generated value    _ User supplied value

Key bit length (integer between 80 and 2048 inclusive):    0

User supplied clear key material (64 hex characters per line):
 _________________________________________________________________
 _________________________________________________________________
```

Interactions & Dependencies

- Software Dependencies
  - None
- Hardware Dependencies
  - Crypto Express card in CCA mode for secure key operations
- Exploiters
  - None

© 2023 IBM Corporation

Upgrade & Coexistence Considerations

- To exploit this solution, all systems in the Plex must be at the new z/OS level: No

© 2023 IBM Corporation

Installation & Configuration

- None

© 2023 IBM Corporation

Summary

- New ICSF panels for simplified and quick key generation for AES CIPHER keys and key generation and import for HMAC keys.

© 2023 IBM Corporation

Appendix

- ICSF Administrator’s Guide

© 2023 IBM Corporation