# z/OS V2.5 IBM Education Assistant

Solution Name: Archived key decrypt only

Solution Element: Integrated Cryptographic Service Facility

# 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

- Discuss the three RFEs addressed by this update
  - Archived key decrypt only
  - Track key usage in data-encryption services
  - Display key data set metadata in CKDS KEYS and PKDS KEYS utilities

# Overview

- Who (Audience)
  - ICSF Administrators
- What (Solution)
  - Control the use of data-encryption cryptographic keys
  - Track the use of cryptographic keys in data-encryption services
  - Display key data set metadata with CKDS KEYS and PKDS KEYS utilities
- Wow (Benefit / Value, Need Addressed)
  - Enhance management of cryptographic keys

# Usage & Invocation - Archived key decrypt only

- RFE: Prohibit the use of archived cryptographic key for data encryption operations. Data decryption operations should be allowed.
  - Prevent new data from being encrypted using an old key
  - Allows the key to be deleted or replaced safely
- New SAF XFACILIT profile CSF.KDS.KEY.ARCHIVE.DATA.DECRYPT
  - Independent of CSF.KDS.KEY.ARCHIVE.USE profile
- When enabled, service requests where
  - Key identifier parameter is an archived key and the service does data-encryption, the service will fail RC 8 RSN D5E (3422)
  - Key identifier parameter is an archived key and the service does data-decryption, the service will succeed

# Usage & Invocation - Archived key decrypt only

- SMF 82 subtype 30 - Key store policy archived and inactive KDS keys

| Offsets | | Name | Length | Format | Description |
|---|---|---|---|---|---|
| 0 | 0 | SMF_ARCH_FLAGS | 4 | binary | Flag Bytes<br>Note: Bits 0 to 2 are mutually exclusive.<br>Bits 8-11 are mutually exclusive.<br><br>**Bit** **Meaning When Set**<br>0 CKDS<br>1 PKDS<br>2 TKDS<br>3-7 Reserved.<br>8 Record that is archived was referenced by service. By policy, service call failed.<br>9 Record that is archived was referenced by service. By policy, service call succeeded.<br>10 Record that is pre-active was referenced by service. Service call failed.<br>11 Record that is inactive was referenced by service. Service call failed.<br>12 Record that is archived was referenced by a service that performs data encryption. By policy, service call failed.<br>13-30 Reserved.<br>31 Archived Key for Data Decryption Use Control is enabled. |

# Usage & Invocation - Archived key decrypt only

- CKDS Key Record Read2 service (CSNBKRR2)
  - Will not return an archived key token when no XFACILIT profiles are defined
  - Will return an archived key token when the CSF.KDS.KEY.ARCHIVE.USE profile exists
  - When the CSF.KDS.KEY.ARCHIVE.DATA.DECRYPT profile exists and
    - a data-encryption key with key usage allows encryption is retrieved
    - the PROTKEY rule array keyword is specified
    - return code will indicate the key should not be used to encrypt data
- Return code 0 RSN D5F (3423)

# Usage & Invocation - Archived key decrypt only

- Reference information: Service does data-encryption
  - Encipher (CSNBENC, CSNEENC, CSNBENC1, and CSNEENC1)
  - Ciphertext Translate2 (CSNBCTT2, CSNECTT2, CSNBCTT3, and CSNECTT3)
    - Outbound key identifier
  - Symmetric Algorithm Encipher (CSNBSAE, CSNESAE, CSNBSAE1, and CSNESAE1)
  - Symmetric Key Encipher (CSNBSYE, CSNESYE, CSNBSYE1, and CSNESYE1)
  - Field Level Encipher (CSNBFLE and CSNEFLE)
  - FPE Encipher (CSNBFPEE and CSNEFPEE)
  - FPE Translate (CSNBFPET and CSNEFPET)
    - Outbound key identifier
  - Format Preserving Algorithms Encipher (CSNBFFXE and CSNEFFXE)
  - Format Preserving Algorithms Translate (CSNBFFXT and CSNEFFXT)
    - Outbound key identifier
  - PKCS #11 Secret key encrypt (CSFPSKE and CSFPSKE6)

# Usage & Invocation - Archived key decrypt only

- Reference information: Service does data-decryption
  - Decipher (CSNBDEC, CSNEDEC, CSNBDEC1, and CSNEDEC1)
  - Ciphertext Translate2 (CSNBCTT2, CSNECTT2, CSNBCTT3, and CSNECTT3)
    - Inbound key identifier
  - Symmetric Algorithm Decipher (CSNBSAD, CSNESAD, CSNBSAD1, and CSNESAD1)
  - Symmetric Key Decipher (CSNBSYD, CSNESYD, CSNBSYD1, and CSNESYD1)
  - Field Level Decipher (CSNBFLD and CSNEFLD)
  - FPE Decipher (CSNBFPED and CSNEFPED)
  - FPE Translate (CSNBFPET and CSNEFPET)
    - Inbound key identifier
  - Format Preserving Algorithms Decipher (CSNBFFXD and CSNEFFXD)
  - Format Preserving Algorithms Translate (CSNBFFXT and CSNEFFXT)
    - Inbound key identifier
  - PKCS #11 Secret key decrypt (CSFPSKD and CSFPSKD6)

# Usage & Invocation – Track Key Usage

- RFE: Track the use of cryptographic keys in a class of services that do data-encryption
- New installation options data set keyword: TRACKCLASSUSAGE
- Store the date a key was last used in a class of services
  - New variable-length metadata block with tag id ‘0008’
- Common record format of the CKDS and TKDS

# Usage & Invocation – Track Key Usage

- New installation options data set parameter
- **TRACKCLASSUSAGE**(*class*[,*class*])
  - The last date a key was used by any service in a class
  - The supported cryptographic classes are:
    - DATAENC - Symmetric key data encryption operations
    - DATADEC - Symmetric key data decryption operations
- Can be modified by SETICSF operator command
  - SETICF OPTIONS,TRACKCLASSUSAGE=(NONE | *class*[,*class*])

# Usage & Invocation – Display metadata blocks

- RFE: Display variable-length metadata blocks in the CKDS KEYS and PKDS KEYS utilities
- Metadata blocks will be displayed on new panels
- User must have same SAF authority to display key attributes to display metadata blocks

# Usage & Invocation – Display metadata blocks

- Key Attributes and Metadata and Record Metadata panels updated

```
CSFBRPK3 ---------- ICSF - PKDS Key Attributes and Metadata -------------------

Active PKDS: CSF.PKDS

Label: KEY.1

 Record status: Active          (Archived, Active, Pre-active, Deactivated)

Select an action: 5
  1  Modify one or more fields with the new values specified
  2  Delete the record
  3  Display variable-length metadata block with tag: ____
  4  Display all IBM variable-length metadata blocks
  5  Display all installation variable-length metadata blocks
-------------------------------------------------------------------------------
```

# Usage & Invocation – Display metadata blocks

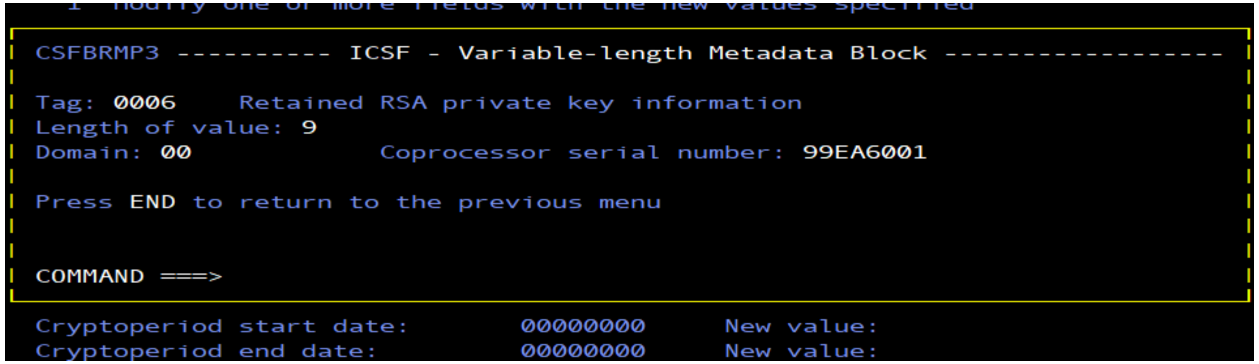
Option 3

Metadata tag 0006

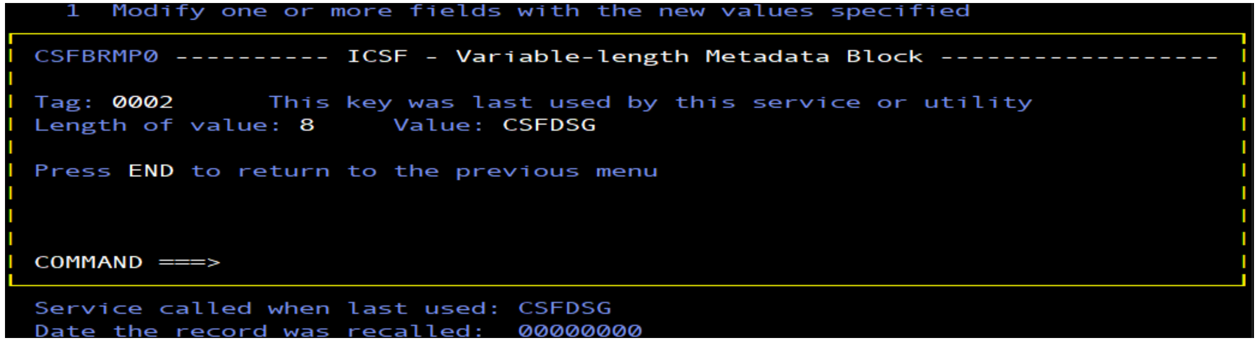
Data formatted and description

Popup panel

Metadata tag 0002



```
   1  Modify one or more fields with the new values specified
 ----------------------------------------------------------------------------
 | CSFBRMP3 ---------- ICSF - Variable-length Metadata Block ------------------ |
 |                                                                            |
 | Tag: 0006     Retained RSA private key information                         |
 | Length of value: 9                                                         |
 | Domain: 00             Coprocessor serial number: 99EA6001                 |
 |                                                                            |
 | Press END to return to the previous menu                                   |
 |                                                                            |
 |                                                                            |
 | COMMAND ===>                                                               |
 ----------------------------------------------------------------------------
   Cryptoperiod start date:        00000000      New value:
   Cryptoperiod end date:          00000000      New value:
```



```
   1  Modify one or more fields with the new values specified
 ----------------------------------------------------------------------------
 | CSFBRMP0 ---------- ICSF - Variable-length Metadata Block ------------------ |
 |                                                                            |
 | Tag: 0002       This key was last used by this service or utility          |
 | Length of value: 8      Value: CSFDSG                                      |
 |                                                                            |
 | Press END to return to the previous menu                                   |
 |                                                                            |
 |                                                                            |
 |                                                                            |
 | COMMAND ===>                                                               |
 ----------------------------------------------------------------------------
   Service called when last used: CSFDSG
   Date the record was recalled:  00000000
```

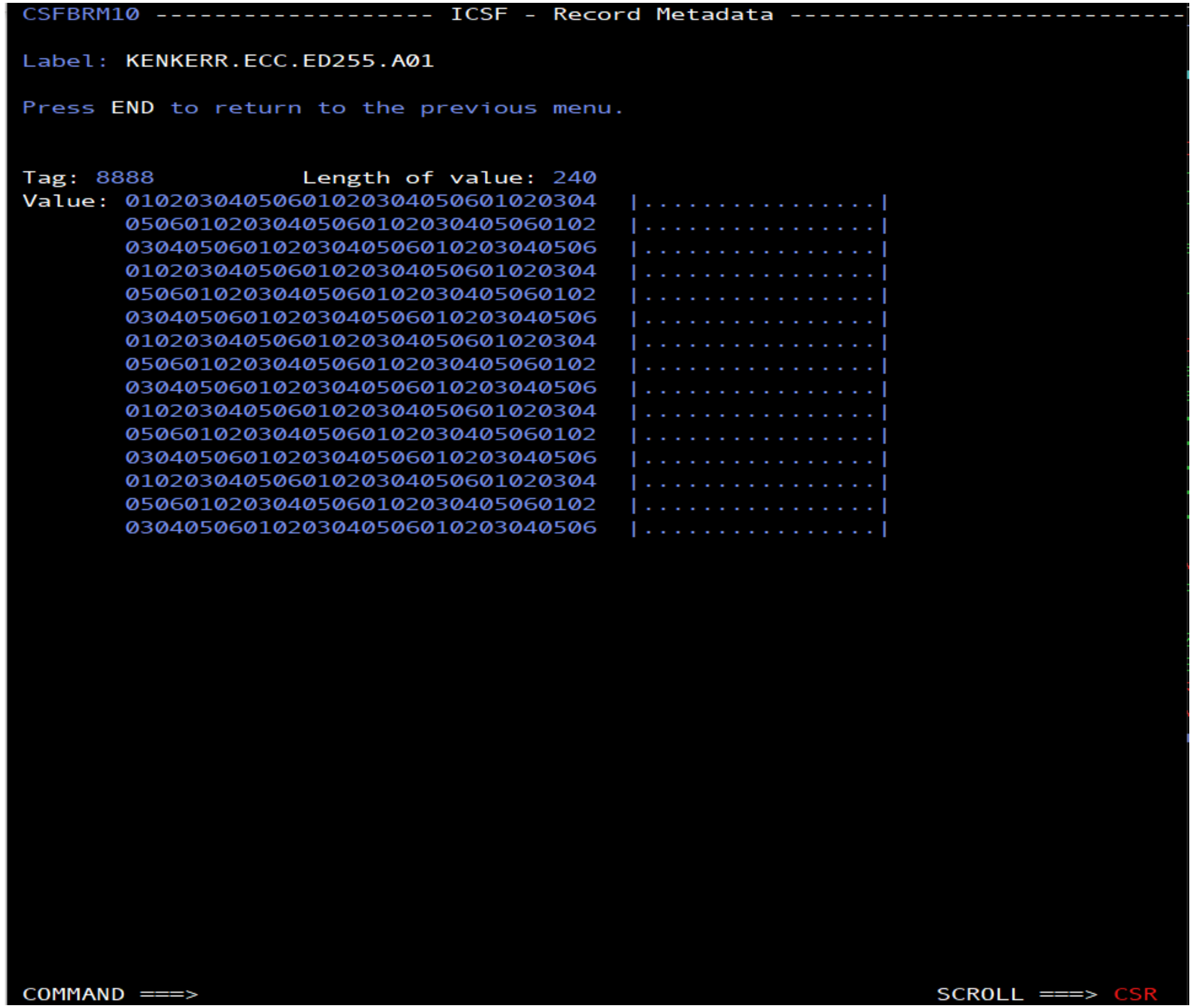
# Usage & Invocation – Display metadata blocks

Option 3

Metadata tag 8888

Installation metadata

Complete block displayed



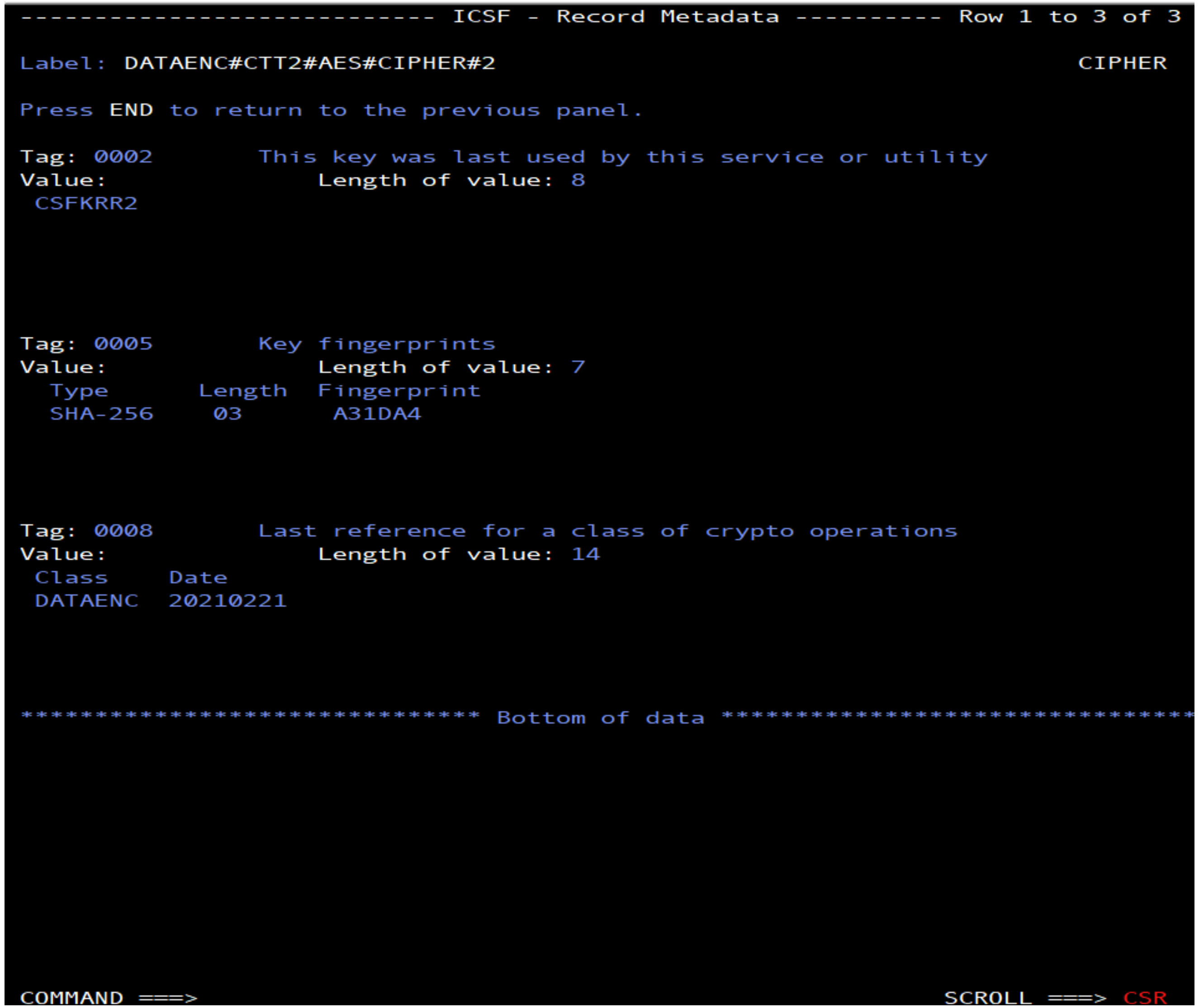
```
CSFBRM10 ------------------- ICSF - Record Metadata ---------------------------

Label: KENKERR.ECC.ED255.A01

Press END to return to the previous menu.


Tag: 8888             Length of value: 240
Value: 01020304050601020304050601020304  |................|
       05060102030405060102030405060102  |................|
       03040506010203040506010203040506  |................|
       01020304050601020304050601020304  |................|
       05060102030405060102030405060102  |................|
       03040506010203040506010203040506  |................|
       01020304050601020304050601020304  |................|
       05060102030405060102030405060102  |................|
       03040506010203040506010203040506  |................|
       01020304050601020304050601020304  |................|
       05060102030405060102030405060102  |................|
       03040506010203040506010203040506  |................|
       01020304050601020304050601020304  |................|
       05060102030405060102030405060102  |................|
       03040506010203040506010203040506  |................|









COMMAND ===>                                                    SCROLL ===> CSR
```

# Usage & Invocation – Display metadata blocks

Option 4

All IBM metadata

Descriptions and data is formatted



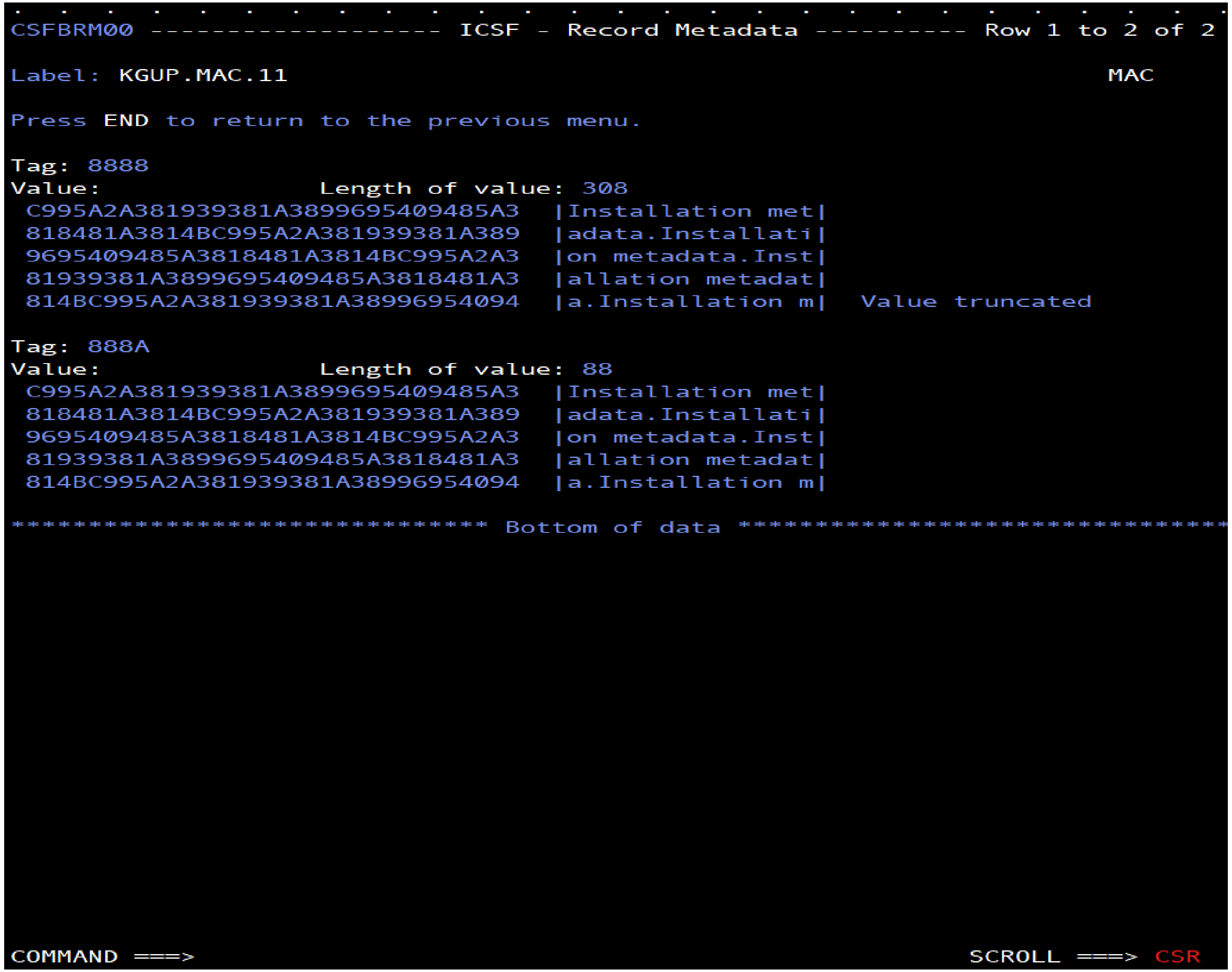
```
---------------------------- ICSF - Record Metadata ---------- Row 1 to 3 of 3

Label: DATAENC#CTT2#AES#CIPHER#2                                       CIPHER

Press END to return to the previous panel.

Tag: 0002       This key was last used by this service or utility
Value:              Length of value: 8
 CSFKRR2



Tag: 0005       Key fingerprints
Value:              Length of value: 7
  Type      Length  Fingerprint
  SHA-256    03      A31DA4



Tag: 0008       Last reference for a class of crypto operations
Value:              Length of value: 14
 Class    Date
 DATAENC  20210221



******************************* Bottom of data ********************************






COMMAND ===>                                                  SCROLL ===> CSR
```

# Usage & Invocation – Display metadata blocks

Option 5

All installation metadata

Only 80 bytes displayed



```
 .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
CSFBRM00 ------------------- ICSF - Record Metadata ---------- Row 1 to 2 of 2

Label: KGUP.MAC.11                                                     MAC

Press END to return to the previous menu.

Tag: 8888
Value:                Length of value: 308
 C995A2A381939381A3899695409485A3  |Installation met|
 818481A3814BC995A2A381939381A389  |adata.Installati|
 9695409485A3818481A3814BC995A2A3  |on metadata.Inst|
 81939381A3899695409485A3818481A3  |allation metadat|
 814BC995A2A381939381A38996954094  |a.Installation m|  Value truncated

Tag: 888A
Value:                Length of value: 88
 C995A2A381939381A3899695409485A3  |Installation met|
 818481A3814BC995A2A381939381A389  |adata.Installati|
 9695409485A3818481A3814BC995A2A3  |on metadata.Inst|
 81939381A3899695409485A3818481A3  |allation metadat|
 814BC995A2A381939381A38996954094  |a.Installation m|

******************************* Bottom of data ********************************










COMMAND ===>                                                  SCROLL ===> CSR
```

# 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
- There are no toleration/coexistence consideration for this item.

# Installation & Configuration

- The archived key decrypt only function is enabled by the existence of the SAF XFACILIT profile CSF.KDS.KEY.ARCHIVE.DATA.DECRYPT.
- The tracking of class of operations is enabled by the installation options data set parameter TRACKCLASSUSAGE.

# Appendix

- Publications
  - Cryptographic Services Integrated Cryptographic Service Facility Messages
  - Cryptographic Services Integrated Cryptographic Service Facility Administrator's Guide
  - Cryptographic Services Integrated Cryptographic Service Facility System Programmer's Guide
  - Cryptographic Services Integrated Cryptographic Service Facility Application Programmer's Guide

# Appendix

- **Terminology**
- CKDS - Cryptographic Key Data Set
- PKDS – Public Key Data Set
- TKDS - Token Data Set