ICSF HCR77C1 and z/OS 2.3 Enhancements

Greg Boyd

gregboyd@mainframecrypto.com

www.mainframecrypto.com

Copyrights and Trademarks

Presentation based on material copyrighted by IBM, and developed by myself, as well as many others that I worked with over the past 14 years

Agenda – z14, ICSF HCR77C1 & z/OS 2.3 Enhancements

- Hardware
  - z14
    - CPACF
    - Crypto Express6
  - TKE 9.0
- HCR77C1
  - PCI HSM
  - Crypto Usage Statistics
  - CKDS Keys Utility
  - Other stuff

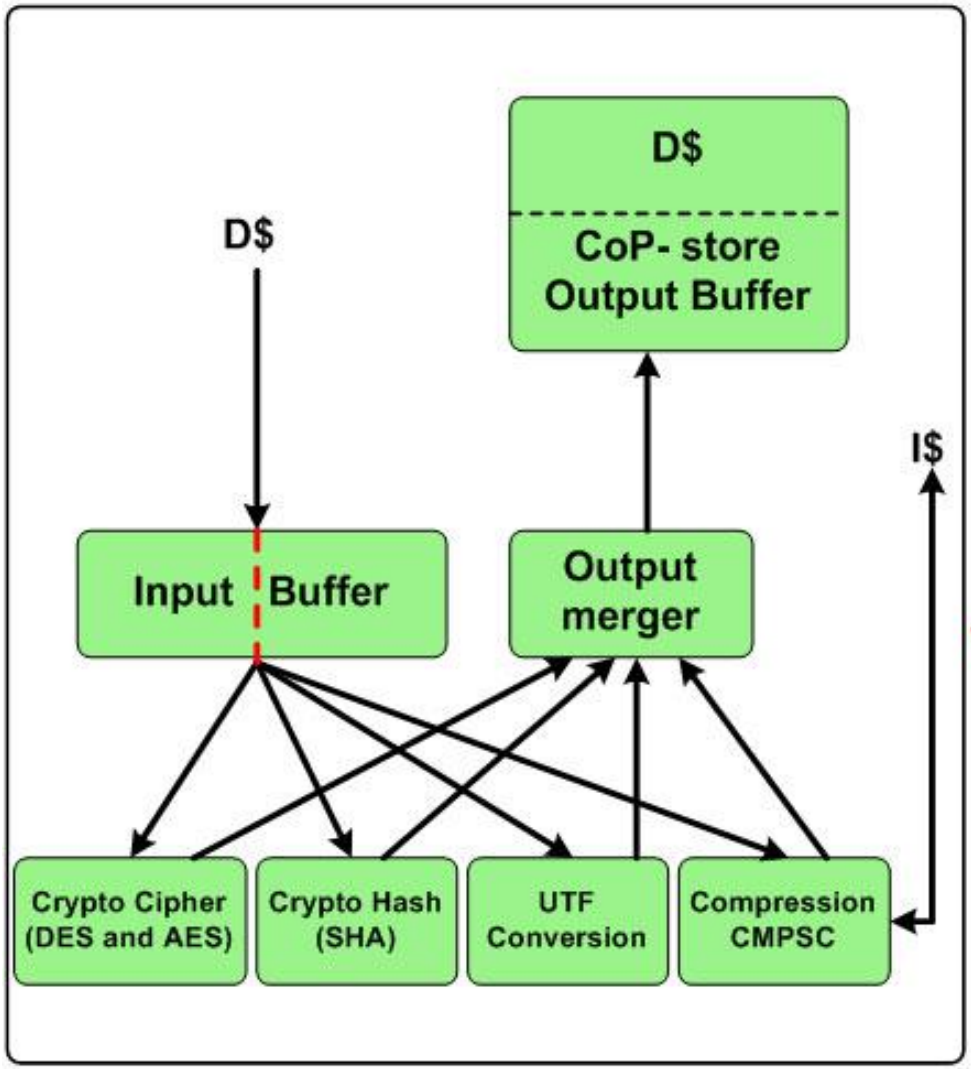
Cryptographic Hardware

- z14
  - Pervasive Encryption
    - Data set and file encryption
    - Coupling facility encryption
    - Network encryption
    - Full disk encryption
    - Integrated crypto hardware
    - Secure service container
    - Enterprise Key Management Foundation
  - True Random Number Generator
  - RSA/ECC acceleration
  - Crypto Express5 FC #0890 (carry forward only)
  - Crypto Express6 FC #0893

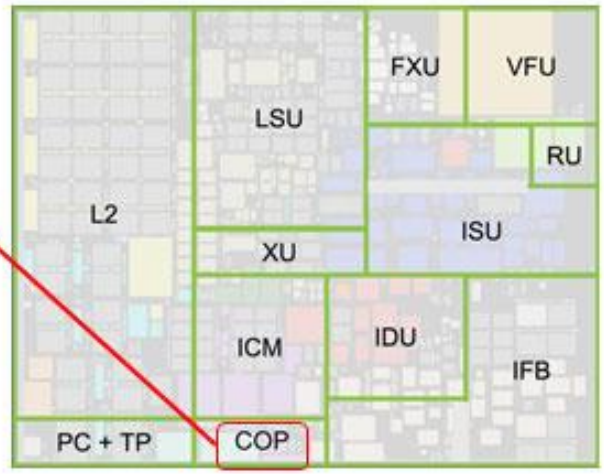
Cryptographic Hardware

- CP Assist for Cryptographic Function (CPACF)
  - AES-GCM – 4 to 6x faster on z14
  - AES-XTS – up to 7x faster on z14
  - AES-CBC – up to 4 x faster
  - SHA-3 & SHAKE support
  - PRNG, DRNG, TRNG (Pseudo, Deterministic & True RNGs)
- Crypto Express6 (FC #0893)
  - 4768 Chip
  - Improved performance
  - Payment Card Industry (PCI) PIN Transaction Security (PTS) Hardware Security Module (HSM) Mode
  - PNG (Prime Number Generator)
  - TKE 9.0 Required (if you want to use a TKE)

Co-Processor (z14 Technical Guide)



- Co-Processor results (data) now stored direct via L1D cache
- Re-designed crypto/hashing/UTF-conversion/compression engines for increased throughput
- D$ - Data Cache
- I$ - Instruction Cache



CPACF Instructions

- **KMA** Cipher Message with Authentication
- **KMAC** Compute Message Authentication Code
- **KM** Cipher Message
- **KMC** Cipher Message with Chaining
- **KMCTR** Cipher Message with Counter
- **KMF** Cipher Message with CFB
- **KMO** Cipher Message with OFB
- **KIMD** Compute Intermediate Message Digest
- **KLMD** Compute Last Message Digest
- **PCKMO** Preform Cryptographic Key Management Operation
- **PRNO** Preform Random Number Operation
- **PCC** Perform Cryptographic Computation

SHA-3

- SHA3-224, SHA3-256, SHA3-384, SHA3-512
- Extendable Output function (XOF)
  - SHAKE-128
  - SHAKE-256
- SHA-3 and SHAKE documented in FIPS PUB 202 at https://dx.doi.org/10.6028/NIST.FIPS.202

CEX6S – Designed to meet

- FIPS 140-2 Level 4
- Common Criteria EP11 EAL4
- ANSI 9.97
- Payment Card Industry (PCI) HSM
- German Banking Industry Commission (GBIC), (formerly DK, Deutsche Kreditwirtschaft)

- Among others …

TKE V9.0

- Tower (FC #0847)
- Rack (FC #0085)

- Carry forward CEX5S to z14
  - TKE V8.x (which contains a 4767 (CEX5S) adapter)
- CEX6S on z14
  - TKE V9.0 (which contains a 4768 (CEX6S) adapter)

TKE V9.0

- Key material copy to alternate zone
- Save TKE data directory structure
- Create key parts without opening a host
- New TKE Audit Log application
- Heartbeat audit record
- Performance improvements for domain groups
- Secure key entry on EP11
- New certificate manager for domains
- Domain mode management
- Set clock
- Domain-specific Host Crypto Module Audit Log management
- Domain-specific roles and authorities
- Setup PCI Environment Wizard

Crypto Cross Reference TechDoc

(http://www.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/TD103782)

FMID	Component Name	Description	z/OS Releases	Availa-bility
HCR77C0	Cryptographic Support for z/OS V2R1 - z/OS V2R2	Key Lifecycle and Usage Auditing, FIPS mode Auditing, Options Dataset Refresh, Enhanced PKCS #11 Secret Key Encrypt and PKCS #11 Secret Key Decrypt callable services to support clear key AES ciphertext stealing, specifically CS1, No longer requiring the CKDSN and PKDSN keywords to be supplied in the Installation Options Data Set, New ICSF Health Check-ICSF_ UNSUPPORTED_CCA_KEYS, Enhanced Digital Signature Generate and Digital Signature Verify callable services to take as input the message to be signed or verified as well as the prehashed message. ICSF enhancements for the Crypto Express5S updates • Digital Signature Generate, Digital Signature Verify, and PKA Key Token Build callable services for RSA-PSS Signatures • PKA Key Generate and PKA Key Token Build callable services expanded to support selectable public exponents in the generation of RSA private/public key pairs	z/OS 2.1; z/OS 2.2; z/OS 2.3	Sept. 2017

Crypto Cross Reference TechDoc

(http://www.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/TD103782)

FMID	Component Name	Description	z/OS Releases	Availa-bility
HCR77C1	Cryptographic Support for z/OS V2R1 - z/OS V2R3	Support for z14 processors and Crypto Express6S include support for a PCI HSM ("Payment Card Industry Hardware Security Module") configured CCA coprocessor: • A TKE ("Trusted Key Entry") workstation is required to administer a PCI HSM-compliant CCA coprocessor. In addition to PCI HSM support, CEX6S also introduces the use of X.509 certificates in CCA. • A TKE is used to manage root and signing certificates installed within the coprocessor. • A new ICSF callable service Public Infrastructure Request (CSNDPIC) is available to generate PKCS#10 certificate requests. • The Digital Signature Verify (CSNDDSV) service has been updated to support the use of an X.509 certificate when verifying a signature.	z/OS 2.1; z/OS 2.2; z/OS 2.3	Sept. 2017

https://www.ibm.com/systems/z/os/zos/tools/downloads/index.html

PCI-HSM

- Improve security in payment card systems
  - Key management
  - HSM API functions
  - Device physical security
  - Controls during manufacturing and delivery
  - Device administration

New ICSF Option

- COMPLIANCEWARN(PCIHSM2016(YES/**NO**/SAF))
  - PCI-HSM 2016 Compliance mode
    - Type 82 Subtype 48
  - SAF – CSF.COMPLIANCEWARN.PCIHSM2016
  - Requires compliant-tagged key tokens
  - SETICSF REFRESH

- ICSF Options 3.1 – COMPLIANCEWARN
  - Yes, No, Not specified, Not supported
- DISPLAY ICSF,CARDS
- CSFIQF/CSFIQF2 – returns Compliance info

Compliant-Tagged Keys

- Internal, fixed-length DES key tokens
- Bit in the token - can’t be turned off
- Must use enhanced wrapping
- No single length keys
- Only ENC-ZERO (3-byte) and CMACZERO KCV
- Migration process defined in SPG

Crypto Usage Statistics

- ICSF Options
  - STATS
    - ENG – track cryptographic engines
    - SRV – track cryptographic services
    - ALG – track cryptographic algorithms
  - STATSFILTER – level of aggregation (for high volume apps)
- SMF Type 82 Subtype 31
- Operational Commands
  - SETICSF OPT,STATS
  - DISPLAY ICSF,OPT
  - DISPLAY ICSF,CARDS
  - DISPLAY ICSF,REMOTEdevice

Monitoring Crypto Operations

- Cryptographic usage statistics can help you determine:
  - The jobs and tasks that are using the various cryptographic engines.
  - The cryptographic card types that are getting the most requests.
  - If any cryptographic requests are being handled in software.
  - The peak periods of cryptographic usage.
  - The ICSF services that are being started by other z/OS components.
  - The jobs and tasks that are using out-of-date algorithms or key sizes.

New API - CSFSTAT

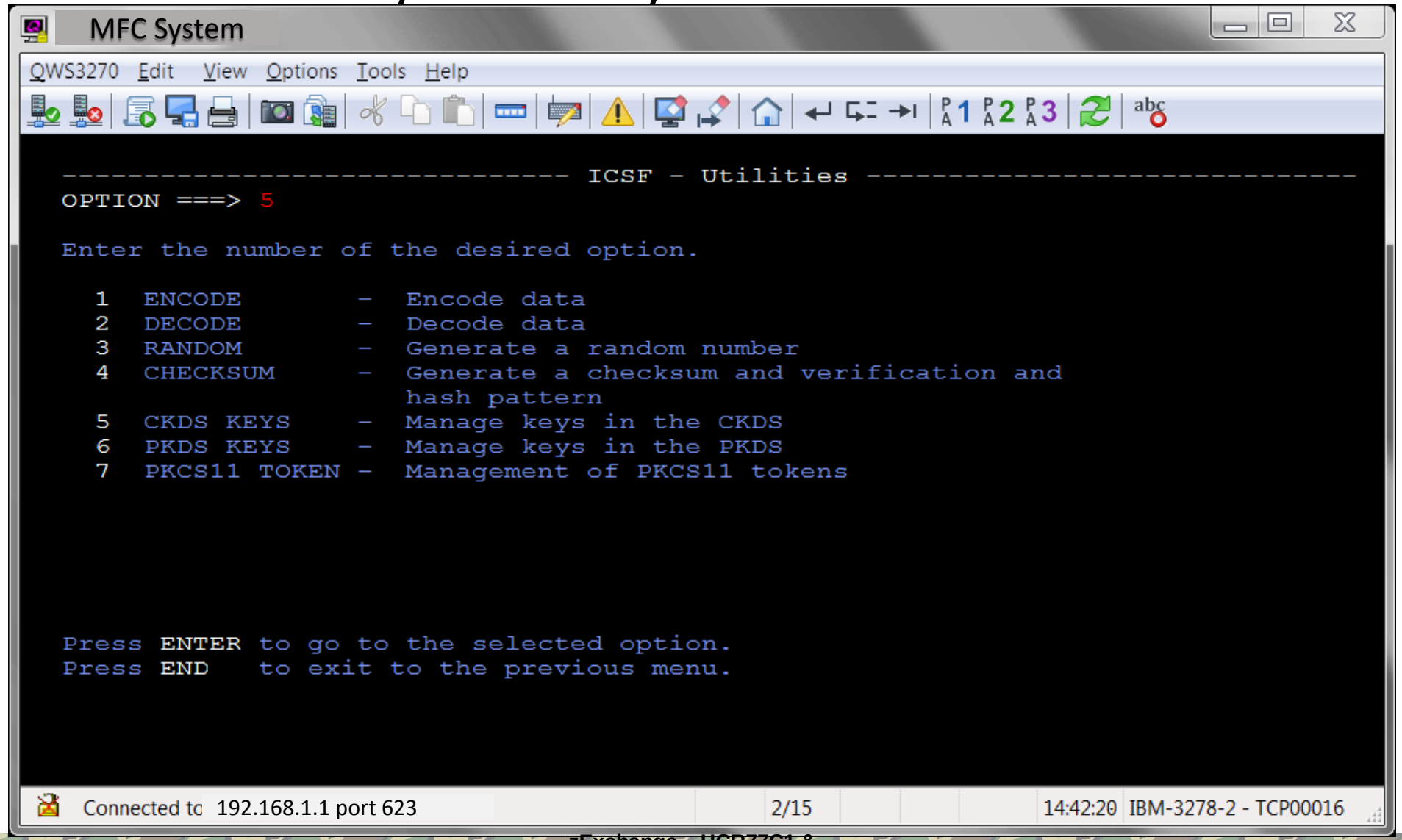
- Track crypto usage external to the ICSF address space
- Captures count between invocations
  - ENG-CPCF – count of CPACF crypto usage
  - ENG-SOFT – number of software cryptographic invocations

CKDS Keys Utility

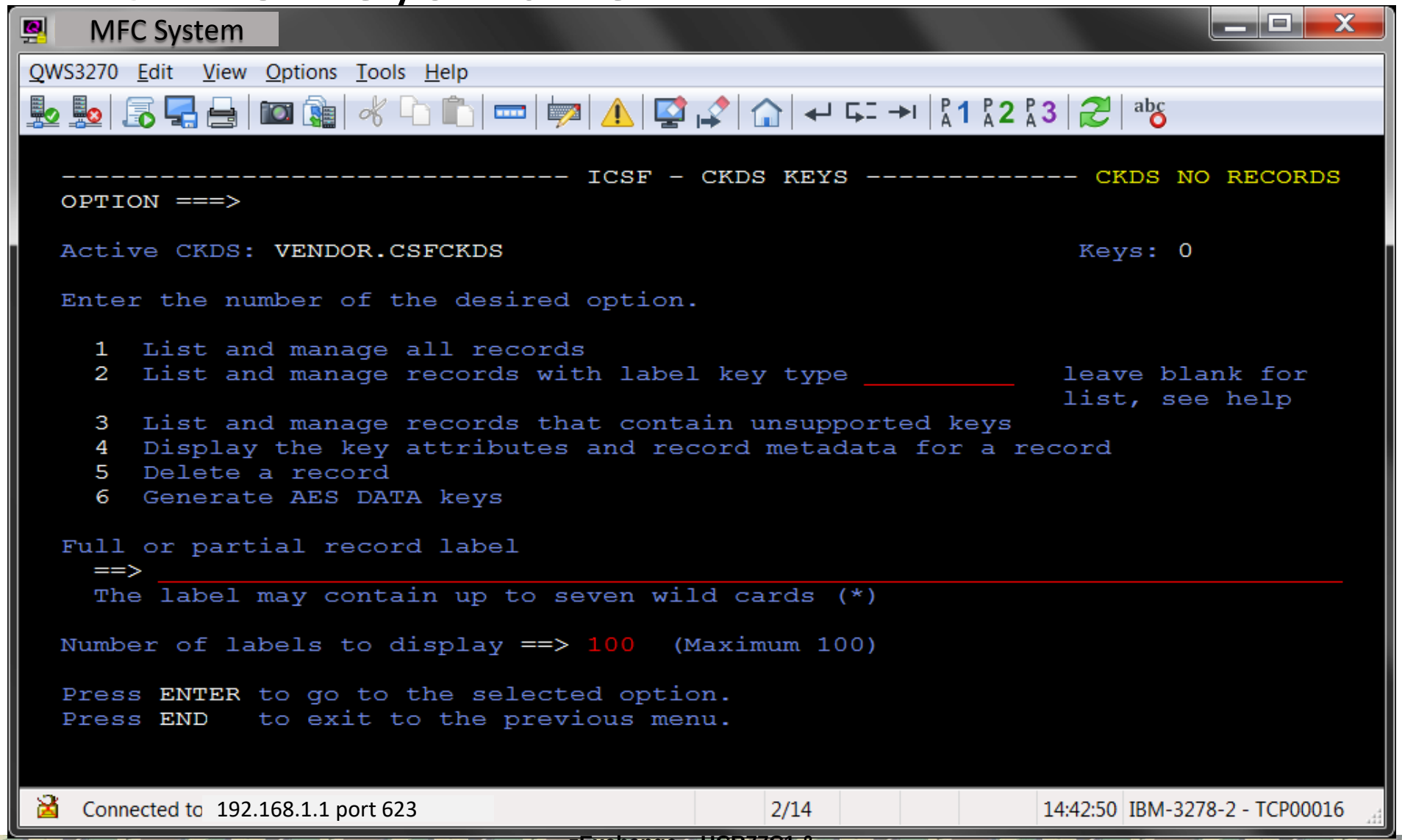
- Browser
  - View key attributes
  - View metadata
  - Change some metadata
- Very limited key generator
  - Secure AES Data Key
- SAF Profile – CSFBRCK
  - List labels – READ
  - Display attributes, metadata – READ
  - Modify metadata – UPDATE plus READ for the key label
  - Delete record – CONTROL and READ for the key label
  - Archiving/recalling – UPDATE and READ for the key label

  Note: ALTER authority to CSFBRCK skips the SAF check on CSFKEYS
  - Generate – also need access to CSFKGN, CSFKRC2, CSFKRR2, CSFKRW2

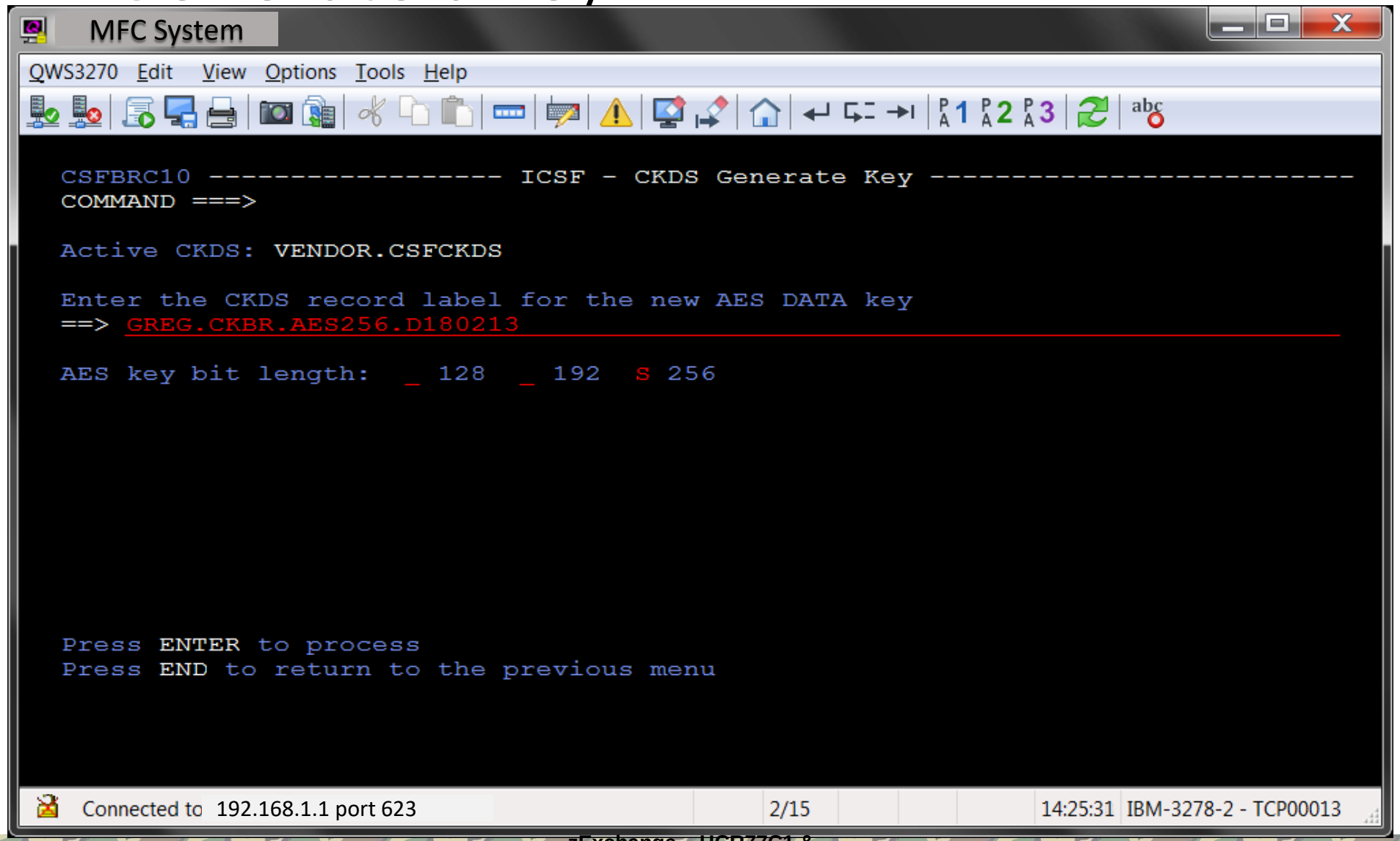
CKDS Keys Utility



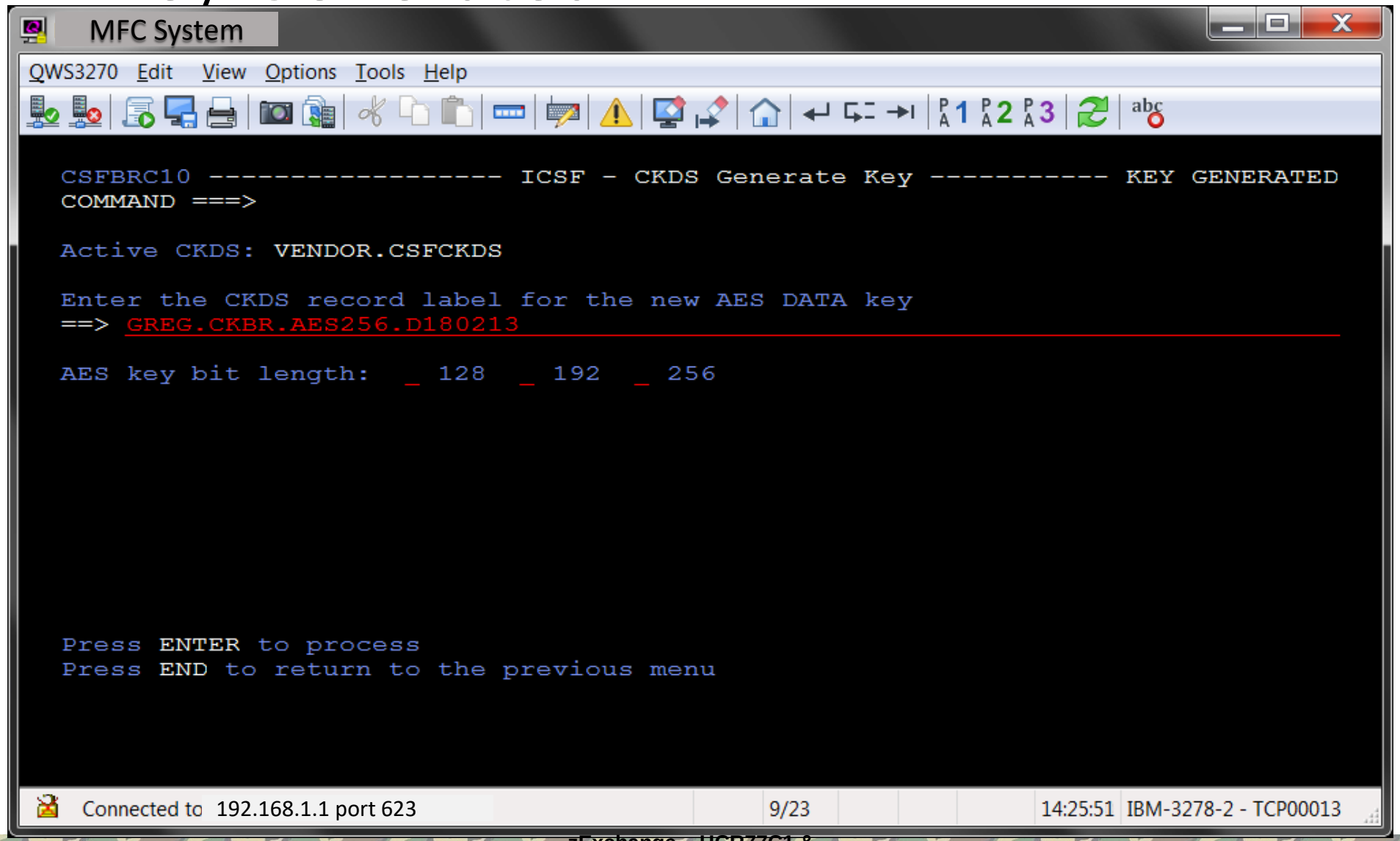
CKDS Keys Panel



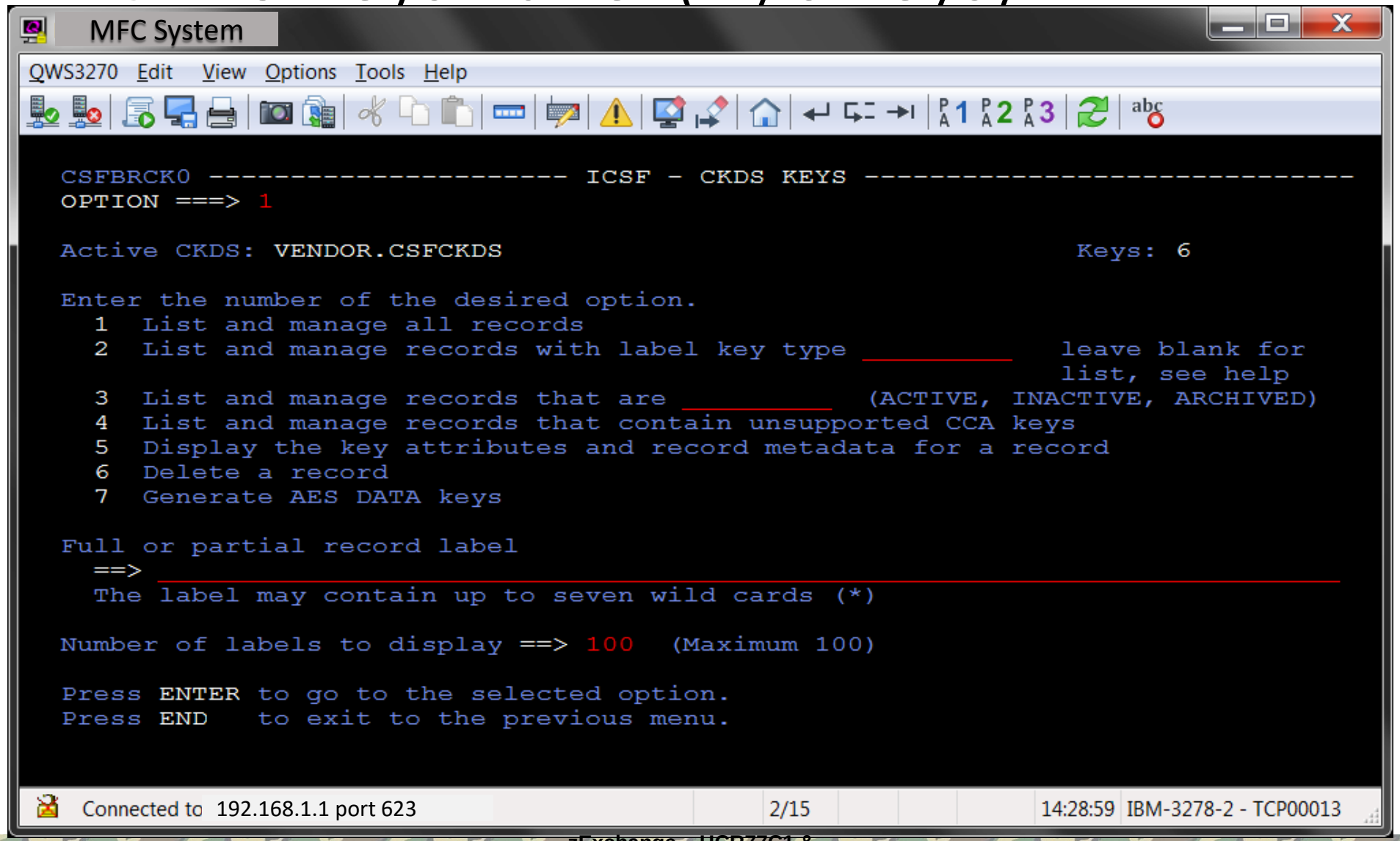
Generate a key



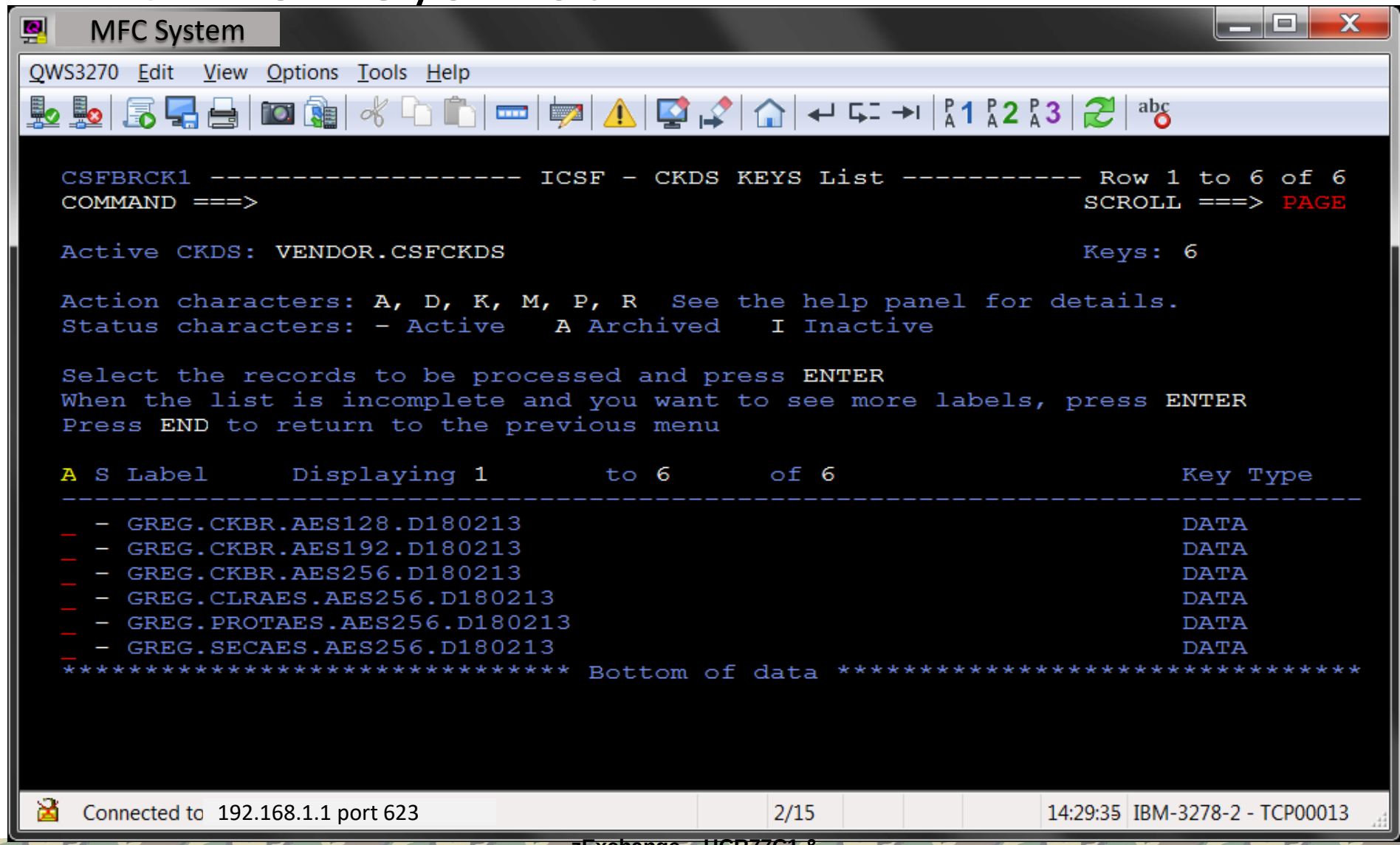
Key Generated



CKDS Keys Panel (w/6 keys)



CKDS Keys List



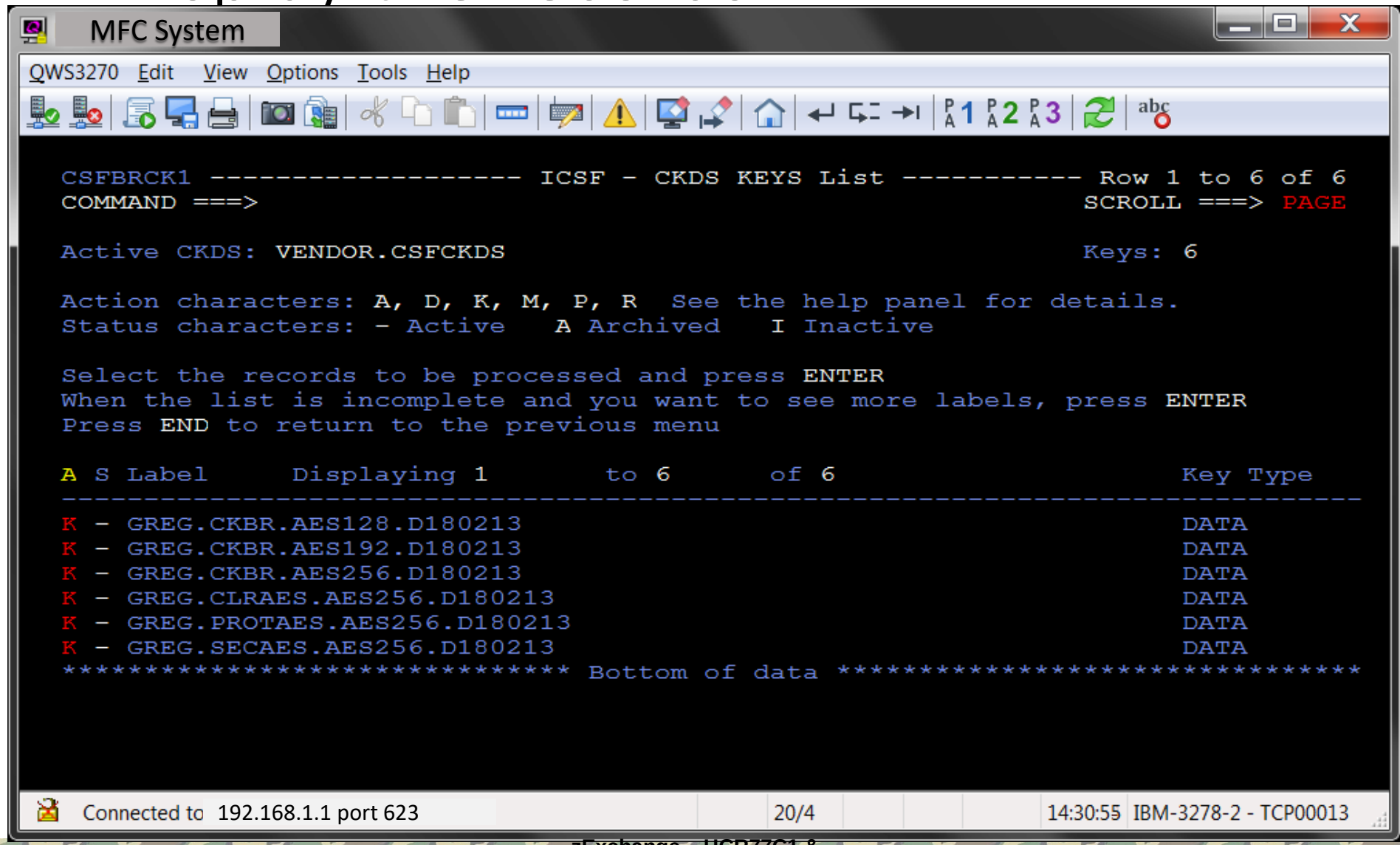
Key Actions

- A – Archive the key
- D – Delete the key
- K – Display key attributes & metadata
- M – Display the metadata
- P – Prohibit Archive
- R – Recall the record (from archive)

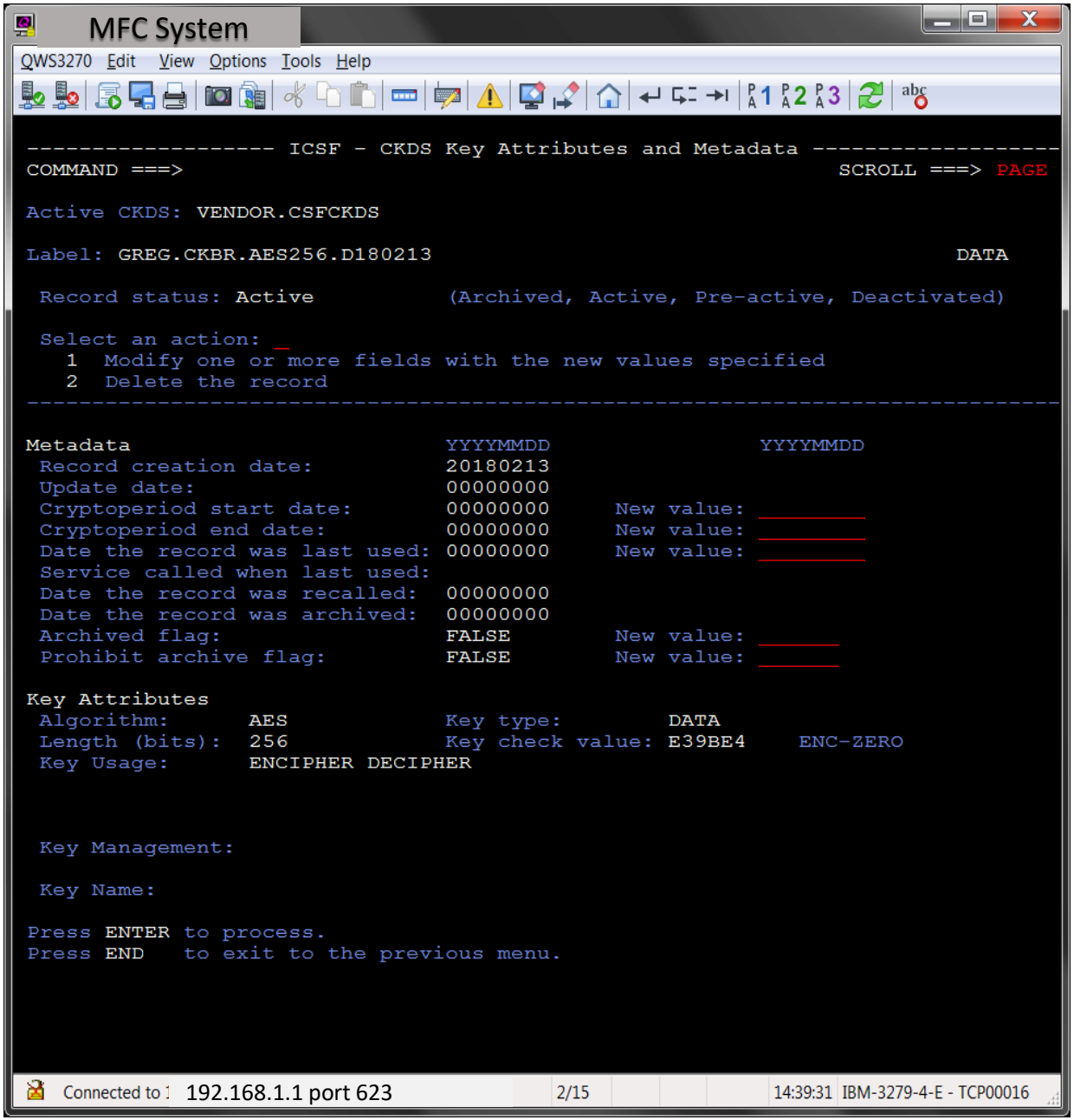
Key Status

- - - Active
- A – Archived
- I – Inactive

Display the records

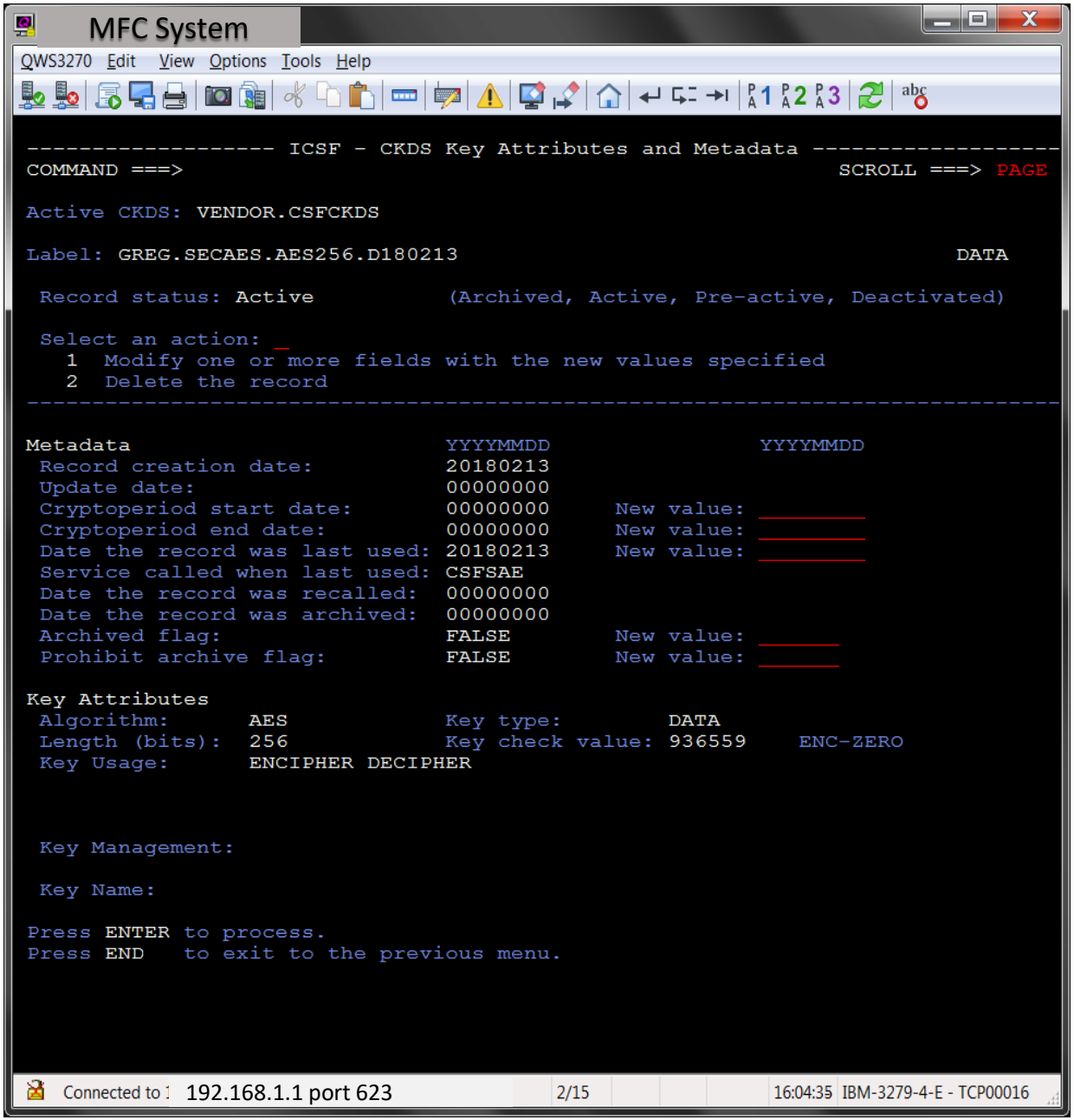


AES-256 Data Key



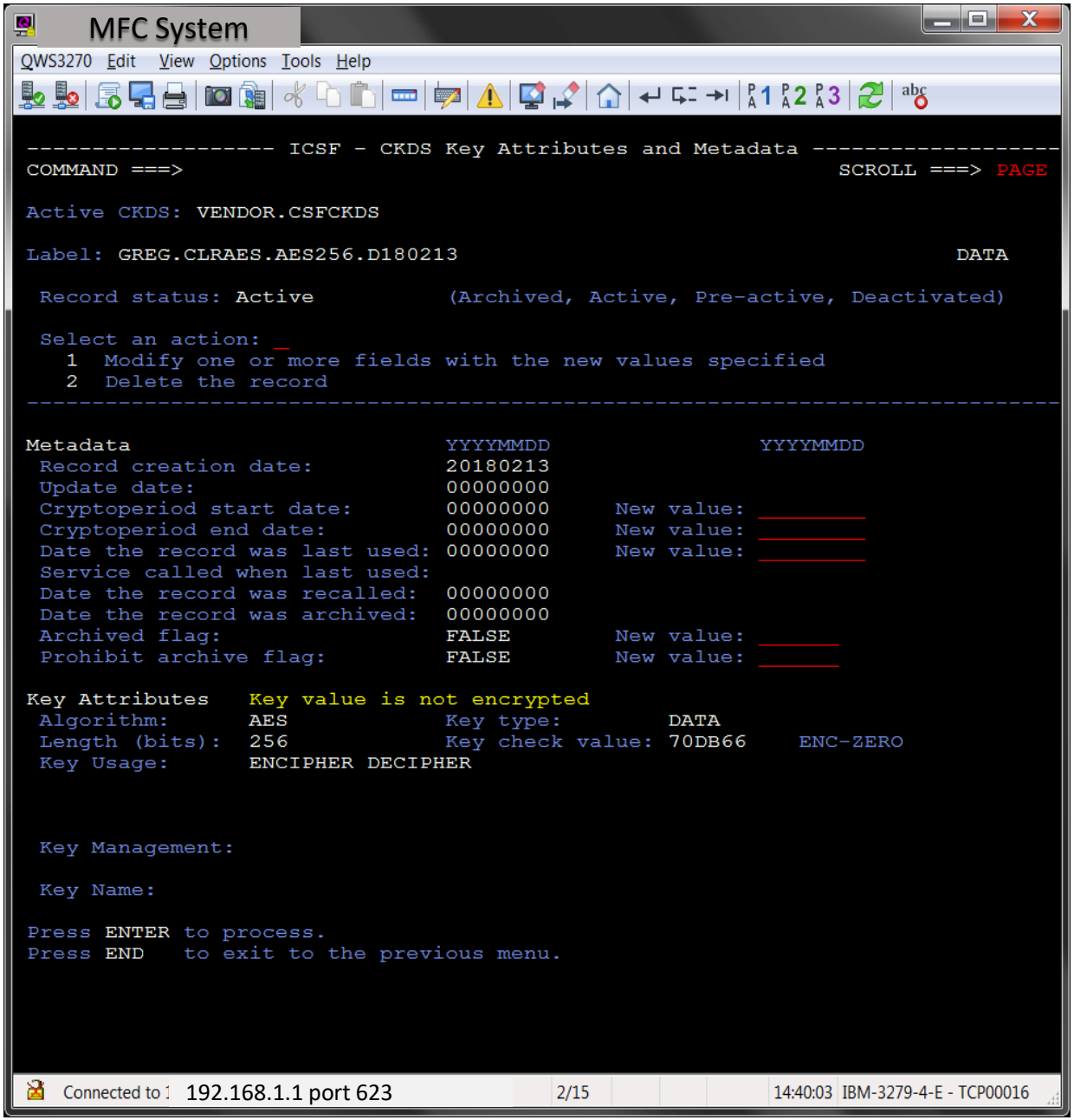
AES-256

Secure AES Key

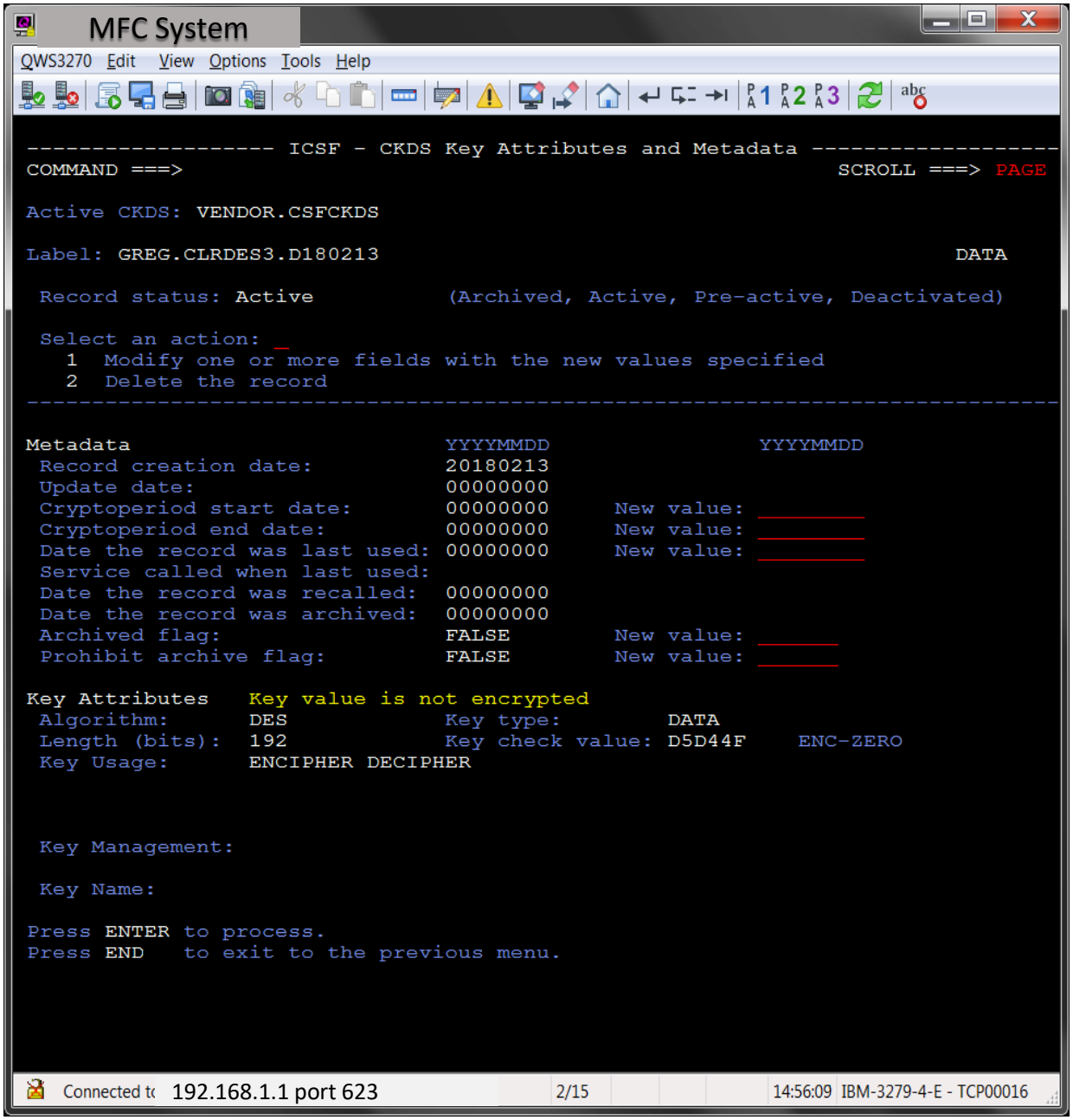


AES-256

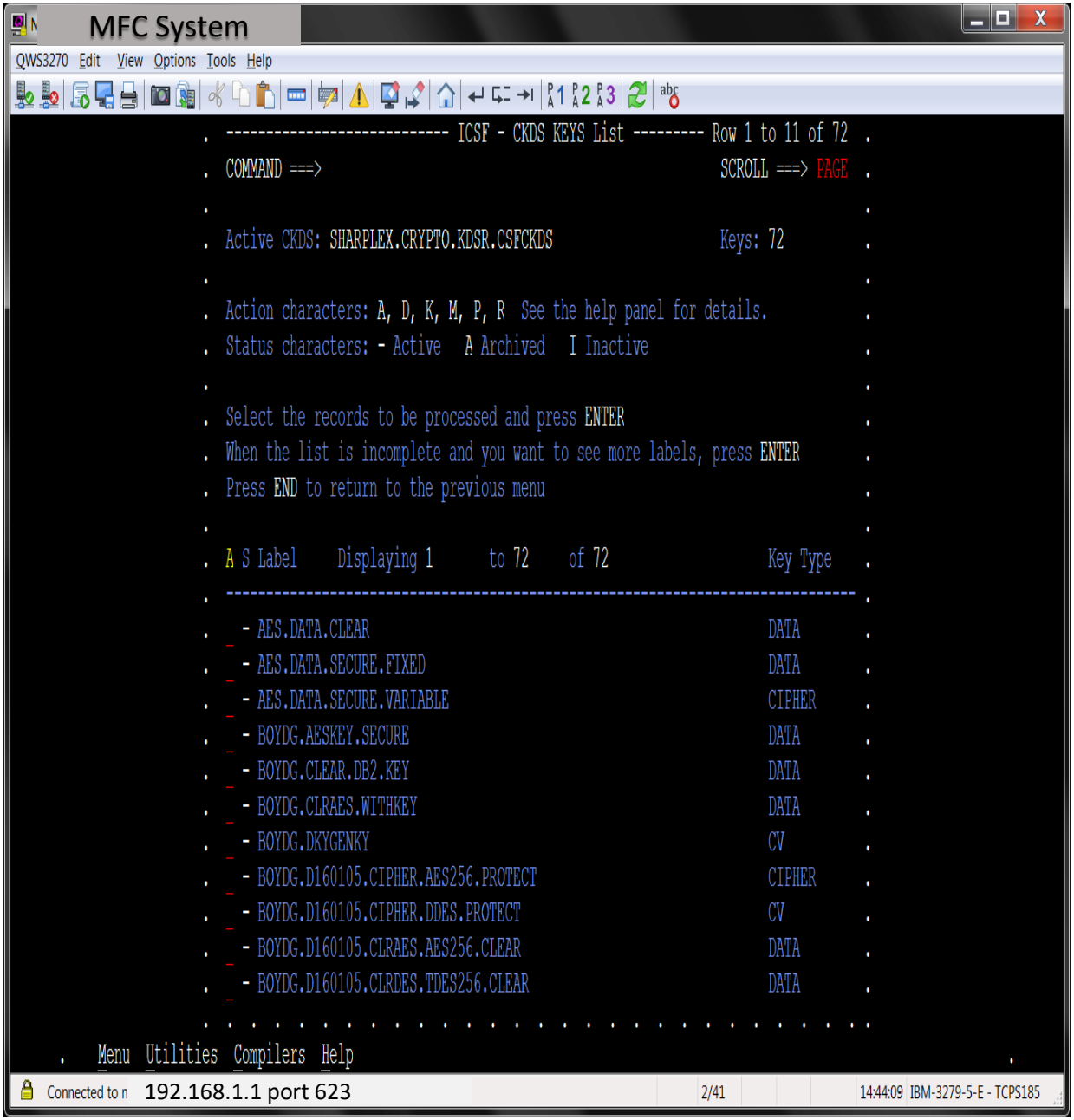
CLRAES Key



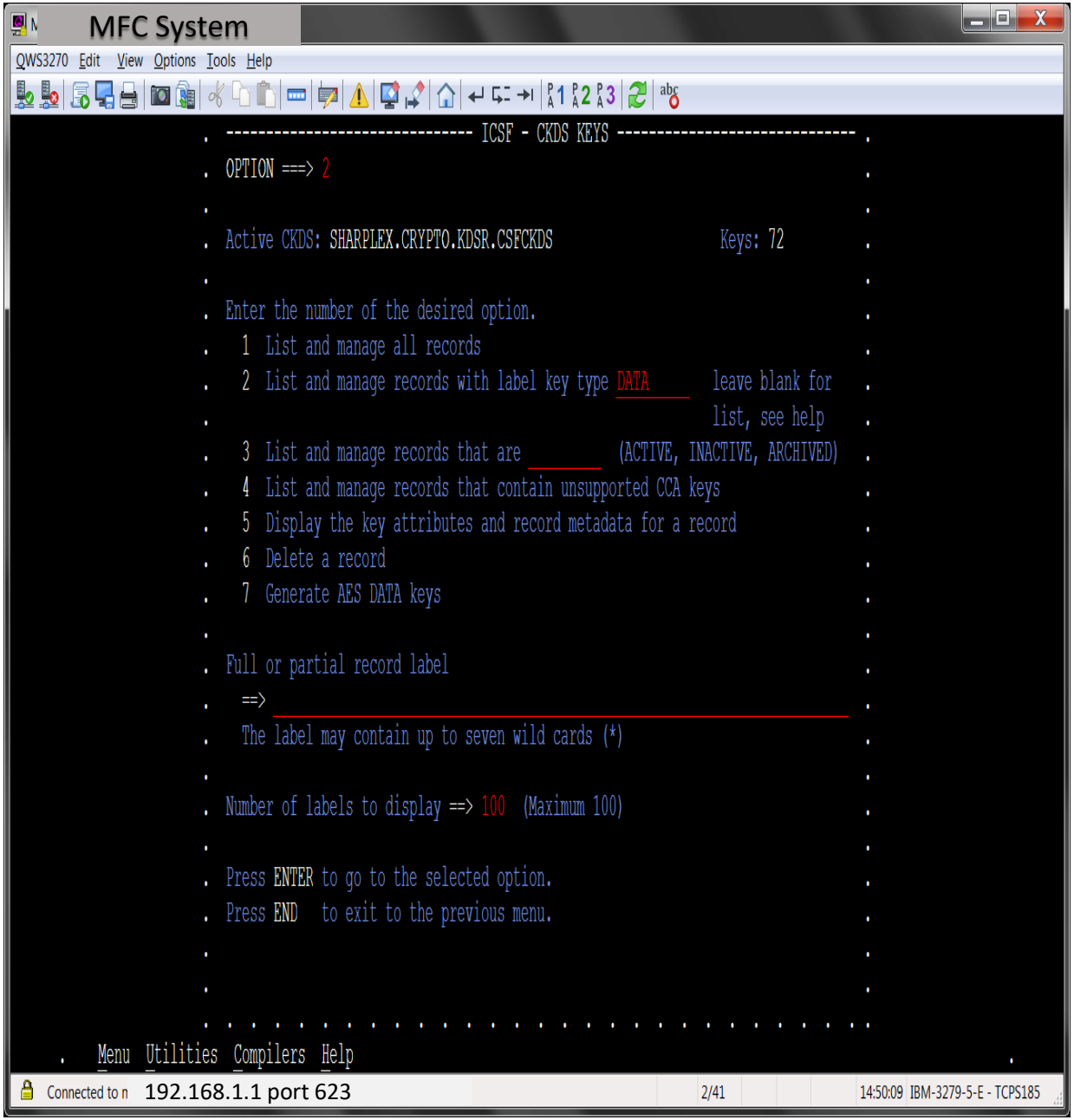
Clear TDES


MFC System
QWS3270 Edit View Options Tools Help
ICSF - CKDS Key Attributes and Metadata
COMMAND ===>
SCROLL ===> PAGE
Active CKDS: VENDOR.CSFCKDS
Label: GREG.CLRDES3.D180213
DATA
Record status: Active (Archived, Active, Pre-active, Deactivated)
Select an action:
1 Modify one or more fields with the new values specified
2 Delete the record
Metadata YYYYMMDD YYYYMMDD
Record creation date: 20180213
Update date: 00000000
Cryptoperiod start date: 00000000 New value:
Cryptoperiod end date: 00000000 New value:
Date the record was last used: 00000000 New value:
Service called when last used:
Date the record was recalled: 00000000
Date the record was archived: 00000000
Archived flag: FALSE New value:
Prohibit archive flag: FALSE New value:
Key Attributes Key value is not encrypted
Algorithm: DES Key type: DATA
Length (bits): 192 Key check value: D5D44F ENC-ZERO
Key Usage: ENCIPHER DECIPHER
Key Management:
Key Name:
Press ENTER to process.
Press END to exit to the previous menu.
Connected to 192.168.1.1 port 623
2/15
14:56:09 IBM-3279-4-E - TCP00016

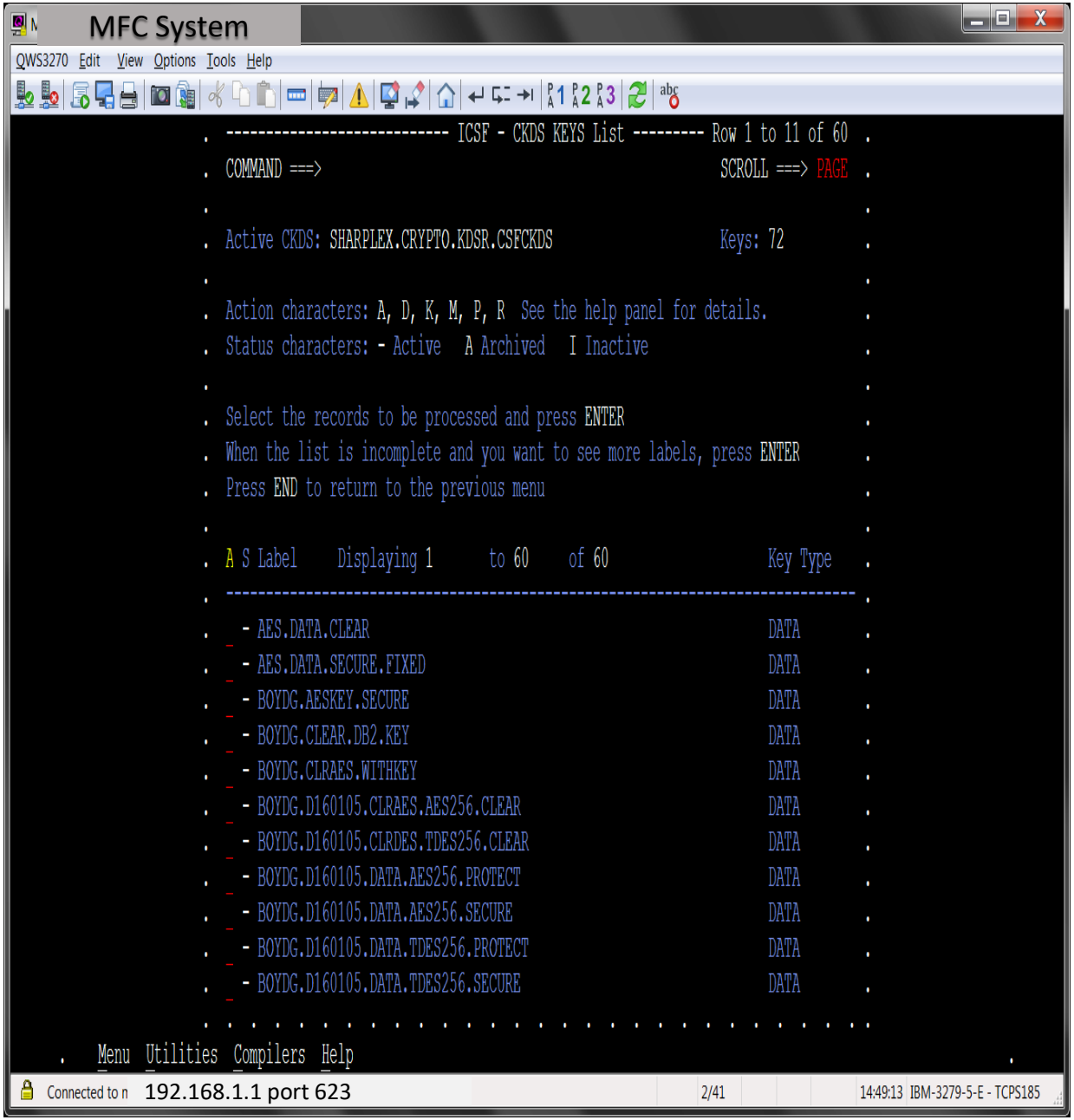
More keys (key types)



Just Data Keys

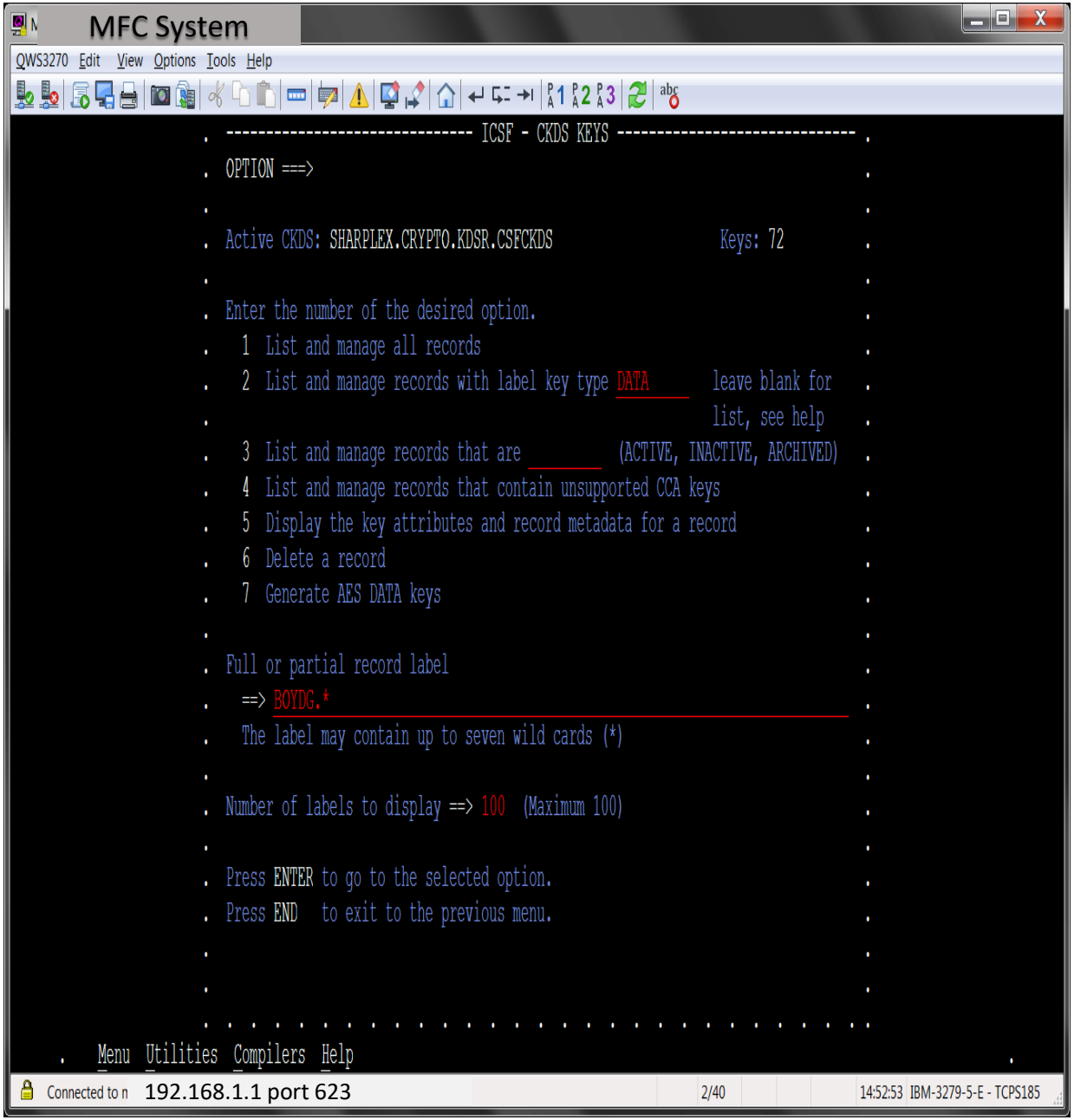


And they are still all mine



List by label

- BOYDG.*
- *.D160105
- *.D160105.*
- *SECRET*
- *.SECRET*



API Updates

- CSNBOWH – One-Way Hash
  - SHA3 (-224, -256, -384, -512)
  - SHAKE128 & SHAKE256
- CSNBFLD/CSNBFLE – Field Level Decipher/Encipher
  - Now support variable-length AES CIPHER key
- CSFKDSL- Key Data Set List API
  - Extended to specify criteria based on metadata
  - Specify algorithm (DES, AES, PKA)
  - New output options

CIPHER Keys

- CIPHER Keys can now be used as Protected Keys
- CSNBKTB2 – Key Token Build2
  - XPRTCPAC – Allow export to CPACF protected key format
  - NOEXCPAC – Prohibit export to CPACF protected key format

Digital Certificates

- CSNDDSV – Digital Signature Verify
  - X.509 certificate in PEM format, EBCDIC or DER-formatted
- CSNDPIC – Public Infrastructure Certificate
  - Create self-signed PKCS #10 CSR

Operations

- S CSF,SUB=MSTR (to avoid waiting for JES)
- P CSF – after omvs is stopped (to allow updates to an encrypted file system to complete
  - And if it won't stop gracefully, use FORCE
    - FORCE csf,arm

New ICSF Options

- CICSAUDIT (SPG p. 42/66)
  - CICS Identity captured
  - SMF Type 82, Subtype 2

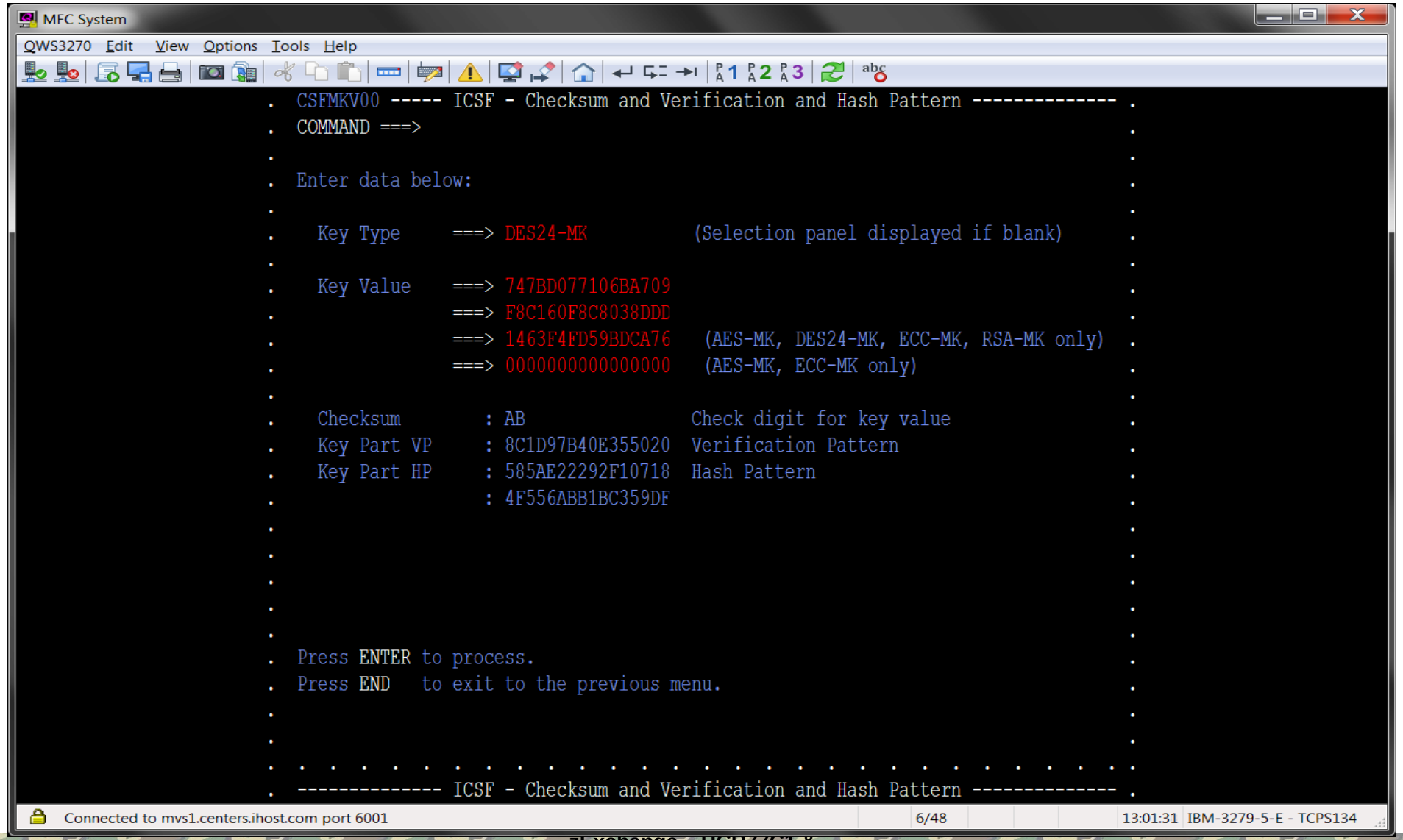
SMF Changes

- Subtype 18 – Cryptographic processor configuration
  - Added a flag for config change
- Subtype 31 – Cryptographic usage statistics
  - 50 Algorithms
  - 182 Services
  - Coprocessors, RCS (Regional Crypto Server), CPACF & Software
- Subtype 48 – Compliance Warning Event
  - Compliant operation flag
  - Compliant key flag

Doc Changes

- SPG – SC14-7507-07
  - CSF_SERVICE_EXIT – ICSF callable services exit
- Overview – SC14-7505-07
  - Clarifies that ICSF caches protected keys
- Limits on validity start and end dates
  - 01/01/1900 for earliest start date
  - 06/04/2185 for latest end date

Checksum DES24-MK



Load DES-MK


MFC System
QWS3270 Edit View Options Tools Help
CSFDKE50 ICSF - Master Key Entry INCORRECT CHECK SUM
COMMAND ===>
AES new master key register : EMPTY
DES new master key register : EMPTY
ECC new master key register : EMPTY
RSA new master key register : EMPTY
Specify information below
Key Type ===> DES-MK (AES-MK, DES-MK, ECC-MK, RSA-MK)
Part ===> FIRST (RESET, FIRST, MIDDLE, FINAL)
Checksum ===> AB
Key Value ===> 747BD077106BA709
===> F8C160F8C8038DDD
===> 1463F4FD59BDCA76 (AES-MK, ECC-MK, and RSA-MK only)
===> (AES-MK, ECC-MK only)
Press ENTER to process.
Press END to exit to the previous menu.

ICSF Manuals

- SC14-7505 ICSF Overview
- SC14-7506 ICSF Administration Guide
- SC14-7507 ICSF Systems Programmer's Guide
- SC14-7508 ICSF Application Programmer's Guide
- SC14-7509 ICSF Messages
- SC14-7510 ICSF Writing PKCS #11 Applications
- GI11-9478-06 Program Directory for Cryptographic Support for z/OS V2R1 – V2R3

External References

- SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions
  - https://dx.doi.org/10.6028/NIST.FIPS.202
- IBM Systems Magazine
  - ICSF Stats http://ibmsystemsmag.com/mainframe/hot-topics/crypto-statistics-monitor/

ICSF References

- Announcement Letters
  - 117-044, July 17, 2017 IBM z14
  - 217-246, July 17, 2017 z/OS 2.3
- TechDocs www.ibm.com/support/techdocs (search on crypto)

Questions?