MAINFRAME CRYPTO

ICSF Keys and KGUP

Greg Boyd

gregboyd@mainframecrypto.com

www.mainframecrypto.com

Copyrights . . .

- Presentation based on material copyrighted by IBM, and developed by myself, as well as many others that I worked with over the past 12 years

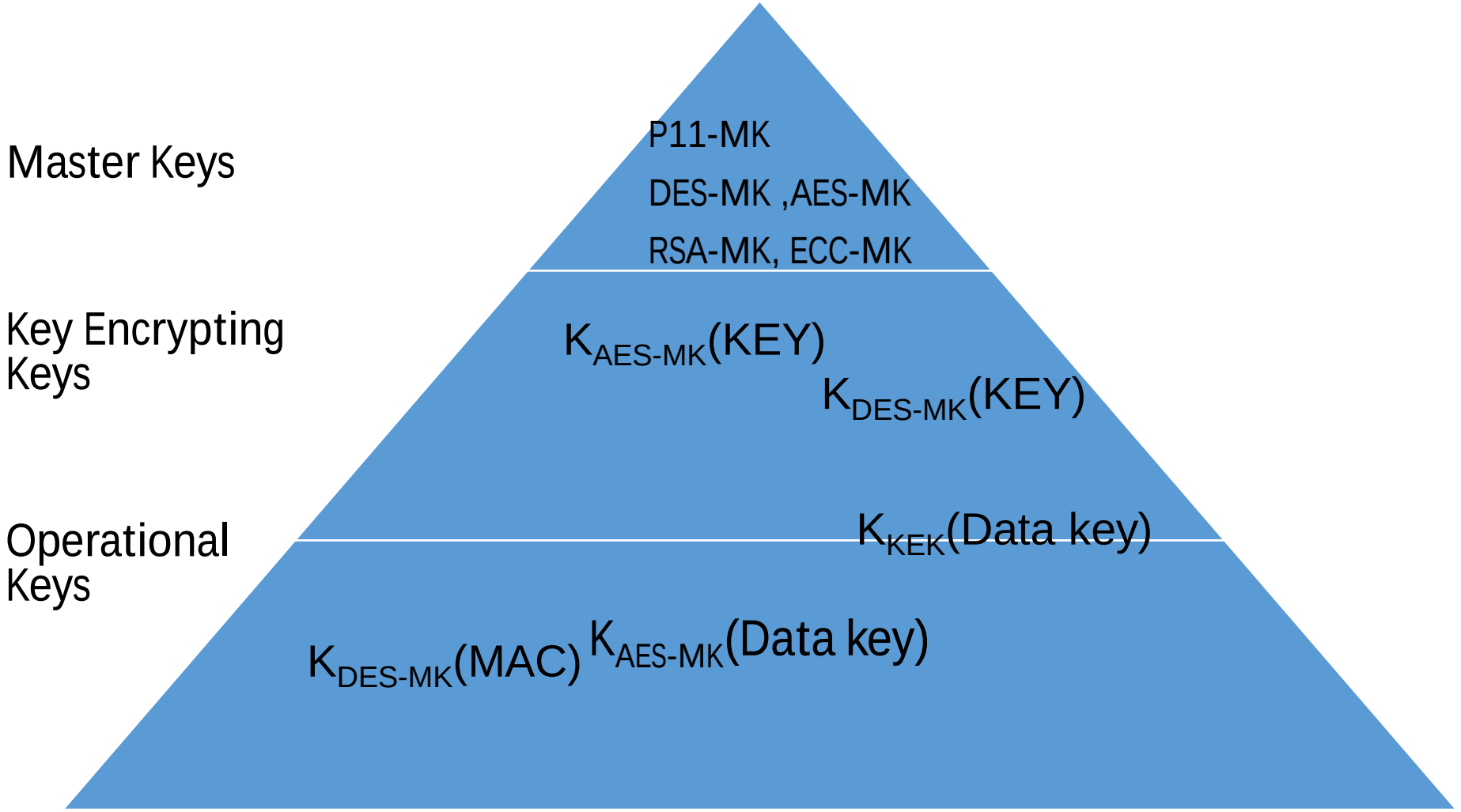
. . . And Trademarks

- Copyright © 2016 Greg Boyd, Mainframe Crypto, LLC. All rights reserved.
- All trademarks, trade names, service marks and logos referenced herein belong to their respective companies. IBM, System z, zEnterprise and z/OS are trademarks of International Business Machines Corporation in the United States, other countries, or both. All trademarks, trade names, service marks and logos referenced herein belong to their respective companies.
- **THIS PRESENTATION IS FOR YOUR INFORMATIONAL PURPOSES ONLY**. Greg Boyd and Mainframe Crypto, LLC assumes no responsibility for the accuracy or completeness of the information. TO THE EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. In no event will Greg Boyd or Mainframe Crypto, LLC be liable for any loss or damage, direct or indirect, in connection with this presentation, including, without limitation, lost profits, lost investment, business interruption, goodwill, or lost data, even if expressly advised in advance of the possibility of such damages.

Agenda – Keys & KGUP

- Key Hierarchy
- Operational Keys
- Key Variants and Control Vectors
- Key Loading
- Key Generation Utility Program

Hierarchy of Keys



Operational Keys

	DES Key Length	AES Key Length	Clear/Secure
Data Class Keys – used to encrypt/decrypt data			
DATA (encrypt & decrypt data), CLRAES, CLRDES	8-, 16- or 24-byte	128-, 192- or 256-bit	Clear or Secure
DATAM (MAC Generate & Verify)	16-byte		Secure
DATAMV (MAC Verify)	16-byte		Secure
Cipher Class Keys – used to encrypt/decrypt data			
CIPHER (encrypt & decrypt data)	8- or 16-byte		Secure
DECIPHER (encrypt & decrypt data)	8- or 16-byte		Secure
ENCIPHER (encrypt & decrypt data)	8- or 16-byte		Secure
CipherXL Class Keys – ciphertext translate keys			
CIPHERXI, CIPHERXL, CIPHERXO	16-byte	128-, 192- or 256-bit	Secure

Operational Keys (cont.)

	DES Key Length	AES Key Length	Clear/Secure
MAC Class Keys – used to generate and verify MACs, CVVs and CSCs			
MAC	8- or 16-byte	128-, 192- or 256-bit	Clear or Secure
MACVER	8- or 16-byte		Secure
HMAC (generate & verify keyed hash message authentication code)		Variable (80-2024-bit)	Secure

Operational Keys (cont.)

	DES Key Length	AES Key Length	Clear/Secure
PIN Class Keys – used to generate and verify PINs and PIN offsets			
PINGEN	16-byte		Secure
PINVER	16-byte		Secure
IPINENC	16-byte		Secure
OPINENC	16-byte		Secure
PINCALC (DK PIN Generate)		128-, 192- or 256-bit	Secure
PINPROT (wrap and unwrap PIN blocks)		128-, 192- or 256-bit	Secure
PINPRW (generate and verify PIN reference words)		128-, 192- or 256-bit	Secure

Operational Keys (cont.)

	DES Key Length	AES Key Length	Clear/Secure
Key-encrypting Key Class Keys – used to wrap other keys			
EXPORTER	16-byte	128-, 192- or 256-bit	Clear or Secure
IMPORTER	16-byte	128-, 192- or 256-bit	Secure
IMP-PKA		Variable (80-2024-bit)	Secure
IKEYXLAT, OKEYXLAT	16-byte		Secure
Key-generate Class Keys – used to derive keys			
KEYGENKY	16-byte	128-, 192- or 256-bit	Secure
DKYGENKY	16-byte	128-, 192- or 256-bit	Secure

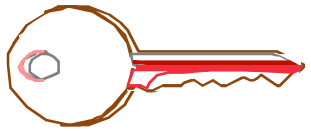
Operational Keys (cont.)

	DES Key Length	AES Key Length	Clear/Secure
Cryptographic-variable Class Keys – used to encrypt special control values in DES key management			
CVARENC	8-byte		Secure
CVARXCVL	8-byte		Secure
CVARXCVR	8-byte		Secure
Secure-messaging Class Keys – used to encrypt keys and PINs for incorporation into a text block			
SECMSG	16-byte		Secure

Key Variants

- Part of the DES ‘invention’
- Applied ‘under the covers’ within the secure boundary of the crypto card
  - Not accessible, nor can it be specified by application interfaces
  - Greater granularity of functions
    - PIN encryption
    - CIPHER only
    - MAC only
    - PIN generate/verify only
    - ATM ‘B’-key
  - Variants imply using the master key AFTER the variant has been applied
    - Limit the need for multiple master key storage

Control Vectors



- Non-secret value in a key-token
- Cryptographically coupled to the key in the current token
- XOR'd onto the key protecting the token
  - Similar to key variant
- Performs as a key variant
  - Greater granularity than existing key variants
    - More key types
    - Full length of key

Some Control Vectors

- From the ICSF APG

Key Type	Control Vector Value (Hexadecimal Value for Left Half of Double-length Key)	Control Vector Value (Hexadecimal Value for Right Half of Double-length Key)
MAC	00 05 4D 00 03 00 00 00	
MAC (Double length)	00 05 4D 00 03 41 00 00	00 05 4D 00 03 21 00 00
IMPORTER	00 42 7D 00 03 41 00 00	00 42 7D 00 03 21 00 00
EXPORTER	00 41 7D 00 03 41 00 00	00 41 7D 00 03 21 00 00
DATA	00 00 00 00 00 00 00 00	
IPINENC	00 21 5F 00 03 41 00 00	00 21 5F 00 03 21 00 00
OPINENC	00 24 77 00 03 41 00 00	00 24 77 00 03 21 00 00
PINGEN	00 22 7E 00 03 41 00 00	00 22 7E 00 03 21 00 00
PINVER	00 22 42 00 03 41 00 00	00 22 42 00 03 21 00 00
…..	**…..**	**…..**

Asymmetric Keys

RSA – used for key distribution and authentication Modulus may be 512-4096 bits Modules-exponent and Chinese Remainder Theorem supported
ECC – used for authentication and symmetric key derivation. AES and DES keys are derived using Diffie-Hellman protocol Private key can be restricted to authentication or key derivation only
Trusted blocks – used in remote key management for ATMs and other remote devices

PKCS #11 Operational Keys

	Key Lengths
AES	128-, 192-, 256-bit
Blowfish	8 to 448-bits, increments of 8 bits
DES/TDES	8-, 16-, 24-byte
Diffie-Hellman	512- to 2048-bits, increments of 64 bits
DSA	512- to 2048-bit prime lengths, increments of 64 bits
EC	160- to 512-bits
RC4	8- to 2048-bits
RSA	512- to 4096-bits

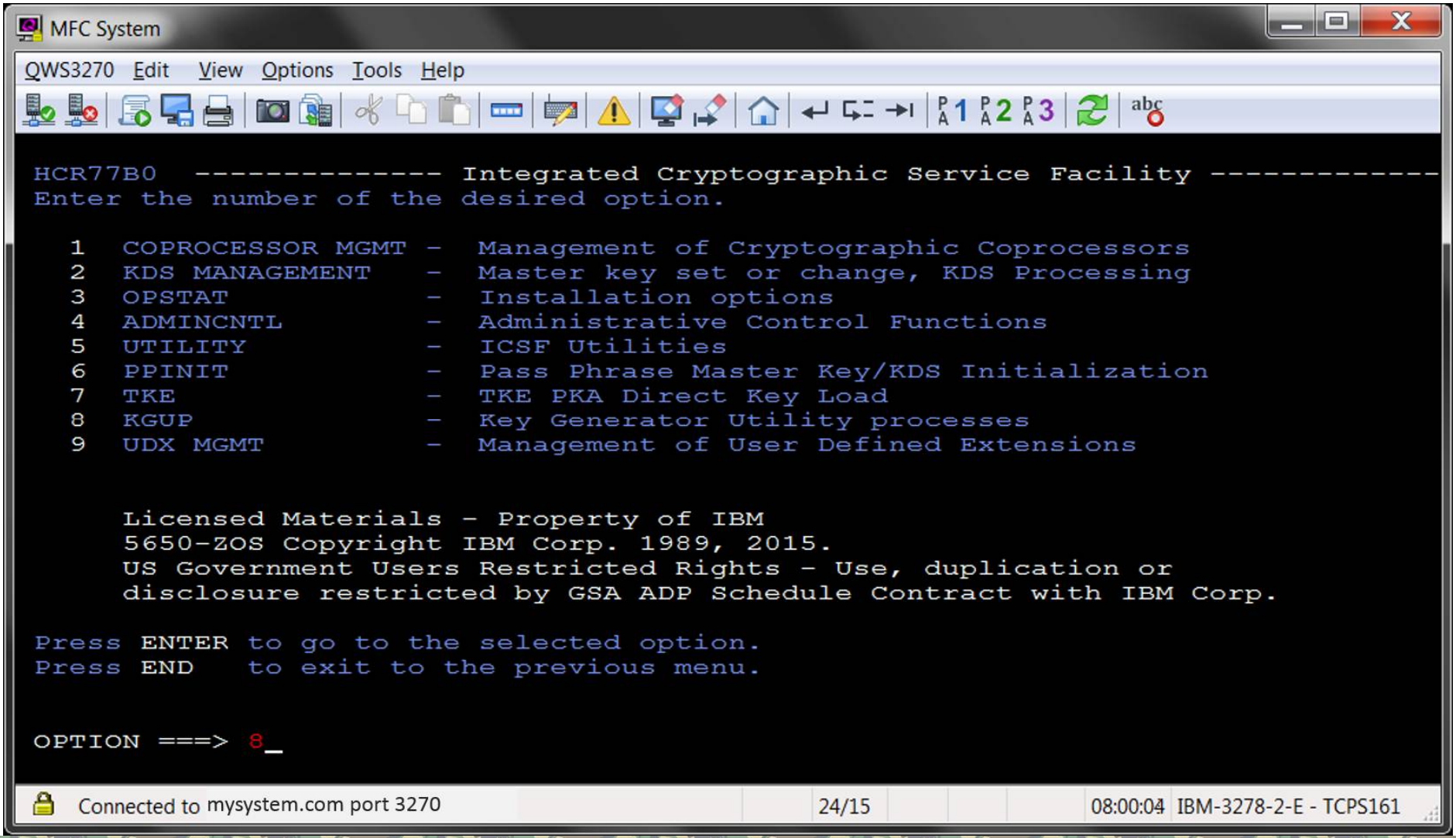
Operational Key Loading

- ICSF APIs
  - Generate and manage keys
  - Import/Export
- Key Generation Utility Program (KGUP)
  - Batch Utility for managing key material - Add, modify, delete
  - ISPF Panel interface for generating JCL and control statements
  - Will generate complimentary keys
  - Can also be used to import or export key material

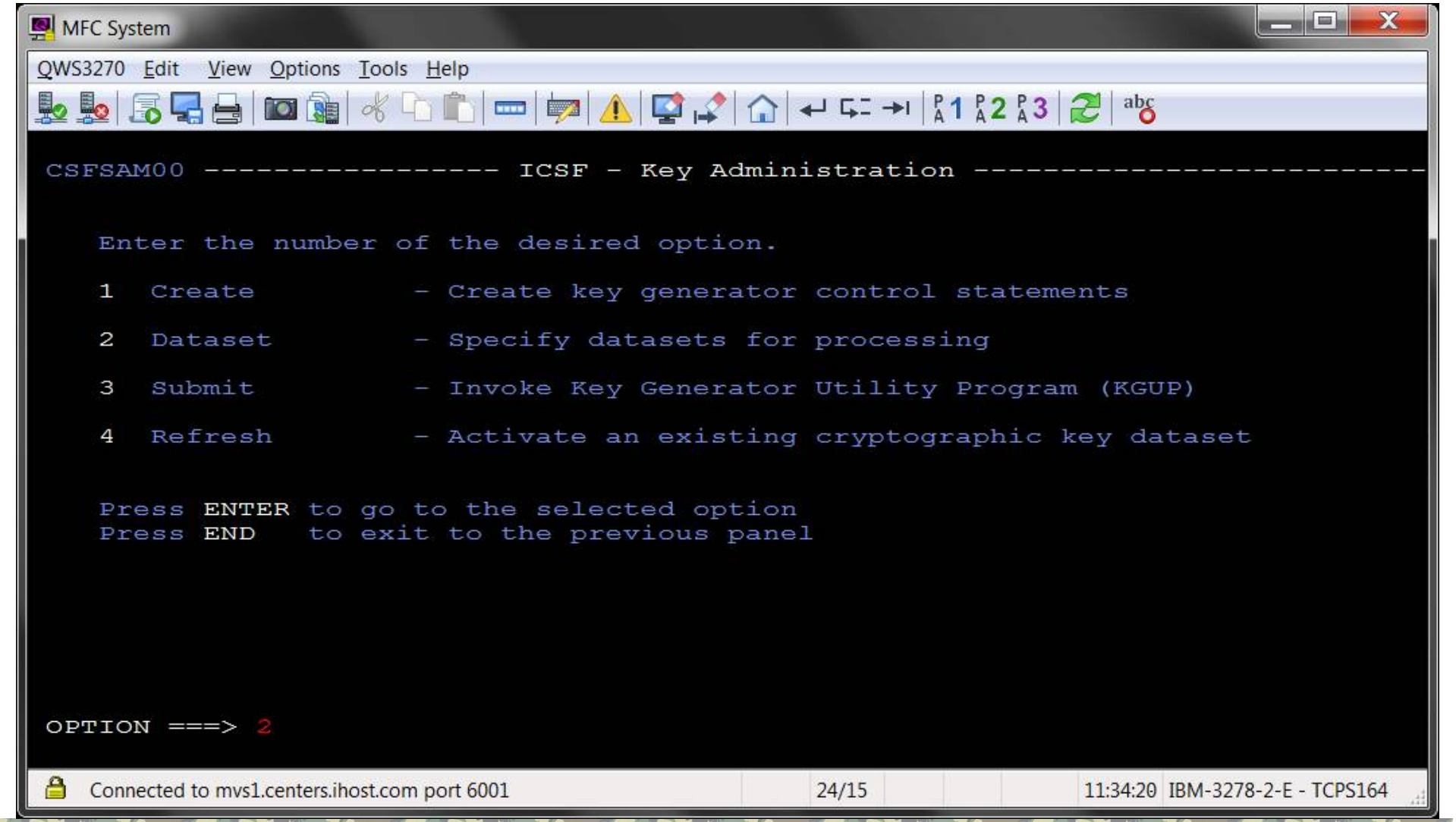
```
/* SALARY PERSONNEL TABLE DB2 ENCR TOOL */
ADD TYPE(DATA) LENGTH(32) ALGORITHM(AES),
        LAB(MFC.PERS.SALARY.D150527)
```

- Trusted Key Entry Workstation

ICSF Main Menu - KGUP



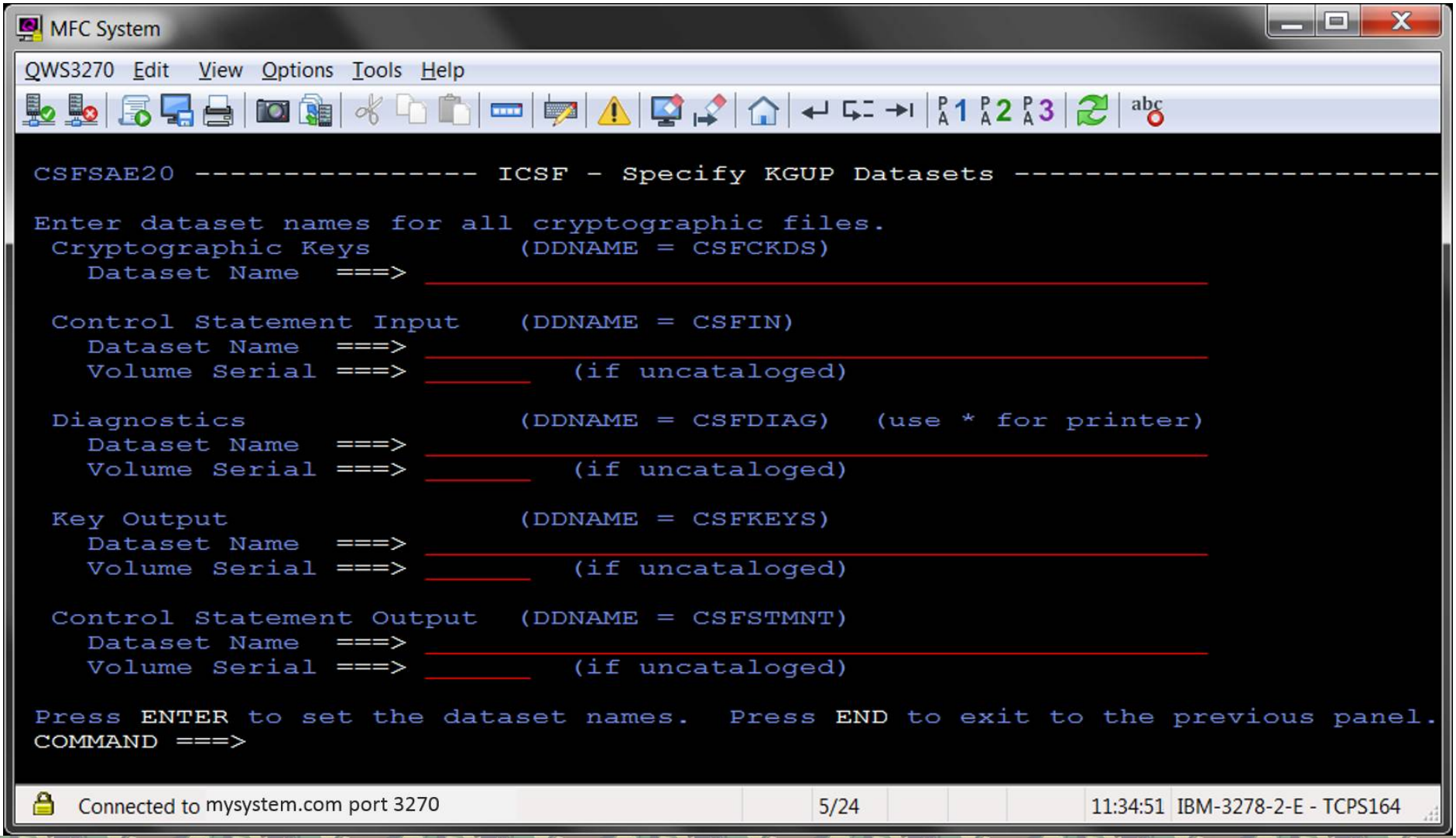
KGUP – Key Administration Menu



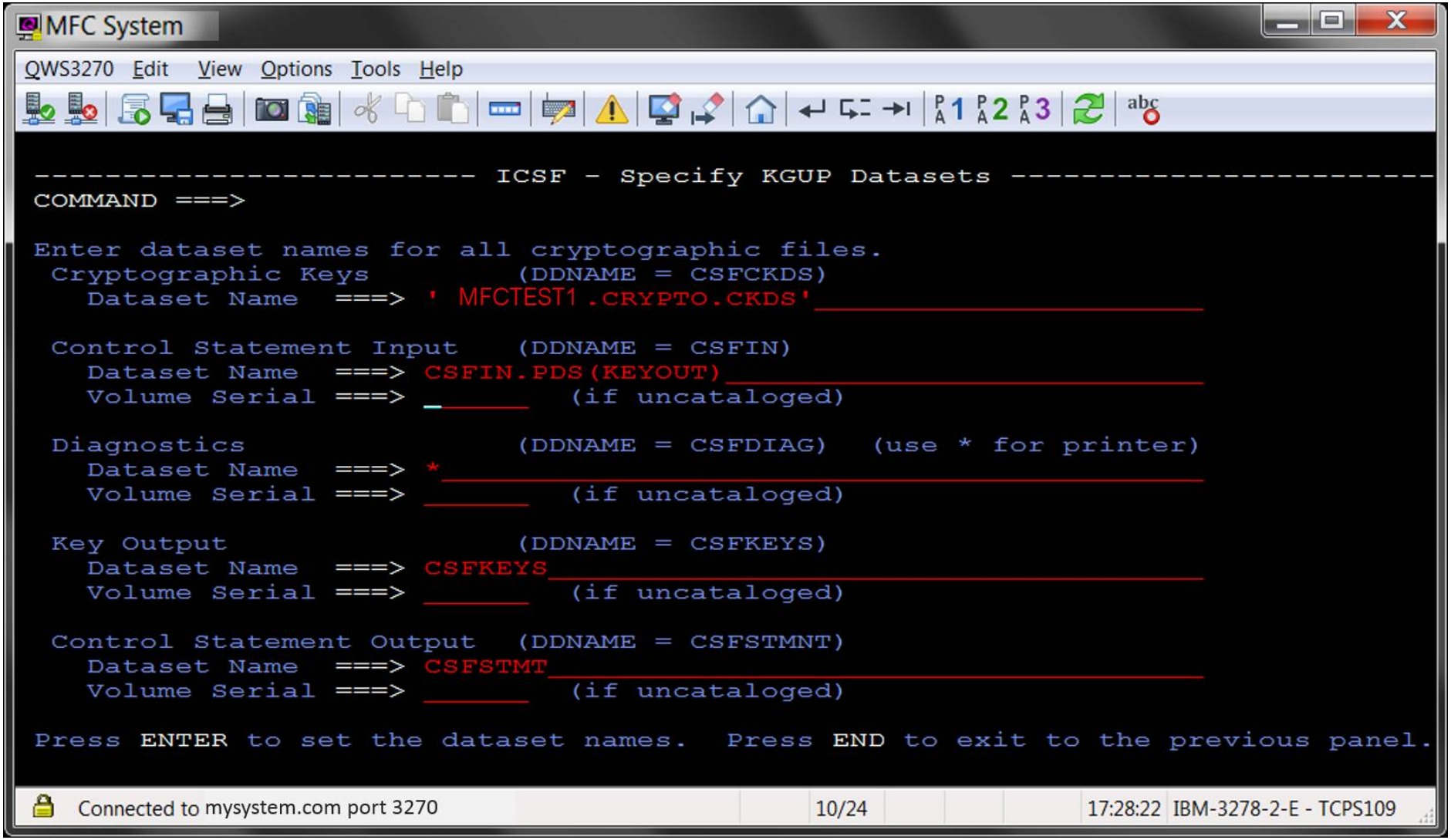
KGUP Datasets

- CSFCKDS – CKDS Keystore
- CSFIN – Control statement data set
  - LRECL(80)
  - Sequential (or PDS member)
- CSFDIAG – KGUP diagnostic messages
  - Typically SYSOUT, but can be a sequential data set
  - LRECL(133)
- CSFKEYS – Key Output Data set
  - Exportable copy of the key, for sharing with partner
  - RECFM(FB), LRECL(208),BLKSIZE(3328)
- CSFSTMNT –Control Statement Output Data Set
  - Used when TRANSKEY (Transport Key) specified
  - KGUP Control statements to be used by partner ICSF
  - LRECL(80)

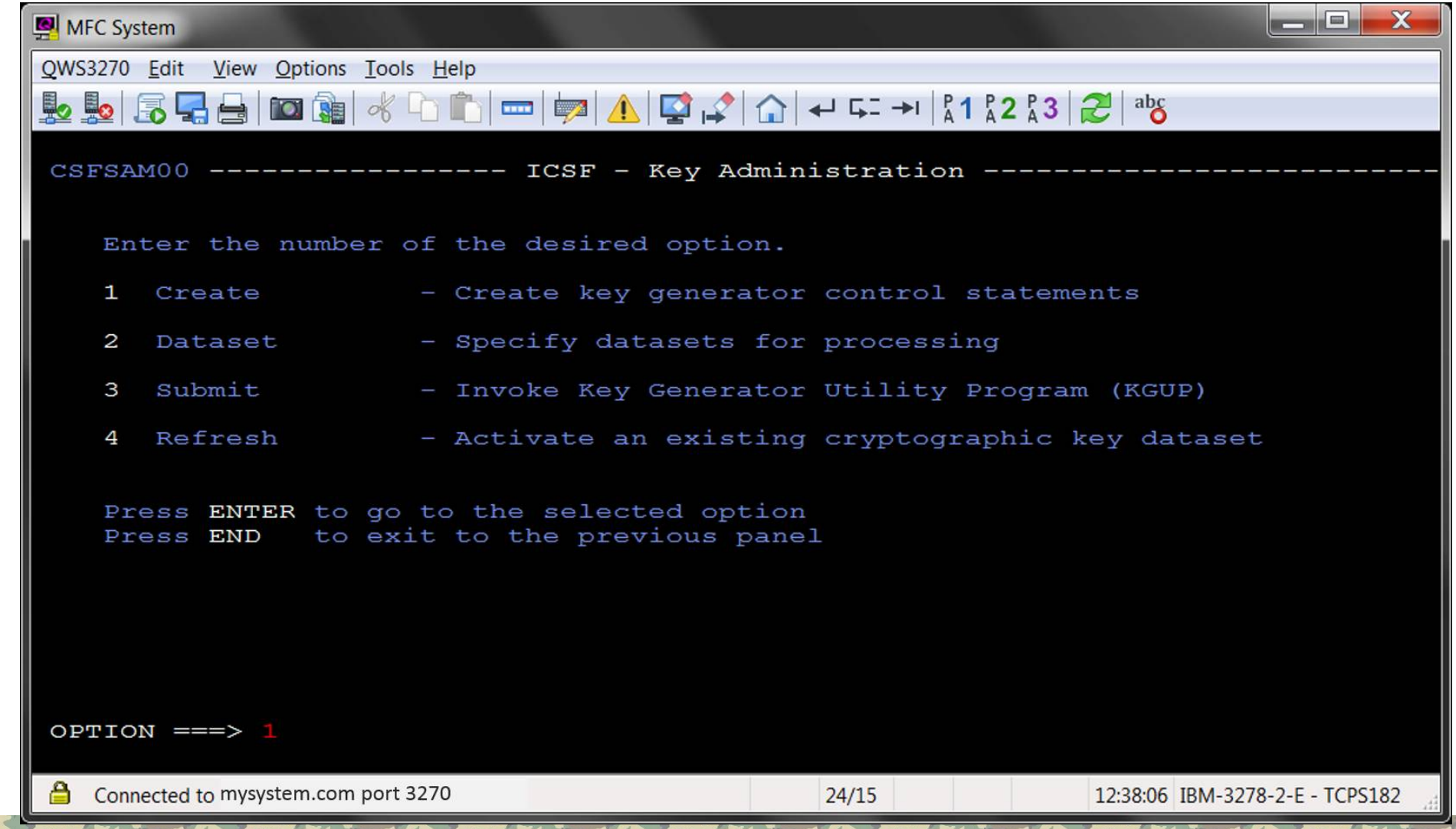
Specify Datasets - Entry



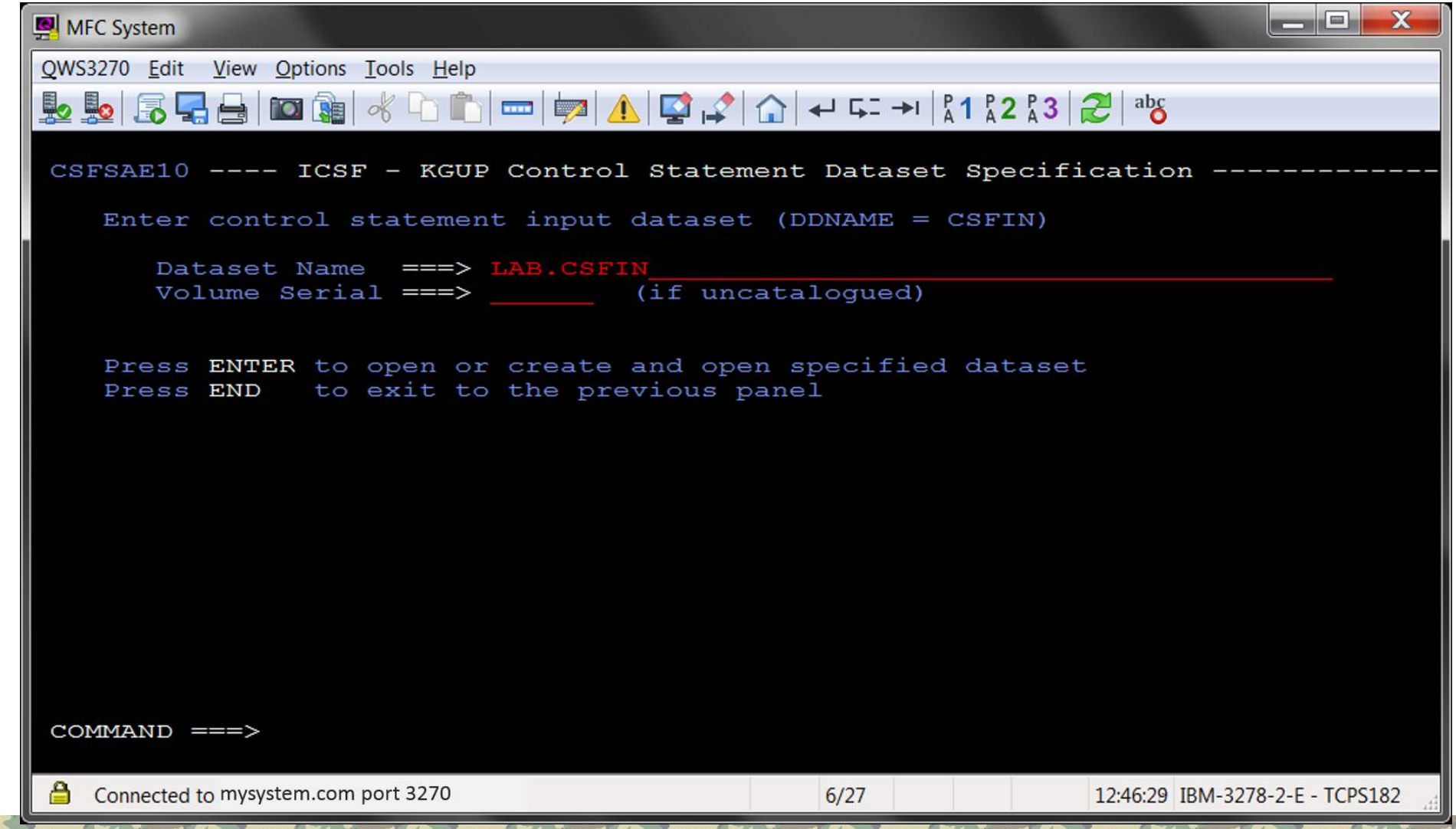
Specify Datasets - Completed



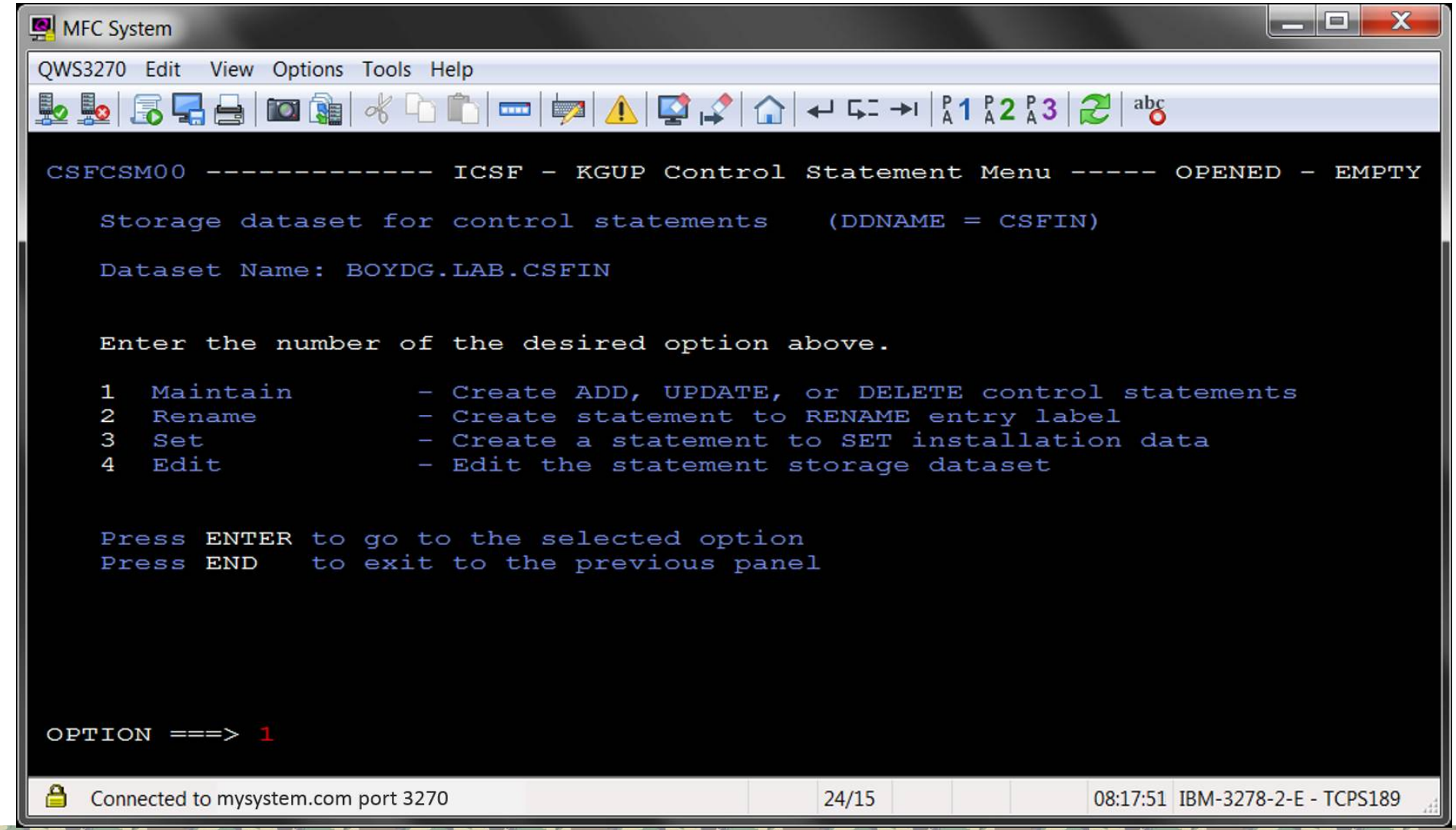
Create the control statements



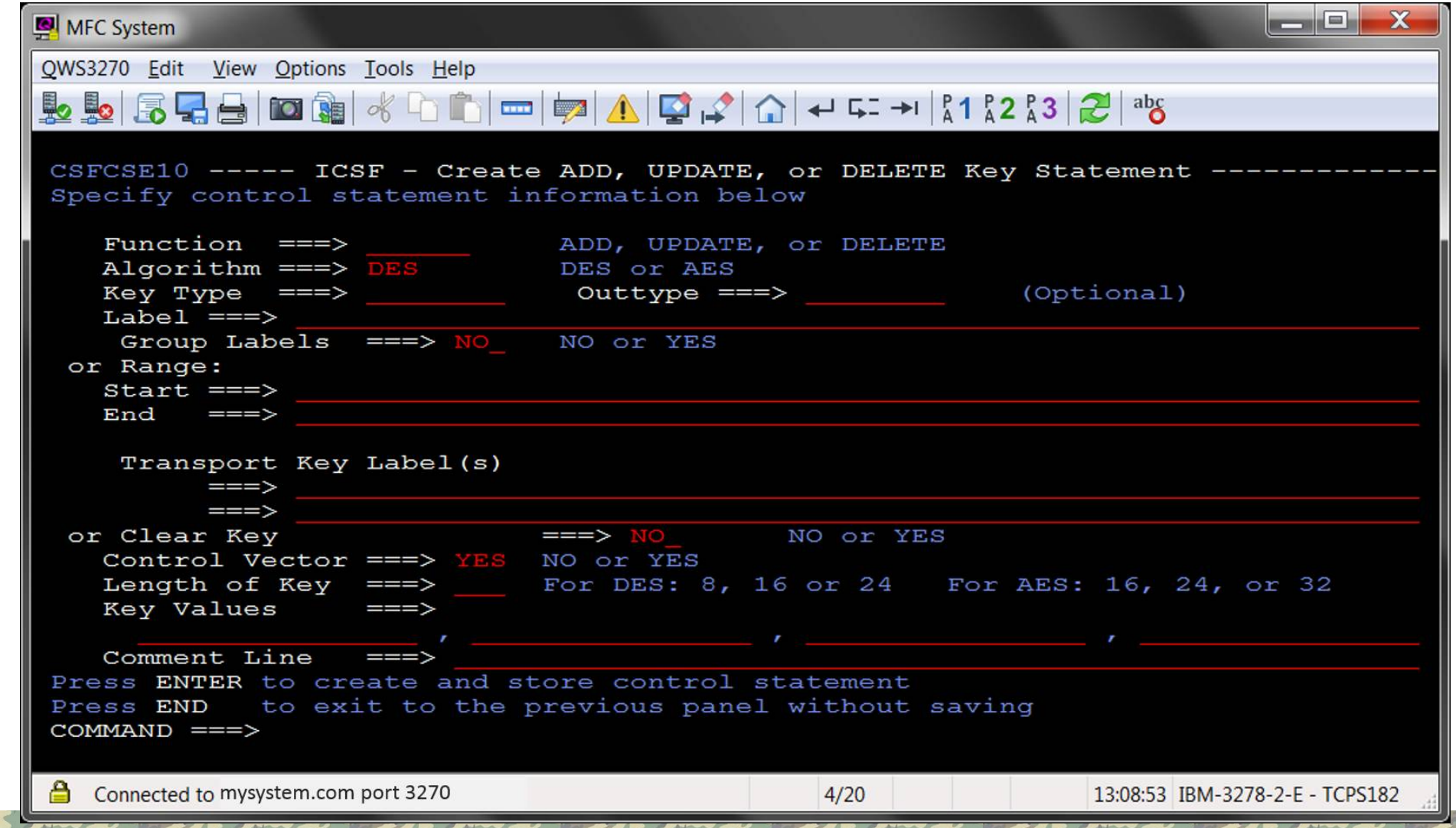
Confirm the CSFIN Data Set



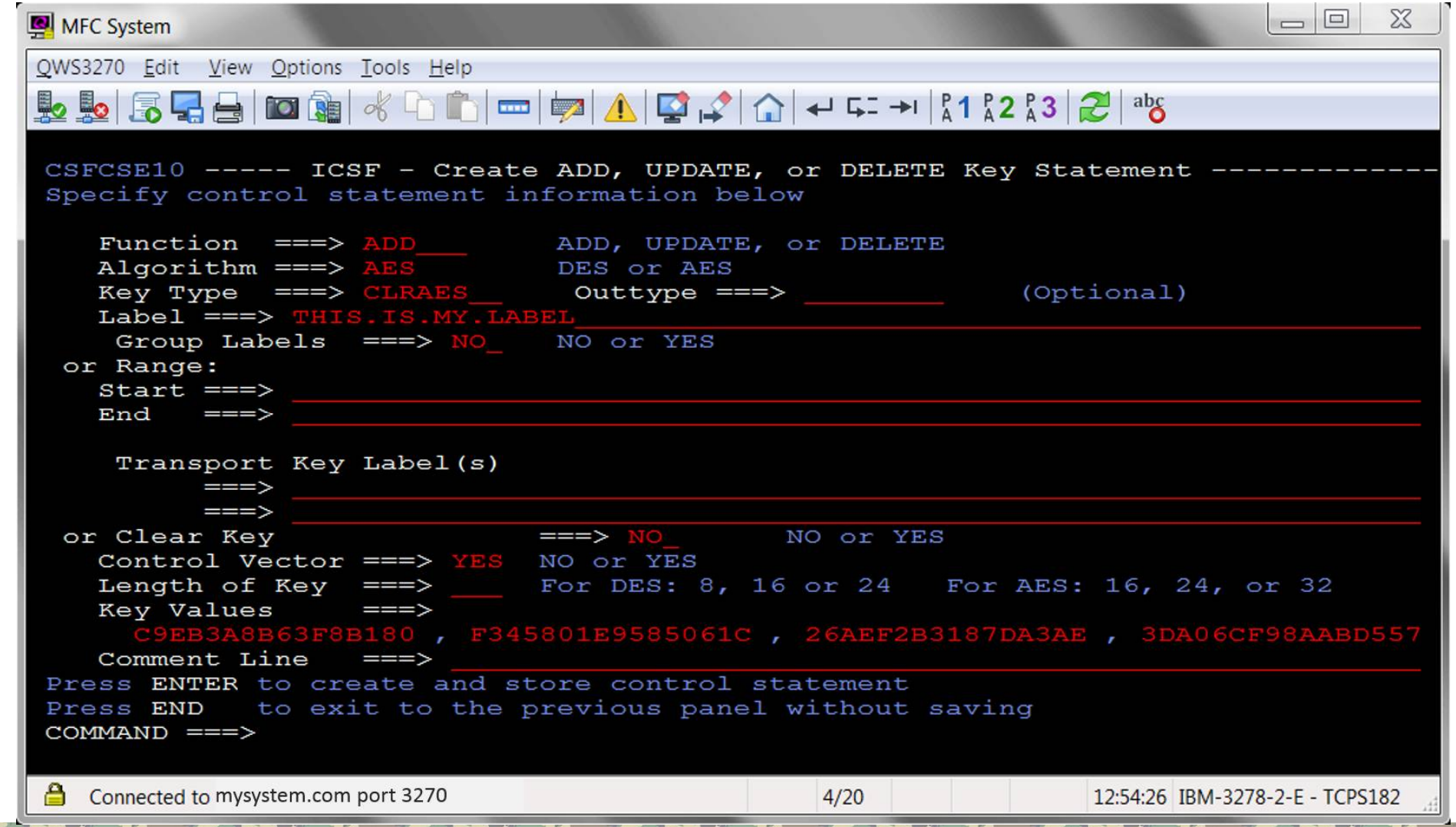
KGUP Control Statement Menu



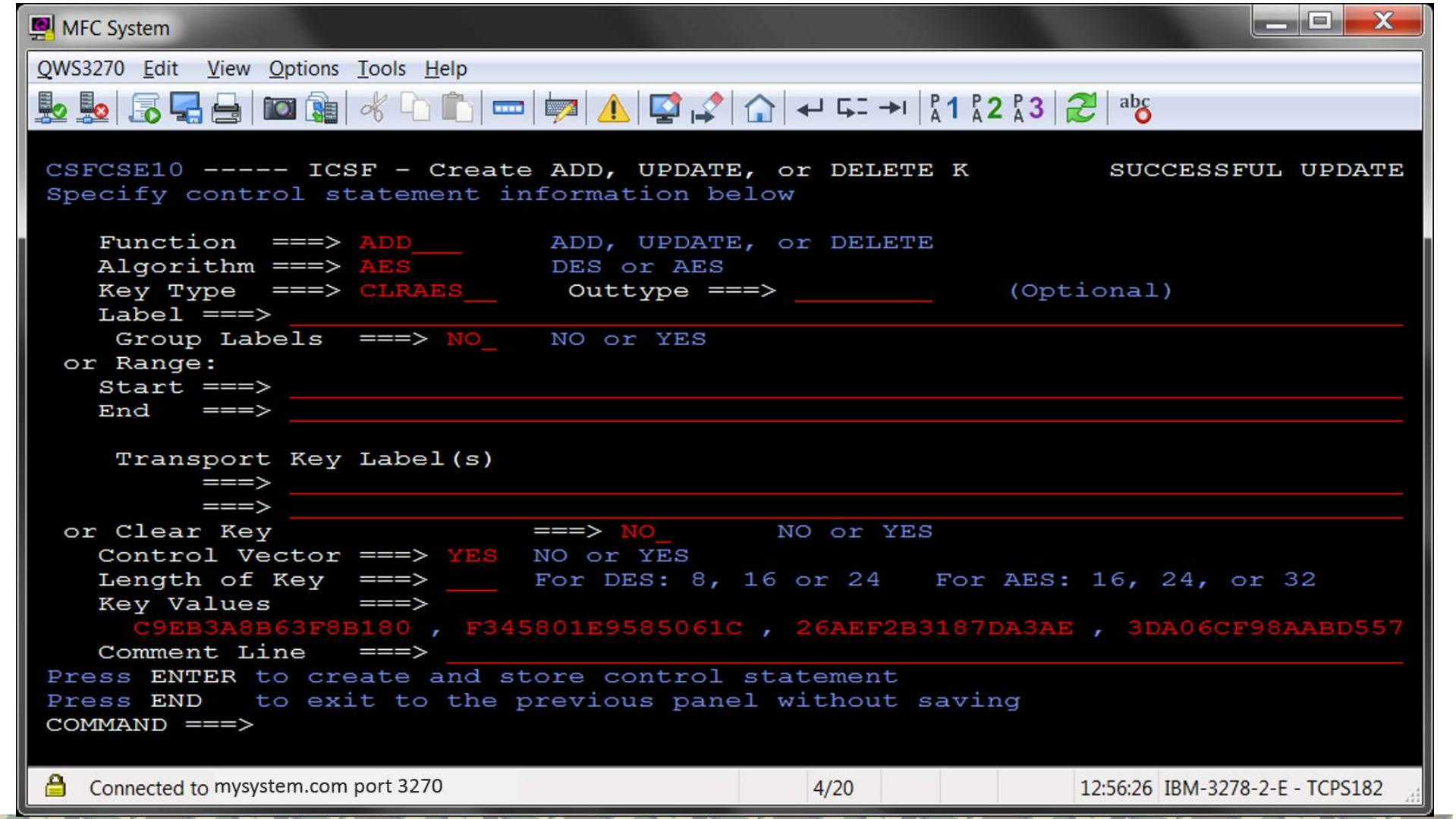
Create a KGUP Control Statement



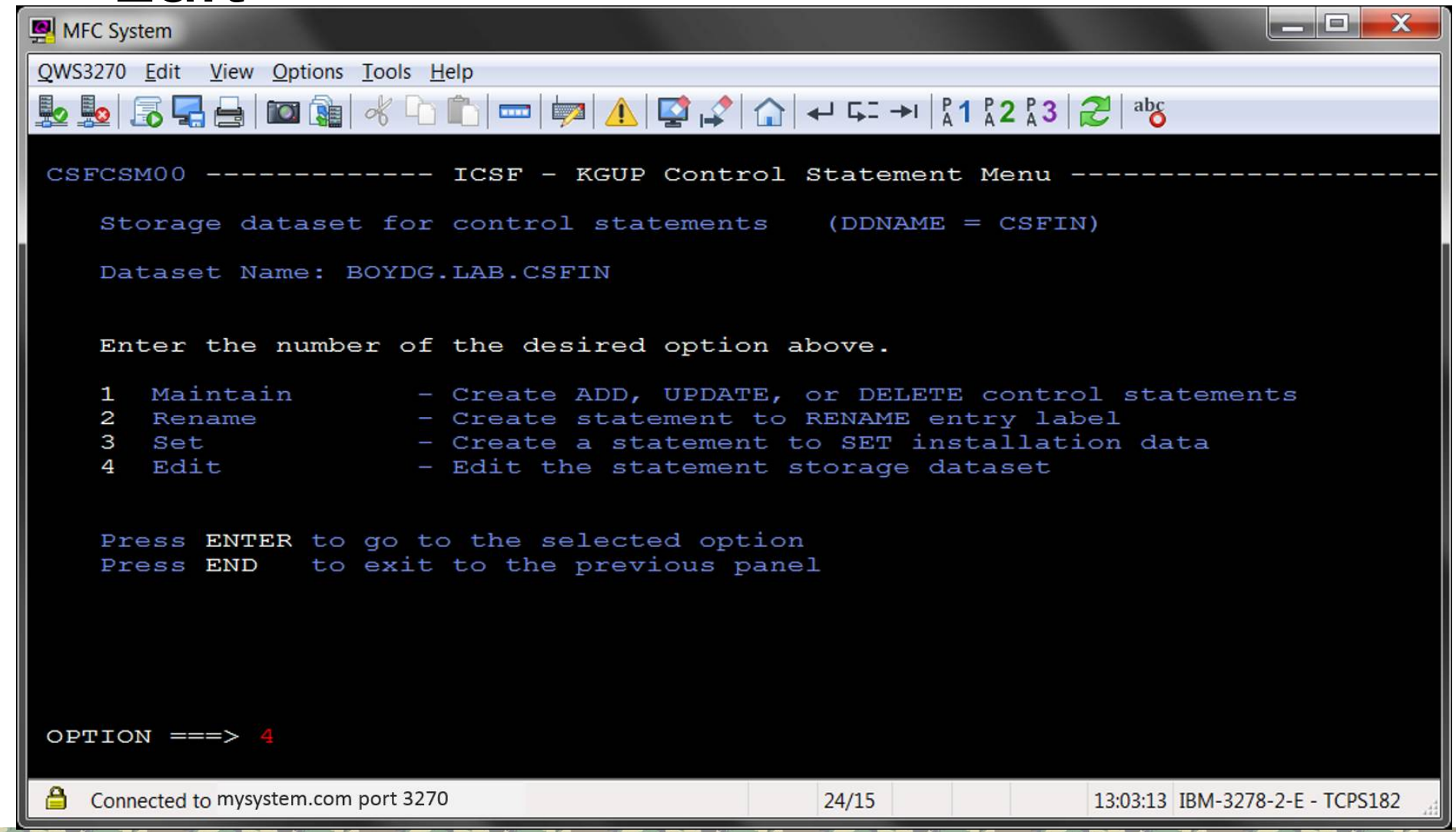
Add an AES Clear Key



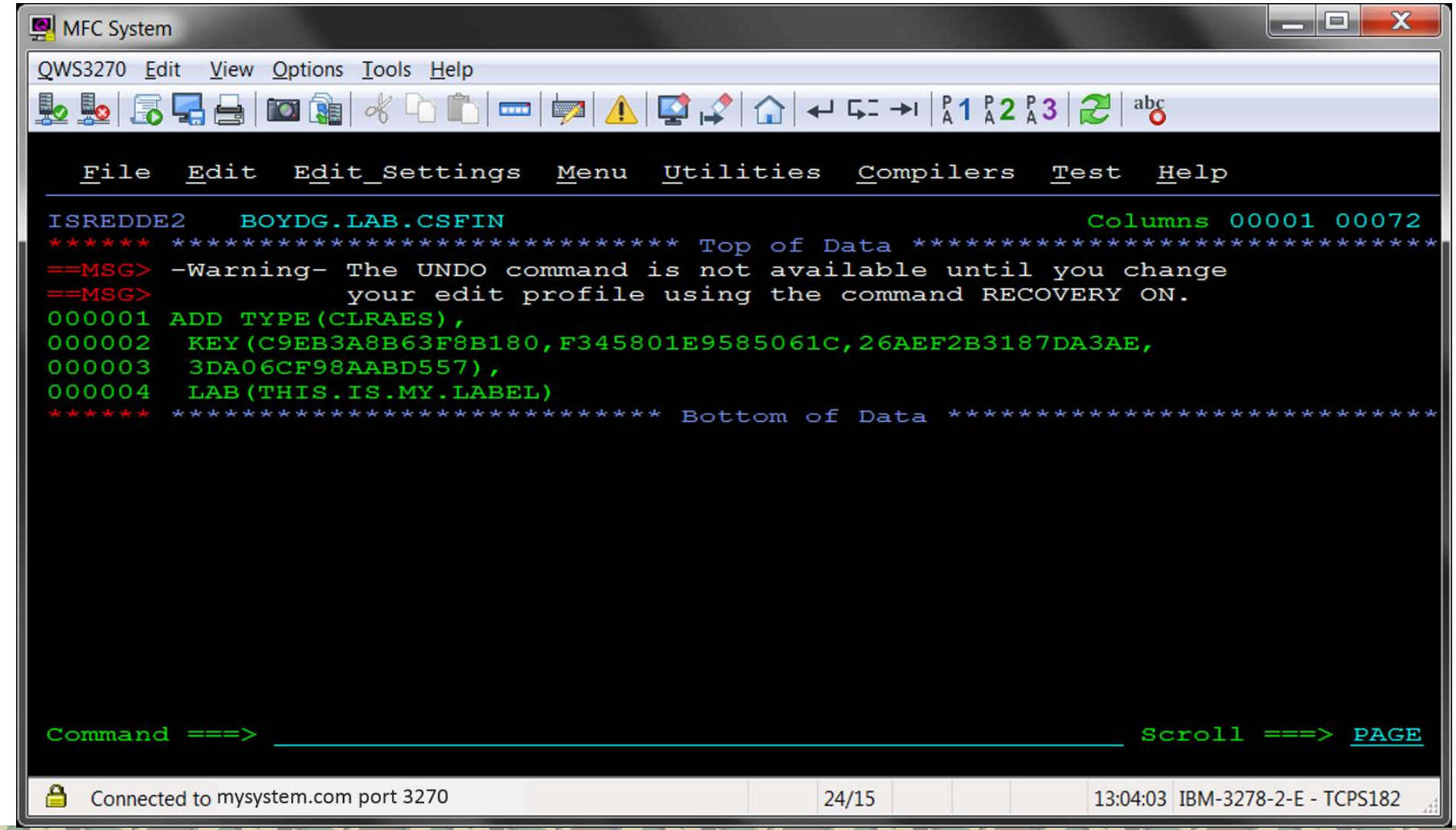
Add - Successful



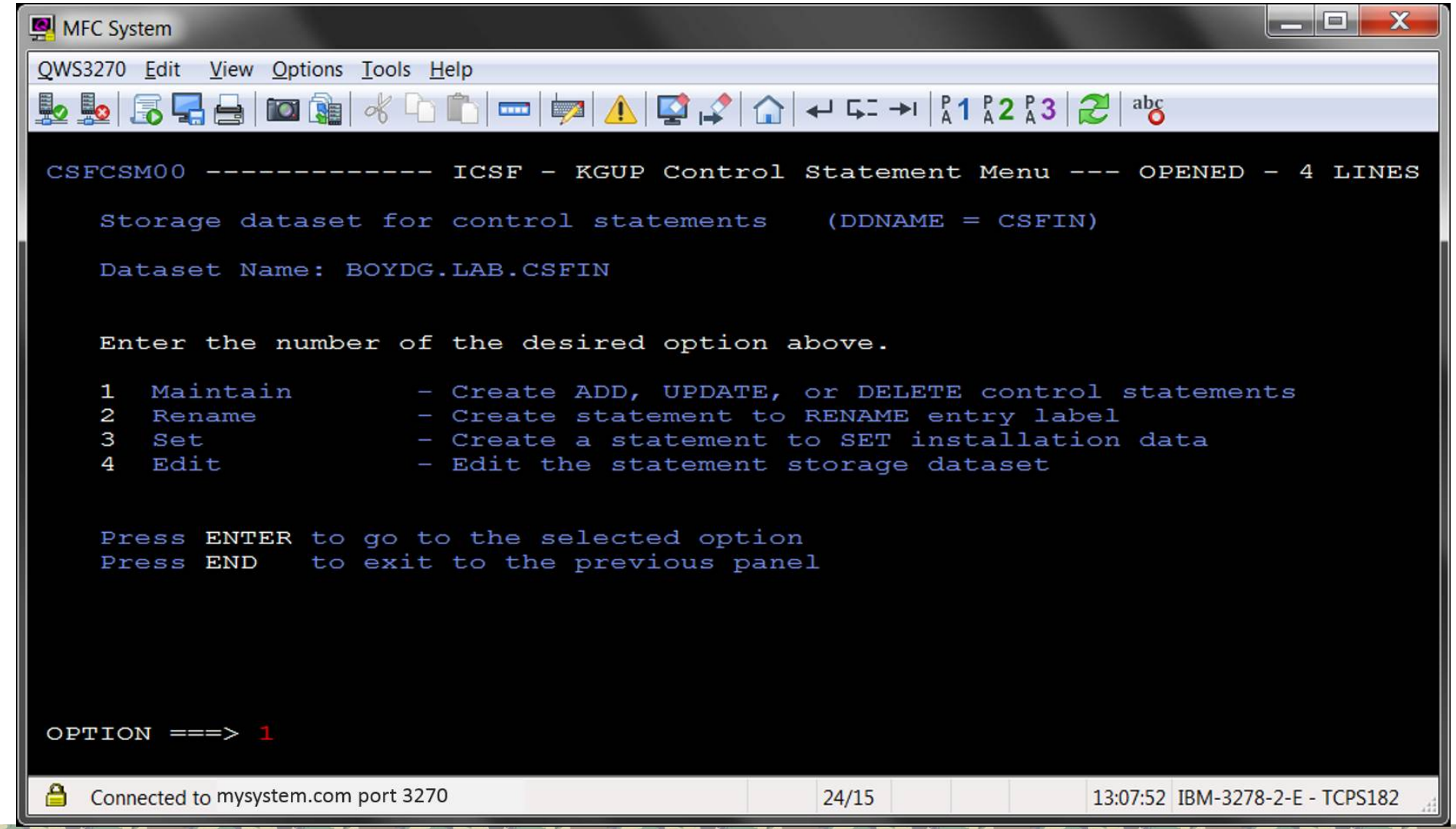
KGUP Control Statement Menu - Edit



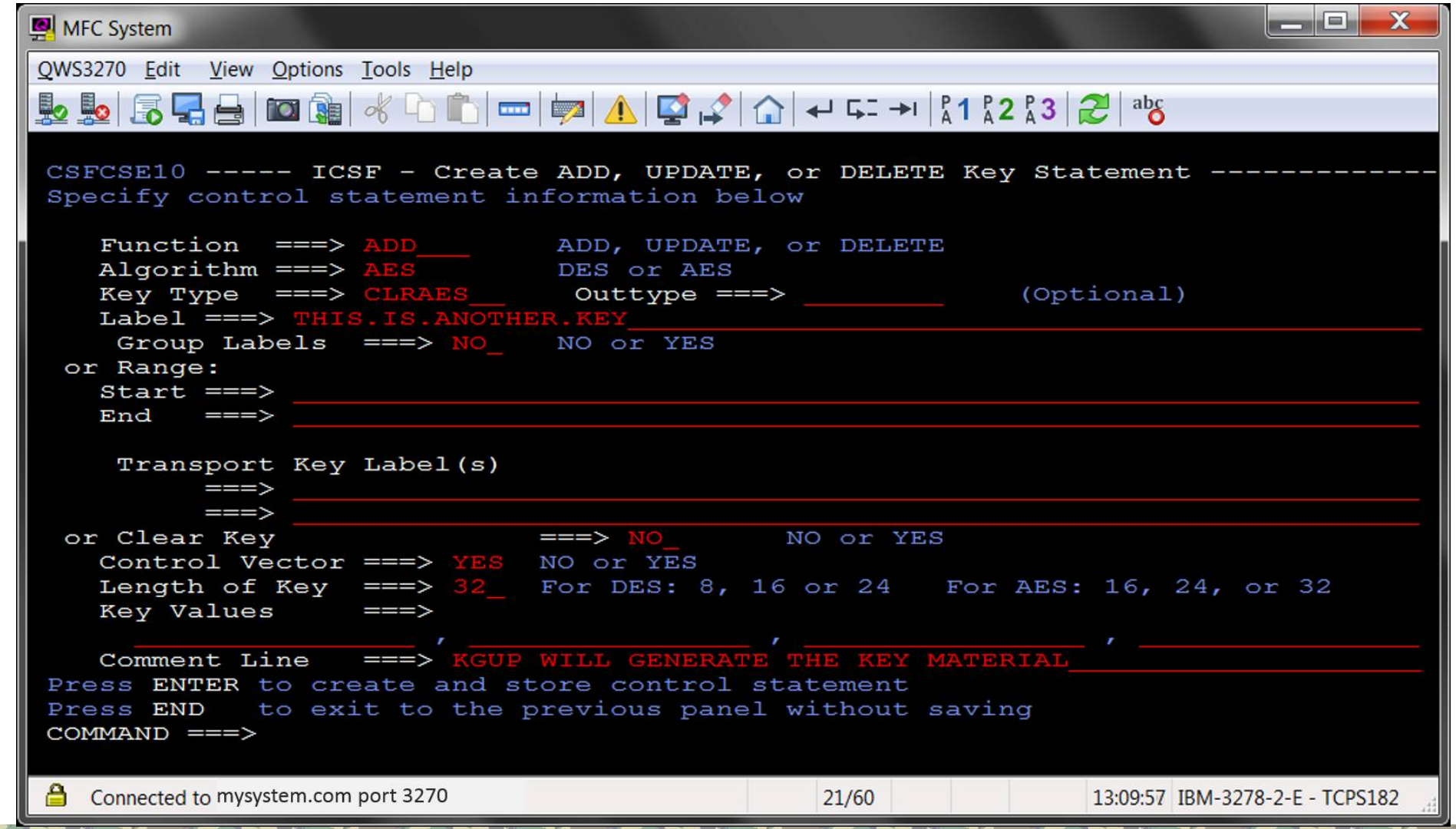
Edit CSFIN


MFC System
QWS3270 Edit View Options Tools Help
File Edit Edit_Settings Menu Utilities Compilers Test Help
ISREDDE2 BOYDG.LAB.CSFIN Columns 00001 00072
****** ********** Top of Data **********
==MSG> -Warning- The UNDO command is not available until you change
==MSG> your edit profile using the command RECOVERY ON.
000001 ADD TYPE(CLRAES),
000002 KEY(C9EB3A8B63F8B180,F345801E9585061C,26AEF2B3187DA3AE,
000003 3DA06CF98AABD557),
000004 LAB(THIS.IS.MY.LABEL)
****** ********** Bottom of Data **********
Command ===> Scroll ===> PAGE
Connected to mysystem.com port 3270
24/15
13:04:03 IBM-3278-2-E - TCPS182

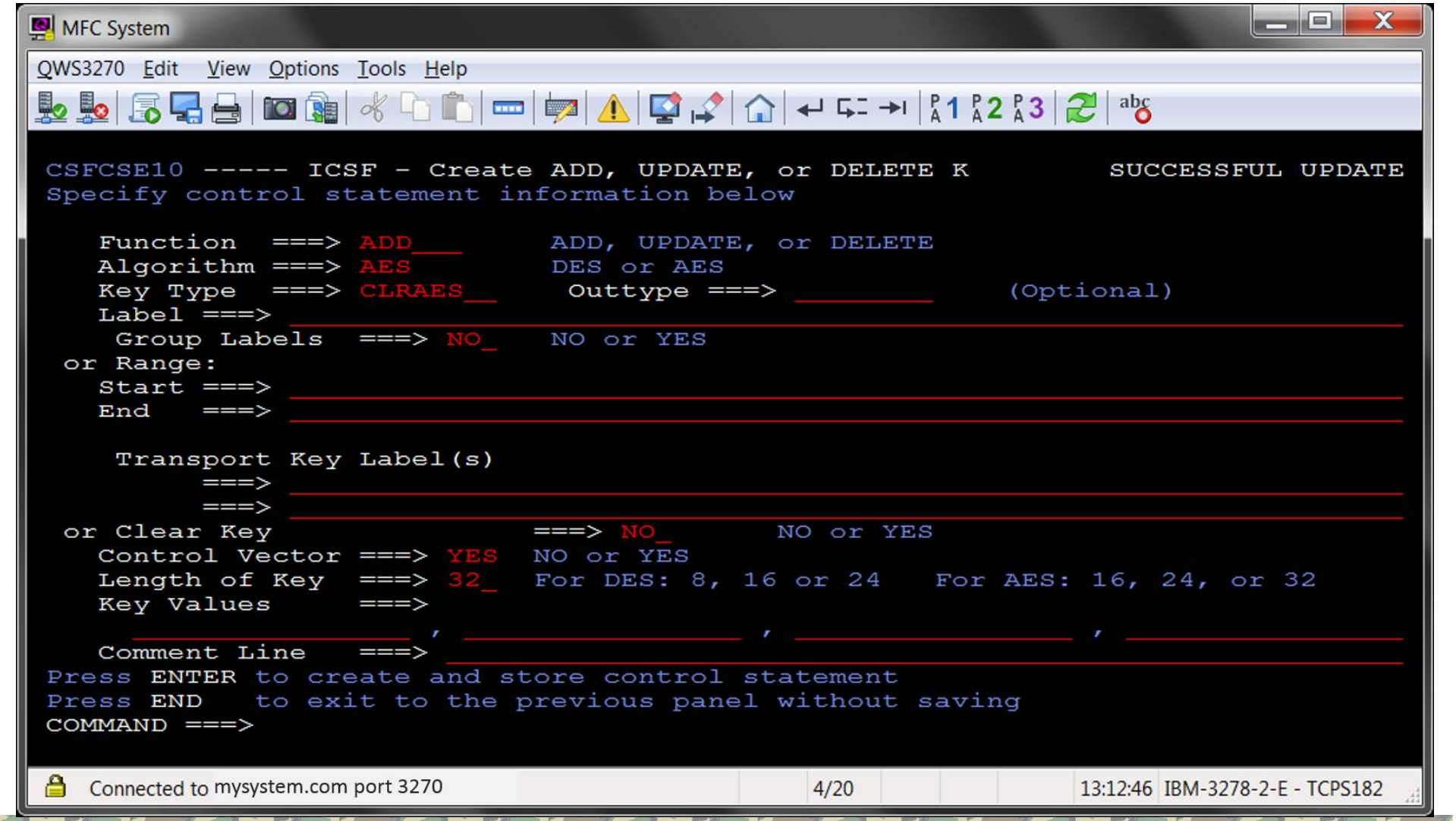
KGUP Control Statement Menu



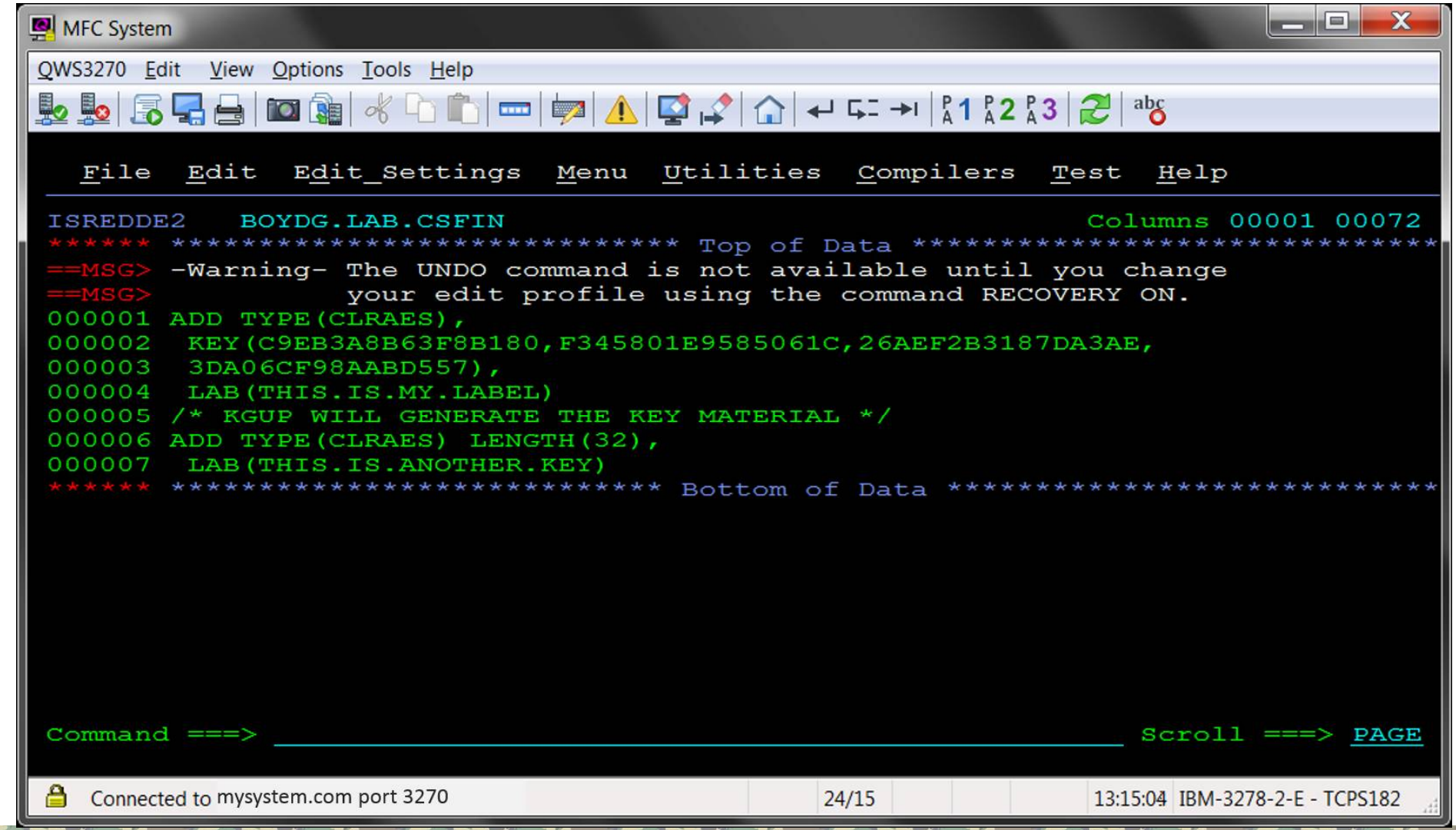
Add another AES Clear Key



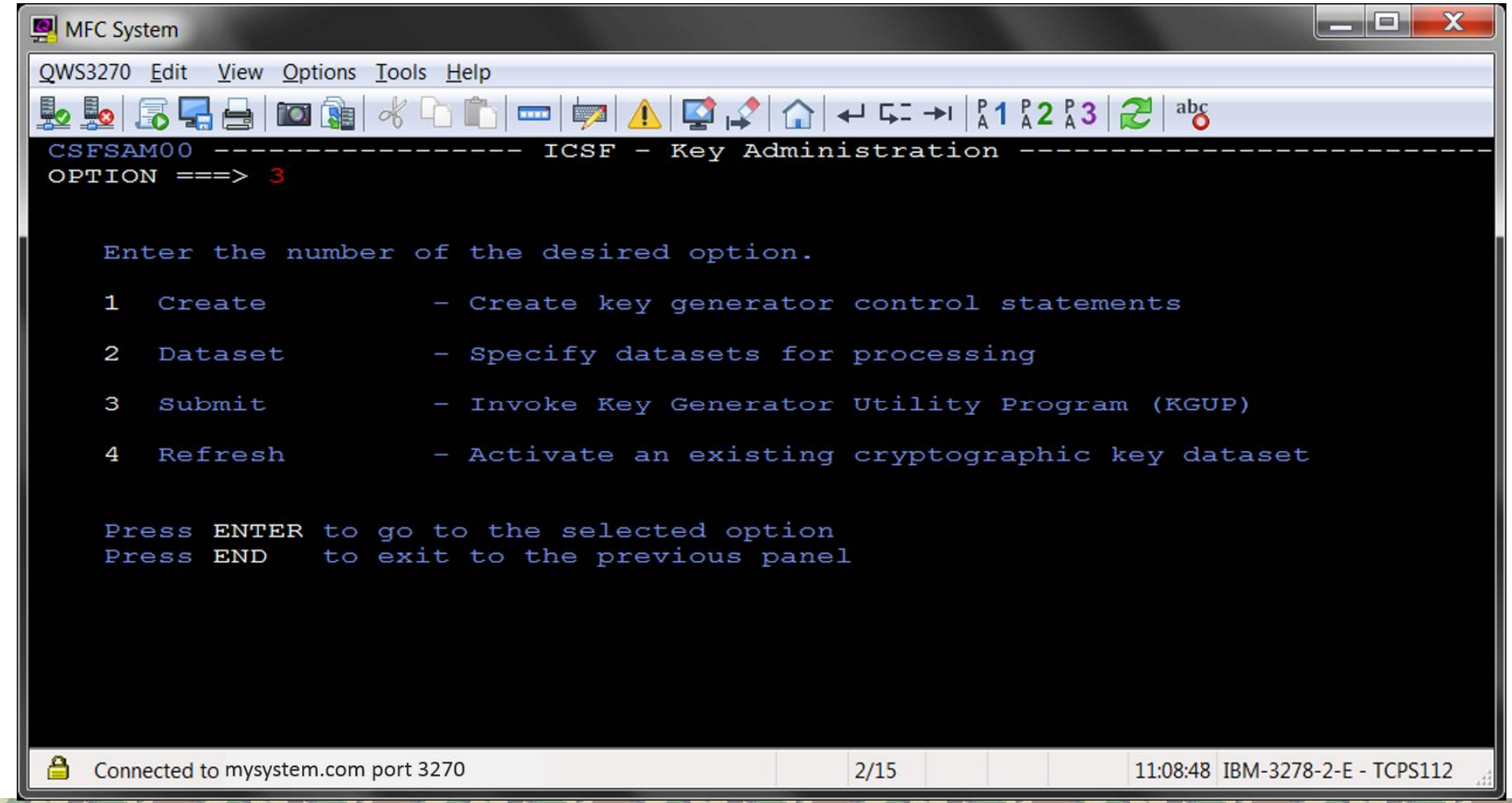
Add - Successful



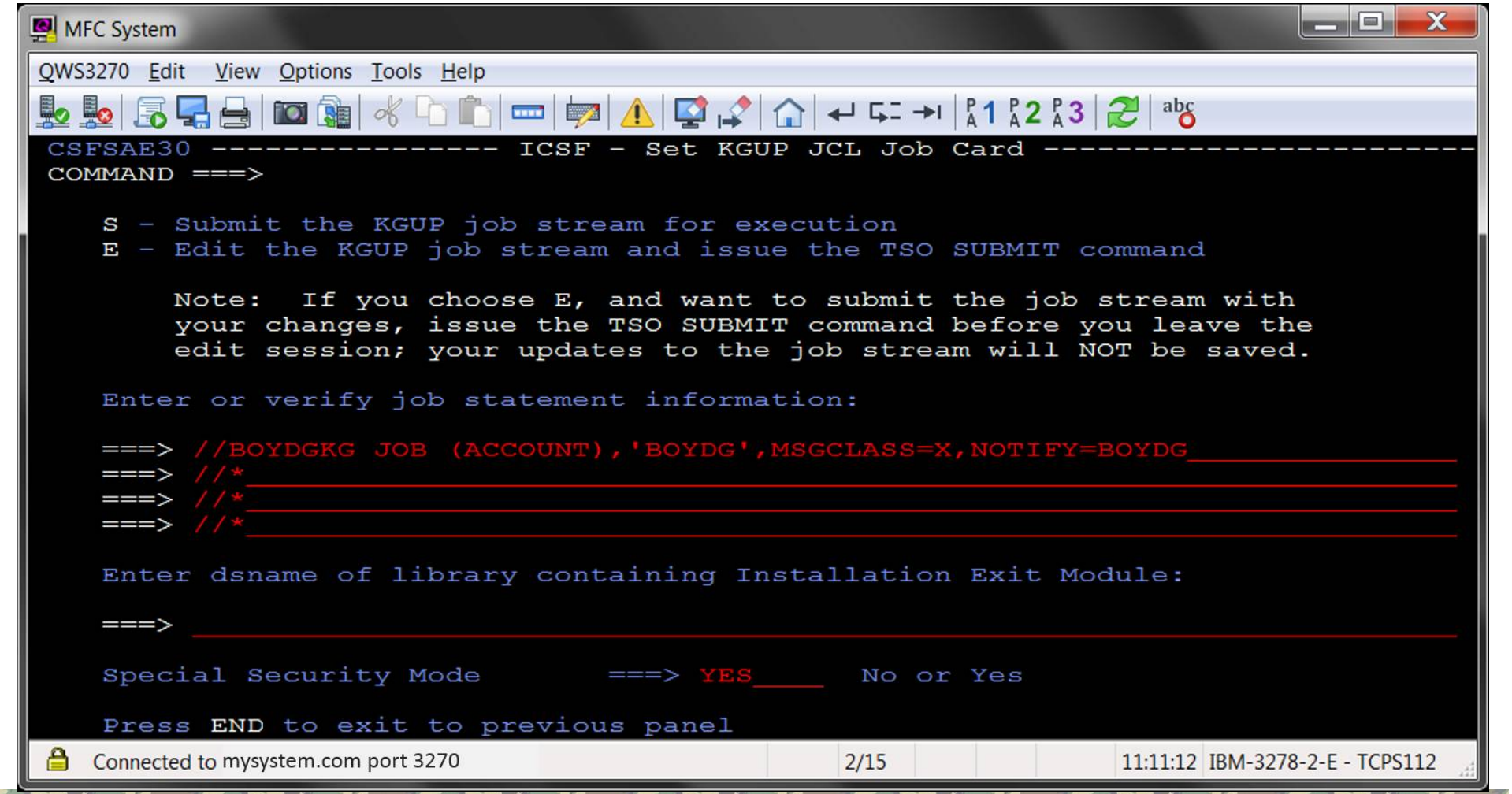
Edit CSFIN


MFC System
QWS3270 Edit View Options Tools Help
File Edit Edit_Settings Menu Utilities Compilers Test Help
ISREDDE2 BOYDG.LAB.CSFIN Columns 00001 00072
****** ******************************** Top of Data ********************************
==MSG> -Warning- The UNDO command is not available until you change
==MSG> your edit profile using the command RECOVERY ON.
000001 ADD TYPE(CLRAES),
000002 KEY(C9EB3A8B63F8B180,F345801E9585061C,26AEF2B3187DA3AE,
000003 3DA06CF98AABD557),
000004 LAB(THIS.IS.MY.LABEL)
000005 /* KGUP WILL GENERATE THE KEY MATERIAL */
000006 ADD TYPE(CLRAES) LENGTH(32),
000007 LAB(THIS.IS.ANOTHER.KEY)
****** ***************************** Bottom of Data ******************************
Command ===> Scroll ===> PAGE
Connected to mysystem.com port 3270
24/15
13:15:04 IBM-3278-2-E - TCPS182

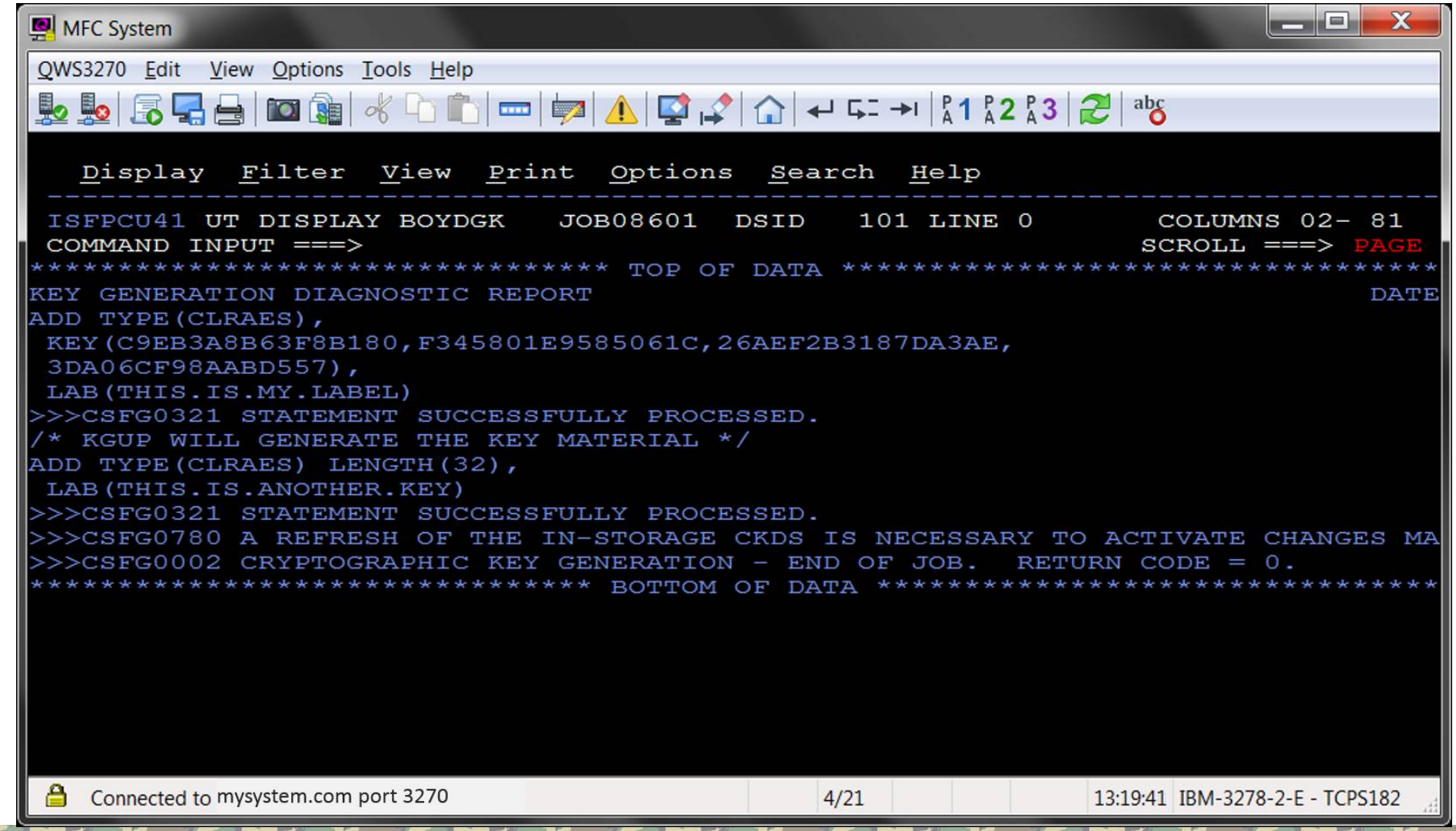
KGUP Key Administration - Submit



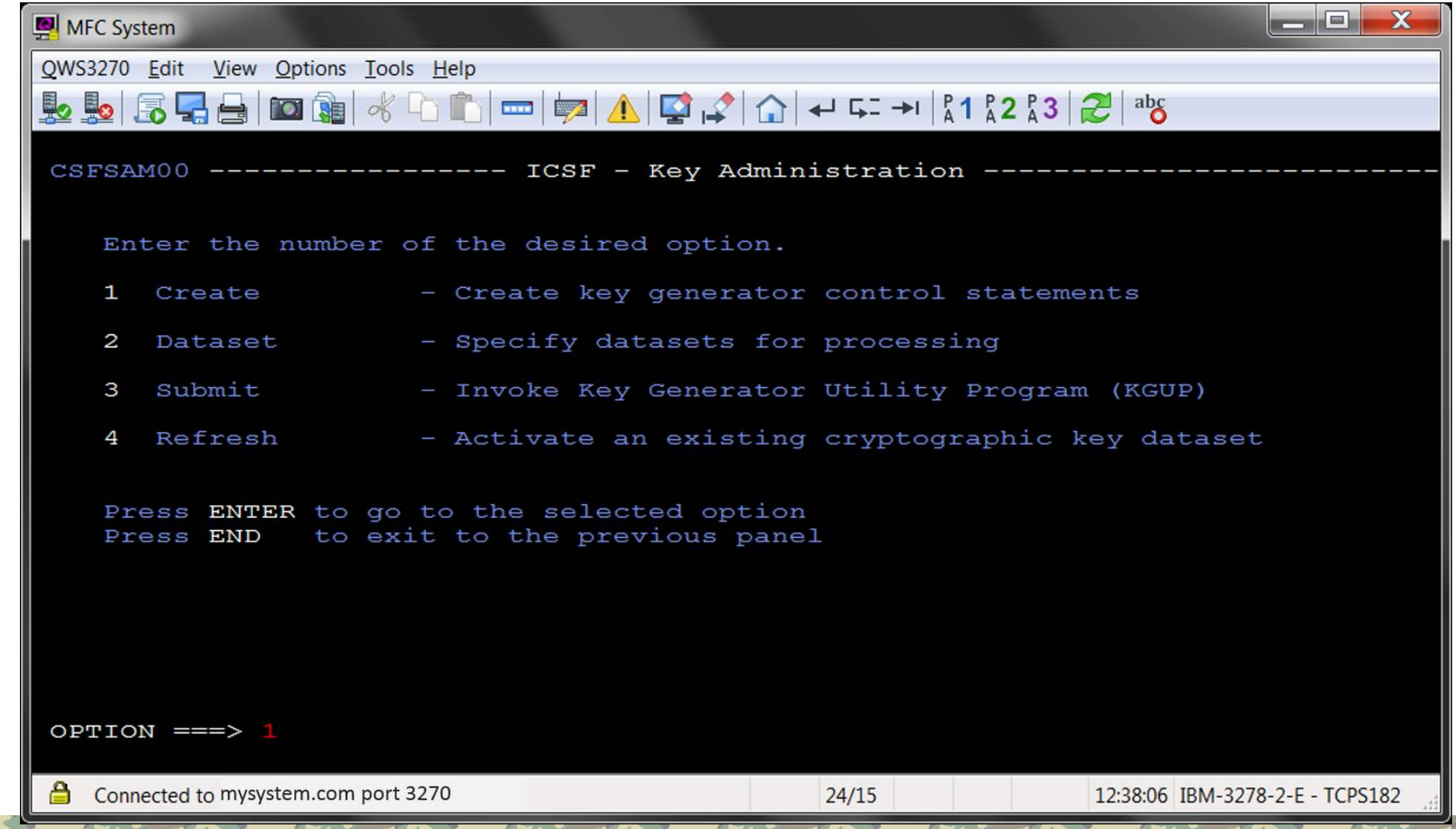
KGUP JCL


MFC System
QWS3270 Edit View Options Tools Help
CSFSAE30 ICSF - Set KGUP JCL Job Card
COMMAND ===>
S - Submit the KGUP job stream for execution
E - Edit the KGUP job stream and issue the TSO SUBMIT command
Note: If you choose E, and want to submit the job stream with your changes, issue the TSO SUBMIT command before you leave the edit session; your updates to the job stream will NOT be saved.
Enter or verify job statement information:
===> //BOYDGKG JOB (ACCOUNT),'BOYDG',MSGCLASS=X,NOTIFY=BOYDG
===> //*
===> //*
===> //*
Enter dsname of library containing Installation Exit Module:
===>
Special Security Mode ===> YES No or Yes
Press END to exit to previous panel
Connected to mysystem.com port 3270
2/15
11:11:12
IBM-3278-2-E - TCPS112

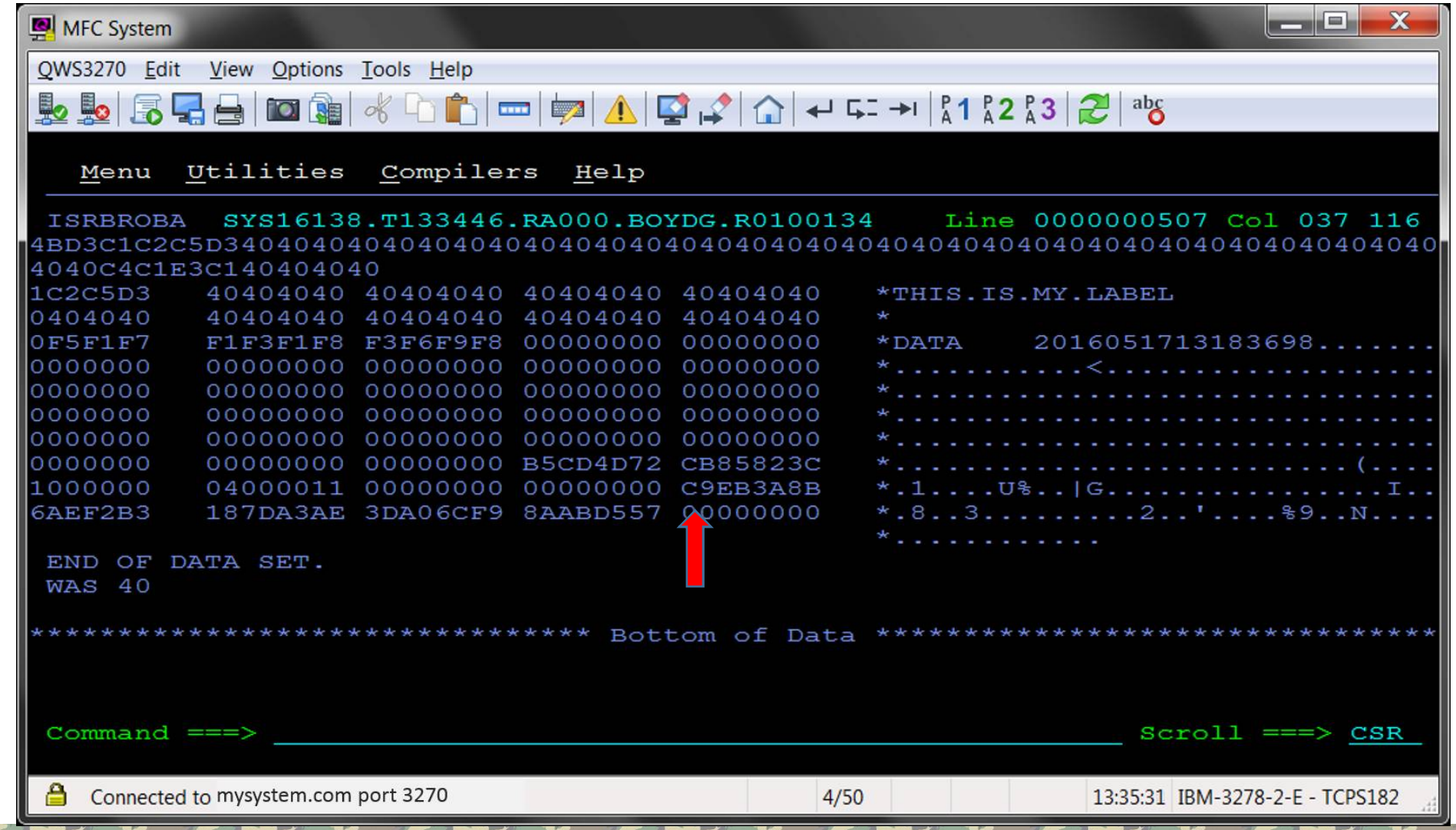
KGUP Diagnostics



REFRESH from the KGUP panels

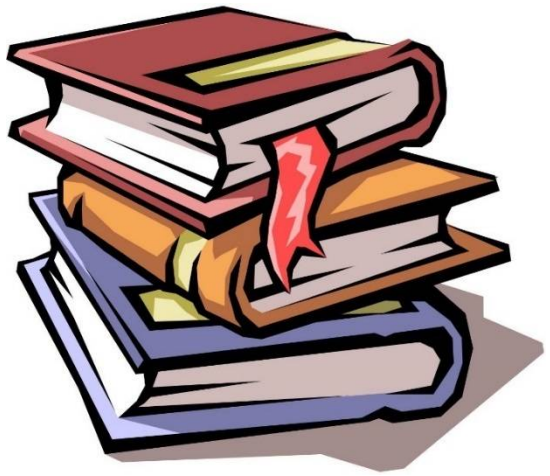


KEY in the CKDS



References

- ICSF Administrator's Guide
  - SC14-7506 (HCR77A1 & later)
  - SA22-7521 (prior versions of ICSF & z/OS)
- ICSF Application Programmer's Guide
  - SC14-7508 (HCR77A1 & later)
  - SA22-7523 (prior versions of ICSF & z/OS)




QUESTIONS
?