



MAINFRAME
CRYPTO

ICSF Keys and KGUP

Greg Boyd

gregboyd@mainframecrypto.com

www.mainframecrypto.com

zExchange – Keys and KGUP

July 2016

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

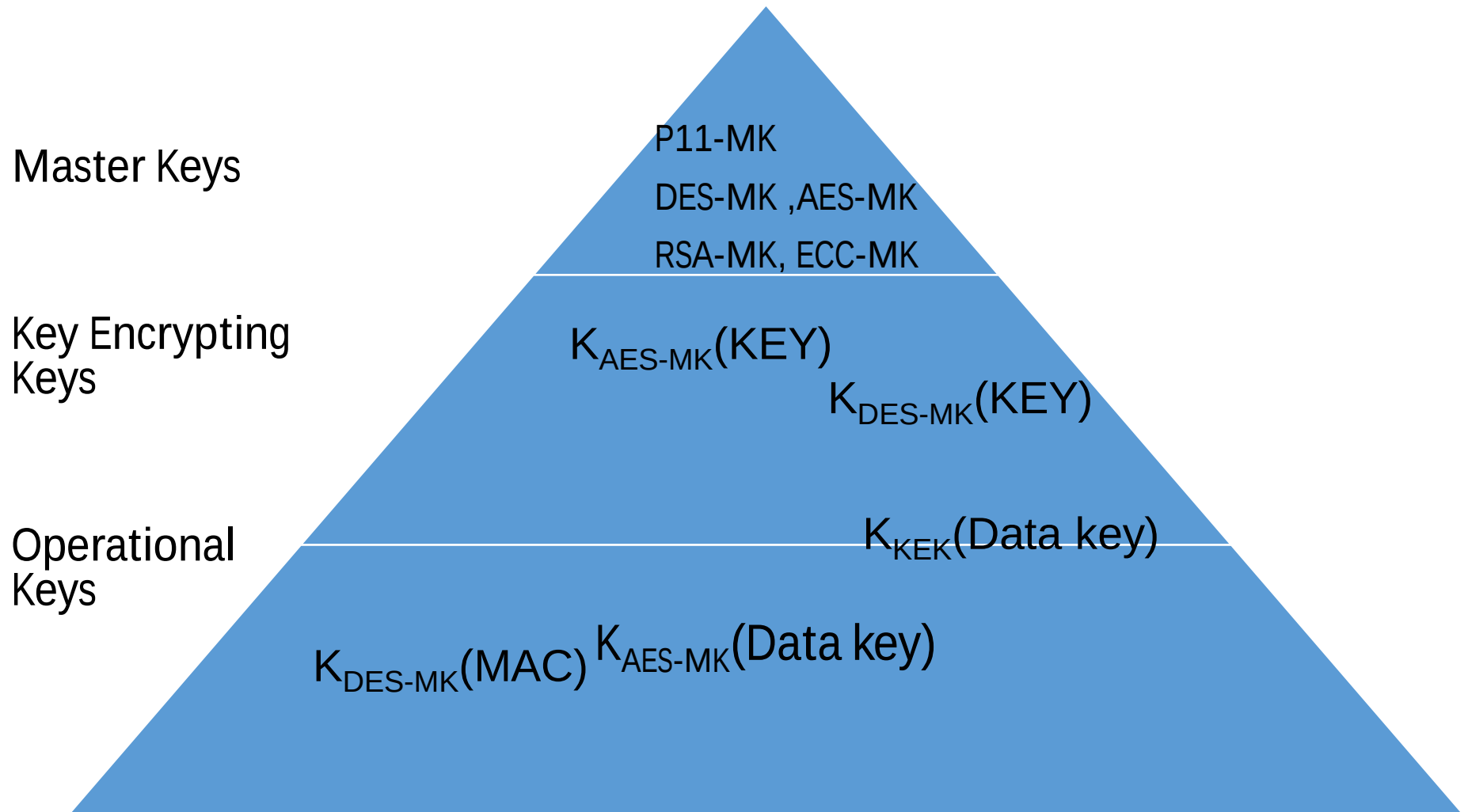
. . . And Trademarks

- 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



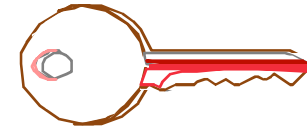
Operational Keys (cont.)

	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

```

MFC System
QWS3270 Edit View Options Tools Help
-----
HCR77B0 ----- Integrated Cryptographic Service Facility -----
Enter the number of the desired option.

 1 COPROCESSOR MGMT - Management of Cryptographic Coprocessors
 2 KDS MANAGEMENT  - Master key set or change, KDS Processing
 3 OPSTAT           - Installation options
 4 ADMINCNTL        - Administrative Control Functions
 5 UTILITY           - ICSF Utilities
 6 PPINIT           - Pass Phrase Master Key/KDS Initialization
 7 TKE              - TKE PKA Direct Key Load
 8 KGUP             - Key Generator Utility processes
 9 UDX MGMT         - Management of User Defined Extensions

Licensed Materials - Property of IBM
5650-ZOS Copyright IBM Corp. 1989, 2015.
US Government Users Restricted Rights - Use, duplication or
disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

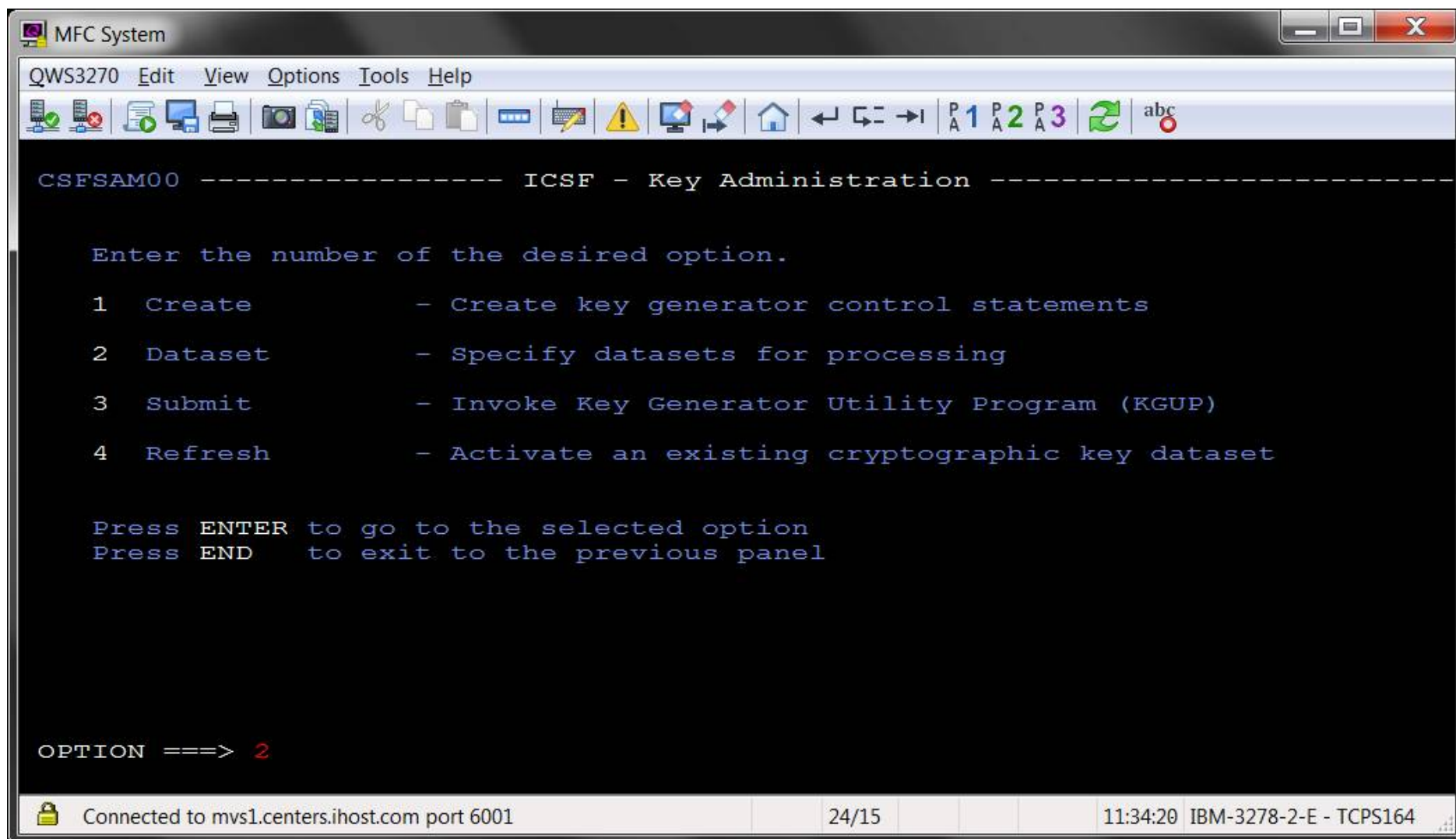
Press ENTER to go to the selected option.
Press END   to exit to the previous menu.

OPTION ==> 8_

Connected to mysystem.com port 3270      24/15      08:00:04 IBM-3278-2-E - TCPS161

```

KGUP – Key Administration Menu



```

MFC System
QWS3270 Edit View Options Tools Help
[Icons: File Explorer, Print, etc.]
CSFSAM00 ----- ICSF - Key Administration -----

Enter the number of the desired option.

1  Create          - Create key generator control statements
2  Dataset         - Specify datasets for processing
3  Submit          - Invoke Key Generator Utility Program (KGUP)
4  Refresh         - Activate an existing cryptographic key dataset

Press ENTER to go to the selected option
Press END   to exit to the previous panel

OPTION ==> 2

[Footer: Connected to mvs1.centers.ihost.com port 6001 | 24/15 | 11:34:20 IBM-3278-2-E - TCPS164]
  
```

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

MFC System

QWS3270 Edit View Options Tools Help

CSFSAE20 ----- ICSF - Specify KGUP Datasets -----

Enter dataset names for all cryptographic files.
Cryptographic Keys (DDNAME = CSFCKDS)
Dataset Name ==> _____

Control Statement Input (DDNAME = CSFIN)
Dataset Name ==> _____
Volume Serial ==> _____ (if uncataloged)

Diagnostics (DDNAME = CSFDIAG) (use * for printer)
Dataset Name ==> _____
Volume Serial ==> _____ (if uncataloged)

Key Output (DDNAME = CSFKEYS)
Dataset Name ==> _____
Volume Serial ==> _____ (if uncataloged)

Control Statement Output (DDNAME = CSFSTMNT)
Dataset Name ==> _____
Volume Serial ==> _____ (if uncataloged)

Press ENTER to set the dataset names. Press END to exit to the previous panel.
COMMAND ==>

Connected to mysystem.com port 3270 5/24 11:34:51 IBM-3278-2-E - TCPS164

Specify Datasets - Completed

```

MFC System
QWS3270 Edit View Options Tools Help
----- ICSF - Specify KGUP Datasets -----
COMMAND ==>

Enter dataset names for all cryptographic files.
Cryptographic Keys      (DDNAME = CSFCKDS)
  Dataset Name ==> ' MFCTEST1.CRYPTO.CKDS '

Control Statement Input  (DDNAME = CSFIN)
  Dataset Name ==> CSFIN.PDS (KEYOUT)
  Volume Serial ==>      (if uncataloged)

Diagnostics              (DDNAME = CSFDIAG) (use * for printer)
  Dataset Name ==> *
  Volume Serial ==>      (if uncataloged)

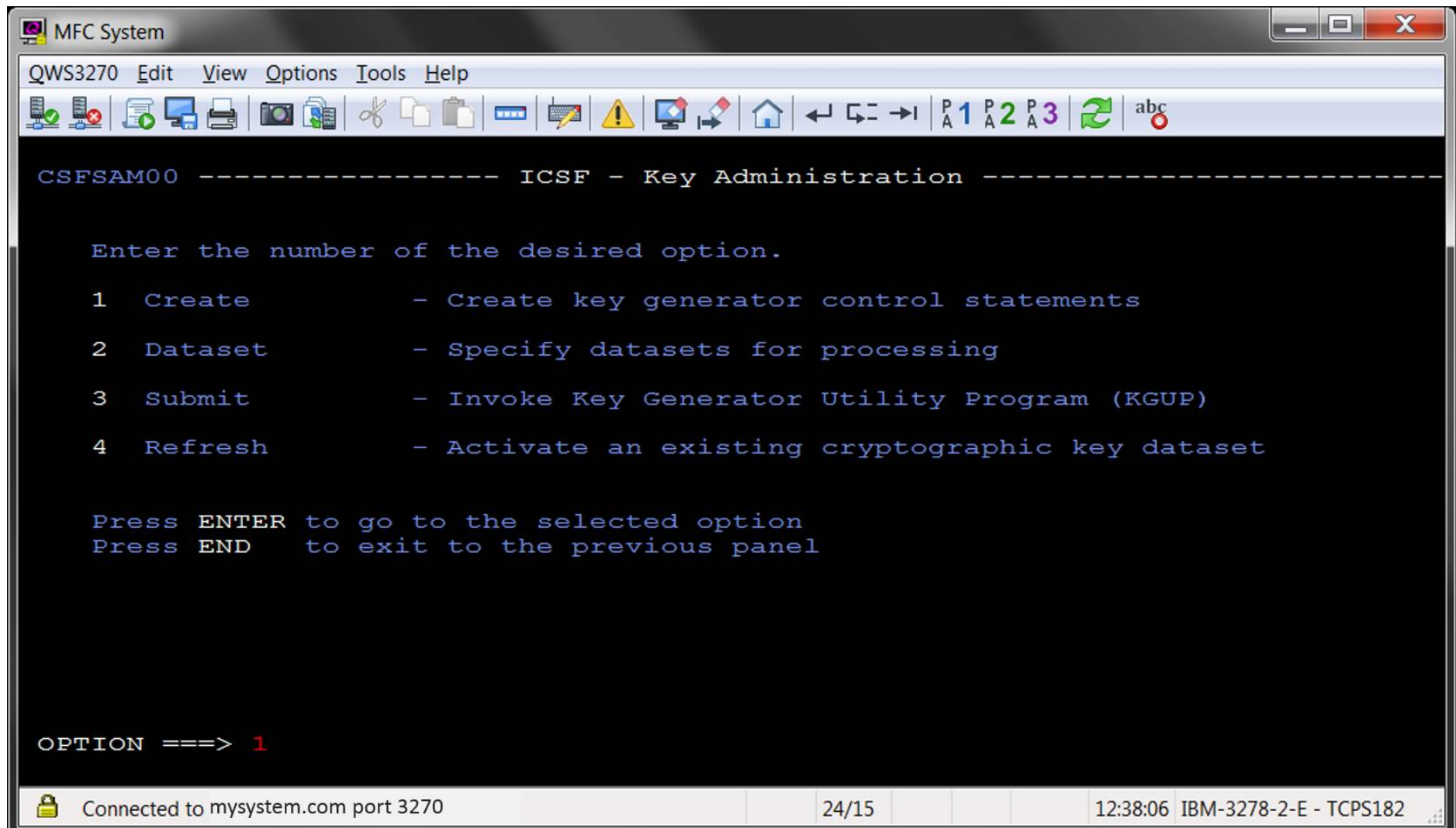
Key Output                (DDNAME = CSFKEYS)
  Dataset Name ==> CSFKEYS
  Volume Serial ==>      (if uncataloged)

Control Statement Output (DDNAME = CSFSTMNT)
  Dataset Name ==> CSFSTMT
  Volume Serial ==>      (if uncataloged)

Press ENTER to set the dataset names. Press END to exit to the previous panel.

Connected to mysystem.com port 3270 10/24 17:28:22 IBM-3278-2-E - TCPS109
  
```

Create the control statements



The screenshot shows a terminal window titled "MFC System" with a menu titled "ICSE - Key Administration". The menu lists four options: 1 Create, 2 Dataset, 3 Submit, and 4 Refresh. The user has entered '1' for the 'Create' option. The terminal also shows a status bar at the bottom indicating the connection to mysystem.com port 3270, the date 24/15, the time 12:38:06, and the system identifier IBM-3278-2-E - TCPS182.

```

MFC System
QWS3270 Edit View Options Tools Help
----- ICSE - Key Administration -----

Enter the number of the desired option.

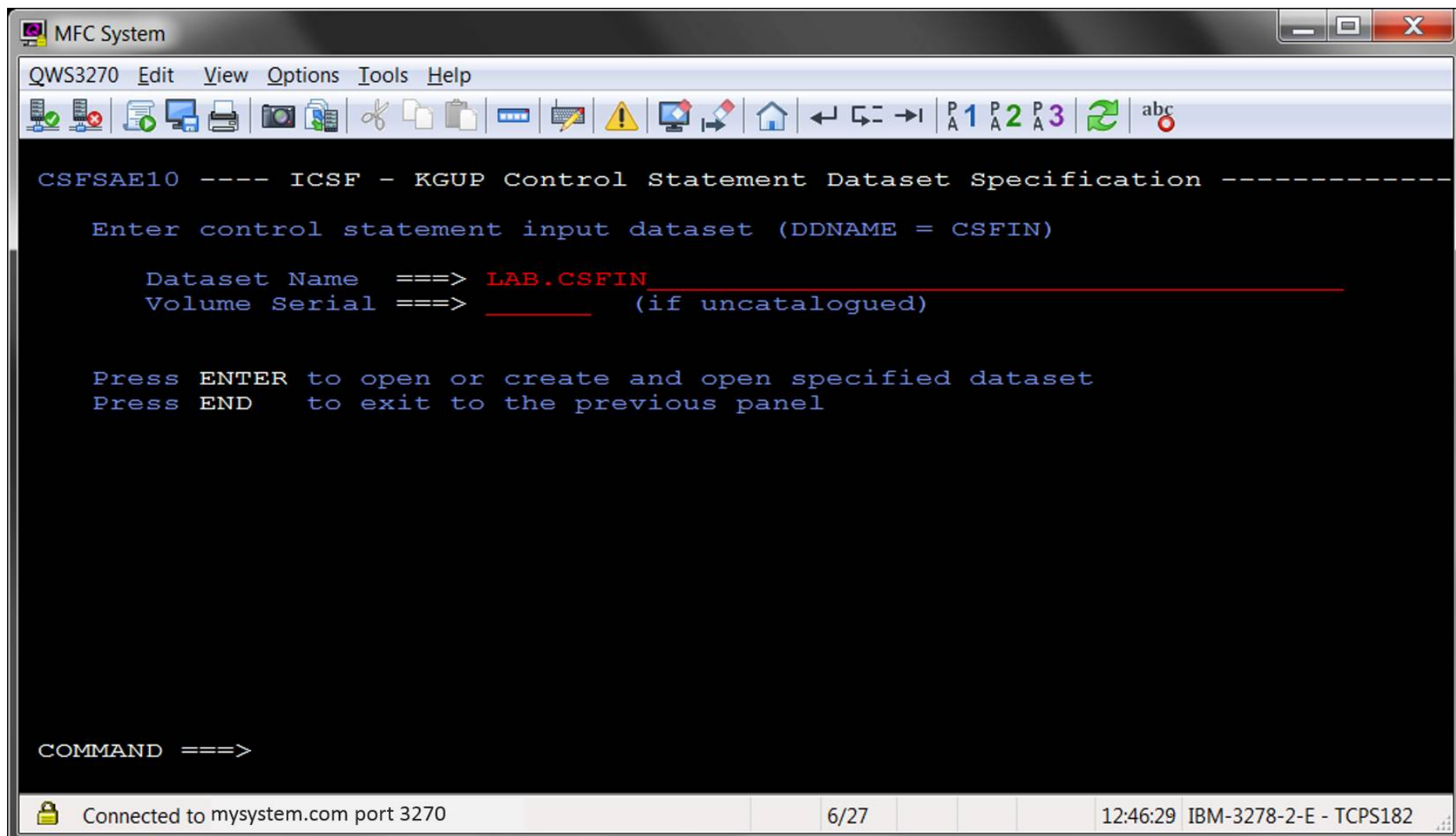
1 Create          - Create key generator control statements
2 Dataset         - Specify datasets for processing
3 Submit          - Invoke Key Generator Utility Program (KGUP)
4 Refresh         - Activate an existing cryptographic key dataset

Press ENTER to go to the selected option
Press END   to exit to the previous panel

OPTION ==> 1

Connected to mysystem.com port 3270      24/15      12:38:06 IBM-3278-2-E - TCPS182
  
```

Confirm the CSFIN Data Set



The screenshot shows a terminal window titled "MFC System" with a menu bar (QWS3270, Edit, View, Options, Tools, Help) and a toolbar. The main display area shows the following text:

```

CSFSAE10 ---- ICSF - KGUP Control Statement Dataset Specification -----
Enter control statement input dataset (DDNAME = CSFIN)

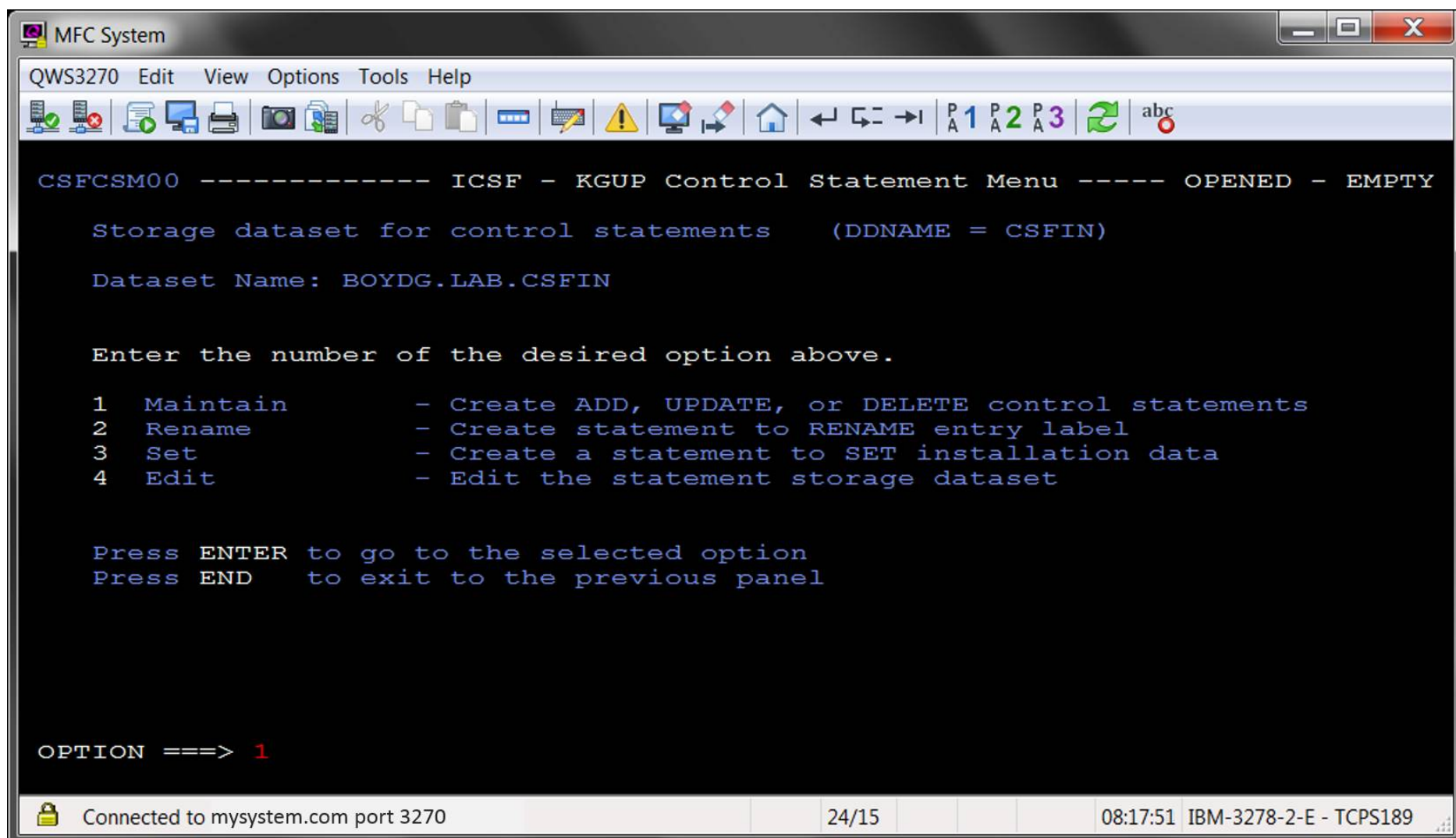
Dataset Name ==> LAB.CSFIN
Volume Serial ==> _____ (if uncatalogued)

Press ENTER to open or create and open specified dataset
Press END   to exit to the previous panel

COMMAND ==>
  
```

The status bar at the bottom of the window displays: "Connected to mysystem.com port 3270", "6/27", "12:46:29", and "IBM-3278-2-E - TCPS182".

KGUP Control Statement Menu



```

MFC System
QWS3270 Edit View Options Tools Help
CSFCSM00 ----- ICSF - KGUP Control Statement Menu ----- OPENED - EMPTY

Storage dataset for control statements      (DDNAME = CSFIN)

Dataset Name: BOYDG.LAB.CSFIN

Enter the number of the desired option above.

1  Maintain      - Create ADD, UPDATE, or DELETE control statements
2  Rename        - Create statement to RENAME entry label
3  Set           - Create a statement to SET installation data
4  Edit          - Edit the statement storage dataset

Press ENTER to go to the selected option
Press END   to exit to the previous panel

OPTION ==> 1

Connected to mysystem.com port 3270      24/15      08:17:51 IBM-3278-2-E - TCPS189
  
```

Create a KGUP Control Statement

MFC System

QWS3270 Edit View Options Tools Help

CSFCSE10 ----- ICSF - Create ADD, UPDATE, or DELETE Key Statement -----
Specify control statement information below

Function ==> _____ ADD, UPDATE, or DELETE
 Algorithm ==> DES DES or AES
 Key Type ==> _____ Outtype ==> _____ (Optional)
 Label ==> _____
 Group Labels ==> NO_ NO or YES
 or Range:
 Start ==> _____
 End ==> _____
 Transport Key Label(s)
 ==> _____
 ==> _____
 or Clear Key ==> NO_ NO or YES
 Control Vector ==> YES NO or YES
 Length of Key ==> _____ For DES: 8, 16 or 24 For AES: 16, 24, or 32
 Key Values ==> _____
 _____ , _____ , _____ , _____
 Comment Line ==> _____
 Press ENTER to create and store control statement
 Press END to exit to the previous panel without saving
 COMMAND ==>

Connected to mysystem.com port 3270 4/20 13:08:53 IBM-3278-2-E - TCPS182

Add an AES Clear Key

MFC System

QWS3270 Edit View Options Tools Help

CSFCSE10 ----- ICSF - Create ADD, UPDATE, or DELETE Key Statement -----
Specify control statement information below

Function ==> **ADD**_____ ADD, UPDATE, or DELETE
 Algorithm ==> **AES**_____ DES or AES
 Key Type ==> **CLRAES**_____ Outtype ==> _____ (Optional)
 Label ==> **THIS.IS.MY.LABEL**_____
 Group Labels ==> **NO**_____ NO or YES

or Range:
 Start ==> _____
 End ==> _____

Transport Key Label(s)
 ==> _____
 ==> _____

or Clear Key ==> **NO**_____ NO or YES
 Control Vector ==> **YES**_____ NO or YES
 Length of Key ==> _____ For DES: 8, 16 or 24 For AES: 16, 24, or 32
 Key Values ==> _____
C9EB3A8B63F8B180 , F345801E9585061C , 26AEF2B3187DA3AE , 3DA06CF98AABD557
 Comment Line ==> _____

Press ENTER to create and store control statement
 Press END to exit to the previous panel without saving
 COMMAND ==> _____

Connected to mysystem.com port 3270 4/20 12:54:26 IBM-3278-2-E - TCPS182

Add - Successful

```

MFC System
QWS3270 Edit View Options Tools Help

CSFCSE10 ----- ICSF - Create ADD, UPDATE, or DELETE K          SUCCESSFUL UPDATE
Specify control statement information below

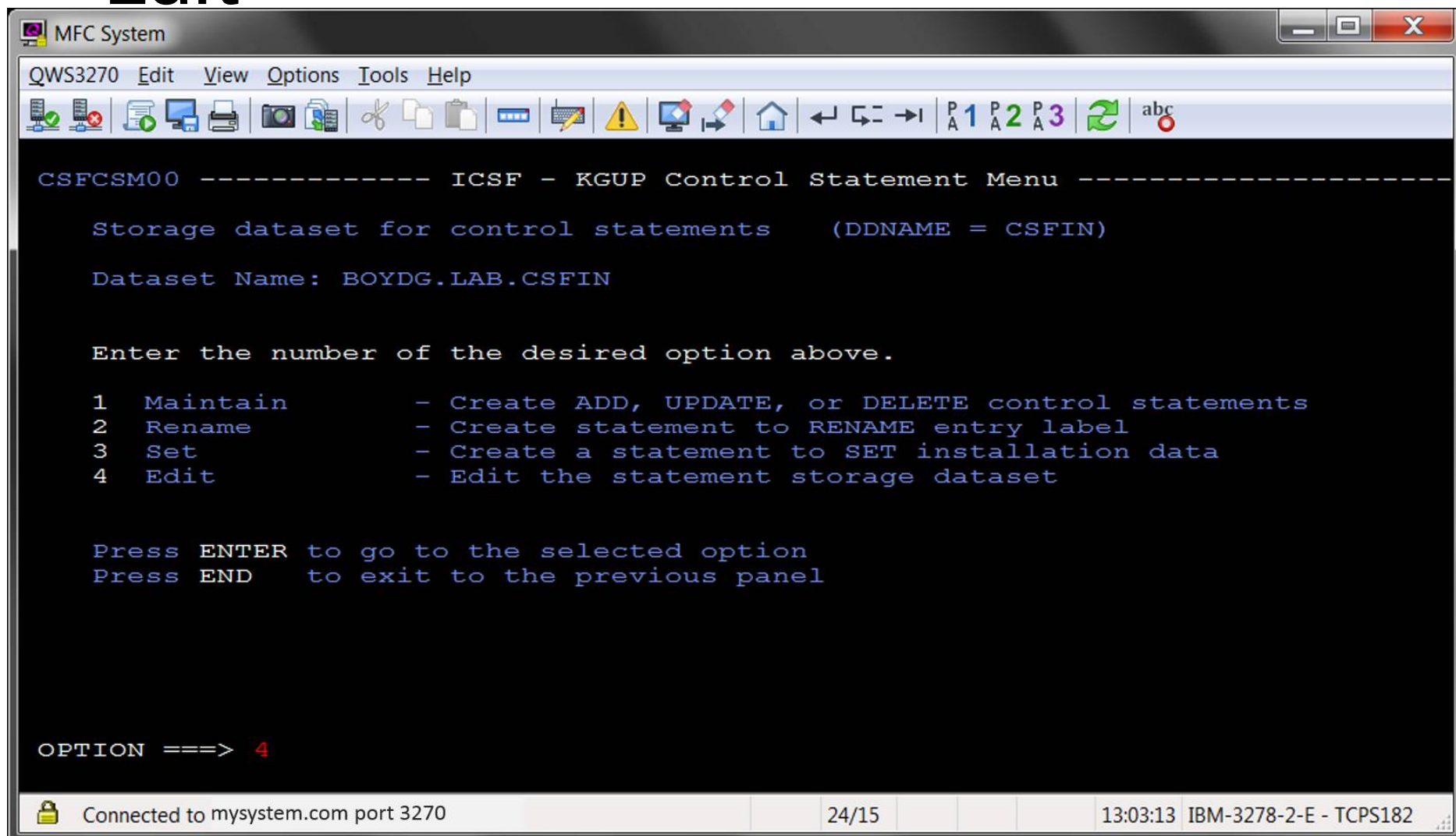
Function   ==> ADD      ADD, UPDATE, or DELETE
Algorithm  ==> AES      DES or AES
Key Type   ==> CLRAES   Outtype ==> _____ (Optional)
Label ==> _____
Group Labels ==> NO_   NO or YES
or Range:
Start ==> _____
End   ==> _____

Transport Key Label(s)
==> _____
==> _____
or Clear Key ==> NO_   NO or YES
Control Vector ==> YES NO or YES
Length of Key ==> ____ For DES: 8, 16 or 24 For AES: 16, 24, or 32
Key Values ==>
C9EB3A8B63F8B180 , F345801E9585061C , 26AEF2B3187DA3AE , 3DA06CF98AABD557
Comment Line ==> _____
Press ENTER to create and store control statement
Press END to exit to the previous panel without saving
COMMAND ==>

Connected to mysystem.com port 3270 4/20 12:56:26 IBM-3278-2-E - TCPS182

```

KGUP Control Statement Menu - Edit



```

MFC System
QWS3270 Edit View Options Tools Help
CSFCSM00 ----- ICSF - KGUP Control Statement Menu -----
Storage dataset for control statements      (DDNAME = CSFIN)
Dataset Name: BOYDG.LAB.CSFIN

Enter the number of the desired option above.

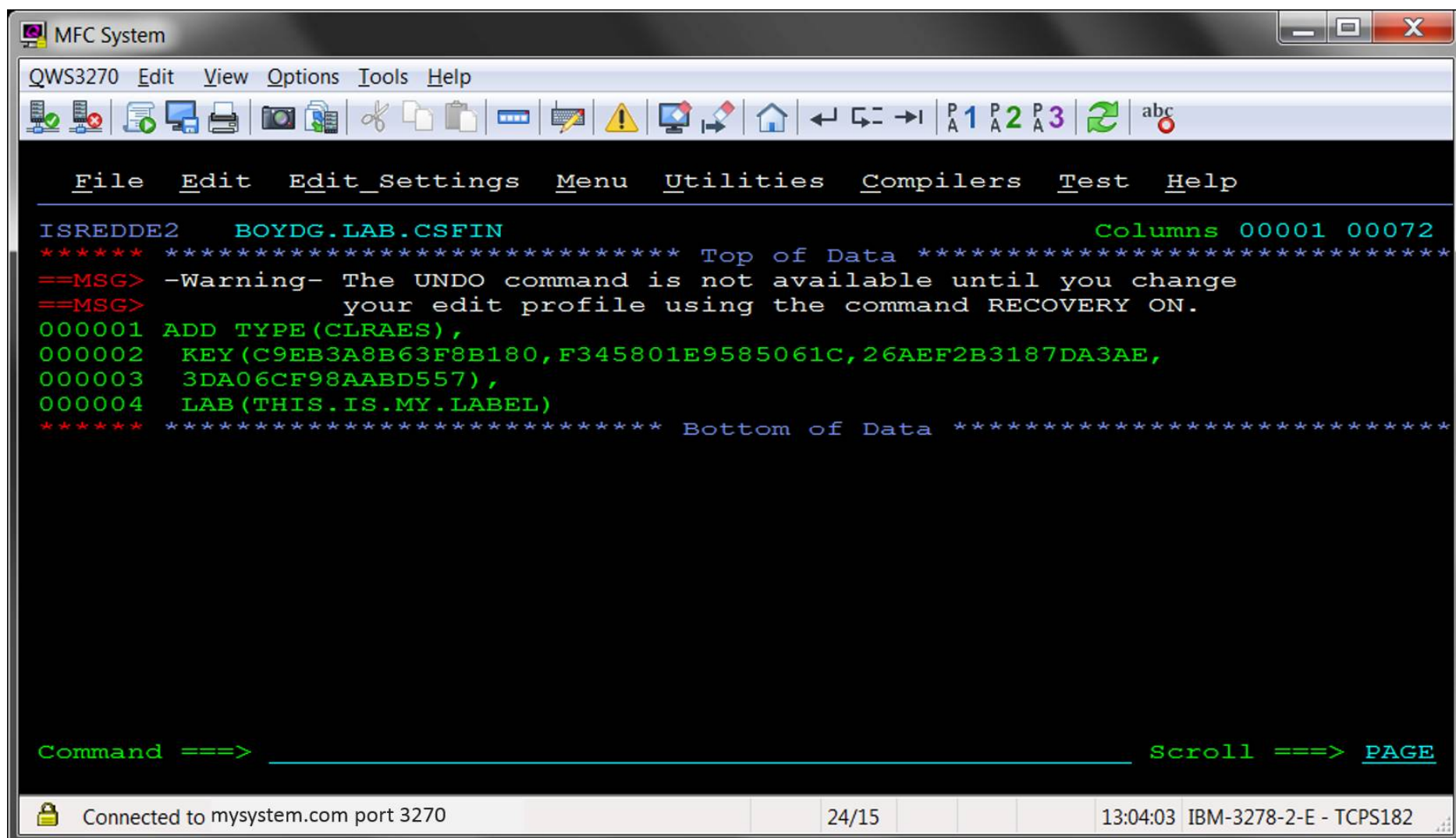
1  Maintain      - Create ADD, UPDATE, or DELETE control statements
2  Rename        - Create statement to RENAME entry label
3  Set           - Create a statement to SET installation data
4  Edit          - Edit the statement storage dataset

Press ENTER to go to the selected option
Press END   to exit to the previous panel

OPTION ==> 4
  
```

Connected to mysystem.com port 3270 24/15 13:03:13 IBM-3278-2-E - TCPS182

Edit CSFIN



The screenshot shows a terminal window titled "MFC System" with a menu bar (File, Edit, View, Options, Tools, Help) and a toolbar. The main text area displays the following content:

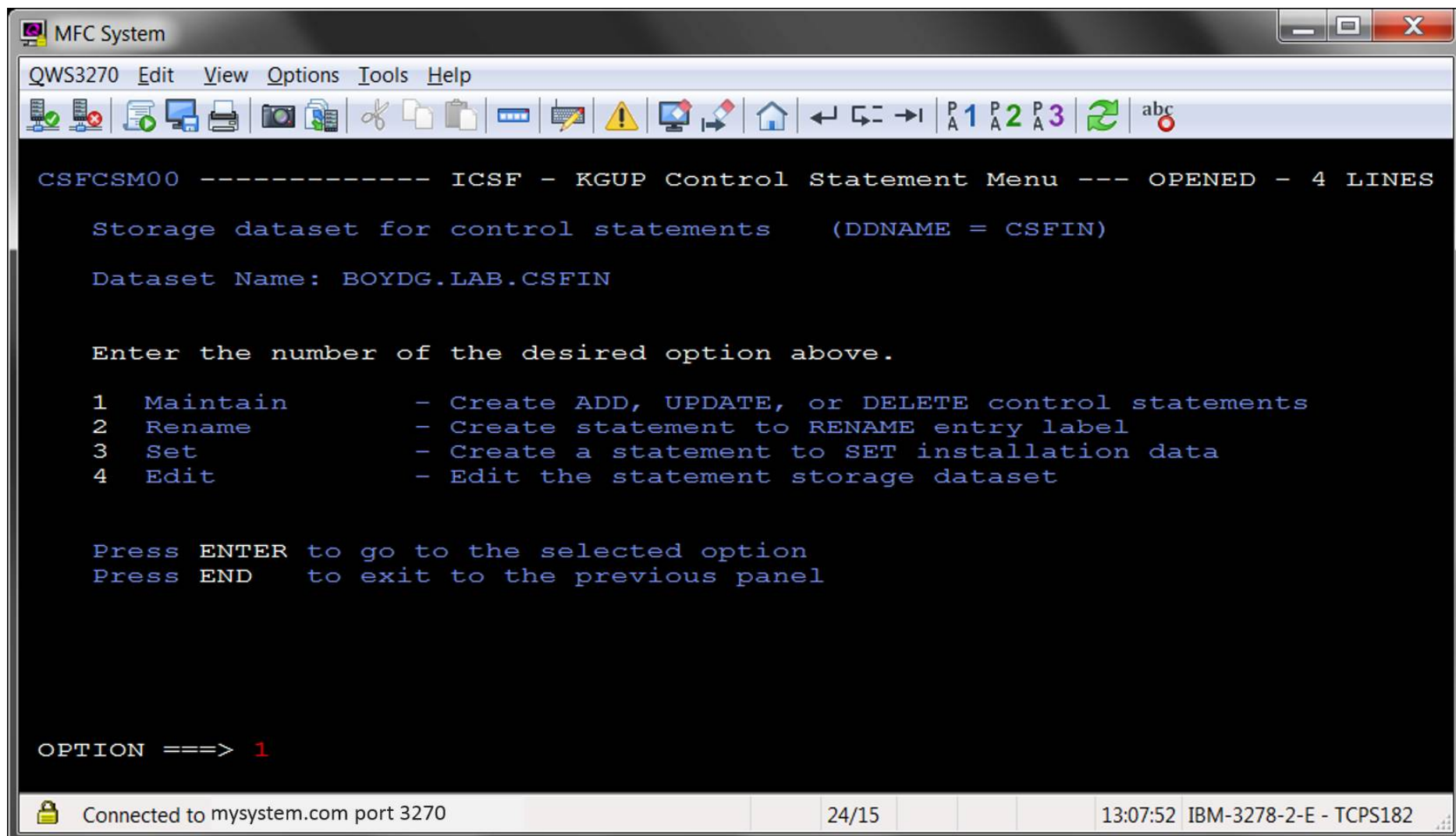
```

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
  
```

At the bottom of the window, a status bar shows: "Connected to mysystem.com port 3270", "24/15", "13:04:03 IBM-3278-2-E - TCPS182".

KGUP Control Statement Menu



```

MFC System
QWS3270 Edit View Options Tools Help
CSFCSM00 ----- ICSF - KGUP Control Statement Menu --- OPENED - 4 LINES

Storage dataset for control statements      (DDNAME = CSFIN)

Dataset Name: BOYDG.LAB.CSFIN

Enter the number of the desired option above.

1  Maintain      - Create ADD, UPDATE, or DELETE control statements
2  Rename        - Create statement to RENAME entry label
3  Set           - Create a statement to SET installation data
4  Edit          - Edit the statement storage dataset

Press ENTER to go to the selected option
Press END   to exit to the previous panel

OPTION ==> 1

Connected to mysystem.com port 3270      24/15      13:07:52 IBM-3278-2-E - TCPS182
  
```

Add another AES Clear Key

MFC System

QWS3270 Edit View Options Tools Help

CSFCSE10 ----- ICSF - Create ADD, UPDATE, or DELETE Key Statement -----
Specify control statement information below

Function ==> **ADD**_____ ADD, UPDATE, or DELETE
Algorithm ==> **AES**_____ DES or AES
Key Type ==> **CLRAES**_____ Outtype ==> _____ (Optional)
Label ==> **THIS.IS.ANOTHER.KEY**_____
Group Labels ==> **NO**_____ NO or YES
or Range:
Start ==> _____
End ==> _____
Transport Key Label(s)
==> _____
==> _____
or Clear Key ==> **NO**_____ NO or YES
Control Vector ==> **YES**_____ NO or YES
Length of Key ==> **32**_____ For DES: 8, 16 or 24 For AES: 16, 24, or 32
Key Values ==> _____
Comment Line ==> **KGUP WILL GENERATE THE KEY MATERIAL**_____
Press ENTER to create and store control statement
Press END to exit to the previous panel without saving
COMMAND ==>

Connected to mysystem.com port 3270 21/60 13:09:57 IBM-3278-2-E - TCPS182

Add - Successful

MFC System

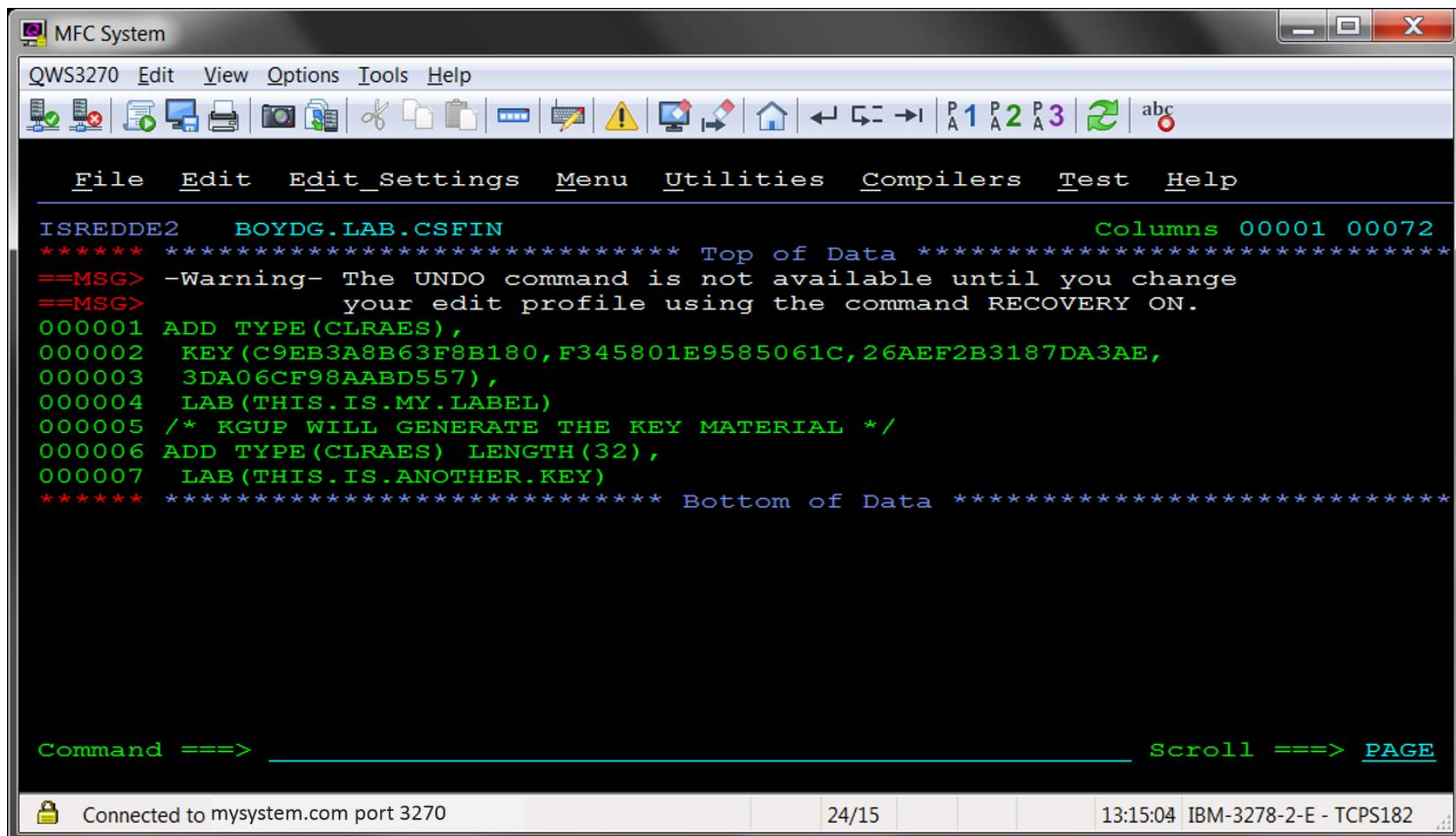
QWS3270 Edit View Options Tools Help

CSFCSE10 ----- ICSF - Create ADD, UPDATE, or DELETE K SUCCESSFUL UPDATE
Specify control statement information below

Function ==> **ADD**_____ ADD, UPDATE, or DELETE
Algorithm ==> **AES**_____ DES or AES
Key Type ==> **CLRAES**_____ Outtype ==> _____ (Optional)
Label ==> _____
Group Labels ==> **NO**_____ NO or YES
or Range:
Start ==> _____
End ==> _____
Transport Key Label(s)
==> _____
==> _____
or Clear Key ==> **NO**_____ NO or YES
Control Vector ==> **YES**_____ NO or YES
Length of Key ==> **32**_____ For DES: 8, 16 or 24 For AES: 16, 24, or 32
Key Values ==> _____
_____ / _____ / _____ / _____
Comment Line ==> _____
Press ENTER to create and store control statement
Press END to exit to the previous panel without saving
COMMAND ==> _____

Connected to mysystem.com port 3270 4/20 13:12:46 IBM-3278-2-E - TCPS182

Edit CSFIN



The screenshot shows a terminal window titled "MFC System" with a menu bar (File, Edit, Edit_Settings, Menu, Utilities, Compilers, Test, Help) and a toolbar. The main text area displays the following content:

```

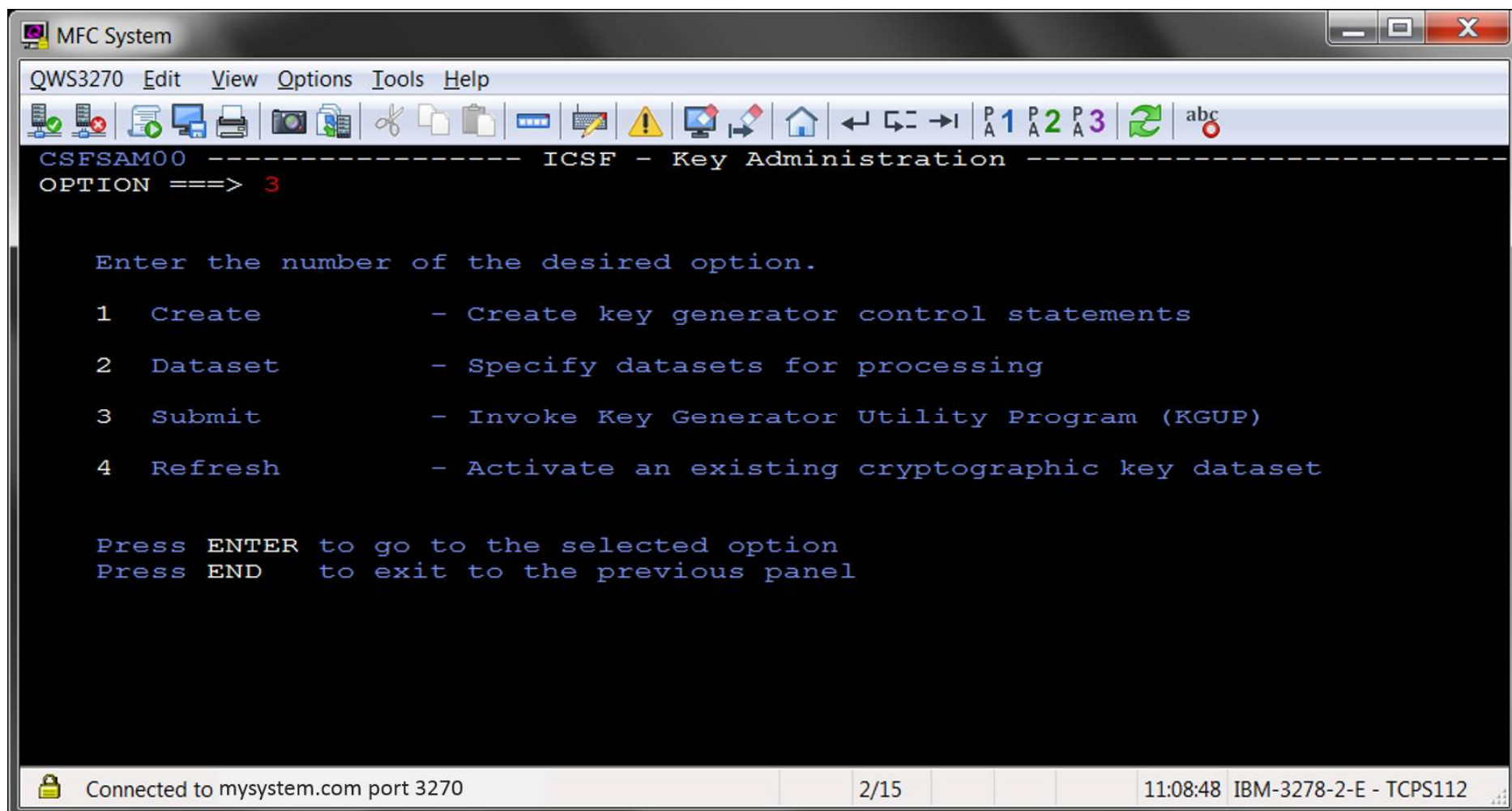
ISREDDE2      BOYDG.LAB.CSFIN                      Columns 00001 00072
***** Top of Data *****
==MSG> -Warning- The UNDO command is not available until you change
==MSG> your edit profile using the command RECOVERY ON.
000001 ADD TYPE(CLRAES),
000002 KEY(C9EB3A8B63F8B180,F345801E9585061C,26AEF2B3187DA3AE,
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
  
```

At the bottom of the window, a status bar shows:

- Connected to mysystem.com port 3270
- 24/15
- 13:15:04 IBM-3278-2-E - TCPS182

KGUP Key Administration - Submit



```

MFC System
QWS3270 Edit View Options Tools Help
----- ICSF - Key Administration -----
OPTION ==> 3

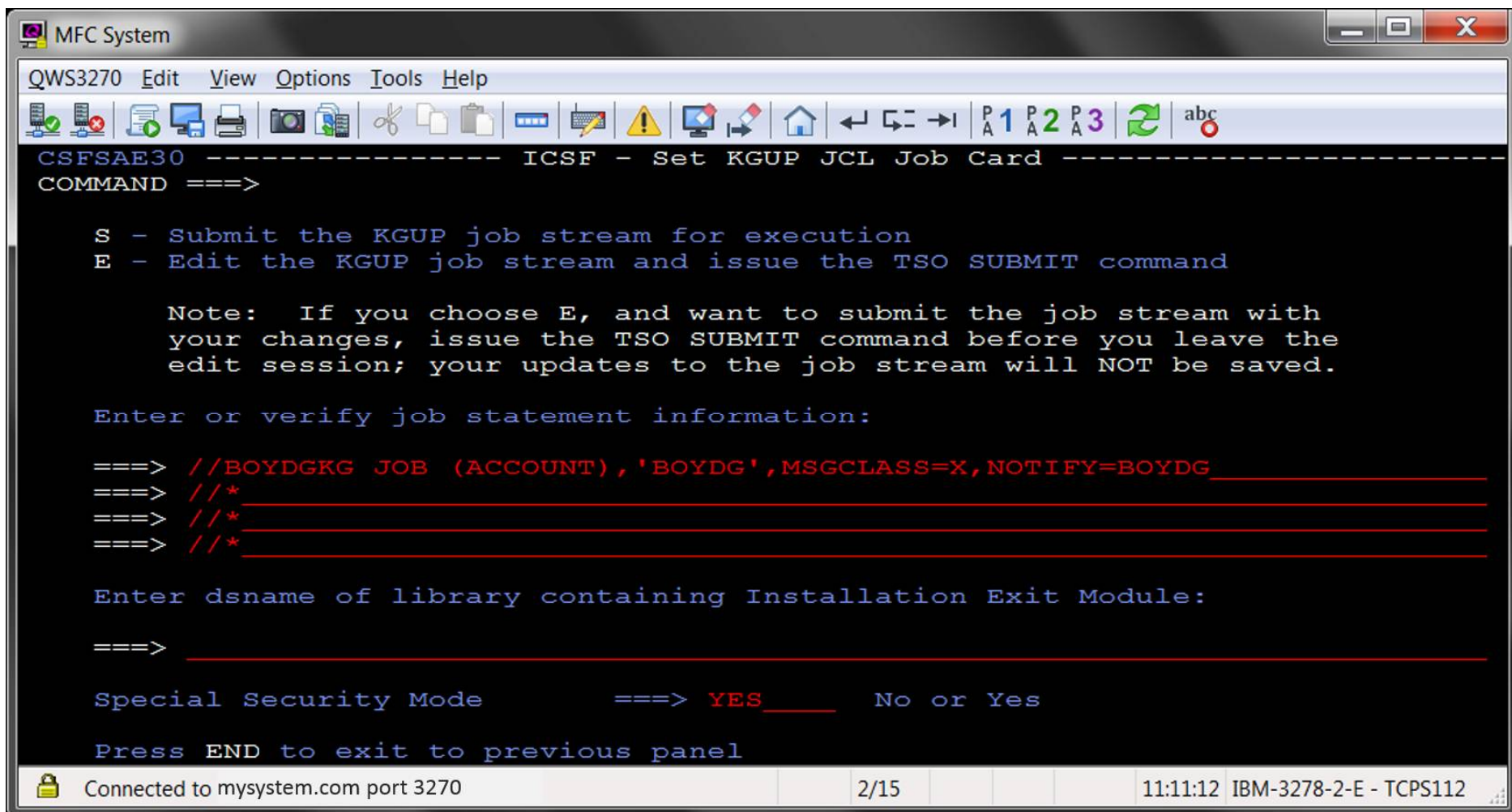
Enter the number of the desired option.

1 Create          - Create key generator control statements
2 Dataset         - Specify datasets for processing
3 Submit          - Invoke Key Generator Utility Program (KGUP)
4 Refresh         - Activate an existing cryptographic key dataset

Press ENTER to go to the selected option
Press END   to exit to the previous panel

Connected to mysystem.com port 3270
2/15
11:08:48 IBM-3278-2-E - TCPS112
  
```

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

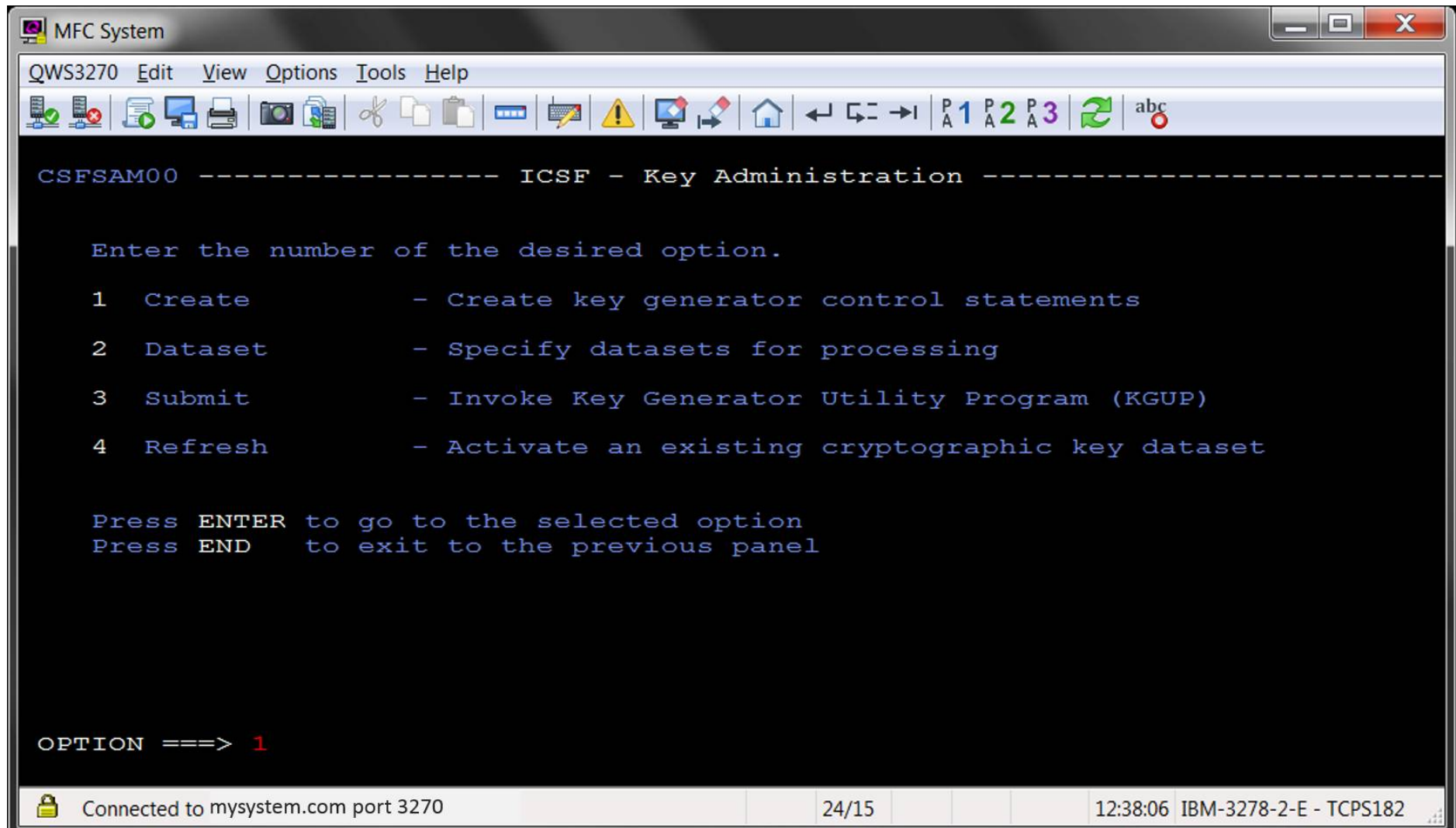
```

MFC System
QWS3270 Edit View Options Tools Help
-----
Display Filter View Print Options Search Help
-----
ISFPCU41 UT DISPLAY BOYDGK JOB08601 DSID 101 LINE 0 COLUMNS 02- 81
COMMAND INPUT ==> SCROLL ==> PAGE
***** TOP OF DATA *****
KEY GENERATION DIAGNOSTIC REPORT
ADD TYPE(CLRAES),
  KEY(C9EB3A8B63F8B180,F345801E9585061C,26AEF2B3187DA3AE,
  3DA06CF98AABD557),
  LAB(THIS.IS.MY.LABEL)
>>>CSFG0321 STATEMENT SUCCESSFULLY PROCESSED.
/* KGUP WILL GENERATE THE KEY MATERIAL */
ADD TYPE(CLRAES) LENGTH(32),
  LAB(THIS.IS.ANOTHER.KEY)
>>>CSFG0321 STATEMENT SUCCESSFULLY PROCESSED.
>>>CSFG0780 A REFRESH OF THE IN-STORAGE CKDS IS NECESSARY TO ACTIVATE CHANGES MA
>>>CSFG0002 CRYPTOGRAPHIC KEY GENERATION - END OF JOB. RETURN CODE = 0.
***** BOTTOM OF DATA *****

Connected to mysystem.com port 3270 4/21 13:19:41 IBM-3278-2-E - TCPS182

```

REFRESH from the KGUP panels

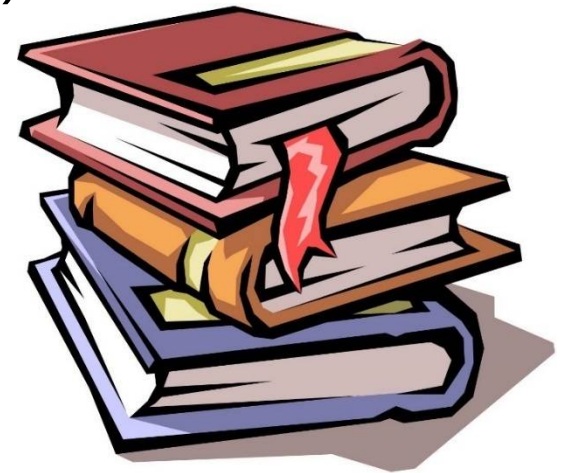


KEY in the CKDS

The screenshot shows a terminal window titled "MFC System". The menu bar includes "QWS3270", "Edit", "View", "Options", "Tools", and "Help". Below the menu is a toolbar with various icons. The main area displays a data set starting with "ISRBROBA SYS16138.T133446.RA000.BOYDG.R0100134 Line 0000000507 Col 037 116". The data consists of hexadecimal strings arranged in columns, followed by asterisks and alphanumeric labels like "THIS.IS.MY.LABEL", "DATA", and "Bottom of Data". A red arrow points to the first column of data. At the bottom, there's a status bar with "Command ==>" and "Scroll ==> CSR". The footer shows connection details: "Connected to mysystem.com port 3270", page number "4/50", time "13:35:31", and system identifier "IBM-3278-2-E - TCPS182".

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

?

