System z

Service Guide for Trusted Key Entry Workstations

Version 6.0 or later

GC28-6862-03

System z

Service Guide for Trusted Key Entry Workstations

Version 6.0 or later

GC28-6862-03

Note

Before using this information and the product it supports, be sure to read the safety information under “Safety” on page v and the general information under “Notices,” on page A-1

Fourth Edition (December 2009)

| This edition, GC28-6862-03, obsoletes and replaces *Service Guide for Trusted Key Entry Workstations*,
| GC28-6862-02, and applies to Trusted Key Entry Workstations at LIC 6.0 or later, used on IBM System z servers. A
| technical change to the text or illustration is indicated by a vertical line to the left of the change.

Figures included in this document illustrate concepts and are not necessarily accurate in content, appearance, or specific behavior.

There might be a newer version of this document in PDF format available on **Resource Link**. Go to http://www.ibm.com/servers/resourcelink and click **Library** on the navigation bar. A newer version is indicated by a lower-case, alphabetic letter following the form number suffix (for example: 00a, 00b, 01a, 01b).

Contents

Safety

Safety notices

Safety notices may be printed throughout this guide. **DANGER** notices warn you of conditions or procedures that can result in death or severe personal injury. **CAUTION** notices warn you of conditions or procedures that can cause personal injury that is neither lethal nor extremely hazardous. **Attention** notices warn you of conditions or procedures that can cause damage to machines, equipment, or programs.

The following **DANGER** notices appear in this manual.

DANGER

When working on or around the system, observe the following precautions:

Electrical voltage and current from power, telephone, and communication cables are hazardous. To avoid a shock hazard:

- **Connect power to this unit only with the IBM® provided power cord. Do not use the IBM provided power cord for any other product.**
- **Do not open or service any power supply assembly.**
- **Do not connect or disconnect any cables or perform installation, maintenance, or reconfiguration of this product during an electrical storm.**
- **The product might be equipped with multiple power cords. To remove all hazardous voltages, disconnect all power cords.**
- **Connect all power cords to a properly wired and grounded electrical outlet. Ensure that the outlet supplies proper voltage and phase rotation according to the system rating plate.**
- **Connect any equipment that will be attached to this product to properly wired outlets.**
- **When possible, use one hand only to connect or disconnect signal cables.**
- **Never turn on any equipment when there is evidence of fire, water, or structural damage.**
- **Disconnect the attached power cords, telecommunications systems, networks, and modems before you open the device covers, unless instructed otherwise in the installation and configuration procedures.**
- **Connect and disconnect cables as described in the following procedures when installing, moving, or opening covers on this product or attached devices.**

  To disconnect:

  1. **Turn off everything (unless instructed otherwise).**
  2. **Remove the power cords from the outlets.**
  3. **Remove the signal cables from the connectors.**
  4. **Remove all cables from the devices.**

  To connect:

  1. **Turn off everything (unless instructed otherwise).**
  2. **Attach all cables to the devices.**
  3. **Attach the signal cables to the connectors.**
  4. **Attach the power cords to the outlets.**
  5. **Turn on the devices.**
- **Sharp edges, corners and joints may be present in and around the system. Use care when handling equipment to avoid cuts, scrapes and pinching.**

(D005)

The following **CAUTION** notices appear in this manual.

CAUTION:
Only trained service personnel may replace this battery. The battery contains lithium. To avoid possible explosion, do not burn or charge the battery.

Do not:
__ **Throw or immerse into water**
__ **Heat to more than 100°C (212°F)**
__ **Repair or disassemble**

Exchange only with the IBM-approved part. Recycle or discard the battery as instructed by local regulations. In the United States, IBM has a process for the collection of this battery. For information, call 1-800-426-4333. Have the IBM part number for the battery unit available when you call. (C002)

World Trade safety information

Several countries require the safety information contained in product publications to be presented in their national languages. If this requirement applies to your country, a safety information booklet is included in the publications package shipped with the product. The booklet contains the safety information in your national language with references to the US English source. Before using a US English publication to install, operate, or service this IBM product, you must first become familiar with the related safety information in the booklet. You should also refer to the booklet any time you do not clearly understand any safety information in the US English publications.

Laser safety information

All System z® models can use I/O cards such as PCI adapters, ESCON®, FICON®, Open Systems Adapter (OSA), InterSystem Coupling-3 (ISC-3), or other I/O features which are fiber optic based and utilize lasers or LEDs.

Laser compliance

All lasers are certified in the U.S. to conform to the requirements of DHHS 21 CFR Subchapter J for class 1 laser products. Outside the U.S., they are certified to be in compliance with IEC 60825 as a class 1 laser product. Consult the label on each part for laser certification numbers and approval information.

CAUTION:
Data processing environments can contain equipment transmitting on system links with laser modules that operate at greater than Class 1 power levels. For this reason, never look into the end of an optical fiber cable or open receptacle. (C027)

CAUTION:
This product contains a Class 1M laser. Do not view directly with optical instruments. (C028)

Preface

Using this guide

Who uses this guide

This guide is for service representatives who perform problem isolation and repair actions on Trusted Key Entry Workstations for the following products:

- System z10™™ Servers
- System z9® Servers
- zSeries® Servers

General comments

- There are representations of windows displayed throughout this manual. These are displayed to help you recognize the information that you will see while performing the procedures in this manual. The information displayed in these representations may not agree with that displayed on your system. Always use the instructions and data displayed on your system.
- There may be product features represented in this manual that are not installed on the system and, although announced, may not be available at the time of publication.
- There may be product features on your system that are not represented in this manual.

Where to start

Start all service activity at Chapter 1, “Basic information,” on page 1-1

How to send your comments

Your feedback is important in helping to provide the most accurate and high-quality information. Send your comments by using Resource Link™ at *http://www.ibm.com/servers/resourcelink*. Select **Feedback** on the Navigation bar on the left. You can also send an e-mail to reslink@us.ibm.com. Be sure to include the name of the book, the form number of the book, the version of the book, if applicable, and the specific location of the text you are commenting on (for example, a page number or table number).

Related publications

- *Trusted Key Entry PCIX Workstation User's Guide*, SA23-2211, at the -05 level or later.
- *Service Guide*, for the server to which this workstation is connected.

Chapter 1. Basic information

This manual contains information used to service Trusted Key Entry Workstations attached to System z servers.

If you are working on a TKE Workstation, the associated Central Processing Complex (CPC) will continue to run. However, the TKE Workstation will not be available to the customer. Authorized customer personnel may use “clear key entry” through ICSF windows on any PC with TSO access.

Depending on the system configuration, when you are directed to exchange Field Replaceable Units (FRUs), run tests, or change configuration data, the customer’s TKE Workstation interface to the system hardware may not be available. Before starting any of these tasks, notify the customer.

It is the customer’s responsibility to correctly configure the Trusted Key Entry Workstation (TKE) software. TKE configuration data may contain sensitive customer information. Do not attempt to access this information without the customer’s permission.

Network connectivity to the operating system is through Ethernet adapters and is the customer’s responsibility.

Note: Customers using TKE 5.0 LIC or higher, and TKE 5.0 or higher Workstations **only** have the Ethernet option for network connectivity. A Token Ring connection option is no longer available.

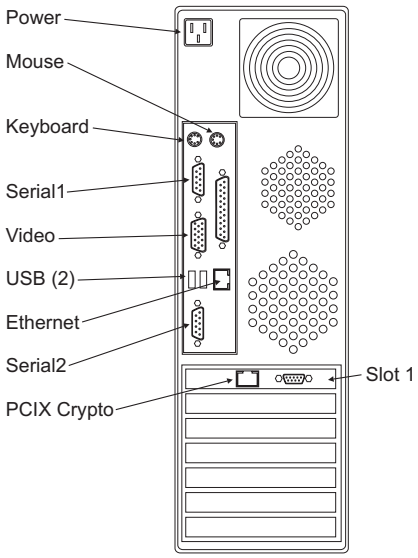
For additional information, refer to the *Trusted Key Entry PCIX Workstation User’s Guide (for LIC 6.0)*, SA23-2211–05.

Identifying the console

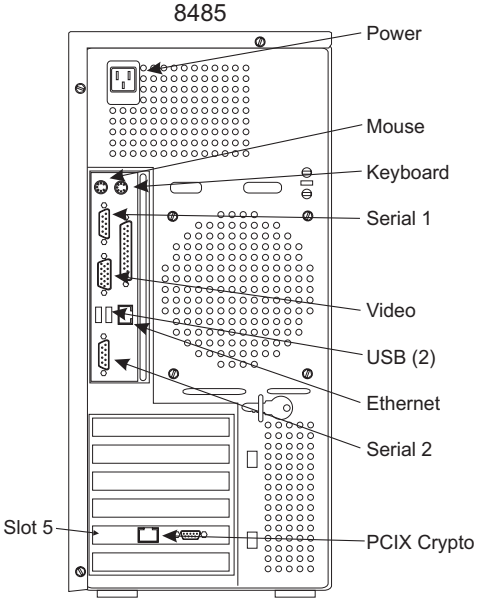
The TKE Workstation console may be one of the following:

- Machine type 8482 using the PCIX 4764 Cryptographic Adapter
- Machine type 8485 using the PCIX 4764 Cryptographic Adapter.
- Machine type 4367 using the PCIX 4764 Cryptographic Adapter.

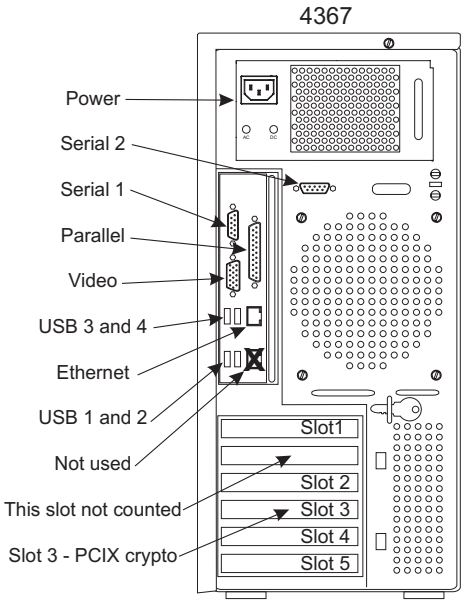
8482



8485



4367



Verify the Cryptographic Adapter card type and model by locating the label next to the adapter's D-Shell connector.

Service tips

TKE Workstations

If you exchange the cryptographic adapter, the customer must initialize the new cryptographic adapter.

- Those using the PCIX 4764 Cryptographic Adapter should refer to the *Trusted Key Entry PCIX Workstation User's Guide*, SA23-2211–05.

Check with the system operator to verify that there are no channel or cryptographic coprocessor errors on the server before proceeding with the TKE Workstation repair.

If you are directed to exchange PC FRUs, refer to the PC maintenance information for removal and replacement instructions.

Hardware Maintenance Manuals

The 8482 and 8485 Hardware Maintenance Manuals (HMM's) are available on the Diagnostic CDROM's **Service** subdirectory (PDF format). Use Adobe® Acrobat Reader on the System Service Representative's (SSR) ThinkPad to view the files. The 4367 Hardware Maintenance Manual is available via download from the IBM support website http://www.ibm.com/support.

8482 hard drive

TKE 5.0 Workstations use the 8482 machine type. The 8482 employs an ATA serial hard drive.

8485 service tips

Enhanced Serviceability

For enhanced serviceability, the 8485 supports a mini Baseboard Management Controller (BMC). The BMC provides environmental monitoring for the server. If environmental conditions exceed thresholds or if system unit components fail, the BMC will light LED indicators on the motherboard and turn on the **System-error** LED [!] located on the front of the server.

The POST error log contains the three most recent error codes and messages that were generated during POST. The BMC System Event log contains the BMC-generated messages. The system event/error log contains messages generated during POST and all system status messages from the BMC.

If the **System-error** LED is lit but there are no other error indications, clear the BMC system event log. This log does not clear itself, and if it begins to fill up, the **System-error** LED will be lit. After you complete a repair or correct an error, clear the BMC System Event log to turn off the **System-error** LED.

Procedures for managing the BMC and logs can be found in the *Problem Determination and Service Guide* (8485 HMM.PDF) in the SERVICE directory of the diagnostic CD.

Ethernet Support

The PCI-Express and planar Ethernet support utilizes BroadCom chipsets. Use their respective MAC addresses to differentiate between the chipsets when running diagnostics.

Installed adapters

Use the following table as a guide to select the correct Adapter/Bus when performing configuration and diagnostic test procedures.

Adapters	8482	8485	4367
Ethernet	Planar	PCI-Express/Planar	Planar
Crypto	PCIX	PCIX	PCIX

Chapter 2. TKE installation and maintenance tasks

This chapter assists you with installing the TKE Workstation, connecting it to the system, and performing maintenance.

Table 2-1. Problem Determination

Action	Go To
Install an 8482 TKE Workstation	“TKE installation - 8482”
Install a PCIX Cryptographic Coprocessor Adapter - 8482	“TKE installation - 8482”
Install an 8485 TKE Workstation	“TKE installation - 8485” on page 2-7
Install a PCIX Cryptographic Coprocessor Adapter - 8485	“TKE installation - 8485” on page 2-7
Install a 4367 TKE Workstation	“TKE installation - 4367” on page 2-15
Install a PCIX Cryptographic Coprocessor Adapter - 4367	“TKE installation - 4367” on page 2-15
Determining Crypto Adapter Code Loaded	“Determining Crypto Adapter Code Loaded” on page 2-29
Correcting PCIX TKE adapter card code	“Correcting PCIX TKE adapter card code” on page 2-32
Loading code to the PCIX TKE adapter card	“Loading PCIX TKE adapter card code” on page 2-34
Loading the Functional Control Vector to the PCIX TKE adapter card	“Loading the function control vector for the PCIX TKE adapter” on page 2-38
Transport a TKE Workstation with PCIX Coprocessor Adapter installed	“Transporting a TKE Workstation with the PCIX coprocessor adapter installed” on page 2-40
Replacing PCIX Coprocessor Batteries	“Replacing the PCIX cryptographic coprocessor batteries” on page 2-24
TKE Workstation CCAxxxx Event Codes	“TKE Workstation CCAxxxx event codes” on page 3-3
Backup hard disk information	“Saving the configuration for PCIX TKE” on page 2-41
PCIX TKE LIC: Install and restore the hard disk	“Installing and restoring the PCIX TKE hard drive internal code” on page 2-43
Internal Code Changes	“Internal code changes for a Trusted Key Entry Workstation” on page 2-45
Installing Internal Code Changes	“Installing internal code changes on a TKE Workstation” on page 2-45
Installing MCIs	“Installing MCLs on a TKE Workstation” on page 2-47

TKE installation - 8482

This section instructs you on how to install the 8482 TKE Workstation and connect it to the system.

1. Open and unpack the ship box containing the TKE Workstation.

   This box also contains the cables, DVD-RAM for internal code restore, the Backup DVD-RAM, diskettes for diagnostics and customer-specific data, and

documentation. Store the Code DVD-RAM, Backup DVD-RAM, diagnostic diskette, customer-specific data diskette, documentation, and the key in an area near the console for future service use.

2. Remove the side cover from the computer.

   Remove the adapter retention bar at slot 1 (topmost slot).

   Install the **PCIX Cryptographic Coprocessor**

   a. Remove the PCIX Cryptographic Coprocessor from its shipping carton and static bag.

      Electrostatic discharge (ESD) can damage the card and its components. Wear an ESD wrist strap while handling and installing the card, or take the following precautions:

      Notes®:

      1) Limit your movements; this helps prevent static electricity building up around you.
      2) Prevent others from touching the card or other components.
      3) Before removing the card from the anti-static bag, touch the bag to an unpainted metal surface on the computer and hold it there for at least two seconds.
      4) Store the carton and bag as they may be needed if the workstation is transported.

   b. Verify that the jumpers on the card are positioned correctly.

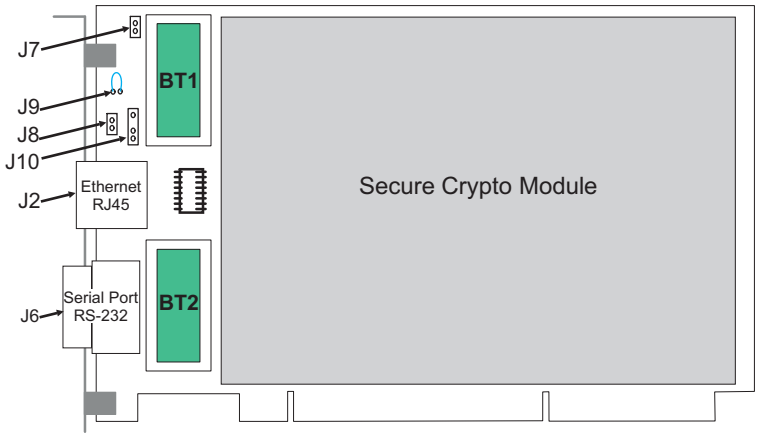


Table 2-2. Jumpers on a PCIX Bus-Based Cryptographic Adapter

Jumper	# Pins	Name of Jumper	Jumper Position
J7	2	PCIX VPD EEPROM WRITE Jumpered = PCIX EEPROM write-enabled No jumper = PCIX EEPROM write disabled	Jumpered
J10	3	BATTERY REPLACEMENT Connects to power cord externally while changing batteries BT1 and BT2.	Not Jumpered
J6	9	RS232 SERIAL PORT D-shell connector	
J2	8	Ethernet PORT RJ45 connector	

Table 2-2. Jumpers on a PCIX Bus-Based Cryptographic Adapter (continued)

Jumper	# Pins	Name of Jumper	Jumper Position
J11	5	EXTERNAL INTRUSION LATCH Pin 1 - Ground Pin 2 - B03 PCIX edge connector Pin 3 - External Warning Pin 4 - B94 PCIX edge connector Pin 5 - Ground Pin layout viewed from the back of the card: o o o o o 5 4 3 2 1	Pins 1,2,3,4 jumpered = Hydra 3, iSeries®, pSeries®, and OEM applications [PCIX slot pin B94] Pins 2,3,4,5 jumpered = Hydra 1.75 applications [PCIX slot pin B03]
J9	2	BATTERY DISCONNECT WIRE Allows opening the battery circuit by cutting the jumper wire. This zeroizes the on-card secure data and keys for the application.	Jumpered
J8	2	EXTERNAL INTRUSION LATCH DISABLE JUMPER HEADER This header may have a BERG jumper installed to disable the warning activation. Platforms that use the External Intrusion Latch Warning feature will remove this jumper in their assembly process.	Not Jumpered

c. Remove the expansion slot cover located on the top-most PCIX slot (slot 1). Insert the Coprocessor in slot 1, making sure it is firmly seated.

d. Replace the adapter retention bar.

e. Replace the computer's cover.

Note:

a. If you do not have the Smart Card Reader option continue to step 5 on page 2-4.

b. The 8482 TKE Workstation has both PS2 and USB ports.

c. In TKE V6.0, 2 types of Smart Card Readers are supported, Omnikey and Kobil.

d. Two Smart Card Readers of the same type, either both Omnikeys or both Kobils, must be attached.

3. Installing the Omnikey Smart Card Reader

   __ a. The Omnikey reader is a USB Smart Card reader. If you are using an Omnikey reader, simply plug it into any available USB port on the TKE machine.

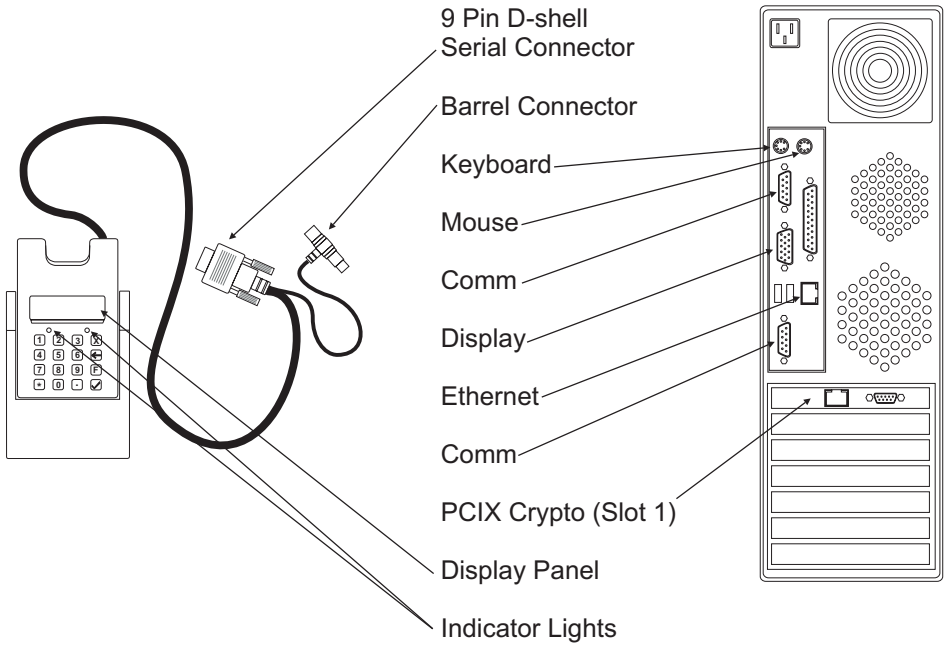
4. Installing the Kobil Smart Card Reader

   __ a. Verify there is no power cord connected to the TKE system unit.

   __ b. Plug one barrel cable connector from the Smart Card Reader(s) to the mouse port at the rear of the system unit.

   __ c. Plug the second barrel cable connector from the Smart Card Reader(s) to the rear of the first barrel connector.

   __ d. Connect the serial cable from one reader to COMM1 and the serial cable from the other reader to the COMM2 serial port connections at the rear of the system unit.

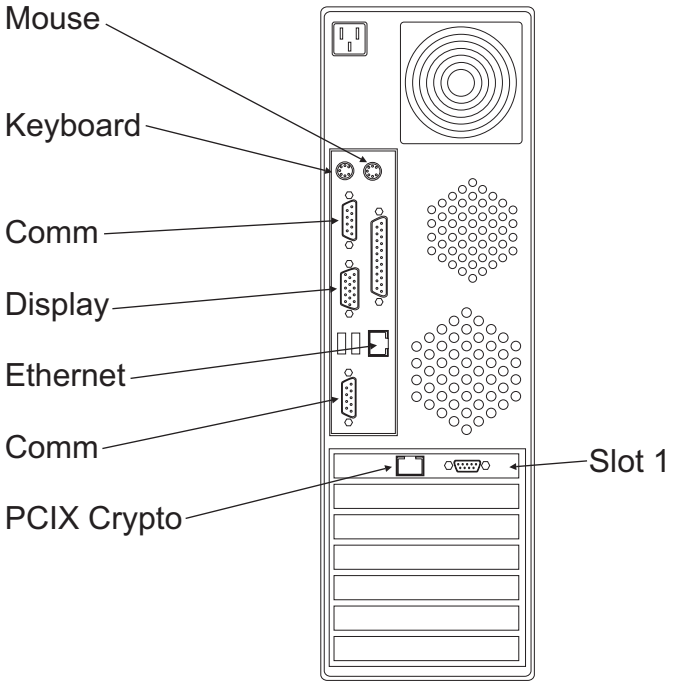


5. Connect the mouse cable to the mouse connector at the rear of the system unit.

   Note: If you have the Smart Card Reader feature, connect the mouse cable to the Smart Card Reader barrel connector, already plugged into the mouse connector on the system unit.

   Connect the keyboard cable to the keyboard connector at the rear of the system unit. You will find a keyboard symbol defining the correct plug location.

6. Connect the display signal cable to the display connection at the rear of the system unit. You will find a display symbol defining the correct plug location.



7. Plug the Ethernet cable, **P/N 05N5292**, into the RJ45 port on the system unit connector panel.

   Connect the other end of the Ethernet cable to the HUB.

8. Perform the impedance measurements using the ECOS C7106 tester (USA only).

   If the ECOS tester is not available, go to step 9.

   When the impedance measurements are correct, continue with the next step.

9. This procedure checks for a ground/earth resistance of one ohm or less at the receptacle ground/earth pin using the CE meter.

   The wall breaker should be OFF. Do the following to check the customer's power source:

   __ a. Using the CE meter, measure the resistance from the ground/earth pin of the receptacle to building ground/earth. The reading should be one ohm or less.

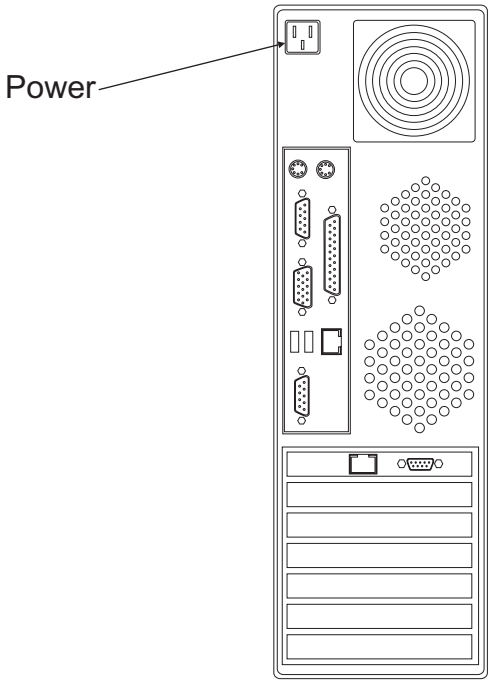
   __ b. For metal receptacle shells, also measure the resistance from the ground/earth pin of the receptacle to the metal shell. This reading should be 0.1 ohm or less.

   Note: Digital meters may give unstable resistance readings if leakage current is flowing in the building ground/earth circuit. If the reading appears unstable, or is greater than one ohm, contact your branch office installation planning representative or field manager.

10. **Attention:** Check the primary voltage switches on the system unit, display, and, if installed, the modem, to ensure proper setting for your customer's power source (115V or 230V).

    Note: The display may not have primary voltage switches. Ensure it is enabled for the input voltage supplied by your customer.

    Connect the following power cables to the rear of the units:
    - System unit
    - Display



Connect the power cables to building power.

11. Do the following to complete the installation:
    __ a. Power on the display, system unit, and, if installed, the modem and security interface unit.
    __ b. Ensure that the power on indicators are on for all units.
    __ c. Wait for the TKE Workstation to complete loading.
    __ d. Do not start the TKE application. Turn the Workstation over to the customer to complete the setup.

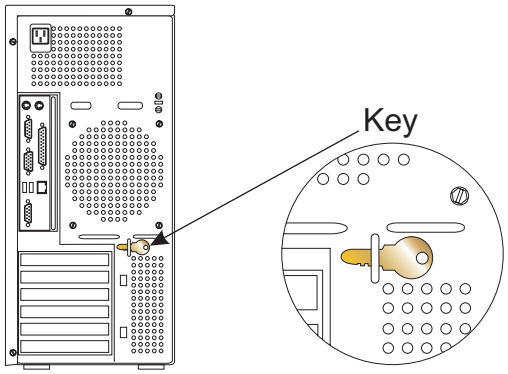
    If the TKE Workstation does not start, use the procedures in this manual to resolve the problem.

TKE installation - 8485

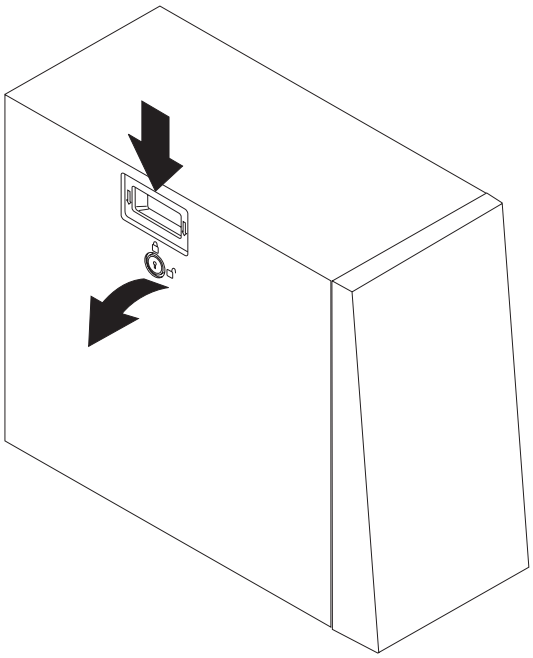
This section instructs you how to install the 8485 TKE Workstation and connect it to the system.

1. Open and unpack the ship box containing the TKE Workstation.

   This box also contains the cables, DVD-RAM for internal code restore, the Backup DVD-RAM, diskettes for diagnostics, and documentation. TKE 5.0 and TKE 5.1 will contain a diskette for customer-specific data. TKE 5.2 and later will contain a DVD-RAM for customer-specific data. Store the Code DVD-RAM, Backup DVD-RAM, diagnostic diskette, customer-specific data diskette or DVD-RAM, documentation, and the key in an area near the console for future service use.
2. Find the key in its storage position on the rear of the machine.

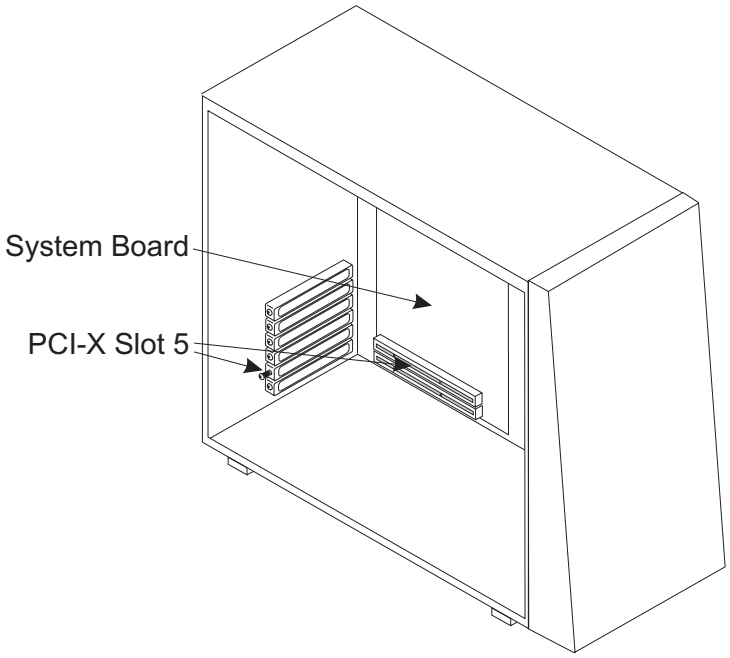


   Unlock the side cover, then press the cover latch down.



   Tilt the top of the cover away from the machine, then lift the cover off and set it aside.
3. Rotate the rear adapter retention bracket (if present) to the open (unlocked) position and remove it from the machine.

   Remove the screw securing the expansion slot cover for slot 5.



Remove the expansion slot cover and store the slot cover and its screw in a safe place for future use.

4. Install the **PCIX Cryptographic Coprocessor**
   a. Remove the PCIX Cryptographic Coprocessor from its shipping carton and static bag.

      Electrostatic discharge (ESD) can damage the card and its components. Wear an ESD wrist strap while handling and installing the card, or take the following precautions:

      Notes:

      1) Limit your movements; this helps prevent static electricity building up around you.
      2) Prevent others from touching the card or other components.
      3) Before removing the card from the anti-static bag, touch the bag to an unpainted metal surface on the computer and hold it there for at least two seconds.
      4) Store the carton and bag as they may be needed if the workstation is transported.

   b. Verify that the jumpers on the card are positioned correctly.

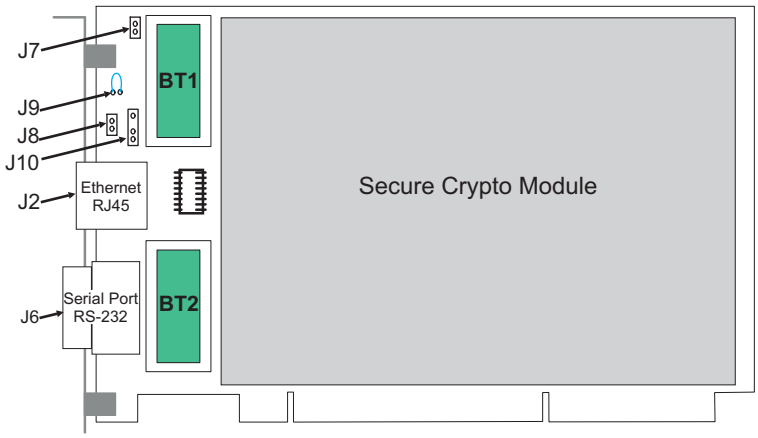


Table 2-3. Jumpers on a PCIX Bus-Based Cryptographic Adapter

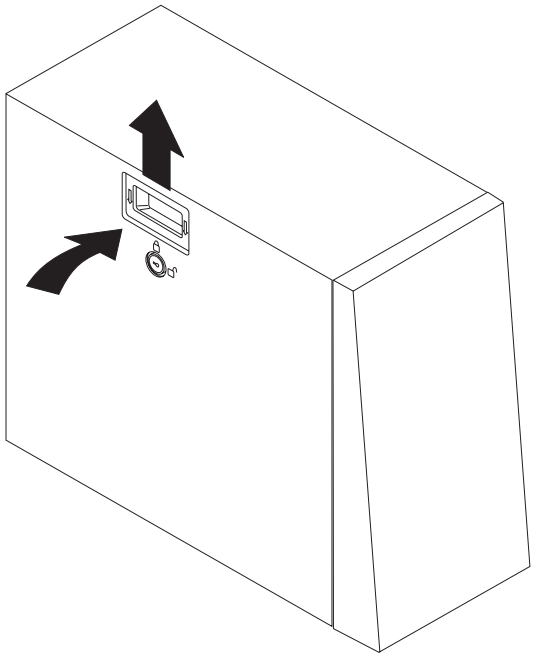
Jumper	# Pins	Name of Jumper	Jumper Position
J7	2	PCIX VPD EEPROM WRITE Jumpered = PCIX EEPROM write-enabled No jumper = PCIX EEPROM write disabled	Jumpered
J10	3	BATTERY REPLACEMENT Connects to power cord externally while changing batteries BT1 and BT2.	Not Jumpered
J6	9	RS232 SERIAL PORT D-shell connector	
J2	8	Ethernet PORT RJ45 connector	
J11	5	EXTERNAL INTRUSION LATCH Pin 1 - Ground Pin 2 - B03 PCIX edge connector Pin 3 - External Warning Pin 4 - B94 PCIX edge connector Pin 5 - Ground Pin layout viewed from the back of the card: o o o o o 5 4 3 2 1	Pins 1,2,3,4 jumpered = Hydra 3, iSeries, pSeries, and OEM applications [PCIX slot pin B94] Pins 2,3,4,5 jumpered = Hydra 1.75 applications [PCIX slot pin B03]
J9	2	BATTERY DISCONNECT WIRE Allows opening the battery circuit by cutting the jumper wire. This zeroizes the on-card secure data and keys for the application.	Jumpered
J8	2	EXTERNAL INTRUSION LATCH DISABLE JUMPER HEADER This header may have a BERG jumper installed to disable the warning activation. Platforms that use the External Intrusion Latch Warning feature will remove this jumper in their assembly process.	Not Jumpered

c. Remove the expansion slot cover located over slot 5. Insert the Coprocessor in slot 5, making sure it is firmly seated.

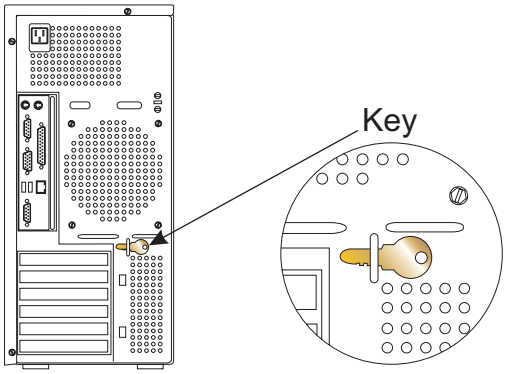
Secure the adapter with the screw supplied. Do not replace the rear adapter retention bracket.

5. Insert the tabs inside the side cover into the slots in the server frame.

   Press the side cover against the frame, making certain that the tabs all fit into their corresponding slots, then push the cover latch up.



Return the key to its storage position on the rear of the machine.



Note:

a. If you do not have the Smart Card Reader option continue to step 8 on page 2-11.

b. The 8485 TKE Workstation has both PS2 and USB ports.

c. In TKE V6.0, 2 types of Smart Card Readers are supported, Omnikey and Kobil.

d. Two Smart Card Readers of the same type, either both Omnikeys or both Kobils, must be attached.

6. Installing the Omnikey Smart Card Reader

   __ a. The Omnikey reader is a USB Smart Card reader. If you are using an Omnikey reader, simply plug it into any available USB port on the TKE machine.

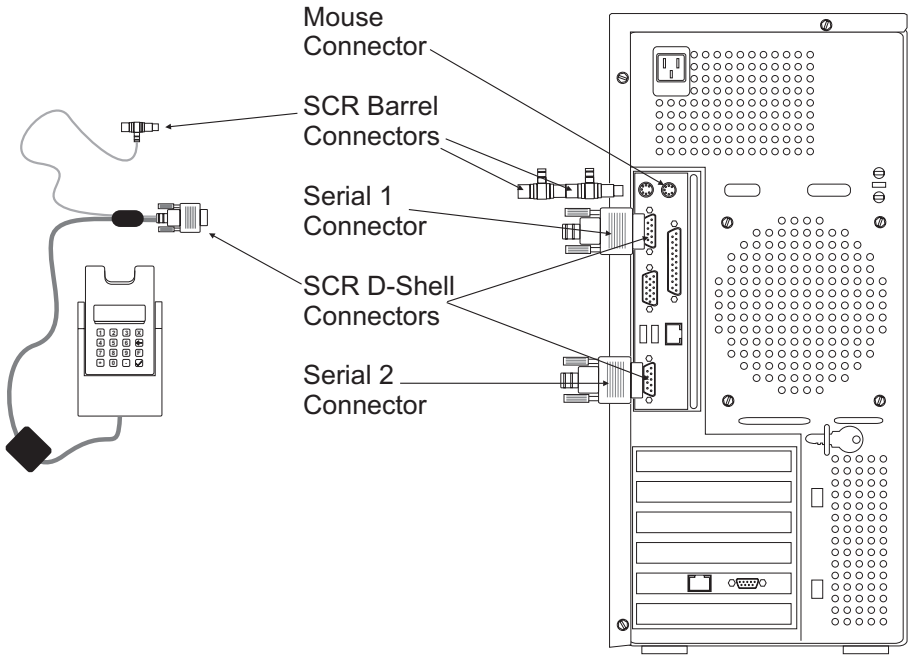
7. Installing the Kobil Smart Card Reader

__ a. Verify there is no power cord connected to the TKE system unit.

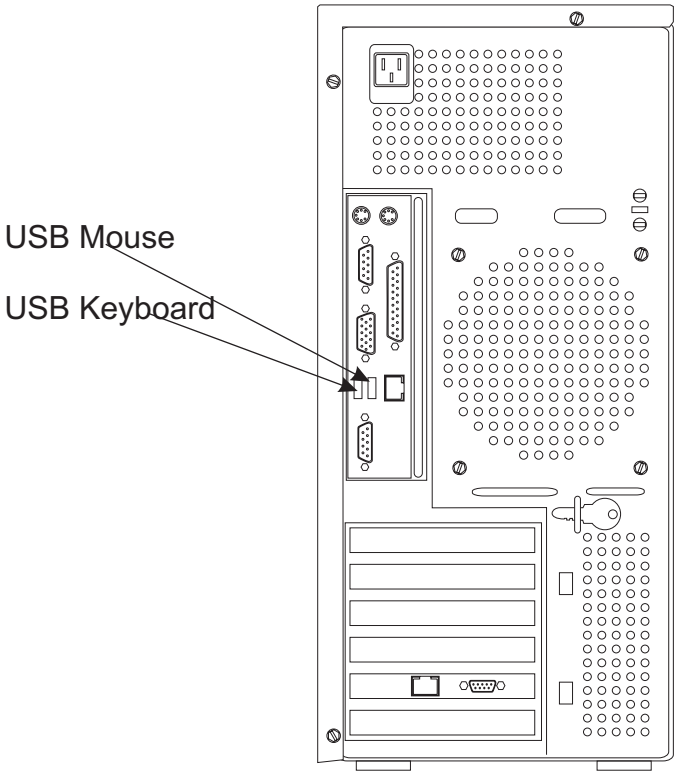
__ b. Plug one barrel connector from the Smart Card Reader(s) to the PS/2 mouse port .

__ c. Plug the second barrel connector from the Smart Card Reader(s) to the back of the first barrel connector.

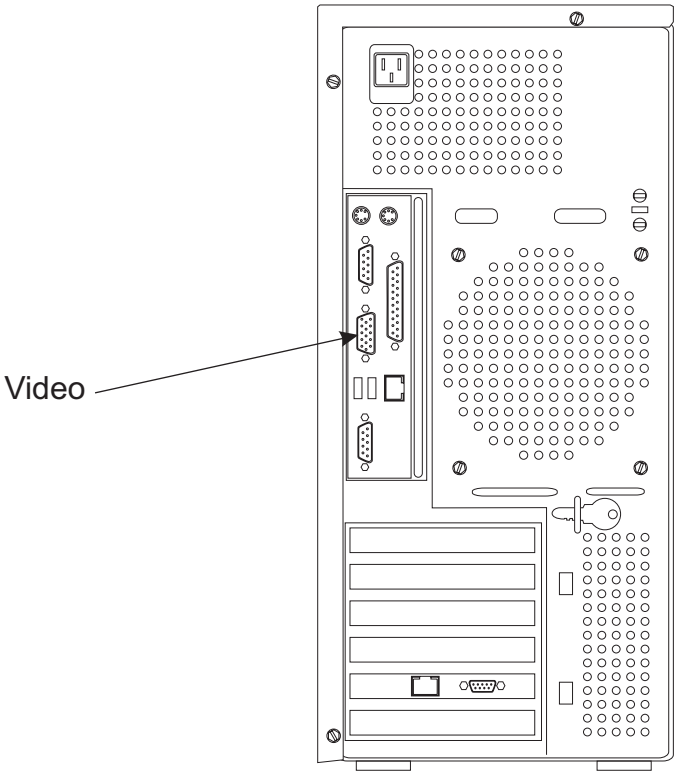
__ d. Connect the D-shell serial cable from one reader to Serial1 and the D-shell serial cable from the other reader to the Serial 2 connection at the rear of the system unit.



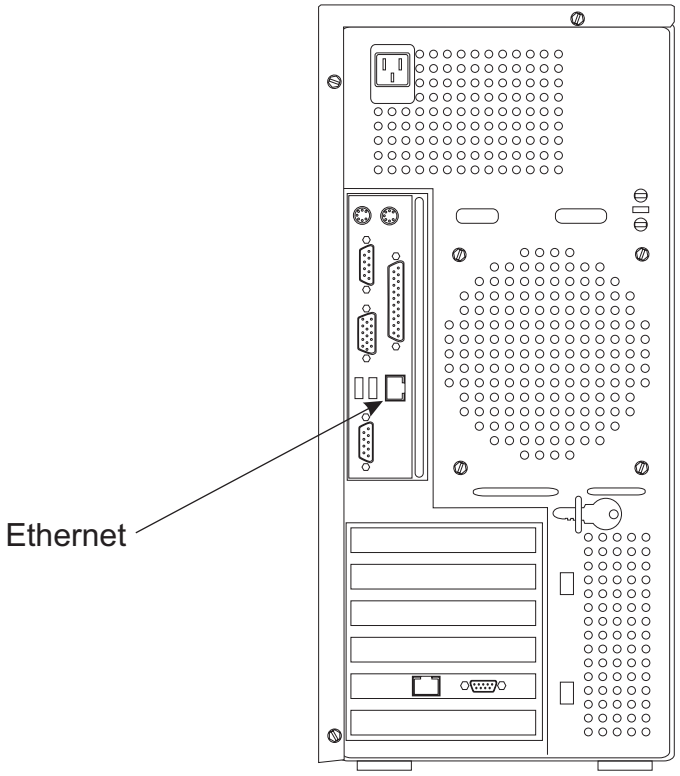
8. Connect the mouse cable to the USB port at the left of the Ethernet connector. Connect the keyboard cable to the left-most USB port.



9. Connect the display signal cable to the display connection at the rear of the system unit. You will find a display symbol defining the correct plug location.



10. Plug the Ethernet cable, **P/N 05N5292**, into the RJ45 port on the system unit connector panel.



Connect the other end of the Ethernet cable to the Switch.

11. Perform the impedance measurements using the ECOS C7106 tester (USA only).

    If the ECOS tester is not available, go to step 12.

    When the impedance measurements are correct, continue with the next step.

12. This procedure checks for a ground/earth resistance of one ohm or less at the receptacle ground/earth pin using the CE meter.

    The wall breaker should be OFF. Do the following to check the customer's power source:

    __ a. Using the CE meter, measure the resistance from the ground/earth pin of the receptacle to building ground/earth. The reading should be one ohm or less.

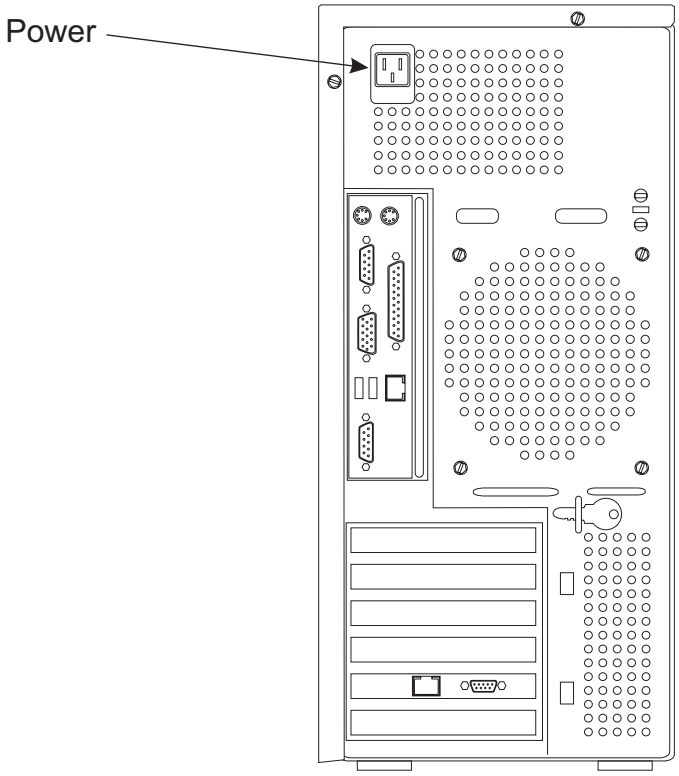
    __ b. For metal receptacle shells, also measure the resistance from the ground/earth pin of the receptacle to the metal shell. This reading should be 0.1 ohm or less.

    Note: Digital meters may give unstable resistance readings if leakage current is flowing in the building ground/earth circuit. If the reading appears unstable, or is greater than one ohm, contact your branch office installation planning representative or field manager.

13. **Attention:** Check the primary voltage switches on the system unit, display, and, if installed, the modem to ensure proper setting for your customer's power source (115V or 230V).

    Note: The display may not have primary voltage switches. Ensure it is enabled for the input voltage supplied by your customer.

    Connect the system unit and video display power cables to the rear of the units



Connect the power cables to building power.

14. Do the following to complete the installation:
    __ a. Power on the display, system unit, and, if installed, the modem and security interface unit.
    __ b. Ensure that the power on indicators are on for all units.
    __ c. Wait for the TKE Workstation to complete loading.
    __ d. Do not start the TKE application. Turn the Workstation over to the customer to complete the setup.

If the TKE Workstation does not start, use the procedures in this manual to resolve the problem.

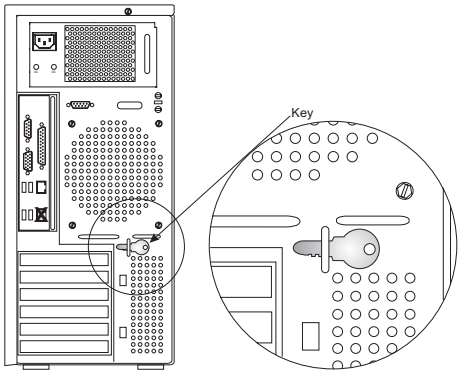
TKE installation - 4367

This section instructs you on how to install the 4367TKE Workstation and connect it to the system.

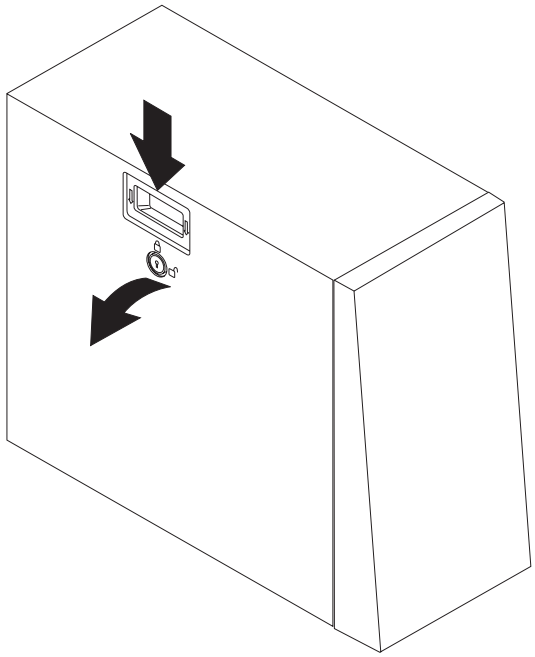
1. Open and unpack the ship box containing the TKE Workstation.

   This box also contains the cables. TKE 6.0 and later will contain a DVD-RAM for customer-specific data. Store the Code DVD-RAM, Backup DVD-RAM, diagnostic CD, customer-specific data DVD-RAM, documentation, and the key in an area near the console for future service use.

2. Find the key in its storage position on the rear of the machine.

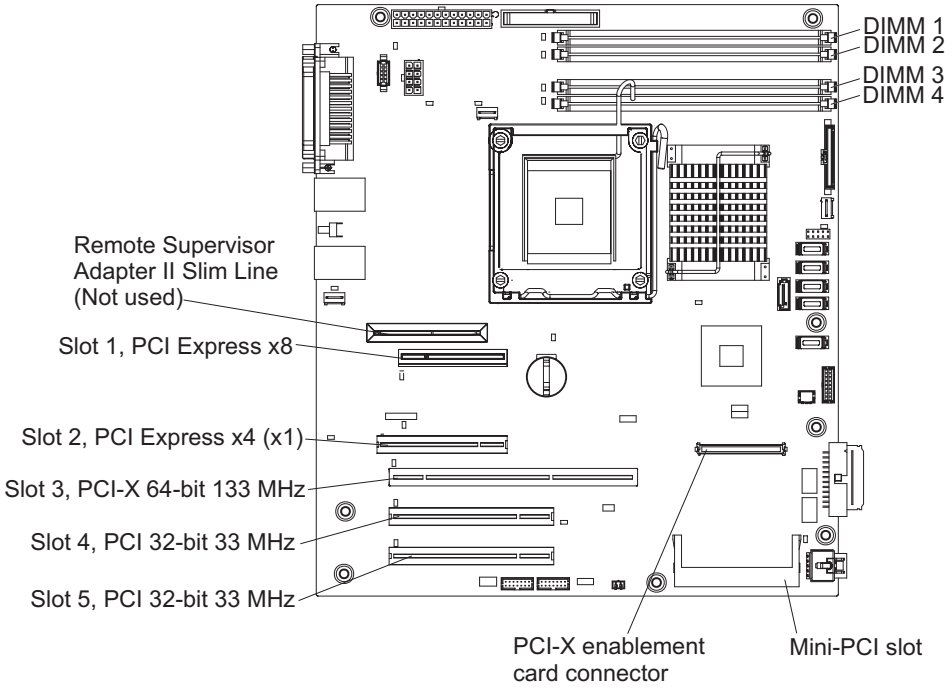


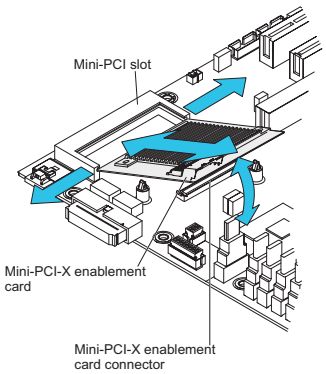
Unlock the side cover, then press the cover latch down.



Tilt the top of the cover away from the machine, then lift the cover off and set it aside.

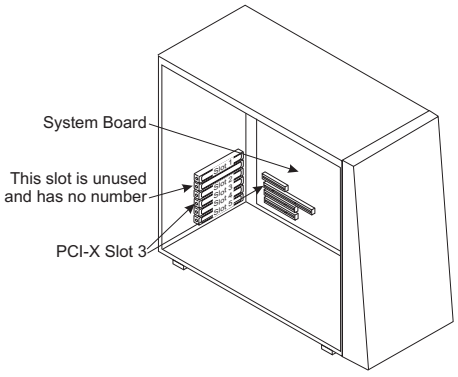
3. Verify there is a PCI-X Enablement Card installed in the lower right hand corner of the system board.





4. Rotate the rear adapter retention bracket (if present) to the open (unlocked) position and remove it from the machine.

   Remove the screw securing the expansion slot cover for slot 3.



   Remove the expansion slot cover and store the slot cover and its screw in a safe place for future use.

5. Install the **PCIX Cryptographic Coprocessor**

   a. Remove the PCIX Cryptographic Coprocessor from its shipping carton and static bag.

      Electrostatic discharge (ESD) can damage the card and its components. Wear an ESD wrist strap while handling and installing the card, or take the following precautions:

      Notes:

      1) Limit your movements; this helps prevent static electricity building up around you.
      2) Prevent others from touching the card or other components.
      3) Before removing the card from the anti-static bag, touch the bag to an unpainted metal surface on the computer and hold it there for at least two seconds.
      4) Store the carton and bag as they may be needed if the workstation is transported.

   b. Verify that the jumpers on the card are positioned correctly.

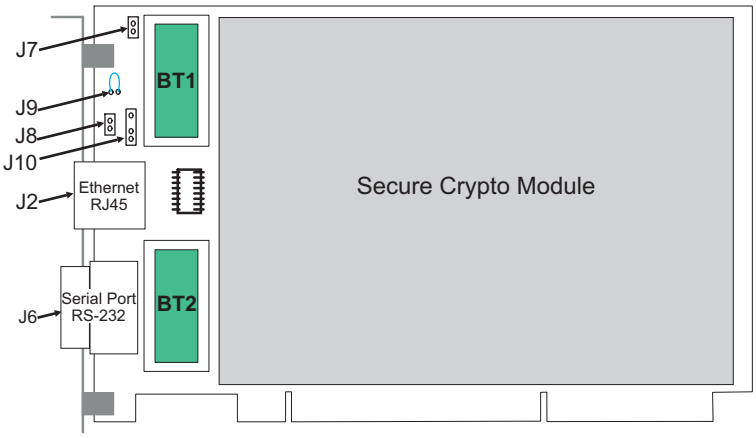


Table 2-4. Jumpers on a PCIX Bus-Based Cryptographic Adapter

Jumper	# Pins	Name of Jumper	Jumper Position
J7	2	PCIX VPD EEPROM WRITE Jumpered = PCIX EEPROM write-enabled No jumper = PCIX EEPROM write disabled	Jumpered
J10	3	BATTERY REPLACEMENT Connects to power cord externally while changing batteries BT1 and BT2.	Not Jumpered
J6	9	RS232 SERIAL PORT D-shell connector	
J2	8	Ethernet PORT RJ45 connector	

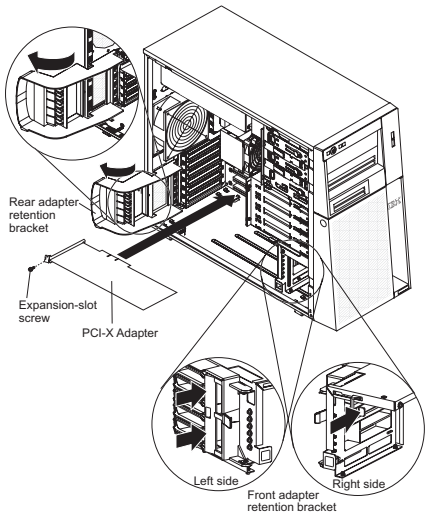
Table 2-4. Jumpers on a PCIX Bus-Based Cryptographic Adapter (continued)

Jumper	# Pins	Name of Jumper	Jumper Position
J11	5	EXTERNAL INTRUSION LATCH Pin 1 - Ground Pin 2 - B03 PCIX edge connector Pin 3 - External Warning Pin 4 - B94 PCIX edge connector Pin 5 - Ground Pin layout viewed from the back of the card: o o o o o 5 4 3 2 1	Pins 1,2,3,4 jumpered = Hydra 3, iSeries, pSeries, and OEM applications [PCIX slot pin B94] Pins 2,3,4,5 jumpered = Hydra 1.75 applications [PCIX slot pin B03]
J9	2	BATTERY DISCONNECT WIRE Allows opening the battery circuit by cutting the jumper wire. This zeroizes the on-card secure data and keys for the application.	Jumpered
J8	2	EXTERNAL INTRUSION LATCH DISABLE JUMPER HEADER This header may have a BERG jumper installed to disable the warning activation. Platforms that use the External Intrusion Latch Warning feature will remove this jumper in their assembly process.	Not Jumpered

c. Remove the expansion slot cover located over slot 3.

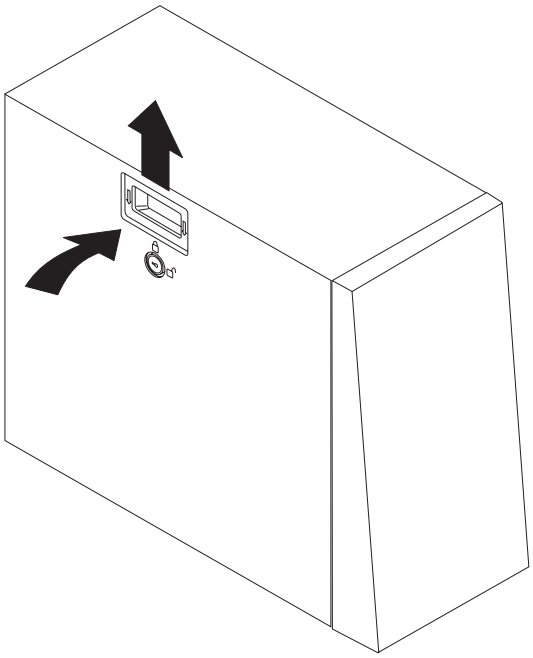
d. Insert the Coprocessor in slot 3, making sure it is firmly seated.

e. Secure the adapter with the screw supplied. Do not replace the rear adapter retention bracket.

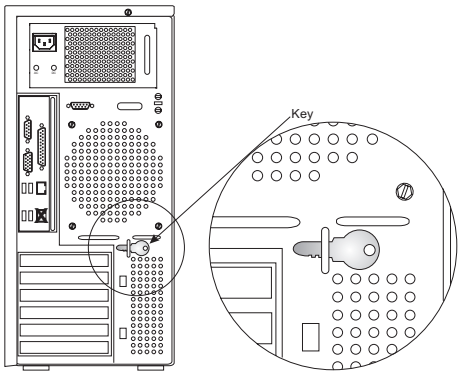


6. Insert the tabs inside the side cover into the slots in the server frame.

   Press the side cover against the frame, making certain that the tabs all fit into their corresponding slots, then push the cover latch up.



Return the key to its storage position on the rear of the machine.



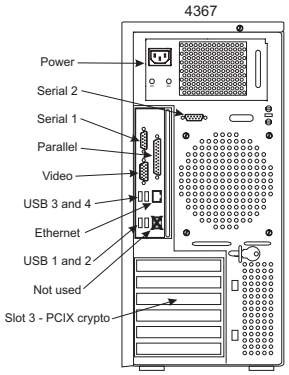
Note:

a. If you do not have the Smart Card Reader option continue to step 8 on page 2-20.

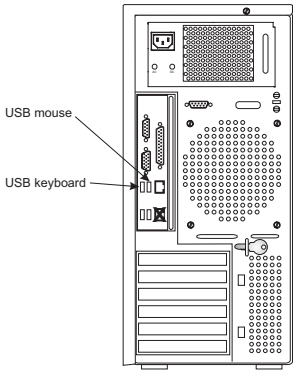
b. The 4367 TKE Workstation contains only USB ports and no PS2 ports. Therefore, the Omnikey Smart Card Reader is the ONLY type of reader that can be used with this model.

7. Installing the Omnikey Smart Card Reader

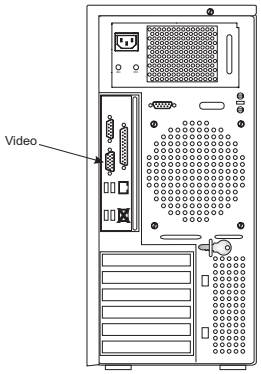
   a. The Omnikey reader is a USB Smart Card reader. If you are using an Omnikey reader, simply plug it into any available USB port on the TKE machine (USB port 1 or 2).



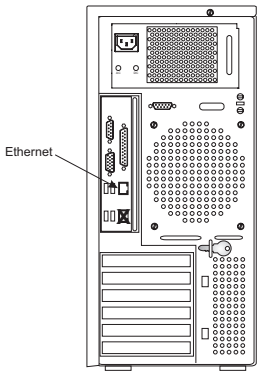
8. Connect the keyboard cable to USB port 3 and mouse cable to USB port 4 at the rear of the system unit.



9. Connect the video signal cable to the video connection at the rear of the system unit.



10. Plug the Ethernet cable, **P/N 05N5292**, into the RJ45 port on the system unit connector panel.



Connect the other end of the Ethernet cable to the HUB.

11. Perform the impedance measurements using the ECOS C7106 tester (USA only).

    If the ECOS tester is not available, go to step 12.

    When the impedance measurements are correct, continue with the next step.

12. This procedure checks for a ground/earth resistance of one ohm or less at the receptacle ground/earth pin using the CE meter.

    The wall breaker should be OFF. Do the following to check the customer's power source:

    __ a. Using the CE meter, measure the resistance from the ground/earth pin of the receptacle to building ground/earth. The reading should be one ohm or less.

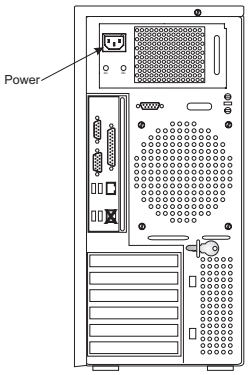
    __ b. For metal receptacle shells, also measure the resistance from the ground/earth pin of the receptacle to the metal shell. This reading should be 0.1 ohm or less.

    Note: Digital meters may give unstable resistance readings if leakage current is flowing in the building ground/earth circuit. If the reading appears unstable, or is greater than one ohm, contact your branch office installation planning representative or field manager.

13. **Attention:** If present, check the primary voltage switches on the system unit, display, and, if installed, the modem, to ensure proper setting for your customer's power source (115V or 230V).

    Note: The display may not have primary voltage switches. Ensure it is enabled for the input voltage supplied by your customer.

    Connect the following power cables to the rear of the units:
    - System unit
    - Display



Connect the power cables to building power.

14. Do the following to complete the installation:
    __ a. Power on the display, system unit, and, if installed, the modem and security interface unit.
    __ b. Ensure that the power on indicators are on for all units.
    __ c. Wait for the TKE Workstation to complete loading.
    __ d. Do not start the TKE application. Turn the Workstation over to the customer to complete the setup.

    If the TKE Workstation does not start, use the procedures in this manual to resolve the problem.

PCIX adapter card locations

8482

The PCI adapter slots are located on the bottom of the system unit (viewed from the rear). The slots are not physically numbered on the machine. However, for simplicity, in this document, they are numbered 1 through 8 from top to bottom looking at the back of the machine.

Slot	Bus	Feature Card
1	PCIX	PCIX Cryptographic Adapter

8485

The PCI adapter slots are located on the bottom of the system unit (viewed from the rear). The slots are not physically numbered on the machine. However, for simplicity, in this document, they are numbered 1 through 6 from top to bottom looking at the back of the machine.

Slot	Bus	Feature Card
5	PCIX	PCIX Cryptographic Adapter

4367

The PCI adapter slots are located on the bottom of the system unit (viewed from the rear). The slots are not physically numbered on the machine. However, for simplicity, in this document, they are numbered 1 through 5 from top to bottom looking at the back of the machine.

Slot	Bus	Feature Card
3	PCIX	PCIX Cryptographic Adapter

Replacing the PCIX cryptographic coprocessor batteries

Before beginning the procedure, read the following descriptive and cautionary information.

CAUTION:
Only trained service personnel may replace this battery. The battery contains lithium. To avoid possible explosion, do not burn or charge the battery.

Do not:
__ **Throw or immerse into water**
__ **Heat to more than 100°C (212°F)**
__ **Repair or disassemble**

Exchange only with the IBM-approved part. Recycle or discard the battery as instructed by local regulations. In the United States, IBM has a process for the collection of this battery. For information, call 1-800-426-4333. Have the IBM part number for the battery unit available when you call. (C002)

DANGER

When working on or around the system, observe the following precautions:

Electrical voltage and current from power, telephone, and communication cables are hazardous. To avoid a shock hazard:

- **Connect power to this unit only with the IBM provided power cord. Do not use the IBM provided power cord for any other product.**
- **Do not open or service any power supply assembly.**
- **Do not connect or disconnect any cables or perform installation, maintenance, or reconfiguration of this product during an electrical storm.**
- **The product might be equipped with multiple power cords. To remove all hazardous voltages, disconnect all power cords.**
- **Connect all power cords to a properly wired and grounded electrical outlet. Ensure that the outlet supplies proper voltage and phase rotation according to the system rating plate.**
- **Connect any equipment that will be attached to this product to properly wired outlets.**
- **When possible, use one hand only to connect or disconnect signal cables.**
- **Never turn on any equipment when there is evidence of fire, water, or structural damage.**
- **Disconnect the attached power cords, telecommunications systems, networks, and modems before you open the device covers, unless instructed otherwise in the installation and configuration procedures.**
- **Connect and disconnect cables as described in the following procedures when installing, moving, or opening covers on this product or attached devices.**

  To disconnect:

  1. **Turn off everything (unless instructed otherwise).**
  2. **Remove the power cords from the outlets.**
  3. **Remove the signal cables from the connectors.**
  4. **Remove all cables from the devices.**

  To connect:

  1. **Turn off everything (unless instructed otherwise).**
  2. **Attach all cables to the devices.**
  3. **Attach the signal cables to the connectors.**
  4. **Attach the power cords to the outlets.**
  5. **Turn on the devices.**
- **Sharp edges, corners and joints may be present in and around the system. Use care when handling equipment to avoid cuts, scrapes and pinching.**

(D005)

Two lithium batteries mounted on the PCIX Cryptographic Coprocessor supply power to the card's components, including protected memory. Your support software or application software can query the Coprocessor to determine whether the batteries need to be replaced.

When shipped from the factory, the protected memory contains a certified device key. If your Coprocessor has been initialized by support software, the protected memory contains secret data, including a master cryptographic key, user profiles, and user passwords.

Attention: If you remove either of the batteries without first backing up the power with a fresh battery, the data in protected memory can be lost. The Replacement Battery Kit for the IBM PCIX Cryptographic Coprocessor (FRU PN 12R6714) provides the battery holder needed to provide backup power while you replace the batteries.

To order the kit, contact your local IBM representative or your IBM Business Partner. OEM customers in the United States should call 1-800-IBMS-OEM (1-800-426-7636).

Lithium battery safety

A lithium battery can cause a fire, an explosion, or a severe burn. Do not recharge, disassemble, heat above 100 degrees C (212 degrees F), solder directly to the cell, incinerate, or expose the cell contents to water.

Keep away from children.

Replace only with the part number specified for this IBM product. Use of a different battery may present the risk of fire or explosion. The battery connector is polarized; do not attempt to reverse the polarity.

Dispose of the battery according to local regulations.

Your Replacement Battery Kit should include:

- Two fresh replacement Varta CR1/2 AA batteries.
- A battery holder with connecting wires.
- Two sets of spare battery attention labels (2X2)

To replace the batteries, follow these steps:

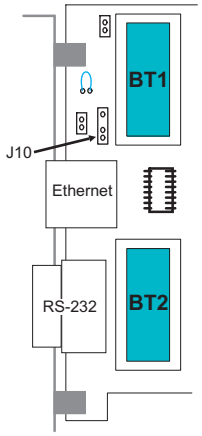
1. Turn off the computer and all attached devices.
2. Disconnect all cables, including the power cable.
3. Remove the cover from the expansion slots according to the directions provided with your computer.
4. Open the Battery Replacement Kit.

   Attention: Electrostatic discharge (ESD) can damage the Coprocessor card and its components. Wear an ESD wrist strap while handling and removing or installing the card, or take the following precautions:

   - Limit your movements; this helps prevent static electricity from building up around you.
   - Prevent others from touching the card or other components.
   - Handle the card by its edges only. Do not touch exposed circuitry and components.
5. Remove the PCIX Cryptographic Coprocessor card from the PCIX bus slot in the TKE Workstation.
6. Insert one of the new batteries into the battery holder provided with the kit. Align the “+” on the battery with the “+” on the battery holder (the end with the red wire).

Connect the holder's wires to the J10 connector located near the Ethernet RJ45 connector (shown at the right). The connector is polarized to ensure correct connection.

Attention: Any loss of power erases data stored in the card's protected memory. To prevent data loss, ensure that the battery holder contains a fresh battery and is attached to the J10 connector.



7. Remove the battery attention labels from the battery holders on the card. These labels can be torn off and discarded. They are to be replaced by the spare ones included in the kit.
8. Remove the battery in the **BT1** position. Turn the Coprocessor card over and insert a small object, such as a screwdriver, through the hole to eject the battery.
9. Replace the battery in the **BT1** position with a new battery.
10. Replace the battery in the **BT2** position with the battery in the battery holder. (The new battery already installed in the **BT1** position provides power to the PCIX Cryptographic Coprocessor while you perform this step.)
11. Disconnect the battery holder from the J10 connector and discard it.
12. Reapply the spare battery attention labels onto the holders on the card covering the batteries.
13. Re-insert the Coprocessor into the PCIX bus slot. Be sure the card is fully seated.
14. Replace the computer's cover.
15. Reconnect the power cable and any other cables you disconnected.
16. Reset the Low Battery indicator. From the Trusted Key Entry Workstation Console:
    - Click on **Trusted Key Entry**.
    - Sign on as **Admin** through the **Privileged Mode Access** on the TKE Welcome page.
    - Click on **Crypto Node Management Utility 3.50**.
    - When the **Crypto Adapter Logon** window appears, select **Passphrase Logon**.

      Note: **TKEADM** is only available if the crypto adapter has been initialized for passphrase use.
    - Type **TKEADM** for the userid.
    - Type **TKEADM** for the password or user defined password.
    - Click on **Logon.**

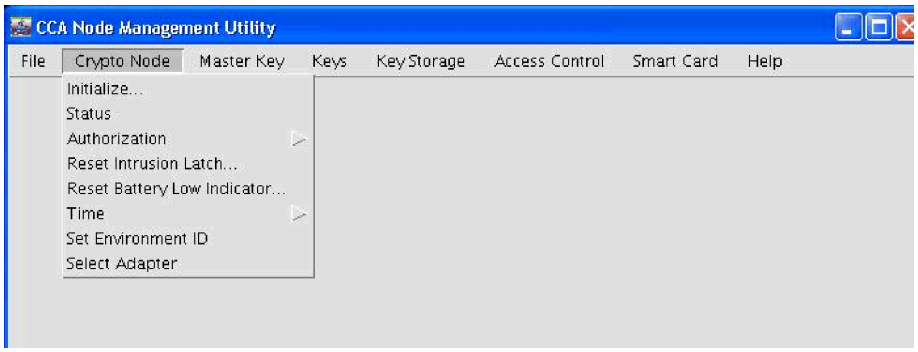
Notes:

a. Using **TKEADM** for the userid is optional. To reset the low battery indicator, logon with a userid whose role permits the **Reset Battery Low Indicator** operation.

b. If logging on as **TKEADM** the userid and password must be entered in upper case. Any other userid and password used does not have to be upper case but is case sensitive.

c. The same applies if a Smart Card environment has been deployed. Refer to *Trusted Key Entry PCIX Workstation User's Guide*, SA23-2211–05, for instructions to log on with Smart Cards.

- Click on **Crypto Node** pulldown menu located at the top of the **CCA Node Management Utility** window.



- Select **Reset Battery Low Indicator**.
- The battery low indicator is reset.
- Click **OK** to finish.
- Exit **CNM**.

17. The batteries are lithium 3-volt batteries. Recycle or dispose of the old batteries as required by local law. You have completed the procedure for replacing the PCIX Cryptographic Coprocessor batteries.

End of procedure

Determining Crypto Adapter Code Loaded

There may be times that the level of code installed in the TKE Workstation Crypto Adapter needs to be queried to determine its Licensed Internal Code (LIC) level. With this information, it can then be determined if the code is at the proper level, enabling steps to be taken to resolve any issues that are identified. These steps should always be done either after replacing or exchanging the crypto adapter in a TKE or when problems are encountered with the TKE Workstation Crypto Adapter.

For details on using the **CCA CLU Utility**, view the **readme file** by selecting the menu item **Help**, then click **Contents**, or in the "TKE Trusted Key Entry PCIX Workstation User's Guide", SA23-2211–05 appendix: "Trusted Key Entry – Workstation Cryptographic Adapter Initialization".

Note: Note: For TKE 5.3 and later, it is important that no other actions are done before the CLU actions after the rebooting of the workstation.

Check Coprocessor Code Level

Note: For TKE 5.0 to 5.2, skip to step 3. For TKE 5.3 and later, begin with step 1.

1. Reboot the TKE:
   a. Click on **Service Management** in the left section of the window: "Trusted Key Entry Console Workplace (Version X.X)".
   b. Click on **Shutdown or Restart**.
   c. Select the radio button next to: **Restart console**.
   d. Click the **OK** button.
2. When the TKE comes back up, login as **Admin or PEMODE**:
   a. Close the window "Trusted Key Entry Console Workplace (Version X.X)" by clicking the **X** button in the upper right corner.
   b. On the "Window Welcome to the Trusted Key Entry Console (Version X.X)", click on the **Privileged Mode Access** link.
   c. Sign on as either **pemode** or **admin**. (admin default password: password)
3. Open the CLU application:
   a. On the left section of the "Trusted Key Entry Console Workplace (Version X.X)"window, click on the **Trusted Key Entry** link.
   b. Click on the link **CCA CLU X.XX**
4. Check the Coprocessor Status
   a. Check the box next to **Check Coprocessor Status**.
   b. Click the **Run** button. The command may take several minutes to execute.
   c. The operation has completed when you see the message “All CLU commands completed successfully.” Click the **OK** button and continue to Step 5.

d. If the error message shown below is returned or you wait for over an hour and do not get the error message or the successful message, send the **cluout.log** in the **TKE Data Directory** and a description of any odd behavior to TKE Service. **Do not continue these procedures.**

5. Check the results of the Check Coprocessor Status and determine action needed
   a. Click **View -> Output Log**
   b. Compare the information in the Output Log with the information here. To do so, scroll to the information after the correct date/time stamp:
      - If the value for Segment 1 Image contains the word **factory**, then go to the section **Loading PCIX TKE adapter card code** and execute the actions described there.
      - If the value for Segment 1 Image does NOT contain the word **factory**, then compare the values for your segments 1, 2 and 3 with the values in the following chart, based on the release of TKE.

Table 2-5. Segment Values Based on TKE Level

TKE Release	Correct values for segments
TKE 5.0 TKE 5.1 TKE 5.2	Segment 1 Image: 3.22 POST1V2, MB1 V1.25 FPGAv78 Segment 2 Image: 3.10 Linux OS Segment 3 Image: 3.10.SC CCA
TKE 5.3	Segment 1 Image: 3.40 POST1v2.16 MB1v1.25 FPGAv78 Segment 2 Image: 3.40.01 Linux OS Segment 3 Image: 3.40.01 CCA
TKE 6.0	Segment 1 Image: 3.50 POST1v2.16 MB1v1.25 FPGAv78 Segment 2 Image: 3.50.00 Linux OS Segment 3 Image: 3.50.00 CCAS

Otherwise, if the values in the Output Log match those of the table for the version of the TKE, then your TKE Workstation Crypto Adapter LIC is at the correct level. If the values in the Output Log do not match the table, your TKE Workstation Crypto Adapter LIC is not at the correct level. Proceed to the section "Correcting PCIX TKE adapter card code"and execute the actions specified to upgrade the TKE Workstation Crypto Adapter LIC to the correct level.

Correcting PCIX TKE adapter card code

The TKE card is preloaded in manufacturing prior to being sent to the customer. Attempting to load code to a card which has already been loaded may result in bad status returned. Perform the following step only if it's been determined the PCIX TKE adapter is loaded incorrectly by executing the tasks in section: "Determining Crypto Adapter Code Loaded".

The following steps will have you install the proper Segment 1, Segment 2, and Segment 3 code to the PCIX TKE adapter card if the code is not at the correct level.

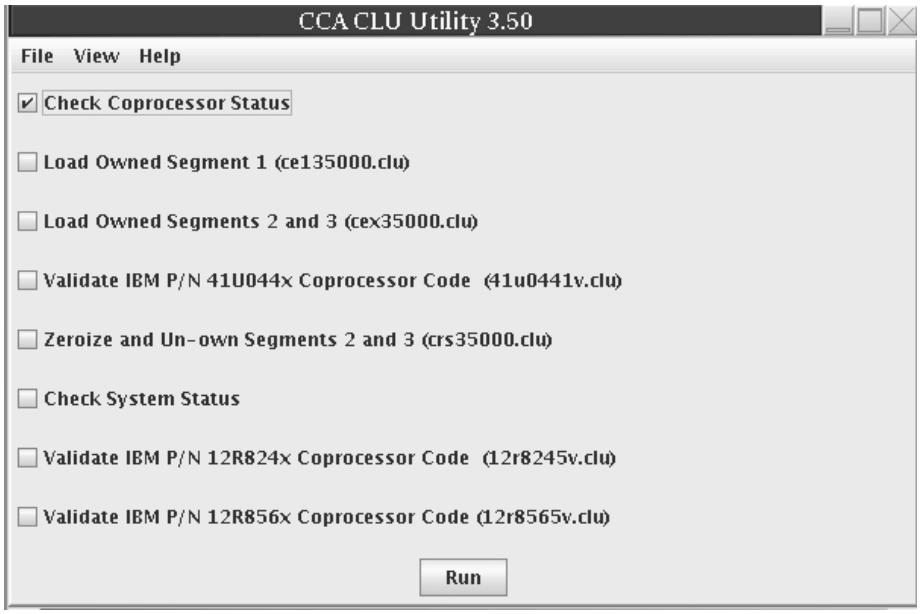
The PCIX TKE adapter card has been installed or replaced and the Workstation has been powered up.

For details on using the **CCA CLU Utility**, view the **readme file** by selecting the menu item **Help**, then click **Contents**, or in the "TKE Trusted Key Entry PCIX Workstation User's Guide", SA23-2211–05 appendix: "Trusted Key Entry – Workstation Cryptographic Adapter Initialization".

Note: For TKE 5.3 and later, it is important that no other actions are done before the CLU actions after the rebooting of the workstation.

Wait for the TKE Workstation to complete Power-On initialization.

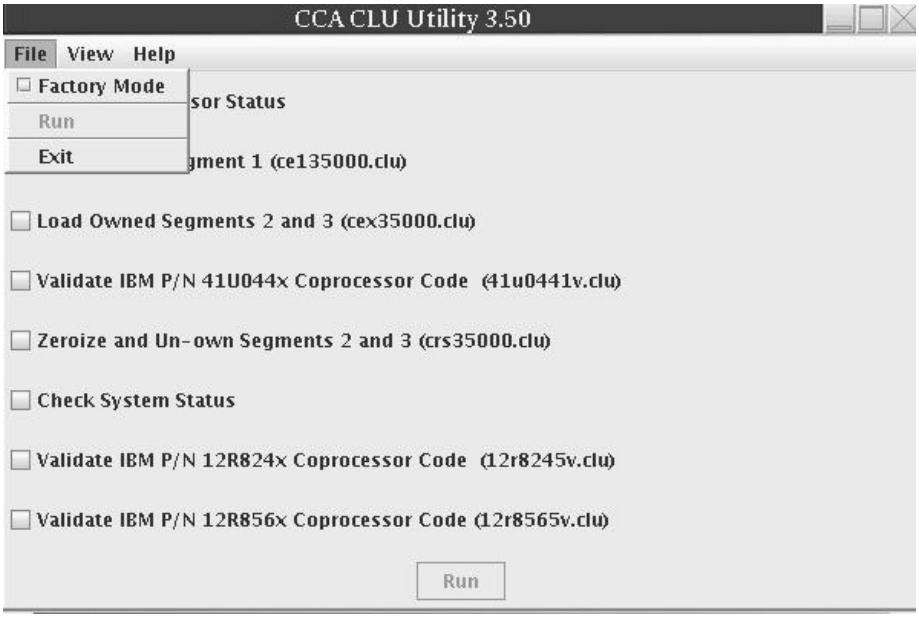
1. Sign on as **ADMIN** through the **Privileged Mode Access** link on the TKE Welcome page.
2. From the **Trusted Key Entry Workstation Console** display window:
   a. Click on **Trusted Key Entry**.
   b. Click on **CCA CLU 3.50**.
3. Display the status of the PCIX TKE adapter card:
   a. Click the checkbox for **Check Coprocessor Status**.



   b. Click **RUN** to execute the command. The command may take several minutes to execute.
   c. Click menu item **View**.

d. Click **Command History** to view the output of the command.

4. To load **Owned Segment 1**:
   a. Make sure the **Factory Mode** checkbox from the **File** menu is NOT checked.



   b. Select the **Load Owned Segment 1** code. **(ce135000.clu)**.
   c. Click **Run**. The command may take several minutes to execute.
   d. Select the menu item **View**.
   e. Select **Command History** to see the output of the command.
5. Select the **Load Owned Segments 2 and 3 (cex35000.clu)** checkbox.
   a. Click **Run**. The command may take several minutes to execute.
   b. Select the menu item **View**.
   c. Select **Command History** to see the output of the command.
6. Display status of the PCIX TKE adapter card.
   a. Click the checkbox for **Check Coprocessor Status**.
   b. Click **RUN** to execute the command. The command may take several minutes to execute.
   c. Click menu item **View**.
   d. Click **Command History** to view the output of the command.

Note: For TKE 6.0, after upgrading the TKE Workstation Crypto Adapter LIC, the function control vector must also be loaded, as it has changed. See section: "Loading the function control vector for the PCIX TKE Adapter", for instructions to do this.

End of Procedure.

Loading PCIX TKE adapter card code

The TKE card is preloaded in manufacturing prior to being sent to the customer. Attempting to load code to a card which has already been loaded may result in bad status returned. Perform the following step only if it's been determined the PCIX TKE adapter is not loaded or is loaded incorrectly.

The following steps will have you add Factory Segment 1, Segment 2, and Segment 3 code to the PCIX TKE adapter card if the code was not previously loaded.

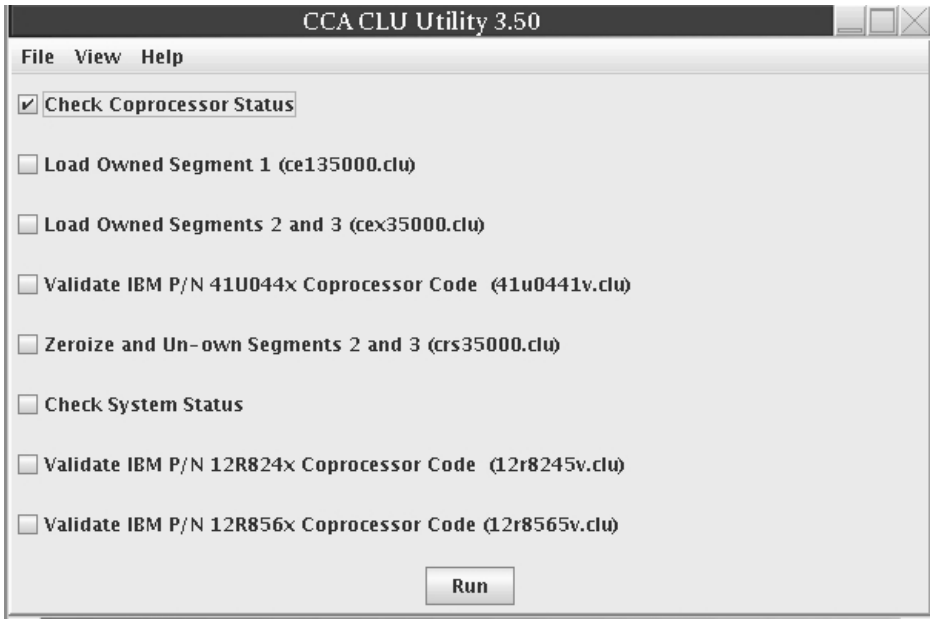
The PCIX TKE adapter card has been installed or replaced and the Workstation has been powered up.

For details on using the **CCA CLU Utility**, view the **readme file** by selecting the menu item. **Help**, then click **Contents**.

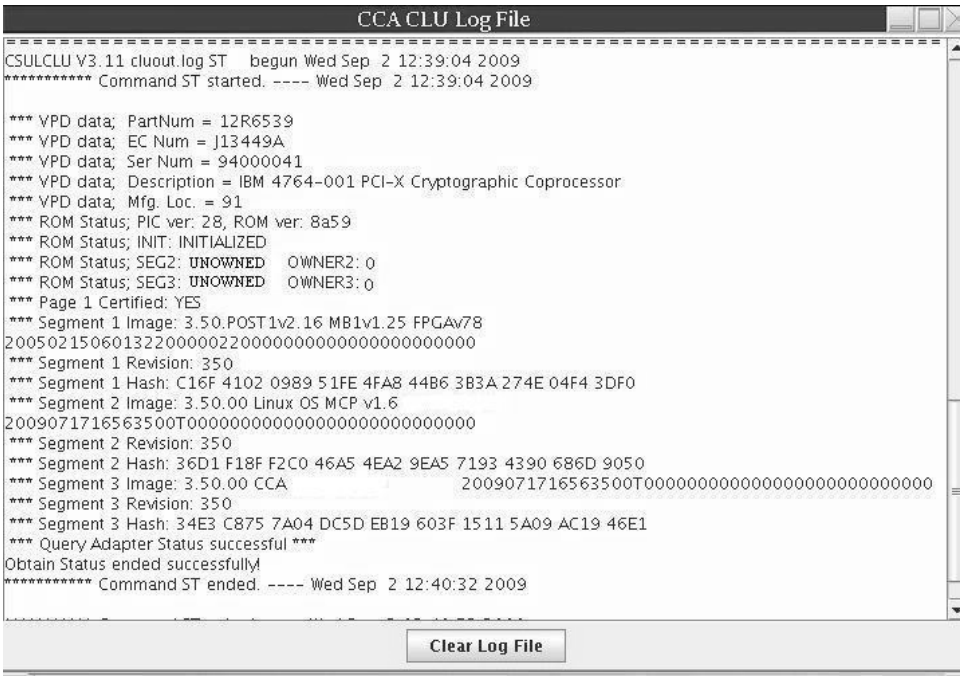
Note: If you are running with TKE 5.3 or 6.0, you must perform CLU actions after your system has been rebooted and before attempting to use any other utility or application that communicates with the TKE adapter card.

Wait for the TKE Workstation to complete Power-On initialization.

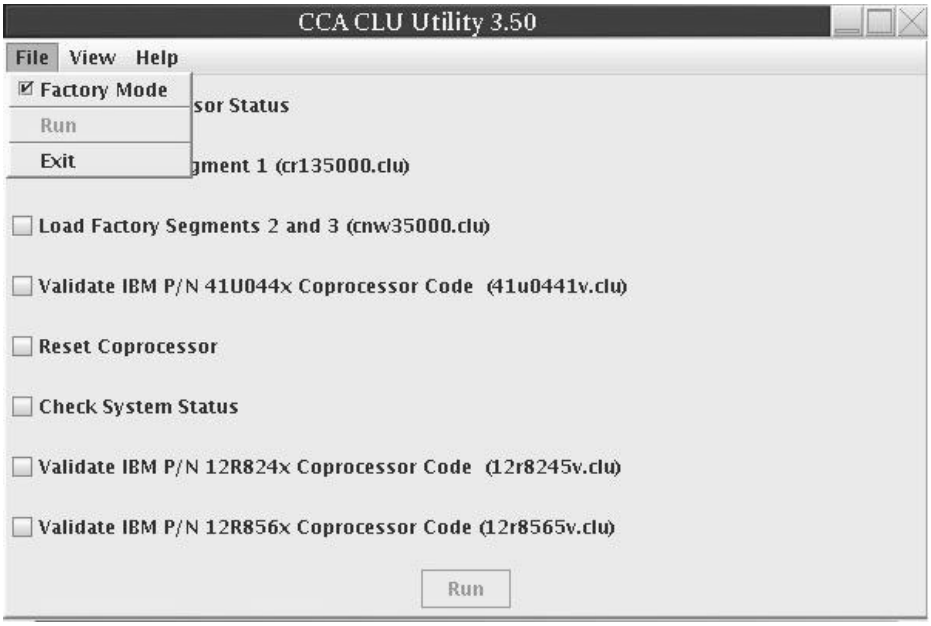
1. Sign on as **ADMIN** through the **Privileged Mode Access** link on the TKE Welcome page.
2. From the **Trusted Key Entry Workstation Console** display window:
   - Click on **Trusted Key Entry**.
   - Click on **CCA CLU 3.50**.
3. Display the status of the PCIX TKE adapter card:
   - Click the checkbox for **Check Coprocessor Status**.



   - Click **RUN** to execute the command. The command may take several minutes to execute.
   - Click menu item **View**.
   - Click **Command History** to view the output of the command.

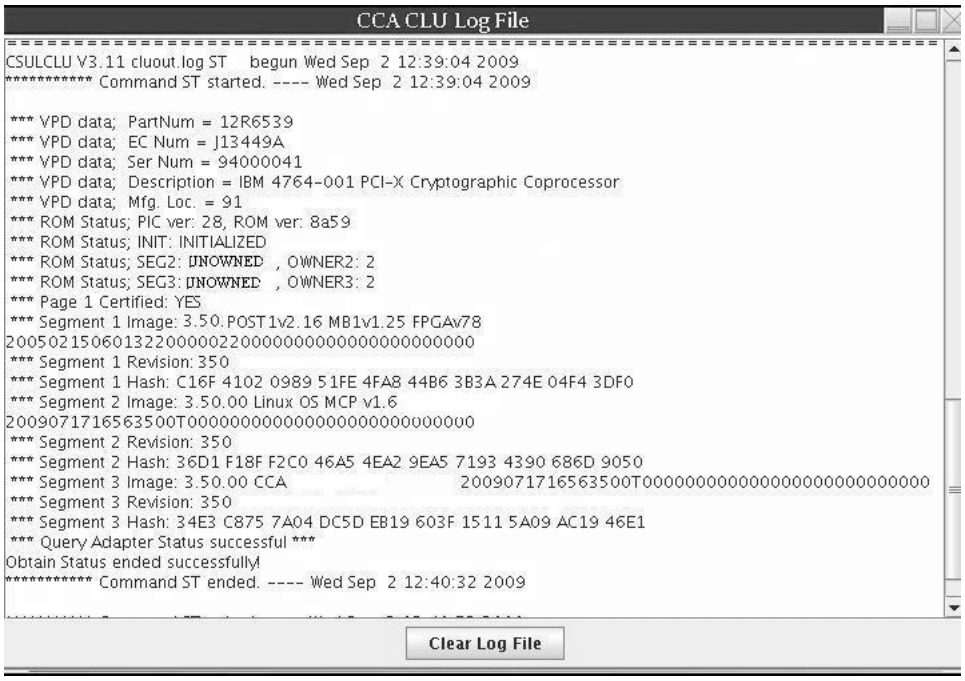


4. To load **Segment 1 Factory Mode**:
   - Select the **Factory Mode** checkbox from the **File** menu.



   - Select the **Load Factory Segment 1** code. **(cr135000.clu)**.
   - Click **Run**. The command may take several minutes to execute.
   - Select the menu item **View**.
   - Select **Command History** to see the output of the command.
5. Select the **Load Factory Segments 2 and 3 (cnw35000.clu)** checkbox:
   - Click **Run**. The command may take several minutes to execute.
   - Select the menu item **View**.
   - Select **Command History** to see the output of the command.
6. Display status of the PCIX TKE adapter card:

- Click the checkbox for **Check Coprocessor Status**.
- Click **RUN** to execute the command. The command may take several minutes to execute.
- Click menu item **View**.
- Click **Command History** to view the output of the command.



Note: After loading the PCIX TKE adapter card code, proceed to the steps in the sections "Initializing the PCIX TKE adapter" and "Loading the function control vector for the PCIX TKE adapter". These procedures are necessary to put the TKE Workstation Crypto Adapter into the correct state to begin "TKE Workstation Setup and Customization" as described in the "Trusted Ket Entry PCIX Workstation User's Guide", SA23-2211-05.

End of Procedure

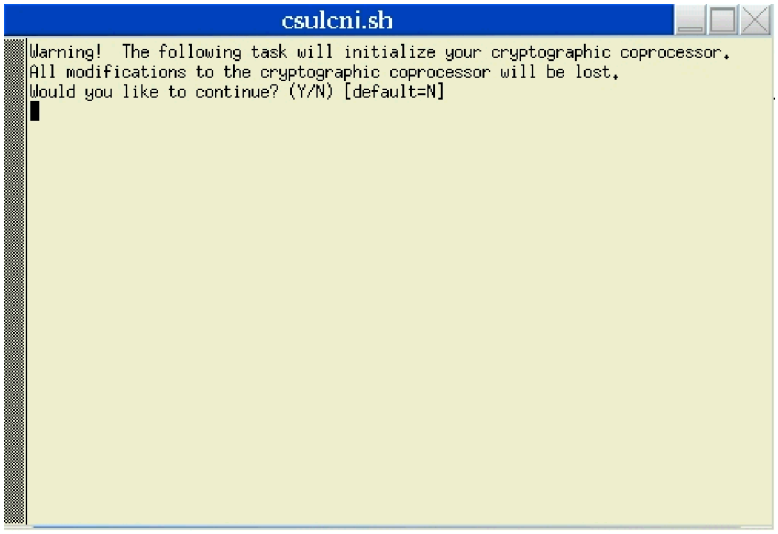
Initializing the PCIX TKE adapter

If a PCIX TKE adapter is replaced or exchanged, it must be initialized before it can be used. The following procedure will initialize a new PCIX TKE Cryptographic Coprocessor Adapter.

Note: To initialize a PCIX TKE adapter, the user must log on to the console as the **ADMIN** user. The initialization task is not available for the default **TKEUSER** logon.

From the **Trusted Key Entry Workstation Console** display window:

- Click on **Trusted Key Entry**.
- Click on **TKE's IBM Crypto Adapter Initialization**.
- Reply **Yes** to the warning:
  The following task will initialize your cryptographic coprocessor. All modifications will be lost. Would you like to continue? (Y/N)



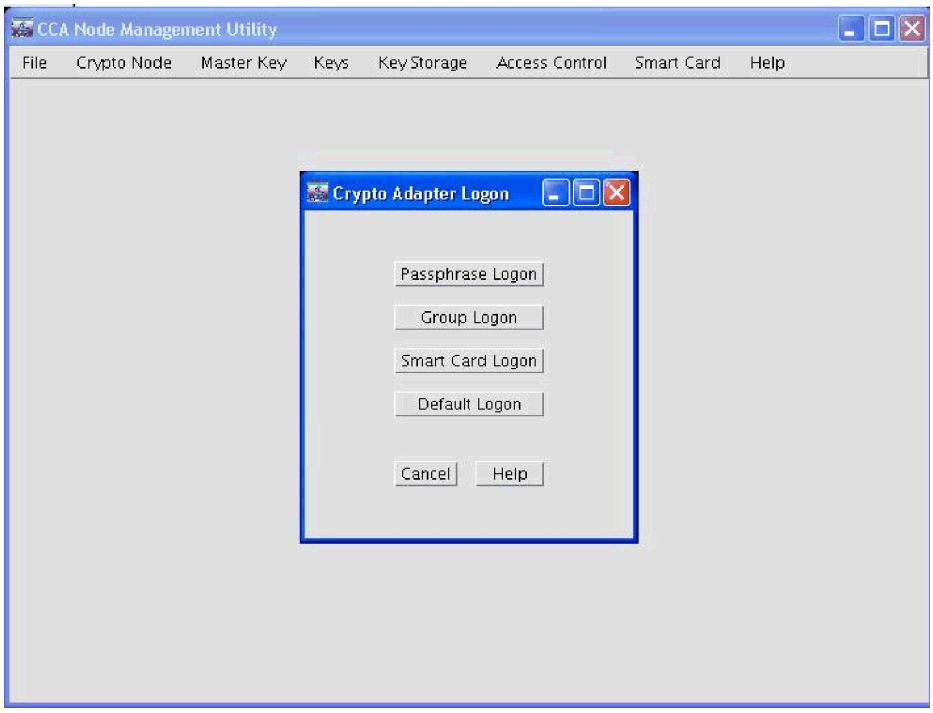
- Reply **P** to the question:
  Would you like to prepare your cryptographic coprocessor for SmartCard or Passphrase use? (S/P)
- Output from the initialization will be displayed.
- Click **Enter** to exit.

Refer to the *Trusted Key Entry PCIX Workstation User's Guide*, SA23-2211–05, if Smart Card configuration is needed.

Loading the function control vector for the PCIX TKE adapter

This section assists you in loading the Function Control Vector to the PCIX TKE adapter card.

1. Sign on as **ADMIN** through the Privileged Mode access link on the TKE Welcome page.
2. From the **Trusted Key Entry Workstation Console** display window:
   - Click on **Trusted Key Entry**
   - Click on **Cryptographic Node Management Utility 3.50**.
   - Select **Passphrase Logon** from the dialog box.



   - Type **TKEADM** for the userid.

     Note: **TKEADM** is only available if the crypto adapter has been initialized for passphrase use.
   - Type **TKEADM** for the password or the user defined password.
   - Click on **Logon**.

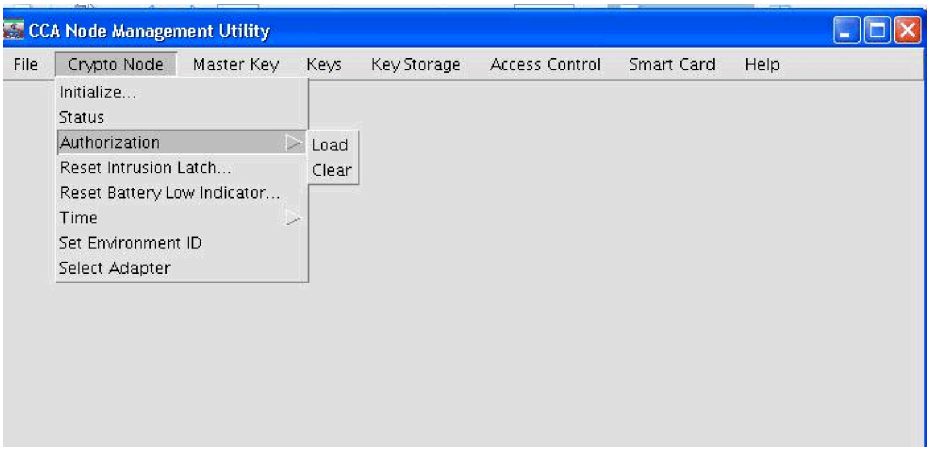
     Notes:

     a. Using **TKEADM** for the userid is optional. To load the Function Control Vector, logon with a userid whose role permits the Load Function-Control Vector operation.

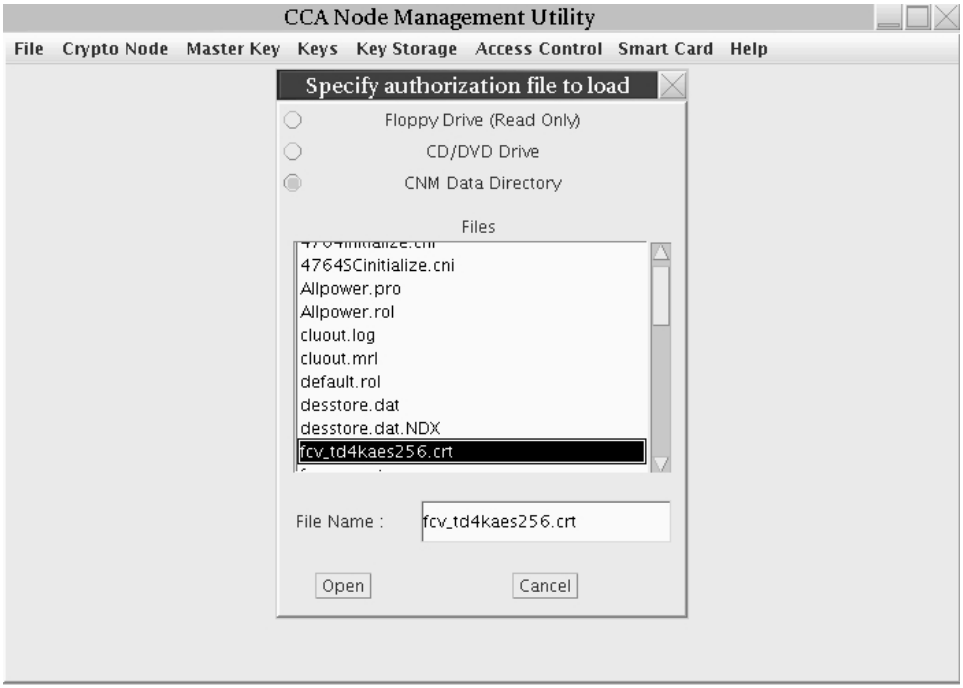
     b. If logging on as **TKEADM**, the userid and password must be entered in upper case. Any other userid and password used does not have to be upper case but is case sensitive.

     c. The same applies if a Smart Card environment has been deployed. Refer to *Trusted Key Entry PCIX Workstation User's Guide*, SA23-2211–05, for instructions to log on with Smart Cards.
3. To select the Function Control Vector (FCV) filename:
   - Click on the **Crypto Node** pull down menu located at the top of the Select **CCA Node Management Utility** window.

- Select **Authorization**. A sub-menu is displayed.



- Select **Load**. You are prompted to specify the filename of the FCV. Ensure you are in the subdirectory **CNM Data Directory**.
- Select **fcv_td4kaes256.crt**.
- Click on **Open** to proceed.



4. A pop-up is displayed prompting you for confirmation. Click on **Yes**. The FCV is loaded to the PCIX TKE adapter card. Click on **OK** to finish.
5. Exit and Logoff the PCIX TKE adapter card.
   - Click on the **File** pull down menu.
   - Select **Exit and Logoff** to logoff the PCIX TKE adapter card.
   - Click on **Yes**. This is in response to the Logoff screen message "Are you sure you want to logoff of the cryptographic coprocessor?"
   - Click on **OK**. This is in response to the Logoff screen message "Logoff successful".

Transporting a TKE Workstation with the PCIX coprocessor adapter installed

This section details the special considerations for the handling, storage, and transport of a TKE Workstation with the PCIX Coprocessor Adapter installed.

Each IBM 4764 PCIX Cryptographic Coprocessor is shipped from the factory with a certified device key. This electronic key, stored in the card's battery-powered protected memory, digitally sends test messages to confirm that the PCIX Cryptographic Coprocessor is genuine and that no tampering has occurred.

Note: If any of the secure module's tamper sensors are triggered by tampering or accident, the coprocessor erases all data in the protected memory, destroying the device key. The PCIX Cryptographic Coprocessor cannot operate without the device key. To protect the key, follow these environmental specifications:

- Operating
  - Temperature: +10 degrees C to +40 degrees C (+50 degrees F to +104 degrees F)
  - Relative Humidity: 8% to 80%
- Storage
  - Temperature: +1 degree C to +60 degrees C (+33.8 degrees F to +140 degrees F)
  - Relative Humidity: 5% to 80%
- Shipping
  - Temperature: -15 degrees C to +60 degrees C (+5 degrees F to +140 degrees F)
  - Relative Humidity: 5% to 100%

Do NOT remove the coprocessor's batteries. Data in the protected memory is lost when battery power is removed.

If the TKE Workstation is to be transported, remove the PCIX Cryptographic Coprocessor, storing it in it's insulated shipping container if temperature and humidity limits cannot be maintained.

TKE licensed internal code

This section contains procedures and information about the Licensed Internal Code (LIC) for TKE Workstations.

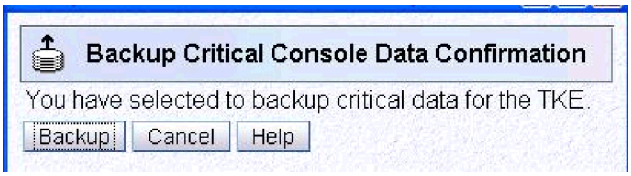
Saving the configuration for PCIX TKE

You should backup the TKE Workstation each time you alter the configuration. The **Backup Critical Console Data** task on TKE 6.0 saves changed customer configuration information from the TKE related data directories as well as any Machine Change Level (MCL) information that may have been applied after the initial code load. The information is saved to a DVD-RAM.

Note: A TKE Backup DVD-RAM is shipped with each TKE 6.0 Workstation. The TKE Backup DVD-RAM must have a volume identifier (VOLID) field that is ACTBKP or the task will fail. The backup DVD-RAM, in addition to the Base Code DVD, is used if an install or recovery of the hard drive becomes necessary.

The **Backup Critical Console Data** is done as follows:

1. Ensure the BACKUP DVD-RAM is inserted in the DVD drive.
2. To invoke this task, logon as either **ADMIN** or **SERVICE**.
3. From the **Trusted Key Entry Console** display window, click on **Service Management** in the left frame.
4. Click on **Backup Critical Console Data** in the right frame.



5. Click on **Backup** on the **Backup Critical Console Data Confirmation** window. Progress windows display.
6. When complete, click **OK.**
7. Give the DVD-RAM to the customer to be stored in a secure place.

   End of procedure

Note: **Backup Critical Console Data** can be executed as a scheduled operation. This is recommended so the customer can always have the latest updates/changes saved to the Backup DVD-RAM. Refer to *Trusted Key Entry PCIX Workstation User's Guide*, SA23-2211–05, for instructions on Customizing Scheduled Operations. For additional details about LIC 5.0 - 5.3, **Backup Critical Console Data** , refer to the *Service Guide for Trusted Key Entry Workstations* at LIC 5.0 and 5.1, GC28-6862-00, the *Service Guide for Trusted Key Entry Workstations* at LIC 5.2, GC28-6862-01. and the *Service Guide for Trusted Key Entry Workstations* at LIC 5.3, GC28-6862-02.

If the customer wants to have specific files saved to diskette or DVD-RAM for backup purposes other than install/recovery situations, files can be backed up manually using the TKE File Management Utility. This task will be performed by the customer.

To back up specific files:

1. Ensure the formatted diskette or DVD-RAM is inserted in the appropriate drive.

2. Sign on as **ADMIN** through the Privileged Mode access link on the TKE Welcome page.
3. From the **Trusted Key Entry Workstation Console** display window, click on **Trusted Key Entry**.
4. Click on **TKE Media Manager**.
5. Select **Activate the appropriate media device**.
6. Click **OK**.
7. Copy the desired files from the applicable Data Directory to the selected media with the File Management Utility. Refer to *Trusted Key Entry PCIX Workstation User's Guide*, SA23-2211–05, for details on using the File Management Utility.
8. Select **Deactivate the appropriate media device**.
9. Click **OK**.
10. Close **TKE Media Manager** by clicking **Cancel**.
11. Remove the diskette or DVD-RAM and store in a secure place.

End of procedure

Installing and restoring the PCIX TKE hard drive internal code

This procedure loads the PCIX TKE Workstation licensed internal code from a DVD to the Workstation's hard disk. Use it when:

- A hardware failure damages the hard drive information
- The hard drive is exchanged

You will need:
- Base code DVD
- TKE Backup DVD-RAM (ACTBKP)

To install/restore the hard drive internal code, logon as either **ADMIN** or **SERVICE**

The DVD is bootable. If the DVD does not boot or fails to load TKE Workstation code, verify the following:

- The DVD is listed as the second startup device under "Startup Sequence Options". Refer to "Trusted Key Entry Workstation configurations" on page 2-48.
- The PCIX TKE adapter is correctly configured and installed.

In TKE V6.0 you can find this under **Service Management**/**Backup Critical Console Data**. If the customer has previously used this utility, there should be a DVD-RAM disk with the output from the utility. When you are instructed to insert the backup DVD, put the customer's disk in the DVD drive to continue.

Restore the hard drive as follows:

1. Install the DVD into the DVD-RAM drive.
2. Shutdown the workstation.
3. From the **Trusted Key Entry Console**, click on **Service Management** in the left frame.
4. Click on **Shutdown or Restart** in the right frame.
5. Select **Power Off/Shutdown.**
6. Power up the workstation.
7. Follow the instructions for **Install/Recovery** to load code on the hard drive.

   Note: During code installation, the PC will reboot several times and will pause displaying the **TKE Restore Program** screen.

If you were restoring the Workstation internal code to the original level, notify the customer that any TKE changes and workstation internal code changes made after the last **Backup Critical Console Data** must be restored or reinstalled.

After the code has been installed/restored, do the following:

1. Wait for the **Trusted Key Entry Console** to complete loading.
2. Click on **Trusted Key Entry**.
3. Click on **Trusted Key Entry Workstation 6.0**.

Note: For TKE LIC V5.0 - V5.2, refer to the *Service Guide for Trusted Key Entry Workstations* at LIC 5.0 and 5.1, GC28-6862-00, the *Service Guide for Trusted Key Entry Workstations* at LIC 5.2, GC28-6862-01. and the *Service Guide for Trusted Key Entry Workstations* at LIC 5.3, GC28-6862-02.

If the TKE application does not start, use the procedures in this manual to resolve the problem.

End of procedure

Upgrading the hard drive internal code

To upgrade the Licensed Internal Code (LIC) of a TKE Workstation, contact IBM Support and order the desired upgrade.

Internal code changes for a Trusted Key Entry Workstation

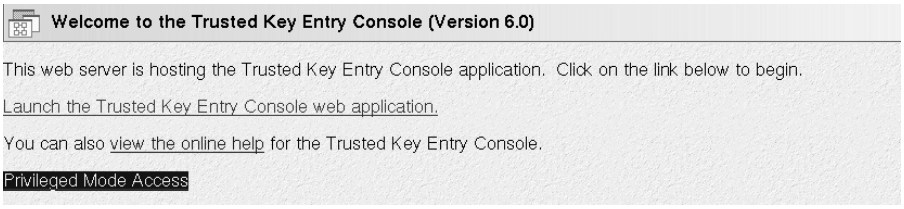
Licensed internal code changes are used to temporarily fix TKE Workstation internal code problems when no formal changes are available.

Note: ***Use this information to install a change only when you are directed to do so by IBM Product Engineering***.

Installing internal code changes on a TKE Workstation

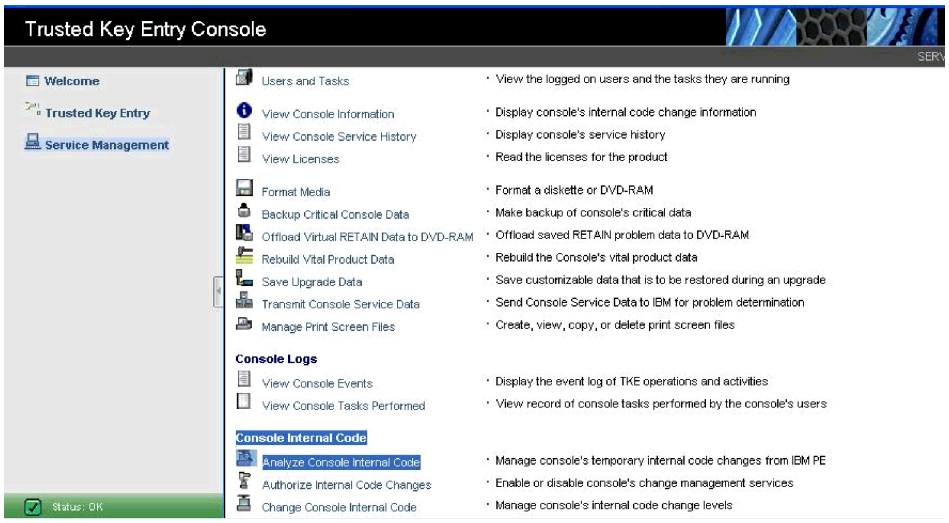
The following procedure is used to retrieve a temporary internal code change from a diskette or DVD RAM and install it on a TKE V6.0 Workstation.

1. To install internal code changes, proceed as follows:
   a. Click in the **X** in the upper right corner to logoff the TKE Workstation.
   b. Then, on the TKE Welcome page, click on the **Privileged Mode Access** link as illustrated below.

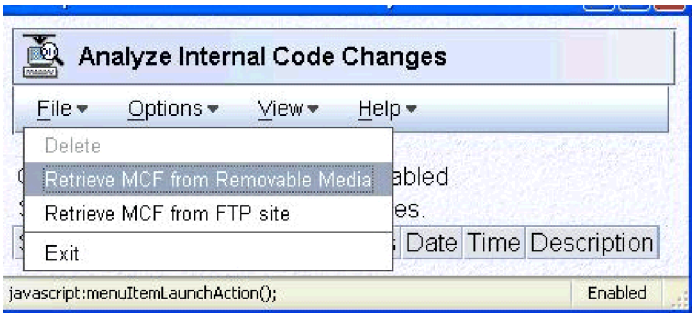


   c. Enter **SERVICE** for the userid.
   d. Enter **Servmode** for the password or enter the user-defined password.
   e. Select **Logon**.
2. Select **Service Management**.
3. Select **Analyze Console Internal Code.**

   Note: This link is found under the **Console Internal Code** category in the **Service Management** screen.



4. If the **No Internal Code changes** window displays, select **OK**, otherwise continue with the next step.
5. Select **File** from the menu bar on the **Analyze Internal Code changes** window.



6. Select **Retrieve MCF from Removable Media** or **Retrieve MCF from FTP Site** from the pull-down.
7. Select **OK** on the **Insert Removable Media** window. If **Retrieve MCF from FTP Site** is chosen, enter the **FTP Site**, **User ID**, **Password**, and **Directory** in the corresponding fields in this screen.
8. Select **Retrieve** on the **Confirm the action** window.
9. Select the temporary internal code change from the menu on the **Analyze Internal Code changes** window.
10. Select **Options** from the menu bar.
11. Select **Activate Internal Code changes** from the pull-down.
12. If the status of the change is **Activated** on the **Analyze Internal Code changes** window, the install task is complete.
13. If the status of the change is **Activated pending reboot**, continue on with the next step.

    If you are processing multiple changes, repeat steps 9 through 13 for each change before proceeding.
14. Reboot the workstation:
    a. From the **Trusted Key Entry Console**, select **Service Management**.
    b. Select **Shutdown or Restart**.
    c. Select **Restart Console**.
    d. Select **OK**.
    e. Select **Yes** on the **Confirm Shutdown or Restart** window.

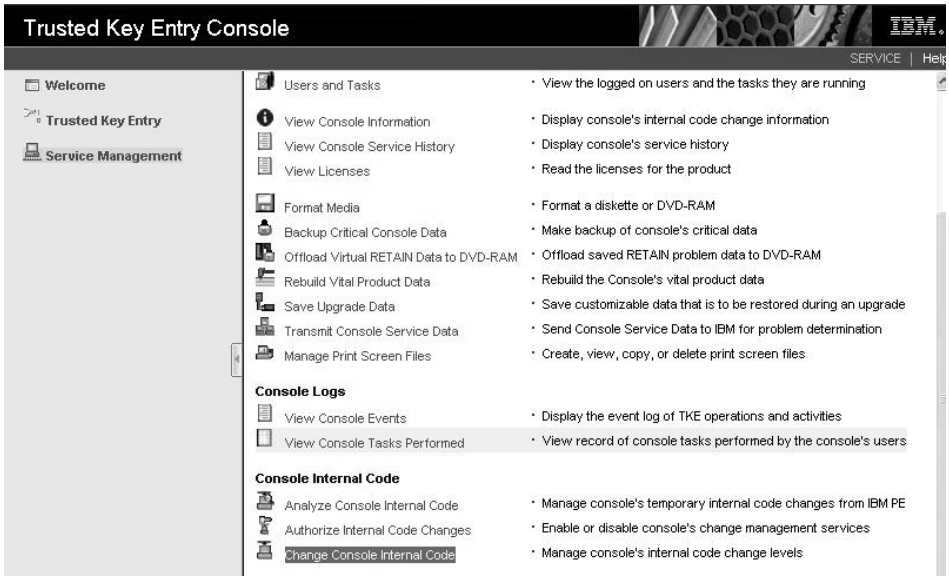
End of procedure

Installing MCLs on a TKE Workstation

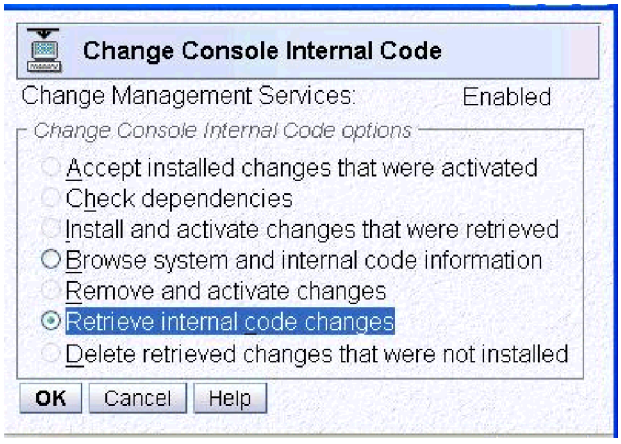
The following procedure is used to retrieve an internal code change (MCL) from a diskette or DVD RAM and install it on a TKE Workstation. Download applicable TKE MCLs from **Retain** using the TKE Workstation under direction from Product Engineering. MCLs may be saved to diskette or DVD-RAM. Take the media to the TKE Workstation.

1. To install MCLs on the TKE workstation, proceed as follows:
   a. Click in the **X** in the upper right corner to logoff the TKE Workstation.
   b. On the TKE Welcome page, select **Privileged Mode Access**.
   c. Enter **SERVICE** for the userid.
   d. Enter **Servmode** for the password or enter the user-defined password.
   e. Select **Logon**.
2. Select **Service Management**.
3. Select **Change Console Internal Code**.

   Note: This link is found under the **Console Internal Code** category in the **Service Management** screen.

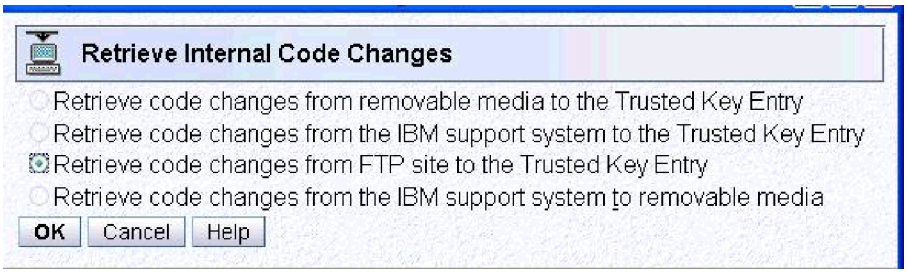


4. Select **Retrieve Internal Code Changes**.



5. Select **OK**.

6. Select one of the following:
   - **Retrieve code changes from removable media to the Trusted Key Entry**
   - **Retrieve code changes from the IBM support system to the Trusted Key Entry**
   - **Retrieve code changes from FTP site to the Trusted Key Entry**
   - **Retrieve code changes from the IBM support system to removable media.**



7. Insert the selected media.
8. Select **OK**.
9. Select **OK** when complete.
10. Select **All internal code changes** that were retrieved.
11. Select **OK**.
12. Select **All internal code changes**.
13. Select **OK**.
14. Select **Install and activate**. The workstation will reboot.
15. Select **OK** when complete.

    End of procedure

Trusted Key Entry Workstation configurations

8485 PC configuration

1. Power on the display.
2. Power on the system unit.
3. On the IBM Logo window, press F1 for **Configuration/Setup**.

   Notes:

   a. If `Press F1 for Setup` is not displayed, observe the video status LED. Press F1 when the LED transitions from **amber** (no video signal present) to **green** (video signal detected).

   b. The IBM Setup Utility window layout differs from previous releases. You can select main headings through a menu bar across the top of the window. **Ensure the Num Lock key is disabled.**

   c. *Select* means to select the heading from the top tool bar.

   d. There is no mouse support. **Navigate by using the arrow and Enter keys.**
4. Select **Continue** if a `POST Startup Error(s)` message is displayed.
5. Select **System Summary**. Verify the following:

```
Processor Summary:
  Extended Memory:                    1024 KB
  Internal Floppy Disk:               Installed
```

```
Hard Disk 0:                    800xxMB SATA0
Hard Disk 1:                    None
Hard Disk 2:                    CD-ROM
Hard Disk 3:                    None
Hard Disk 4:                    None
Mouse:                          Installed
System Memory Type:             DDR2
```

6. Press Esc. Select **Processor Summary**. Select **CPU IDs**. Verify the following:

```
CPU IDs:                        0F43
```

7. Press Esc. Select **Platform IDs**. Verify the following:

```
Platform IDs:                   0010
```

8. Press Esc. Select **Microcode revisions**. Verify the following:

```
Microcode Revisions:            0005
```

9. Press Esc. Select **Processor Speeds**. Verify the following:

```
Processor Speeds:               3.20 GHz
Front-side Bus:                 800 MHz
```

10. Press Esc. Select **L2 Cache Sizes** . Verify the following:

```
L2 Cache Size:                  2048 KB
```

11. Press Esc. Select **System Information**. Verify the following:

```
Machine Type/Model:             8485PAQ
System Serial Number:           Identical to front label
System UUID:                    32-digit hexadecimal number
System Board Identifier:        IBM (or alphanumerics)
System Asset Tag Number:        No Asset Tag

BIOS Version:                   1.29       (required level)
BIOS Date (MM/DD/YY):           02/09/06   (required level)
BIOS Build Level:               PAE129AUS  (required level)
```

Note: Flash BIOS release levels are upgraded on a continual basis. Ensure BIOS is at the latest level.

12. Press Esc. Select **Devices and I/O Ports** . Verify the following:

```
 Serial Port A:                 Port 3F8, IRQ4
 Serial Port B:                 Port 2F8, IRQ3
-Parallel Port Setup:
-Remote Console Redirection:
 Internal Floppy Disk:          Enabled
 Mouse:                         Installed
 Planar0 Ethernet:              Enabled
-System MAC Addresses:
-Advanced Chipset Control:
-Video:
-IDE Primary/Master:            800xxMB SATA0
-IDE Secondary/Master:          CD-ROM
-IDE Secondary/Slave:           None
```

13. Press Esc. Select **Parallel Port Setup**. Verify the following:

```
Parallel port:                  Enabled
  Mode:                         EPP and ECP
  Base I/O Address:             378
  Interrupt:                    IRQ 7
  DMA:                          DMA 1
```

14. Press Esc. Select **Remote Console Redirection**. Verify the following:

```
Remote Console Serial Port:     Disabled
Baud Rate:                      19.2K
Console Type:                   PC ANSI
Flow Control:                   CTS/RTS
Console Connection:             Direct
Continue C.R. after Post:       Off
```

15. Press Esc. Select **System MAC Addresses**. Verify the following:

```
Planar Ethernet MAC Addressc:          Hexidecimal
PCI-E slot 2 MAC Address:              Hexidecimal
                                       (if adapter installed)
```

16. Press Esc. Select **Advanced Chipset Control**. Verify the following:

```
Internal Floppy Disk:                  Installed
Parallel ATA:                          Enabled
Serial ATA:                            Enabled
Native Mode Operation:                 Auto
SATA Controller Mode Operation:        Compatable

USB Support:                           Enabled
USB 2.0 Support:                       Enabled
Clock Generator Spectrum:              Disabled
```

17. Press Esc. Select **Video**. Verify the following:

```
Video Controller:                      ATI ES1000
Video Memory:                          16 MB
```

18. Select **IDE Primary/Master**. Verify the following:

```
*  Type:                               Auto
   LBA Format:
   Total Sectors:                      15xxxxxxx
   Maximum Capacity:                   800xxMB SATA0
   Multi-Sector Transfers:             16 Sectors
   LBA Mode Control:                   Enabled
*  32 Bit I/O:                         Disabled
   Transfer Mode:                      FPIO 4 / DMA 2
   Ultra DMA Mode:                     Mode 5

*  Changeable Values, the other values are typical but may not
       exactly match.
```

19. Press Esc. Select **IDE Secondary/Master**. Verify the following:

```
*  Type:                               Auto

   Multi-Sector Transfers:             Disabled
   LBA Mode Control:                   Disabled
*  32 Bit I/O:                         Disabled
   Transfer Mode:                      FPIO 4 / DMA2
   Ultra DMA Mode:                     Mode 4

*  Changeable Values, the other values are typical but may not
       exactly match.
```

20. Press Esc. Select **IDE Primary/Slave**. Verify the following:

```
*  Type:                               Auto

   Multi-Sector Transfers:             Disabled
   LBA Mode Control:                   Disabled
*  32 Bit I/O:                         Disabled
   Transfer Mode:                      Standard
   Ultra DMA Mode:                     Disabled

*  Changeable Values, the other values are typical but may not
       exactly match.
```

21. Select **IDE Secondary/Slave**. Verify the following:

```
*  Type:                               Auto

   Multi-Sector Transfers:             Disabled
   LBA Mode Control:                   Disabled
*  32 Bit I/O:                         Disabled
   Transfer Mode:                      Standard
   Ultra DMA Mode:                     Disabled

*  Changeable Values, the other values are typical but may not
       exactly match.
```

22. Press Esc twice. Select **Date and Time**. Verify the following:

```
System Date                          MM/DD/YYYY (Set to current date)
System Time                          HH:MM:SS   (Set to current time,
                                                 24 hr.)
```

23. Press Esc. Select **System Security**. Verify the following:

```
Administrator Password:              Clear
Power-On Password:                   Clear

Administrator Password:              Do not open
Power-On Password:                   Do not open
```

24. Press Esc. Select **Start Options**. Verify the following:

```
- Startup Sequence Options:
  Planar Ethernet PXE/DHCP:          Planar0 Ethernet
  Planar PXE/DHCP Priority:          High
  PCI Device Boot Priority:          SAS/HostRAID
  Displayless Operation:             Enabled
  Keyboardless Operation:            Enabled
  Leyboard NumLock State:            Off
  Legacy USB Support:                Enable
  Boot on POST/BIO Error:            Disabled
  Boot Fail Count:                   Enabled
  Automatic Power Restore:           Last State
  F12 Boot Menu Prompt:              Disabled
```

25. Select **Startup Sequence Options**. Verify the following:

```
Primary Startup Sequence:
First Startup Device:                Removable
Second Startup Device:               CD/DVD-ROM
Third Startup Device:                Hard Disk
Fourth Startup Device:               Disabled

Wake On Lan Startup Sequence:        Disable

Wake On Lan Startup Sequence:
First Startup Device:                Disabled
Second Startup Device:               Disabled
Third Startup Device:                Disabled
Fourth Startup Device:               Disabled
```

26. Select **Select the Boot Hard Disk**, **Hard Drive**. Verify the following:

```
-Hard Drive:
WDC ....                             (HDD Model)
```

27. Press Esc. Select **Select the Boot Removable Devices**, **Removable**. Verify the following:

```
   -Removable Devices:
       Diskette Drive A:
```

28. Press Esc. Select **Advanced Setup**. Verify the following:

```
  Power Button:                      Enabled
  Wake-up from:                      Normal
- CPU Options:
- PCI Bus Control:
- Baseboard Management Controller (BMC) Setting:
  Fourth Startup Device:             Disabled
```

29. Select **CPU Options**. Verify the following:

```
Hyperthreading:                      Enabled
Prefetch Queue:                      Enabled
C1 Enhanced Mode:                    Disabled
No Execute Mode Mem Protection:      Enabled
```

30. Press Esc. Select **PCI Bus Control**. Verify the following:

```
   CI MLT:                           20h
 - PCI Interrupt Routing:
```

31. Select **PCI Interrupt Routing**. Verify the following:

```
Ensure all instances of Planar xxxx IRQ are set to:
  Auto Configure or No IRQ Requested
Ensure all instances of PCI... or PCIX... are set to:
  Auto Configure or No IRQ Requested
```

32. Press Esc twice. Select **Baseboard Management Controller (BMC) Settings**. Verify the following:

```
No Execute Mode Mem Protection:         Enabled
IPMI Specification Version:             1.5
BMC Hardware/Firmware Version:          (Hexadecimal)
Clear System Event Log:                 Disabled
Existing Event Log Number:              (Decimal)
BIOS PORT Watchdog:                     Disabled
Post WatchDog Timeout:                  5 min

- System Event Log:                     (Do not select)

- LAN Settings:                         (Do not select)
```

33. Press Esc twice. Select **Error Logs**. Verify the following:

```
- Post Error Log                        (Do not select)
- System Event/Error Log
```

34. Select **System Event/Error Log**. Verify the following:

```
    - Press Enter twice to clear the system Event/Error Log.
```

35. Press Esc twice. Press F10 (Save and Exit). Select **Yes**.
36. Select **Save and exit the Setup Utility**. Select **Yes**.
37. Select **Configuration/Setup Utility: Save Settings**. Select **Yes**.
38. Select **Save Settings**. Press Enter.

    End of Procedure.

8482 PC configuration

1. Power on the display.
2. Power on the system unit.
3. On the IBM Logo window, press F1 for **Configuration/Setup**.

   Notes:

   a. If `Press F1 for Setup` is not displayed, observe the video status LED. Press F1 when the LED transitions from **amber** (no video signal present) to **green** (video signal detected).

   b. The IBM Setup Utility window layout differs from previous releases. You can select main headings through a menu bar across the top of the window. **Ensure the Num Lock key is disabled.**

   c. *Select* means to select the heading from the top tool bar.

   d. There is no mouse support. **Navigate by using the arrow and Enter keys.**

4. Select **Continue** if a `POST Startup Error(s)` message is displayed.
5. Select **System Summary**. Verify the following:

```
Processor Summary:
  Extended Memory:                      1024 KB
  Extended Memory                      1023 KB
  Internal Floppy Disk:                 Installed
                                        (may require setting later)
  Hard Disk 0:                          800xxMB SATA1
  Hard Disk 1:                          None
  Hard Disk 2:                          CD-ROM
  Hard Disk 3:                          None
```

```
Hard Disk 4:                        None
Hard Disk 5:                        None
Mouse:                              Installed
System Memory Type:                 DDR2
```

6. Press Esc. Select **Processor Summary**. Verify the following:

```
CPU ID:                             06F5        (may vary)
Plartform ID                        0001        (may vary)
Microcode Revision                  0033        (may vary)
Processor Speed                     1.86 GHz
Front-side Bus                      1066 MHz
L2 Cache Size                       2048 KB
```

7. Press Esc twice. Select **System Information**. Verify the following:

```
Machine Type/Model:                 4362PAU or 4362PAT
System Serial Number:               Identical to front label
System UUID:                        32-digit hexadecimal number
System Board Identifier:            IBM (or alphanumerics)
System Asset Tag Number:            No Asset Tag

BIOS Version:                       1.26       (required level)
BIOS Date (MM/DD/YY):               01/15/07   (required level)
BIOS Build Level:                   GBE126AUS  (required level)
```

Note: Flash BIOS release levels are upgraded on a continual basis. Ensure BIOS is at the latest level.

8. Press Esc. Select **Devices and I/O Ports** . Verify the following:

```
Serial Port A:                      Port 3F8, IRQ4
Serial Port B:                      Port 2F8, IRQ3
-Parallel Port Setup
-Remote Console Redirection
 Internal Floppy Disk:              Enabled
 Mouse:                             Enabled
 Planar Ethernet:                   Enabled
-System MAC Addresses
  Parallel ATA:                     Enabled
  Serial ATA:                       Enabled
    Native Mode operation:          Auto
    SATA Controller Mode Option:    Compatible
-Video
```

9. Press Esc. Select **Parallel Port Setup**. Verify the following:

```
Parallel port:                      Enabled
  Mode:                             EPP and ECP
  Base I/O Address:                 Port 378
  Interrupt:                        IRQ 7
  DMA:                              DMA 1
```

10. Press Esc. Select **Remote Console Redirection**. Verify the following:

```
Remote Console Serial Port:         Disabled
Baud Rate:                          19.2K
Console Type:                       PC ANSI
Flow Control:                       CTS/RTS
Console Connection:                 Direct
Continue C.R. after Post:           Off
```

11. Press Esc. Select **System MAC Addresses**. Verify the following:

```
Planar Ethernet MAC Addressc:       Hexidecimal
PCI-E slot 2 MAC Address:           Hexidecimal
                                    (if adapter installed)
```

12. Press Esc. Select **Video**. Verify the following:

```
Video Controller:                   ATI ES1000
Video Memory:                       16 MB
```

13. Press Esc twice. Select **Date and Time**. Verify the following:

```
System Date                          MM/DD/YYYY (Set to current date)
System Time                          HH:MM:SS   (Set to current time,
                                                 24 hr.)
```

14. Press Esc. Select **System Security**. Verify the following:

```
Administrator Password:              Clear
Power-On Password:                   Clear

Administrator Password:              Do not open
Power-On Password:                   Do not open
```

15. Press Esc. Select **Start Options**. Verify the following:

```
- Startup Sequence Options:

Planar Ethernet PXE/DHCP:            Planar Ethernet
Planar PXE/DHCP Priority:            High
PCI Device Boot Priority:            Mini PCI-E
Displayless Operation:               Enabled
Keyboardless Operation:              Enabled
Leyboard NumLock State:              Off
Legacy USB Support:                  Enable
Boot on POST/BIO Error:              Disabled
Boot Fail Count:                     Enabled
Automatic Power Restore:             Last State
F12 Boot Menu Prompt:                Disabled
```

16. Select **Startup Sequence Options**. Verify the following:

```
-Primary Startup Sequence:

First Startup Device:                Internal FDD
Second Startup Device:               IDE CD:  HL-DT-ST DVDRAM
Third Startup Device:                HDD:  WDC WD800JD
Fourth Startup Device:               None
Fifth Startup Device:                None
Sixth Startup Device:                None
Seventh Startup Device:              None
Eighth Startup Device:               None

Wake On Lan Startup Sequence:        Disabled

Wake On Lan Startup Sequence:
First Startup Device:                None (greyed out)
Second Startup Device:               None (greyed out)
Third Startup Device:                None (greyed out)
Fourth Startup Device:               None (greyed out)
```

17. Press Esc twice. Select **Advanced Setup ... CPU Options**. Verify the following:

```
Dual Core Processor Logic:           Enabled
C1 Enhanced Mode:                    Enabled
Thermal Management 2:                Enabled
Execute-Disable Bit:                 Enabled
EIST Feature:                        Enabled
```

18. Press Esc. Select **PCI Bus Control**. Verify the following:

```
 - PCI MLT:                           40h
 - PCI Interrupt Routing:
```

19. Select **PCI Interrupt Routing**. Verify the following:

```
Ensure all instances of Planar xxxx IRQ are set to:
  Auto Configure or No IRQ Requested
Ensure all instances of Slotx INTA IRQ are set to:
  Auto Configure or No IRQ Requested
```

20. Press Esc twice. Select **IMPI**. Verify the following:

```
IPMI Specification Version:          1.5
BMC Hardware/Firmware Version:       (Hexadecimal)
Clear System Event Log:              Disabled
```

```
  Existing Event Log Number:            (Decimal)
  BIOS PORT Watchdog:                   Disabled
  Post WatchDog Timeout:                5 min

- System Event Log:                     (Do not select)

- LAN Settings:
```

21. Select **LAN Settings**. Verify the following:

```
  MINI-BMC MAC Address:                 hh.hh.hh.hh.hh.hh (valid hex values)
  IP Address:                           000.000.000.000
  Subnet Mask:                          000.000.000.000
  Gateway Address:                      000.000.000.000
Note: The last 3 fields must be set manually.  Type one 0 and use
      the arrow keys to page from field to field.
```

22. Press Esc twice. Select **NMI Option**. Verify the following:

```
- Reboot System on NMI:                 Enabled
```

23. Press Esc twice. Select **Memory Throttling Option**. Verify the following:

```
- Memory Throttling Control:            Disabled
```

24. Press Esc twice. Select **Error Logs**. Verify the following:

```
- Post Error Log                        (Do not select)
- System Event/Error Log
```

25. Select **System Event/Error Log**. Do the following:

```
- Press Enter twice to clear the system Event/Error Log.
```

26. Press Esc twice.
27. Select **Save Settings**. Press Enter.
28. Select **Exit Setup**.
29. Select **Yes, exit the Setup Utility**.

End of Procedure.

4367 PC configuration

1. Power on the display.
2. Power on the system unit.
3. On the IBM Logo window, press F1 for **Configuration/Setup**.

   Notes:

   a. If `Press F1 for Setup` is not displayed, observe the video status LED. Press F1 when the LED transitions from **amber** (no video signal present) to **green** (video signal detected).

   b. The IBM Setup Utility window layout differs from previous releases. You can select main headings through a menu bar across the top of the window. **Ensure the Num Lock key is disabled.**

   c. *Select* means to select the heading from the top tool bar.

   d. There is no mouse support. **Navigate by using the arrow and Enter keys.**

4. Select **Continue** if a `POST Startup Error(s)` screen is displayed.
5. Select **System Summary**. Verify the following:

```
Processor Summary
        Installed Memory      1024 KB
        Available Memory      1022 KB
        Internal Floppy Disk  None
        Device 0              250GB  SATA0  (Note: Must be SATA0)
        Device 1              None
        Device 2              None
```

```
Device 3              None
Device 4              None
Device 5              CD/DVD-ROM
Mouse                 Installed
System Memory Type    DDR2
```

6. Press Esc. Select **Processor Summary**. Verify the following:

```
CPU ID               0676      (may vary)
Platform ID          0001      (may vary)
Microcode Revision   0606      (may vary)
Processor Speed      3.00 GHz
Front-side Bus       1333 MHz
L2 Cache Size        6144 KB
```

7. Press "Esc" 2 times. Select **System Information**. Verify the following:

```
Machine Type/Model            436732U (or PAA/PAM)
System Serial Number          Identical to front label
System UUID                   32 digit hexadecimal number
System Board Identifier       11 Alphanumerics
System Asset Tag Number       N/A (May be Blank)

BIOS Version                  1.39
BIOS Date (MM/DD/YY)          08/06/08
BIOS Build Level              GUE139AUS
```

Note: Flash BIOS release levels are upgraded on a continual basis. Ensure BIOS is at latest zSeries supported level.

8. Press "Esc". Select **Devices and I/O Ports**. Verify the following:

```
  Serial Port 1                 Port 3F8, IRQ4
  Serial Port 2                 Port 2F8, IRQ3
- Parallel Port Setup
- Remote Console Redirection

  Internal Floppy Support       Disabled
  SATA Programming Interface    Native
  Planar Ethernet               Enabled
- USB Support

- Video
- System MAC Addresses
```

9. Select **Parallel Port Setup**. Verify the following:

```
Parallel Port          Port 378
Parallel Port Mode     Standard
Parallel Port IRQ      IRQ 7
```

10. Press Esc. Select **Remote Console Redirection**. Verify the following:

```
Remote Console Serial Port        Disabled
```

Note: The following are "greyed out":

```
Baud Rate                         9600
Console Type                      VT100, 8bit
Flow Control                      None
Remote Console Active After Boot  On
```

11. Press Esc. Select **USB Support**. Verify the following:

```
USB Controller         Enabled

USB Port 1             Enabled
USB Port 2             Enabled
USB Port 3             Enabled
USB Port 4             Enabled
USB Port 5             Enabled
USB Port 6             Enabled
```

12. Press Esc. Select **Video**. Verify the following:

```
Video Controller    ATI ES1000
Video Memory        16 MB
```

13. Press Esc. Select **System MAC Addresses**. Verify the following:

```
Planar Ethernet MAC Address     Hexadecimal
BMC MAC Address                 Hexadecimal
Slot 2 MAC Address              Hexadecimal  (if adapter installed)
```

14. Press Esc 2 times. Select **Date and Time**. Verify the following:

```
System Time     HH:MM:SS    (set to current time, 24Hr)
System Date     DD/MM/YYYY  (set to current date)
```

15. Press Esc. Select **System Security**. Verify the following:

```
Administrator Password    Clear
Power-on Password         Clear

- Administrator Password    (do not open)
- Power-on Password         (do not open)
```

16. Press Esc. Select **Advanced Chipset Control**. Verify the following:

```
Internal Floppy Disk:                   Installed
Parallel ATA:                           Enabled
Serial ATA:                             Enabled
Native Mode Operation:                  Auto
SATA Controller Mode Operation:         Compatable

USB Support:                            Enabled
USB 2.0 Support:                        Enabled
Clock Generator Spectrum:               Disabled
```

17. Press Esc. Select **Start Options**. Verify the following:

```
- Startup Sequence Options

  Planar Ethernet PXE/DHCP     Enabled
  Planar PXE/DHCP Priority     High
  PCI Device Boot Priority     Mini PCI-E
  Displayless Operation        Enabled
  Keyboard NumLock State       Off
  Boot on POST/BIO Error       Disabled
  Boot Fail Count              Enabled
  Automatic Power Restore      Previous State
  F12 Boot Menu Prompt         Disabled
  HDD S.M.A.R.T. Capability    Enabled
```

18. Select **Startup Sequence Options**. Verify the following:

```
Primary Startup Sequence
   First Startup Device       CD/DVD-ROM: HL-DT-STDVD...
   Second Startup Device      HDD(S0): Hitachi HDT... (may vary)
   Third Startup Device       None
   Fourth Startup Device      None
   Fifth Startup Device       None
   Sixth Startup Device       None
   Seventh Startup Device     None
   Eighth Startup Device      None

WakeOnLan Startup Sequence    Disabled

Wake On Lan Startup Sequence
   First Startup Device       (Greyed Out)  Note: Set these to
   Second Startup Device      (Greyed Out)        "None" prior to
   Third Startup Device       (Greyed Out)        disabling WOL.
   Fourth Startup Device      (Greyed Out)
```

19. Press Esc 2 times. Select **Advanced Setup**. Verify the following:

```
- CPU Options
- PCI Bus Control
- Baseboard Management Controller (BMC) Settings
  High Precision Event Timer                    Enabled
- WHEA Settings
```

20. Select **CPU Options**. Verify the following:

```
Core Multi-Processing            Enabled
Execute-Disable Bit Capability   Enabled
Intel EIST Feature               Enabled
Hardware Prefetcher              Enabled
Adjacent Cache Line Prefetch     Enabled
Intel Virtualization Technology  Enabled
```

21. Press Esc. Select **PCI Bus Control**. Verify the following:

```
  PCI MLT                40h
- PCI Interrupt Routing
- PCI ROM Control Execution
```

22. Select **PCI Interrupt Routing**. Verify the following:

```
Insure all instances of "USB x.x Controller x IRQ" are set to:

     "Auto Configure"

Insure all instances of "Planar Video IRQ" are set to:

     "Auto Configure"

Insure all instances of "Planar Ethernet IRQ" are set to:

     "Auto Configure"

Insure all instances of "Slotx INTA IRQ" are set to:

     "Auto Configure" or "No IRQ Requested"

Insure all instances of "Mini PCI-E IRQ" are set to:

     "Auto Configure" or "No IRQ Requested"
```

23. Press Esc. Select **PCI ROM Control execution**. Verify the following:

```
Slot 1 ROM Control Execution      Enabled
Slot 2 ROM Control Execution      Enabled
Slot 3 ROM Control Execution      Enabled
Slot 4 ROM Control Execution      Enabled
Slot 5 ROM Control Execution      Enabled
Mini PCI-E ROM Control Execution  Enabled
```

24. Press Esc 2 times. Select **Baseboard Management Controller (BMC) Settings**. Verify the following:

```
 IPMI Specification Version         2.0
 BMC Firmware Version               1.06       (or greater)
 BMC Build Date                     08/07/08   (or greater)
 BMC Build Level                    GUET16A    (or greater)
 Existing Event Log Number          (Decimal)

 BMC Post Watchdog                  Disabled
 BMC Post Watchdog Timeout          5 min (greyed out)
 System - BMC Serial Port Sharing   Enabled
 BMC Serial Port Access Mode        Disabled
 Reboot System on NMI               Enabled

- User Account Settings
- BMC Network Configuration
- BMC System Event Log
```

Note: ″BMC Serial Port Access Mode″ may have to be set PRIOR to setting ″System - BMC Serial Port Sharing″.

The CMOS initialization utility does not alter ″User Account Settings″ values. These must be set manually using the following procedure.

25. Select **User Account Settings**. Verify the following:

```
  UserID #  Enabled/Disabled
- UserID 1  Disabled
- UserID 2  Disabled
- UserID 3  Disabled
- UserID 4  Disabled
```

Note: This task is to insure ALL UserID's are DISABLED.

26. Select **UserID 1**. Verify the following:

```
  UserID 1                              Disabled
  User Name
  Privileged Limit                      No ACCESS
- Set BMC User Password                 (do not select)
  <<Save User Account Settings in BMC>>
```

27. Select **<<Save user Account Settings in BMC>>**.
28. Select Enter to save the settings.
29. Press Esc. Select **UserID 2**. Verify the following:

```
  UserID 2                              Disabled
  User Name
  Privileged Limit                      No ACCESS
- Set BMC User Password                 (do not select)
  <<Save User Account Settings in BMC>>
```

30. Select **<<Save user Account Settings in BMC>>**
31. Select Enter to save the settings.
32. Press Esc. Select **UserID 3**. Verify the following:

```
  UserID 3                              Disabled
  User Name
  Privileged Limit                      No ACCESS
- Set BMC User Password                 (do not select)
  <<Save User Account Settings in BMC>>
```

33. Select **<<Save user Account Settings in BMC>>**
34. Select Enter to save the settings.
35. Press Esc. Select **UserID 4**. Verify the following:

```
  UserID 4                              Disabled
  User Name
  Privileged Limit                      No ACCESS
- Set BMC User Password                 (do not select)
  <<Save User Account Settings in BMC>>
```

36. Select **<<Save user Account Settings in BMC>>**
37. Select Enter to save the settings.
38. Press Esc 2 times. Select **BMC Network Configuration**. Verify the following:

```
MINI-BMC MAC address          hh.hh.hh.hh.hh.hh  (valid hex values)
Host Name                     BMC_DHCP
DHCP Control                  Static IP

Static IP Settings
Static IP Address             000.000.000.000
Subnet Mask                   000.000.000.000
Gateway                       000.000.000.000
```

Note: Last 3 fields must be set manually. Type one ″0″ and use arrow keys to page from field to field.

39. Select **Save Network Settings in BMC** and press Enter twice.
40. Press Esc. Select **BMC System Event Log**.

    Note: If **BMC System Event Log** does not exist, press Esc until **Advanced Setup** screen is displayed and proceed to the **WHEA Settings** section.
41. Select **Clear BMC SELs** and press Enter twice.
42. Press Esc twice.
43. Select **WHEA Settings**. Verify the following:

    ```
    Error Injection       Disabled
    ```
44. Press Esc twice.
45. Select **Event/Error Logs**.
46. Select **Clear system logs**. Perform the following:
47. Press Enter to clear the system Event/Error Log.
48. Press Esc twice. Perform the following:

    ```
    - Insert the "GUYT47A" Diagnostic CD-ROM media
    - Select "Save Settings" and Press "Enter"
    - Select "Exit Setup"
    - Select "Yes, exit the Setup Utility"
    ```

End of Procedure.

Chapter 3. TKE repair procedures

Start of repair

Service Tips

The TKE Workstation uses Problem Analysis (PA). You will also use POST codes, “beeps”, System Messages, and hardware status indicators for problem determination.

The PCIX adapter used in TKE has no standalone (bootable diskette) diagnostics. All serviceability is done using CCA Event Codes. Refer to “TKE Workstation CCAxxxx event codes” on page 3-3.

Check with the system operator to verify that there are no channel or cryptographic coprocessor errors on the server before proceeding with the TKE Workstation repair.

TKE Workstation initialization may take up to two minutes. This is not an error condition. The adapter is performing initialization tests.

If you are directed to exchange PC FRUs, refer to the PC maintenance information for removal and replacement instructions.

1. Ensure all display, network, mouse, and keyboard cables are properly connected. If your TKE Workstation is using Smart Card readers, verify secure connection of all cables associated with the readers.

   Ensure all display and Workstation power cables are installed and are plugged into active AC outlets.

   Are all cables and the AC power source correct?

   If **YES**, go to step 3. If **NO**, go to step 2.
2. Power off the system unit and display.

   Reseat any loose cables and ensure all cables are plugged in the correct location. Ensure the AC source is active (get the customer’s assistance if necessary).

   When complete, go to step 7 on page 3-2.
3. Ensure the display and system unit are powered on. Check the power indicators on the display and system unit.

   Are all the power indicators on (green)?

   If **YES**, go to step 5. If **NO**, go to step 4.
4. There may be a power problem on the TKE Workstation.

   Go to Table 3-1 on page 3-24 and find **Power** under **Problem Area Reported**. Go to the information under **Go To**.
5. Ensure the TKE Version 6.0 Workstation initializes correctly. The TKE Workstation is initialized when **Trusted Key Entry Console Welcome** displays.

   Is the TKE V6.0 Workstation correctly initialized?

   If **YES**, go to step 6. If **NO**, go to step 7 on page 3-2.
6. Use the information in “Ethernet status LEDs” on page 3-32 to determine what type of network adapter is installed in the Workstation. Then, check “Ethernet status LEDs” on page 3-32 to determine correct network operation.

   Is network operation correct for the adapter installed in the Workstation?

If **YES**, go to step 7. If **NO**, go to “Ethernet tests for PCI bus adapter” on page 3-20. After you have completed the Ethernet repair, return to step 1 on page 3-1 and repeat this procedure.

7. Ask the customer to verify that the TKE Workstation is correctly configured.

   Direct the customer to V6.0 of the *Trusted Key Entry PCIX Workstation User's Guide*, SA23-2211–05. See Chapter 4, **TKE Setup and Customization**, Chapter 5, **TKE Up and Running**, and Chapter 2, **Using Smart Cards with TKE**.

   If a configuration problem is found, close the call. Refer to “Completing the repair” on page 3-37.

   If there is a hardware problem that prevents the customer from completing the configuration task, or if the customer reports a hardware problem, go to Table 3-1 on page 3-24 and find the failure description under **Problem Area Reported**. Go to the information under **Go To**.

8. If possible, shut down the Workstation.

   Check for any of the following:
   - POST error codes (numeric characters on the display)
   - More than two POST “beeps”.

   If an error condition occurs, go to Table 3-1 on page 3-24 and find the failure description under **Problem Area Reported**. Go to the information under **Go To**.

   If no errors occur but the customer still cannot use the Workstation, go to “Undetermined errors” on page 3-25.

End of procedure

TKE Workstation CCAxxxx event codes

Return code and reason code overview:

The return code provides a general indication of the results of verb processing and is the value that your application program should use in determining the course of further processing. The reason code provides more specific information about the outcome of verb processing. Note that reason code values generally differ between CCA product implementations. Therefore, the reason code values should generally be returned to individuals who can understand the implications in the context of your application on a specific platform.

The return codes have these general meanings:

Value	Meaning
0	Indicates normal completion; a few nonzero reason codes are associated with this return code.
4	Indicates the verb processing completed, but without full success. For example, this return code can signal that a supplied PIN was found to be invalid.
8	Indicates that the verb prematurely stopped processing. Generally, the application programmer will need to investigate the problem and will need to know the associated reason code.
12	Indicates that the verb prematurely stopped processing. The reason is most likely related to a problem in the setup of the hardware or in the configuration of the software.
16	Indicates that the verb prematurely stopped processing. A processing error occurred in the product. If these errors persist, a repair of the hardware or a correction to the product software may be required.

Each return code is associated with a reason code that supplies details about the result of verb processing. A successful result can include return code 0 and reason code 0 or another combination of a return code and a reason code. Generally, you should be able to base your application program design on the return codes; the reason codes amplify the meaning supplied by the return codes.

A verb supplies a return code and a reason code in the return_code parameter and in the reason_code parameter.

Return codes

A return code provides a summary of the results of verb processing. A return code can have the following values:

Hex Value	Decimal Value	Meaning
00	00	This return code indicates a normal completion of verb processing. To provide additional information, a few nonzero reason codes are associated with this return code.
04	04	This return code is a warning that indicates that the verb completed processing; however, an unusual event occurred. The event is most likely related to a problem created by the user, or it is a normal occurrence based on the data supplied to the web.
08	08	This return code indicates that the verb stopped processing. Either an error occurred in the application program or a possible recoverable error occurred in the Coprocessor support code.
0C	12	This return code indicates that the verb stopped processing. Either a Coprocessor is not available or a processing error occurred in the Coprocessor support code. The reason is most likely related to a problem in the setup of the hardware or in the configuration of the software.
10	16	This return code indicates that the verb stopped processing. A processing error occurred in the Coprocessor support code. If these errors persist, a repair of the Coprocessor hardware or a correction to the Coprocessor support code may be required.

Reason codes

A reason code details the results of verb processing.

It is expected that User Defined Extensions (UDX) will return reason codes in the range of 20480 (X'5000') through 24575 (X'5FFF'). See the documentation for UDXs for these reason code meanings.

The following tables show the reason codes, listed in numeric sequence and grouped by their corresponding return code. The return codes appear in decimal form, and the reason codes appear in decimal and hexadecimal (hex) form.

Reason codes for return code 0

Return Code Dec	Reason Code Dec (Hex)	Meaning
0	000 (000)	The verb completed processing successfully.
0	002 (002)	One or more bytes of a key do not have odd parity.
0	008 (008)	No value is present to be processed.
0	151 (097)	The key token supplies the MAC length or MACLEN4 is the default for key tokens that contain MAC or MACVER keys.
0	701 (2BD)	A new master-key value was found to have duplicate thirds.
0	702 (2BE)	A provided master-key part did not have odd parity.
0	10001 (2711)	A key encrypted under the old master-key was used.

Reason codes for return code 4

Return Code Dec	Reason Code Dec (Hex)	Meaning
4	001 (001)	The verification test failed.
4	013 (00D)	The key token has an initialization vector and the initialization_vector parameter value is nonzero. The verb uses the value in the key token.
4	016 (010)	The rule array and the rule array count are too small to contain the complete result.
4	017 (011)	The requested ID is not present in any profile in the specified cryptographic hardware component.
4	019 (013)	The financial PIN in a PIN block is not verified.
4	158 (09E)	The Key_Token_Change or Key_Record_Delete verb did not process any records.
4	166 (0A6)	The control vector is not valid because of parity bits, anti-variant bits, or inconsistent KEK bits, or because bits 59 to 62 are not zero.
4	179 (0B3)	The control-vector keywords that are in the rule array are ignored.
4	282 (11A)	The Cryptographic Coprocessor intrusion latch is set.
4	283 (11B)	The Cryptographic Coprocessor battery is low.
4	287 (11F)	The PIN-block format is not consistent.
4	429 (1AD)	The digital signature is not verified. The verb completed its processing normally.
4	1024 (400)	Sufficient shares have been processed to create a new master-key.
4	2039 (7F7)	At least one control vector bit cannot be parsed.
4	2042 (7FA)	The supplied passphrase is invalid.

Reason codes for return code 8

Return Code Dec	Reason Code Dec (Hex)	Meaning
8	012 (00C)	The token-validation value in an external key token is not valid.
8	022 (016)	The ID number in the request field is not valid.
8	023 (017)	An access to the data area was outside the data-area boundary.
8	024 (018)	The master key verification pattern is not valid.
8	025 (019)	The value that the *text_length* parameter specifies is not valid.
8	026 (01A)	The value of the PIN is not valid.
8	029 (01D)	The token-validation value in an internal key token is not valid.
8	030 (01E)	No record with a matching key label is in key storage.
8	031 (01F)	The control vector did not specify a DATA key.
8	032 (020)	A key label format is not valid.
8	033 (021)	A rule array or other parameter specifies a keyword that is not valid.
8	034 (022)	A rule-array keyword combination is not valid.
8	035 (023)	A rule-array count is not valid.
8	036 (024)	The action command must be specified in the rule array.
8	037 (025)	The object type must be specified in the rule array.
8	039 (027)	A control vector violation occurred. Check all control vectors employed with the verb. For security reasons, no detail is provided.
8	040 (028)	The service code does not contain numerical character data.
8	041 (029)	The keyword supplied with the *key_form* parameter is not valid.
8	042 (02A)	The expiration date is not valid.
8	043 (02B)	The keyword supplied with the *key_length* or the *key_token_length* parameter is not valid.
8	044 (02C)	A record with a matching key label already exists in key storage.
8	045 (02D)	The input character string cannot be found in the code table.
8	046 (02E)	The card-validation value (CVV) is not valid.
8	047 (02F)	A source key token is unusable because it contains data that is not valid or undefined.
8	048 (030)	One or more keys has a master key verification pattern that is not valid.
8	049 (031)	A key-token-version-number found in a key token is not supported.
8	050 (032)	The key-serial-number specified in the rule array is not valid.
8	051 (033)	The value that the *text_length* parameter specifies is not a multiple of eight bytes.
8	054 (036)	The value that the *pad_character* parameter specifies is not valid.
8	055 (037)	The initialization vector in the key token is enciphered.
8	056 (038)	The master key verification pattern in the OCV is not valid.
8	058 (03A)	The parity of the operating key is not valid.
8	059 (03B)	Control information (for example, the processing method or the pad character) in the key token conflicts with that in the rule array.

Return Code Dec	Reason Code Dec (Hex)	Meaning
8	060 (03C)	A cryptographic request with the **FIRST** or **MIDDLE** keywords and a text length less than 8 bytes is not valid.
8	061 (03D)	The keyword supplied with the *key_type* parameter is not valid.
8	062 (03E)	The source key was not found.
8	063 (03F)	A key token had an invalid token header (for example, not an internal token).
8	064 (040)	The RSA key is not permitted to perform the requested operation. Likely causes are key distribution usage is not enabled for the key.
8	065 (041)	The key token failed consistency checking.
8	066 (042)	The recovered encryption block failed validation checking.
8	067 (043)	RSA encryption failed.
8	068 (044)	RSA decryption failed.
8	072 (048)	The value that the *size* parameter specifies is not valid (too small, too large, negative, or zero).
8	081 (051)	The modulus length (key size) exceeds the allowable maximum.
8	085 (055)	The date or the time value is not valid.
8	090 (05A)	Access control checking failed. See the Required Commands descriptions for the failing verb.
8	091 (05B)	The time sent in your logon request was more than five minutes different from the clock in the secure module.
8	092 (05C)	Your user profile has expired.
8	093 (05D)	Your user profile has not yet reached its activation date.
8	094 (05E)	Your authentication data (for example, passphrase) has expired.
8	095 (05F)	Access to the data is not authorized.
8	096 (05F)	An error occurred reading the secure clock.
8	100 (064)	The PIN length is not valid.
8	101 (065)	The PIN check length is not valid. It must be in the range from 4 to the PIN length inclusive.
8	102 (066)	The value of the decimalization table is not valid.
8	103 (067)	The value of the validation data is not valid.
8	104 (068)	The value of the customer-selected PIN is not valid, or the PIN length does not match the value supplied with the *PIN_length* parameter or defined by the PIN-block format specified in the PIN profile.
8	105 (069)	The value of the *transaction_security parameter* is not valid.
8	106 (06A)	The PIN-block format keyword is not valid.
8	107 (06B)	The format control keyword is not valid.
8	108 (06C)	The value or the placement of the padding data is not valid.
8	109 (06D)	The extraction method keyword is not valid.
8	110 (06E)	The value of the PAN data is not numeric character data.
8	111 (06F)	The sequence number is not valid.
8	112 (070)	The PIN offset is not valid.
8	114 (072)	The PVV value is not valid.

Return Code Dec	Reason Code Dec (Hex)	Meaning
8	116 (074)	The clear PIN value is not valid. For example, digits other than 0, ..., 9 were found.
8	120 (078)	An origin or destination identifier is not valid.
8	121 (079)	The value of the *inbound_key* or *source_key* parameter is not valid.
8	122 (07A)	The value of the *inbound_KEK_count* or *outbound_count* parameter is not valid.
8	125 (07D)	A PKA92-encrypted key having the same EID as the local node cannot be imported.
8	153 (099)	The text length exceeds the system limits.
8	154 (09A)	The key token that the *key_identifier* parameter specifies is not an internal key token or a key label.
8	155 (09B)	The value that the *generated_key_identifier* parameter specifies is not valid, or it is not consistent with the value that the *key_form* parameter specifies.
8	156 (09C)	A keyword is not valid with the specified parameters.
8	157 (09D)	The key-token type is not specified in the rule array.
8	159 (09F)	The keyword supplied with the *option* parameter is not valid.
8	160 (0A0)	The key type and the key length are not consistent.
8	161 (0A1)	The value that the *data_set_name_length* parameter specifies is not valid.
8	162 (0A2)	The offset value is not valid.
8	163 (0A3)	The value that the *data_set_name* parameter specifies is not valid.
8	164 (0A4)	The starting address of the output area falls inside the input area.
8	165 (0A5)	The carry_over_character_count that is specified in the chaining vector is not valid.
8	168 (0A8)	A hexadecimal MAC value contains characters that are not valid, or the MAC on a request or reply failed because the user session key in the host and the adapter card do not match.
8	169 (0A9)	An MDC_Generate text length error occurred.
8	170 (0AA)	Special authorization through the operating system is required to use this verb.
8	171 (0AB)	The *control_array_count* value is not valid.
8	175 (0AF)	The key token cannot be parsed because no control vector is present.
8	180 (0B4)	A null key token was presented for parsing.
8	181 (0B5)	The key token is not valid. The first byte is not valid, or an incorrect token type was presented.
8	183 (0B7)	The key type is not consistent with the key type of the control vector.
8	184 (0B8)	An input pointer is null.
8	185 (0B9)	A disk I/O error occurred: perhaps the file is in use, does not exist, etc.
8	186 (0BA)	The key-type field in the control vector is not valid.
8	187 (0BB)	The requested MAC length (MACLEN4, MACLEN6, MACLEN8) is not consistent with the control vector (key-a, key-b).

Return Code Dec	Reason Code Dec (Hex)	Meaning
8	191 (0BF)	The requested MAC length (MACLEN6, MACLEN8) is not consistent with the control vector (MAC-LN-4).
8	192 (0C0)	A key-storage record contains a record validation value that is not valid.
8	204 (0CC)	A memory allocation failed. This can occur in the host and in the Coprocessor. Try closing other host tasks. If the problem persists, contact IBM.
8	205 (0CD)	The X9.23 ciphering method is not consistent with the use of the CONTINUE keyword.
8	323 (143)	The ciphering method that the Decipher verb used does not match the ciphering method that the Encipher verb used.
8	335 (14F)	Either the specified cryptographic hardware component or the environment does not implement this function.
8	340 (154)	One of the input control vectors has odd parity.
8	343 (157)	Either the data block or the buffer for the block is too small, or a variable has caused an attempt to create an internal data structure that is too large.
8	374 (176)	Less data was supplied than expected or less data exists than was requested.
8	377 (179)	A key-storage error occurred.
8	382 (17E)	A time-limit violation occurred.
8	385 (181)	The cryptographic hardware component reported that the data passed as part of a command is not valid for that command.
8	387 (183)	The cryptographic hardware component reported that the user ID or role ID is not valid.
8	393 (189)	The command was not processed because the profile cannot be used.
8	394 (18A)	The command was not processed because the expiration date was exceeded.
8	397 (18D)	The command was not processed because the active profile requires the user to be pre-verified.
8	398 (18E)	The command was not processed because the maximum PIN/password failure limit is exceeded.
8	407 (197)	A PIN-block consistency-check-error occurred.
8	605 (25D)	The number of output bytes is greater than the number that is permitted.
8	703 (2BF)	A new master-key value was found to be one of the weak DES keys.
8	704 (2C0)	The new master-key would have the same master key verification pattern as the current master-key.
8	705 (2C1)	The same key-encrypting key was specified for both exporter keys.
8	706 (2C2)	Pad count in deciphered data is not valid.
8	707 (2C3)	The Master-Key registers are not in the state required for the requested function.
8	713 (2C9)	The algorithm or function is not available on current hardware (DES on a CDMF-only system, or T-DES on DES-only or CDMF-only system).

Return Code Dec	Reason Code Dec (Hex)	Meaning
8	714 (2CA)	A reserved parameter was not a null pointer or an expected value.
8	715 (2CB)	A parameter that must have a value of zero is invalid.
8	718 (2CE)	The hash of the data block in the decrypted RSA-OAEP block does not match the hash of the decrypted data block.
8	719 (2CF)	The block format (BT) field in the decrypted RSA-OAEP block does not have the correct value.
8	720 (2D0)	The initial byte (I) in the decrypted RSA-OAEP block does not have a valid value.
8	721 (2D1)	The V field in the decrypted RSA-OAEP does not have the correct value.
8	752 (2F0)	The key-storage file path is not usable.
8	753 (2F1)	Opening the key-storage file failed.
8	754 (2F2)	An internal call to the key_test command failed.
8	756 (2F4)	Creation of the key-storage file failed.
8	760 (2F8)	An RSA-key modulus length in bits or in bytes is not valid.
8	761 (2F9)	An RSA-key exponent length is not valid.
8	762 (2FA)	A length in the key value structure is not valid.
8	763 (2FB)	The section identification number within a key token is invalid.
8	770 (302)	The PKA key token has an invalid field.
8	771 (303)	The user is not logged on.
8	772 (304)	The requested role was not found.
8	773 (305)	The requested profile was not found.
8	774 (306)	The profile already exists.
8	775 (307)	The supplied data is not replaceable.
8	776 (308)	The requested id is already logged on.
8	777 (309)	The authentication data is invalid.
8	778 (30A)	The checksum for the role is in error.
8	779 (30B)	The checksum for the profile is in error.
8	780 (30C)	There is an error in the profile data.
8	781 (30D)	There is an error in the role data.
8	782 (30E)	The Function-Control-Vector header is invalid.
8	783 (30F)	The command is not permitted by the Function-Control-Vector value.
8	784 (310)	The operation you requested cannot be performed because the user profile is in use.
8	785 (311)	The operation you requested cannot be performed because the role is presently in use.
8	816 (330)	The certificate length is not valid
8	817 (331)	The public key used for encryption does not match that of the Workstation cryptographic adapter.
8	818 (332)	The certificate signature verification failed.
8	1025 (401)	Registered Public Key or Retained Private Key Name already exists.

Return Code Dec	Reason Code Dec (Hex)	Meaning
8	1026 (402)	Key name (Registered Public Key or Retained Private Key) does not exist.
8	1027 (403)	Environment Identification Data is already set.
8	1028 (404)	Master Key Share Data is already set.
8	1029 (405)	There is an error in the Environment Identifier Data.
8	1030 (406)	There is an error in using the Master Key Share Data.
8	1031 (407)	There is an error in using Registered Public Key or Retained Private Key data.
8	1032 (408)	There is an error in using Registered Public Key Hash data.
8	1033 (409)	The Public Key Hash was not registered.
8	1034 (40A)	The Public Key was not registered.
8	1035 (40B)	The Public Key Certificate Signature was not verified.
8	1037 (40D)	There is a Master Key Shares distribution error.
8	1038 (40E)	The Public Key Hash is not marked for cloning.
8	1039 (40F)	The Registered Public Key Hash does not match the Registered Hash.
8	1040 (410)	The Master Key Share Enciphering Key failed encipher.
8	1041 (411)	The Master Key Share Enciphering Key failed decipher.
8	1042 (412)	The Master Key Share Digital Signature Generate failed.
8	1043 (413)	The Master Key Share Digital Signature Verify failed.
8	1044 (414)	There is an error in reading VPD data from the adapter.
8	1045 (415)	Encrypting the Cloning Information failed.
8	1046 (416)	Decrypting the Cloning Information failed.
8	1047 (417)	There is an error loading New Master Key from Master Key Shares.
8	1048 (418)	The Clone Information has one or more invalid sections.
8	1049 (419)	The Master Key Share Index is not valid.
8	1050 (41A)	The public-key encrypted-key is rejected because the EID with the key is the same as the EID for this node.
8	1051 (41B)	The private-key is rejected because the key is not flagged for use in master-key cloning.
8	1052 (41C)	An error occurred while accessing the Workstation cryptographic adapter card certificate. Ensure that the Workstation cryptographic adapter card has been enrolled in a zone.
8	1053 (41D)	An error occurred while accessing the Workstation cryptographic adapter CA certificate. Ensure that the Workstation cryptographic adapter card has been enrolled in a zone.
8	1100 (44C)	General hardware device driver execution error.
8	1101 (44D)	Hardware device driver invalid parameter.
8	1102 (44E)	Hardware device driver invalid buffer length.
8	1103 (44F)	Hardware device driver too many opens. Cannot open device now.
8	1104 (450)	Hardware device driver access denied. Cannot access device.

Return Code Dec	Reason Code Dec (Hex)	Meaning
8	1105 (451)	Hardware device driver device is busy and cannot perform request now.
8	1106 (452)	Hardware device driver buffer too small. Received data truncated.
8	1107 (453)	Hardware device driver request interrupted. Request aborted.
8	1108 (454)	Hardware device driver security tamper. Hardware intrusion detected.
8	2034 (7F2)	The environment variable used to set the default Coprocessor is invalid, or does not exist for a Coprocessor in the system.
8	2036 (7F4)	The contents of a chaining vector are not valid. Ensure that the chaining vector was not modified by your application program.
8	2038 (7F6)	No RSA private key information was provided.
8	2041 (7F9)	An invalid default card environment variable has been detected.
8	2050 (802)	The current key serial number field in the PIN profile variable is invalid (not hexadecimal or too many one bits).
8	2051 (803)	Invalid message length in OAEP-decoded information.
8	2053 (805)	No message found in the OAEP-decoded data.
8	2054 (806)	Invalid RSA Enciphered Key cryptogram: OAEP optional encoding parameters failed validation.
8	2055 (807)	The RSA public key is too small to encrypt the DES key
8	2062 (80E)	The active role does not permit changing the characteristic of a double-length key in Key_Part_Import.
8	2065 (811)	The specified key token is not null.
8	2080 (820)	The group profile does not exist.
8	2081 (821)	The authentication data contains duplicate elements.
8	2082 (822)	The logon request contains authentication data from one or more users who are not members of the group.
8	2083 (823)	The number of group members in the group logon request is not correct.
8	2084 (824)	The group logon failed because authentication of one or more group members failed.
8	2085 (825)	The profile is included in one or more groups.
8	2086 (826)	The group role does not exist.
8	2087 (827)	The group profile has not yet reached its activation date.
8	2088 (829)	The group profile has expired.
8	3001 (BB9)	The RSA-OAEP block contains a PIN block and the verb did not request PINBLOCK processing.
8	3014 (BC6)	Invalid entity ID.
8	6000 (1770)	The specified device is already allocated.
8	6001 (1771)	No device is allocated.
8	6002 (1772)	The specified device was not found.
8	6003 (1773)	The specified device is an improper type.

Return Code Dec	Reason Code Dec (Hex)	Meaning
8	6004 (1774)	Use of the specified device is not authorized for this user.
8	6005 (1775)	The specified device is not varied on line.
8	6006 (1776)	The specified device is in a damaged state.
8	6007 (1777)	The key storage file has not been allocated.
8	6008 (1778)	The key storage file has not been found.
8	6009 (1779)	The specified key storage file is either the wrong type or the wrong format.
8	6010 (177A)	The user is not authorized to use the key storage file.
8	6011 (177B)	The specified CCA verb request is not permitted from a secondary thread.

Reason codes for return code 12

Return Code Dec	Reason Code Dec (Hex)	Meaning
12	093 (05D)	The security server is not available or not loaded.
12	097 (061)	File space in key storage is insufficient to complete the operation.
12	196 (0C4)	The device driver, the security server, or the directory server is not installed, or is not active, or in AIX® , file permissions are not valid for your application.
12	197 (0C5)	A key-storage file I/O error occurred, or a file was not found.
12	206 (0CE)	The key-storage file is not valid, or the master-key verification failed. There is an unlikely but possible synchronization problem with the Master_Key_Process verb.
12	207 (0CF)	The verification method flags in the profile are not valid.
12	324 (144)	The device driver attempted to allocate memory, but no memory is available.
12	338 (152)	This cryptographic hardware device driver is not installed or is not responding.
12	339 (153)	A system error occurred in interprocess communication routine.
12	764 (2FC)	The master key(s) are not loaded and therefore a key could not be recovered or enciphered.
12	768 (300)	One or more paths for key storage directory operations is improperly specified.
12	2073 (819)	The cryptographic coprocessor has been disabled on the Support Element. The coprocessor must be enabled on the Support Element before the TKE can access it.
12	11072 (2B40)	CEX2C has been reconfigured to a CEX2A. TKE will not recognize the coprocessor until it is reconfigured back to a CEX2C.

Reason codes for return code 16

Return Code Dec	Reason Code Dec (Hex)	Meaning
16	099 (063)	An unrecoverable error occurred in the security server; contact your IBM service representative.
16	167 (0A7)	An error occurred in the security server, possibly due to inconsistent device-driver and security-server logic.
16	336 (150)	An error occurred in a cryptographic hardware or software component.
16	337 (151)	A device software error occurred.
16	444 (1BC)	The verb-unique-data had an invalid length.
16	556 (22C)	The request parameter block failed consistency checking.
16	708 (2C4)	Inconsistent data was returned from the cryptographic engine.
16	709 (2C5)	Cryptographic engine internal error, could not access the master-key data.
16	710 (2C6)	An unrecoverable error occurred while attempting to update master-key data items.
16	712 (2C8)	An unexpected error occurred in the master-key manager.
16	769 (301)	The host system code or the CCA application in the Coprocessor encountered unexpected errors and was unable to process the request.

Testing PCI bus-based consoles

Use the information in this section when you are directed to test the TKE workstation to isolate a problem or verify a repair.

Note: If you are directed to **Run All Selected**, start with the **System Unit** diagnostic procedures for the console you are repairing.

Problem Area	Go To
Personal Computer: System Unit • DVD-RAM • Hard Disk • Diskette Drive • Display • Keyboard/Mouse • Memory • Power • Run All Selected	“System unit testing” on page 3-19
Personal Computer: PCI Adapters • Ethernet (planar board or adapter)	“Ethernet tests for PCI bus adapter” on page 3-20

Information and test menu selection

Information	Menu Selection
To test 8485 system units: **Diagnostics**, Hardware Maintenance Manual (8485HMM.PDF) located in the Service subdirectory of the server Diagnostic CD-ROM	**Desktop System Diagnostics**
To test 8482 system units: **Diagnostics**, Hardware Maintenance Manual (8482HMM.PDF) located in the Service subdirectory of the server Diagnostic CD-ROM	**Desktop System Diagnostics**
“Ethernet tests for PCI bus adapter” on page 3-20	**Intel® PRO or Broadcom® Ethernet Diagnostics**

System unit testing

All system diagnostics for the TKE workstation reside on the bootable Hardware Management Console CD-ROM. Performing actions other than those specified in the following procedure may cause errors. Desktop PC diagnostics display **PC Doctor** as their source:

1. If you know which device is failing or you were sent here by another procedure, do the following:
   a. Power on the PC.
   b. Insert the Diagnostic CD into DVD-RAM drive.
   c. Wait until the **Startup Menu** is displayed.
   d. Select **Desktop System Diagnostics**.
   e. Wait until a diagnostic selection menu is displayed; then go to step 2.

      Locate the corresponding documentation and menu selection for the console you are testing. Refer to “Information and test menu selection” on page 3-18.

      If the Main Menu cannot be displayed because of a power or other PC failure, use the maintenance information shipped with the PC to correct the problem.
2. Select either **Diagnostics** or **Interactive Tests** for a list of devices to test.
   - If you select **Interactive Tests**, then select the device requiring manual intervention (keyboard, video, mouse, diskette, CD-ROM).
   - If you select **Diagnostics**, then select **Run Normal/Quick Test** for predefined test sequences or select the device that does not require manual intervention (CPU, system board, I/O ports, fixed disks, memory).

   After you select devices or tests, follow the instructions.

   If the device or test you have selected fails, go to step 3. Otherwise, go to step 4.
3. If the diagnostics fail, refer to the XXXXHMM.PDF file located in the Service subdirectory of the System z10, System z9, or zSeries HWMCA-CDR for FRU replacement.

   If you replaced the system board or battery and you have not been previously directed to configure the system unit, do so now. Refer to “Trusted Key Entry Workstation configurations” on page 2-48.
4. If you were instructed to **Run All Selected**, continue with “Testing PCI bus-based consoles” on page 3-17 and select **PCI Adapters**. Otherwise, return to the procedure that directed you here.

   End of procedure.

Ethernet tests for PCI bus adapter

Use the following information to test the Ethernet network adapter.

Review “Service tips” on page 1-3 and “Installed adapters” on page 1-5.

No Ethernet feature configuration is needed. The adapter auto-detects network ring speed and duplex (half or full) mode during power-on initialization. The adapter LEDs (near the external connector) provide information useful for monitoring Ethernet status and for problem solving. Refer to “Ethernet status LEDs” on page 3-32.

1. Power on the console.

   Insert the Diagnostic CD into DVD-RAM drive. Wait until the **Startup Menu** is displayed.
2. Determine whether to use Broadcom or Intel diagnostics from your review of the “Service tips” on page 1-3 and “Installed adapters” on page 1-5. At the **Startup Menu**, select one of the following:
   - **Intel PRO Ethernet Diagnostics**
   - **Broadcom Ethernet Diagnostics**.

   Was a message displayed stating no Ethernet or supported devices were detected?

   If **YES**, go to step 3. If **NO**, go to step 5 on page 3-21.
3. If the diagnostics did not detect any Ethernet support, do the following:
   - For **Ethernet adapter**:
     a. Verify the Ethernet adapter is securely installed and run the diagnostic again.
     b. If the adapter is still not detected, it must be replaced. Go to step 13 on page 3-22.
   - For **planar Ethernet**:

     Use the following procedure to verify Ethernet Support is enabled. Leave the Ethernet diagnostic diskette installed in the computer.
     a. Power off the system unit.

        Note: When the system unit is powered on, watch for the `Press F1 for Configuration/Setup` message.
     b. Power-on the computer.
     c. Start the **Configuration and Setup Utility** by pressing F1.
     d. Select the **Devices and I/O Ports** menu.
     e. Select the **Ethernet Setup** menu.
     f. Verify that Ethernet Support is `Enabled`.

   Was the Ethernet Support `Enabled`?

   If **YES**, go to step 13 on page 3-22. If **NO**, go to step 4.
4. Diagnostics failed to detect Ethernet support because it was not enabled on the system unit.
   - Enable the Ethernet support by pressing the **->** Key.
   - Save the configuration changes by repeatedly pressing the Esc key until only the **Configuration/Setup Utility** menu is displayed.
   - Select **Save Settings**, **Exit Setup**, **Exit the Setup Utility**.
   - The system will reboot from the Diagnostic CD.

   Return to step 2.

5. Ethernet support was successfully detected.

   In step 2 on page 3-20, were the BroadCom diagnostics selected?

   If **YES**, go to step 7. If **NO**, go to step 6.

6. An Intel-based Ethernet adapter is being tested.

   If both planar and adapter Ethernet support have the same manufacturer, an adapter selection menu is displayed.

   Was a numbered list of detected Ethernet adapters displayed?

   If **YES**, go to step 9. If **NO**, go to step 11 on page 3-22.

7. A BroadCom-based Ethernet adapter is being tested.

   If both planar and adapter Ethernet support have the same manufacturer, an adapter selection menu is displayed based on the MAC address. Select the address for the adapter being tested.

   A series of diagnostic tests will run automatically. Verify that all tests end with a result of **Passed** or **N/A**.

   Were all test results either **Passed** or **N/A**?

   If **YES**, go to step 8. If **NO**, go to step 13 on page 3-22.

8. Broadcom Ethernet diagnostics have run successfully. Use the following procedure to verify network connectivity:

   a. Connect the Ethernet network cable to the adapter you are testing and to the switch.

   b. Ensure the switch is powered on and, if present, the switch cable detect LED is lit.

   c. Ensure the adapter's network connectivity LED is lit. The LED is located to the left of the RJ45 network socket.

   If either of the two previously described LEDs is not lit, replace the following FRUs in order:

   a. Network cable

   b. Ethernet adapter

   c. Switch.

   Verify LED operation after replacing each FRU. If all FRUs have been replaced and either LED is still unlit, call for assistance.

   End of procedure.

9. Selection items referred to as **adapter** are PCI Ethernet adapters. Otherwise, the item refers to Ethernet support on the planar.

   a. Select the device for test, and press Enter to continue.

   b. Select **Test Adapter** from the **Main Menu**, and press Enter to continue.

   The **Test Menu** displays. To support multiple Ethernet Test releases, answer the following:

   Is **Continuous Network Test** present in the **Test Menu**?

   If **YES**, go to step 12 on page 3-22. If **NO**, go to step 10.

10. Ethernet support has been detected.

    To test the adapter:

    a. Ensure the adapter is cabled to the network.
    b. Ensure the switch is powered on.
    c. Ensure cable connection LED on the switch is on.
    d. Select **Test Adapter** from the **Main Menu** window.
    e. Select **Begin Adapter Tests** from the **Test Menu**.
    f. If additional messages are displayed before the tests start, select **Continue**.
    g. From the Test Adapter window, note the test results.

Replace the Ethernet adapter If any of the following tests fail:
- Device Registers
- FIFOs
- EEPROM
- Interrupt
- MAC Loopback
- Physical Loopback.

Go to step 13.

If all of the tests pass, continue as follows.

Note: Network tests require a second station (responder) to test station-to-station communication. Refer to the help windows for additional information.

Link and **Network Test** verify network connectivity. If they are not run automatically, do the following:

1) Press Esc to return to the **Test Menu**.
2) Select **Change Test Options**.
3) Select **Link** and **Network Test**.
4) Press Enter to enable the tests.
5) Press Esc to return to the **Test Menu**.
6) Select **Begin Adapter Tests**.

If either the **Link** or **Network Test** fails, there is a network connectivity problem. Go to step 15 on page 3-23.

If all the tests pass, go to step 14 on page 3-23.

11. One Ethernet device was detected; testing may proceed.

    To test the adapter, select **Test Adapter** from the **Main Menu**.

    The **Test Menu** displays. To support multiple Ethernet test releases, answer the following:

    Is **Continuous Network Test** present in the **Test Menu**?

    If **YES**, go to step 12. If **NO**, go to step 10 on page 3-21.

12. Ethernet support was successfully detected; testing may proceed.

    Note: If attached, disconnect the Ethernet network cable before proceeding.

    a. Select **Test Adapter** from the Test Adapter window.

       Note: If the Ethernet cable is connected to the system unit, a message requesting you to disconnect it is displayed.

    b. Select **Continue** from the `Setup set the adapter's master memory` message window.

    c. From the Test Adapter window, ensure the following tests passed:
       - Adapter tests
       - Loopback x, xxx Mbps.

    Did all tests indicate `passed`?

    If **YES**, go to step 14 on page 3-23. If **NO**, go to step 13.

13. Ethernet support was not successfully verified.

    Replace the Ethernet adapter or planar.

    Note: For planar board replacement instructions, refer to the HMM for the console machine type.

If the planar board has been replaced, verify the system unit configuration using the “Trusted Key Entry Workstation configurations” on page 2-48. Verify Ethernet support after replacing the failing FRU.

Go to step 14.

14. The computer’s Ethernet support was successfully verified. Use the following procedure to verify network connectivity.
    a. Press Enter to return to the **Test Adapter** menu.
    b. Connect the Ethernet network cable to the system unit and the switch.
    c. Ensure the switch is powered on and, if present, the switch's cable detect LED is lit.
    d. Select **Continuous Network test** from the **Test Adapter** menu.

       Notes:

       1) For additional information on **Continuous Network Test** select **View Help Files** from the **Main Menu**.
       2) If the Ethernet cable is not connected to the system unit and switch, a message requesting the connection of the cable is displayed.
       3) For the **No responder** scenario, the Ethernet adapter will send test data to itself after verifying network connectivity.

    Did you see either of the following?

    • A message stating:

      ```
      The adapter isn't receiving any test packets.
      ```

    • A message requesting the connection of a cable

    If **YES**, go to step 15. If **NO**, go to step 16.

15. There is a problem with the Ethernet support communicating with the network.
    a. Ensure the switch is powered on and, if present, the switch's cable-detect LED is lit.
    b. Replace the Ethernet cable and test again. If the test continues to fail, call for assistance.

16. Allow the test to run for at least 15 seconds before pressing Esc.

    Verify the following:

    • Network data rate (10 Mbps, 100 Mbps, or 1000 Mbps) is displayed in the upper right-hand corner. If these values are not present, there may be a problem with the customer’s network.
    • Transmit Requests = Transmitted OK = Received OK. If these values are not identical and **No responder** has been used, there may be a problem with the Ethernet support on the system unit. Replace the planar.
      a. Press Esc until the **Main Menu** is displayed.
      b. Select **Exit Setup** to exit diagnostics.
      c. Go to step 17.

17. If you were instructed to **Run All Selected**, test all the installed adapters in the **Run All Selected** list, one at a time. Otherwise, return to the procedure that directed you here.

    End of procedure

Table 3-1. Problem Area Reported

Problem Area Reported	Go To
Operator reported that the TKE Workstation application did not start but there were no other error indications.	“Undetermined errors” on page 3-25
DVD RW (RAM) drive	“DVD-RAM errors” on page 3-27
Hard disk	“Hard disk errors” on page 3-29
Diskette drive	“Diskette errors” on page 3-30
Display	“Display problems” on page 3-31
Ethernet LAN	“Ethernet LAN errors” on page 3-32
Cryptographic Adapter and Smart Card Reader	“Cryptographic adapter and smart card reader errors” on page 3-34
All other problems (for example: parity errors, power, POST codes, blank display, mouse, keyboard, USB ports or devices)	“Undetermined errors” on page 3-25
Task procedures for TKE workstations	**BOOKS** in the TKE Workplace or **Library** on Resource Link

Undetermined errors

Use this section when the operator detected a failure and Problem Analysis did not run automatically or Problem Analysis could not be run because of a problem on the TKE workstation.

Refer to the table, "Information and test menu selection" on page 3-18. **After making the repair, return to this procedure to complete the call**.

For the locations of the feature cards, refer to "Installed adapters" on page 1-5.

Note: If you are directed to replace FRUs, for removal and replacement instructions, refer to your specific machine type's HMM on the Diagnostic CD.

1. Do you have ***all*** of the following symptoms during power on?
   - No POST error codes
   - One or two short beeps
   - Trusted Key Entry Workstation or licensed internal code for the Trusted Key Entry Workstation fails to start
   - No reference code or any other error information displayed.

   If **YES**, go to step 2. If **NO**, go to step 7.

   After power on, the TKE Welcome should be displayed, then the Logon window for the TKE.
2. Verify system unit configuration. Refer to "Trusted Key Entry Workstation configurations" on page 2-48. Select **System Unit** configuration area. When configuration is complete, continue to the next step.
3. If there were any resources that were not correctly configured (for example, USB Support `Disabled` instead of `Enabled`), retry the failing component. If the failure recurs or there were no configuration errors, go to step 4. Otherwise, go to step 16 on page 3-26.
4. Use the information in "Testing PCI bus-based consoles" on page 3-17 to test the PC. Select **System Unit** problem area. Use the test **Run All Selected**.

   When the test is complete, go to step 5.
5. Did the tests detect any errors?

   If **YES**, go to step 7. If **NO**, go to step 6.
6. Reload the licensed internal code on the hard drive using the procedure in "Installing and restoring the PCIX TKE hard drive internal code" on page 2-43.

   When the licensed internal code is restored, press and hold Ctrl and Alt, and then press Delete (Ctrl+Alt+Delete).
   - If the licensed internal code in the TKE workstation starts correctly the problem is resolved. Close the call.
   - If the failure still occurs, retest the workstation using the instructions in "Testing PCI bus-based consoles" on page 3-17. Make the appropriate selection for the unit under repair.
   - If you were not able to isolate a failure, call for assistance.

   Did the tests run without errors?

   If **YES**, go to step 8 on page 3-26. If **NO**, go to step 7.
7. Continue exchanging FRUs from the FRU list and testing with the diagnostic procedure until the problem is resolved.

   Reinstall any FRUs that do not fix the problem.

   If you cannot resolve the problem, call for assistance.

8. Did you exchange the system board or the battery?

   If **YES**, go to step 9. If **NO**, go to step 10.

9. If you have not already done so, configure the system board.

   Refer to “Trusted Key Entry Workstation configurations” on page 2-48. Select **System Unit** configuration area.

   When configuration is complete, go to step 10.

10. Did you exchange any other PCI or PCIX adapter feature card?

    If **YES**, go to step 11. If **NO**, go to step 14.

11. If you have not already done so, verify the adapter’s configuration. Refer to “Testing PCI bus-based consoles” on page 3-17. Select **PCI adapter** configuration area.

    When configuration is complete, go to step 12.

12. Did you exchange the hard disk drive?

    If **YES**, go to step 13. If **NO**, go to step 15.

13. If there are jumpers or tab settings on the new hard drive, ensure the settings are the same as on the old drive.

    In the HMM for your TKE machine type, refer to the section about hard disk drive jumper settings.

    When complete, go to step 14.

14. Load system licensed internal code on the new hard disk. This step copies system licensed internal code and customization information to the new hard disk. For instructions, refer to the procedures in “Installing and restoring the PCIX TKE hard drive internal code” on page 2-43.

    When hard disk recovery is complete, go to step 15.

15. Did you exchange the DVD-RAM drive?

    If **YES**, go to step 16. If **NO**, go to step 17.

16. If there are jumpers or tab settings on the new DVD-RAM drive, ensure the settings are the same as on the old drive.

    Use the HMM (in PDF format) on the Diagnostic CD-ROM shipped with the console.

    When complete, go to step 17.

17. Create a backup DVD-RAM for hard disk data by using the instructions in “Internal code changes for a Trusted Key Entry Workstation” on page 2-45 for the version of the code installed.

    When the backup is complete, go to step 18.

18. Do the following:
    a. Power the system unit off.
    b. Power the system unit on.

    Close the call.

    End of procedure.

DVD-RAM errors

Use this procedure when a Repair and Verify window directs you to this chapter and the FRU list contains xxxx_DVD_RW_DRIVE or xxxx_DVD_RW_DISK or the customer reports a DVD read/write problem on the TKE workstation.

Service Tips

- Unless the customer added drives or partitions, the DVD-RAM drive identifier is G:. The drive is accessible only from media tasks (Format Media, and so forth).
- Use Format Media only on the TKE workstation.
- There is no write protection support for DVD-RAM media (no cartridge).

1. The media is either a DVD-RAM or CD/DVD ROM. Clean the media:
   - Do not use benzine, thinners, or any other cleaners on the disk surface.
   - Hold the disk by its edge. Do not touch the surface.
   - Remove surface dust and fingerprints by wiping from the center to the outside using a dry, soft cloth.

   Reinstall the disk, label side up.

   Go to step 2.
2. Retry the failing task using the original media.

   Did the failure occur again?

   If **YES**, go to step 3. If **NO**, close the call.
3. Leave the original media in the drive.
   - If you are trying a restore procedure, power off the workstation.
   - For any other operation, shut down the console, and then power off the workstation.

   Power on the PC and test the DVD-RAM drive using the procedure in “Testing PCI bus-based consoles” on page 3-17.

   Select **System Unit** problem area, and then select the test for the DVD-RAM drive. If you cannot start the test because of errors or when the test is complete, continue to step 4.
4. Did the DVD-RAM test fail while testing with the original media?

   Note: If you could not start the test because of errors, answer this question **YES**.

   If **YES**, go to step 5. If **NO**, go to step 10 on page 3-28.
5. Exchange the original media with a new one.

   Note: If you are replacing DVD-RAM media, the new media must be formatted. If possible, use another TKE-supporting DVD-RAM.
   a. From **TKE Workplace/View**, select **Console Actions**.
   b. From **Console Actions Work Area**, select Format Media.
   c. Select the **Format Type** based on usage.
   d. If the attempt to format the DVD fails, go to step 8 on page 3-28.
6. Test the DVD-RAM.
   a. Power off the TKE.
   b. Power on the TKE and test the DVD-RAM drive with the new media. Use the procedure in “Testing PCI bus-based consoles” on page 3-17.
   c. Select **System Unit** problem area, and then select the test for the DVD-RAM drive.
7. Did the DVD-RAM tests fail when you used the new media?

Note: If you could not start the test because of errors, answer the question **YES**.

If **YES**, go to step 8.

If **NO**, the original media was defective. Close the call.

8. Verify the following:
   - All DVD-RAM drive data and power cables are secure.
   - The DVD-RAM drive is jumpered as “Master” and is cabled to the “Secondary” IDE Bus.

   If diagnostics continue to fail, exchange the DVD-RAM drive. When complete, run the DVD-RAM tests again.

   Note: If there are any jumpers or tab settings on the new drive, ensure the settings are the same as on the old drive.

   Did the DVD-RAM drive tests continue to fail?

   If **YES**, go to step 9. If **NO**, the original DVD-RAM drive was defective. Close the call.
9. Continue exchanging FRUs from the FRU list and running the DVD-RAM drive tests.

   If the FRUs fix the problem, close the call. If you cannot isolate the problem, go to step 10.
10. The TKE resources (example: interrupt, I/O address) may be configured incorrectly. Verify the PC resources are correctly configured using the procedure in “Trusted Key Entry Workstation configurations” on page 2-48.

    Select **System Unit** configuration area, and verify configuration for the server unit and all adapters.

    When you complete the verification, retry the failing procedure and continue on step 11.
11. Does the failing procedure continue to fail?

    If **YES**, call for assistance. If **NO**, the resource settings were incorrect. Close the call.

End of procedure.

Hard disk errors

Use this procedure when a Repair and Verify window directs you to this chapter and the FRU list contains xxxx_FIXED_DISK or when the customer reports a hard disk problem.

1. Use the information in “Testing PCI bus-based consoles” on page 3-17 to test the TKE workstation. Select **Hard Disk** problem area.

   Return here when the test is complete, then continue below.

2. Did the hard disk tests fail?

   If **YES**, go to step 3. If **NO**, go to step 5.

3. Exchange the FRUs called by the diagnostics one at a time. For FRU removal and replacement instructions, refer to the HMM for the appropriate machine type on the Diagnostic CD-ROM.

   After each FRU is exchanged, test the repair using the procedure in “Testing PCI bus-based consoles” on page 3-17. Select **Hard Disk** problem area.

   Return here when the test is complete, then continue below.

   Did the hard disk tests continue to fail?

   If **YES**, call for assistance. If **NO**, use the HMM on the Diagnostic CD-ROM shipped with the console and continue with step 4.

4. If you exchanged the hard disk and there are jumpers or tab settings on the new hard disk, **ensure the settings are the same as on the old drive**.

   You must restore the licensed internal code and back up critical data to the new hard disk using the following procedure:

   a. Find the **TKE DVD-ROM** and the **Backup Critical Data DVD-RAM** for this TKE.

   b. Insert the **TKE DVD-ROM** in the TKE media reader.

   c. Initialize the TKE by holding down the **Ctrl** key and pressing the **Alt** and **Del** keys at the same time. The TKE will boot from the **TKE DVD-ROM**.

   d. Follow the **Install/Recovery** prompts on the TKE monitor to restore the Licensed Internal Code.

   e. After the LIC is loaded, you will be directed to insert the **Backup Critical Data DVD-RAM**. Follow the prompts on the TKE monitor to complete the backup.

5. Test using the procedure in “Testing PCI bus-based consoles” on page 3-17. Select **Run All Selected** problem area.

   Return here when the test is complete, then continue below.

   Close the call. For instructions, refer to the *Service Guide* for the server to which this console is connected.

   Note: If the tests do not fail and the problem remains, call for assistance.

END OF PROCEDURE.

Diskette errors

Use this procedure when a Repair and Verify window directs you to this chapter and the FRU list contains xxxx_DISKETTE or xxxx_DISKETTE_DRIVE or the customer reports a diskette problem.

1. Test the diskette drive using the procedure in “Testing PCI bus-based consoles” on page 3-17. Select **System Unit** problem area, and select the test for **Diskette Drive**.

   Note: Do not test with the diskette on which the errors occurred. Use a new diskette.

   When the test is complete, return to step 2 of this procedure.

   Note: If you cannot start the test because of the diskette drive failure, go to step 2 and answer the question **YES.**

2. Did the diskette tests fail while testing with the new diskette?

   Note: Answer **YES** if you were not able to run the tests because of diskette errors.

   If **YES**, go to step 3. If **NO**, go to step 5.

3. Exchange the diskette drive.

   When complete, run the diskette tests again.

   Did the diskette tests fail again?

   If **YES**, go to step 4. If **NO**, Close the call.

4. Continue exchanging FRUs from the FRU list and running tests. For FRU removal and replacement procedures, refer to the TKE HMM. If the FRUs fix the problem, close the call. If you cannot resolve the problem, call for assistance.

5. If the **original failure** occurred while **writing** to a diskette, retry the original task using a new diskette.

   Note: You must format the new diskette before trying to write on it.

   Does the diskette task still fail?

   If **YES**, go to step 6.

   If **NO**, the original diskette was defective. Close the call.

6. Recreate the information on the diskette or get a new diskette with the information.

   Retry the original task.

   If the failure occurs again, go to step 7. If no failures occur, close the call.

7. Test using the procedure in “Testing PCI bus-based consoles” on page 3-17. Select **System Unit** problem area, and then select **Run All Selected**.
   - If the tests fail, isolate the problem using the procedures in the HMM (in PDF format) on the Diagnostic CD-ROM shipped with the console. When complete, close the call.
   - If the tests do not fail or if you cannot isolate the problem, call for assistance.

   End of procedure.

Display problems

Use this procedure when the customer reports a display problem.

The display has no internal FRUs.

1. Test the display using the documentation shipped with it. If the problem is not resolved, replace the display.
2. Verify the repair using the procedure in “Testing PCI bus-based consoles” on page 3-17. Select **System Unit** for the problem area, and then select **Display**. When the test and repair are complete, close the call.

   End of procedure.

Ethernet LAN errors

Ethernet LEDs provide adapter and cable connectivity status. See “Ethernet status LEDs” for assistance interpreting LED status.

For 10Base-T and 100Base-TX networks, the customer’s switch may support a connectivity status indicator LED that is active when there is a good connection between the switch and active Ethernet adapter.

Ethernet status LEDs

Adapter LEDs provide data traffic and link status network connectivity information. The link status LED is active only for a 10BASE-T or 100BASE-TX (RJ45) network.

The Link LED reports the following:
- The adapter is linked (connected) to an Ethernet switch.
- The adapter has power. If the adapter does not have power, the Link LED is not active.

If the Link LED is not lit, verify the following:
- The network adapter is securely plugged into the console’s card socket.
- The Ethernet cable is securely connected between the network adapter and a switch.
- The switch is powered on.
- The Ethernet cable is not broken or damaged.

The Activity LED reports Ethernet adapter network data transmission and reception.

If the Link LED is lit and the Activity LED is not lit, verify the following:
- The Ethernet cable is securely connected between the network adapter and a switch.
- The switch is powered on.

8485 and 4362 (PCI planar Ethernet)

The status LEDs for the 8485 and 4362 tower planar board are located to the upper right (Link) and to the lower right (Activity) of the RJ45 connector. The planar board Ethernet connection supports 10/100/1000 Mbps data rates.

- Link Status: Green LED
- Activity Status: Green LED.

8485 and 4362 (PCI adapter Ethernet)

The status LEDs for the 8485 and 4362 PCI adapters are located above (Act/Link) and below (100 TX) the RJ45 connector. The PCI adapter card supports 10/100 Mbps data rates.

- Data Traffic and Link Status (Act/Link): Green LED
- Data Rate (100 TX): Green LED, Off = 10 Mbps, On = 100 Mbps

Ethernet repair procedure

In the following procedure, the term *workstation* refers to a TKE workstation that provides one of the input/output points for the Ethernet network.

1. Is only one Ethernet connection failing?

   If **YES**, go to step 3 on page 3-33. If **NO**, go to step 2 on page 3-33.

2. Remove the workstation you are working on from the network. If the network operates correctly, go to step 3. Otherwise, notify the network administrator of the network problem.
3. At the failing workstation verify the following:
   - The adapter cable is securely connected to either the adapter card or the on-board (planar) adapter.
   - The adapter cable is securely connected to the network.

   Depending on the type of connector used, verify one of the following:
   - 10Base T/100Base TX: Verify the Link LED is active and the network cable is connected to the switch.

     Note: If the Link LED is not active, exchange the cable or plug the cable into a different switch port. If the Link LED remains inactive, go to step 5.
   - 10Base2: Verify the workstation is connected to the adjacent workstation or workstations.
   - AUI: Verify the workstation is connected to the external transceiver.

   Unless otherwise directed, continue on step 4.
4. Was the cable securely connected in step 3?

   If **YES**, go to step 6. If **NO**, go to step 5.
5. Restart the failing workstation to test the Ethernet adapter.

   To restart the failing workstation, ensure there are no diskettes in the diskette drive nor any bootable media in the DVD drive. Press and hold Ctrl and Alt; then press Delete (Ctrl+Alt+Delete).
   - If the failure still occurs and you have not already done so, exchange the cable and test again. If the failure still occurs, go to step 6.
   - If the Ethernet adapter connects to the customer's network, close the call.
6. Test the Ethernet adapter card at the failing workstation.

   For desktop (PCI bus based) consoles, refer to "Testing PCI bus-based consoles" on page 3-17. Select **Ethernet** as the problem area to test.

   When the test is complete, go to step 7.
7. Did the Ethernet tests fail?

   If **YES**, go to step 8. If **NO**, go to step 9.
8. If you have not already done so, exchange the FRUs called by the diagnostics one at a time and rerun the tests to verify the repair.

   When the repair is complete, remove any diskettes from the drive or bootable media in the DVD drive, and ensure the Ethernet cable is connected. Initialize the console by powering it off, then on.
9. Does the adapter work correctly on the customer's network?

   If **YES**, close the call. If **NO**, go to step 10.
10. The Ethernet adapter runs all tests and is configured correctly but does not have connectivity to the customer's network.
    - Notify the customer's network administrator that the problem is on the Ethernet network.
    - If necessary, call for assistance.

    End of procedure

Cryptographic adapter and smart card reader errors

Use this procedure when the customer reports a problem with the Cryptographic Adapter or the Smart Card Reader feature.

The Transaction Security System provides comprehensive support for Data Encryption Standard (DES)-based and public-key-based cryptographic processing.

Service Tips

The PCIX Cryptographic Adapter FRU part number is located on the adapter.

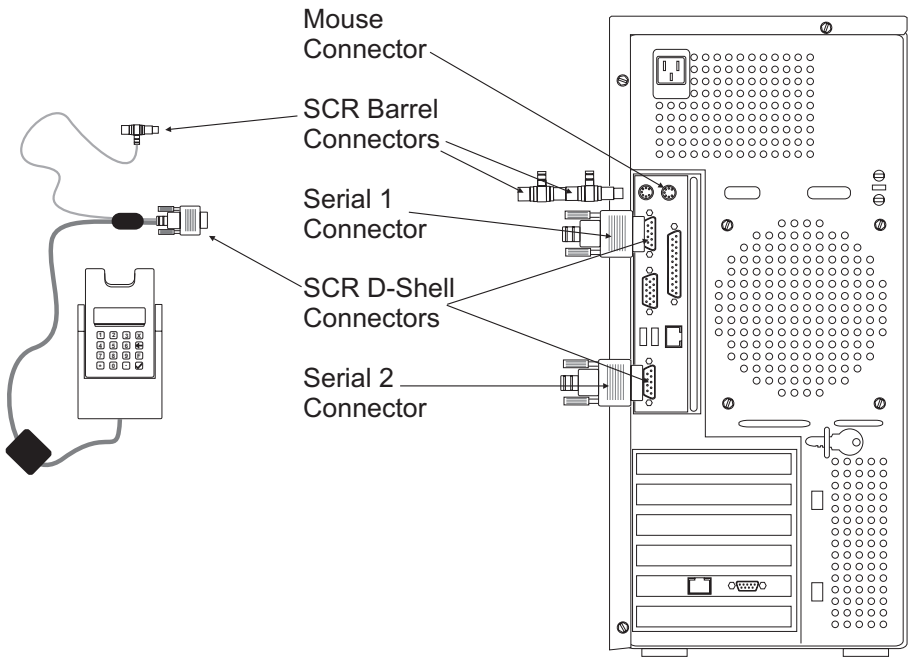
The Smart Card Reader FRU part number is located on the box in which the Smart Card Reader is shipped.

It is the customer's responsibility to correctly configure the Trusted Key Entry Workstation (TKE) software. TKE configuration data may contain customer sensitive information. Do not attempt to access this information without the customer's permission. The customer may refer to V6.0 of *Trusted Key Entry PCIX Workstation User's Guide*, SA23-2211–05.

If you exchange the adapter, the customer must initialize the new adapter. Refer to:

- "Loading PCIX TKE adapter card code" on page 2-34.
- "Initializing the PCIX TKE adapter" on page 2-36.
- "Loading the function control vector for the PCIX TKE adapter" on page 2-38.
- For additional customization tasks, see Chapter 4, **TKE Workstation Setup and Customization**, the section entitled "Initializing the TKE Cryptographic Adapter" in *Trusted Key Entry PCIX Workstation User's Guide*, SA23-2211-05.

1. If you have a 4367 TKE Workstation, it has only USB ports and no serial ports. Only Omnikey readers can be used with this model.
2. If you have an Omnikey Smart Card Reader attached to your TKE system, you simply need to connect its USB cable to an available USB port on the TKE Workstation.
3. If Kobil Smart Card Readers are installed, verify the cables connecting them to the TKE Workstation system unit are securely connected. The following illustration shows a Kobil Smart Card Reader with its various connectors and where they connect to the TKE Workstation.



4. Verify Cryptographic Adapter configuration in “Trusted Key Entry Workstation configurations” on page 2-48.
5. Was the adapter configuration correct?

   If **YES**, go to step 7. If **NO**, go to step 6.
6. Retry the failing procedure.

   If there is no error, close the call. For information, refer to “Completing the repair” on page 3-37.

   If an error still exists, go to step 7.
7. Use the information in “Testing PCI bus-based consoles” on page 3-17 to test the Cryptographic Adapter.

   Select “Personal Computer: PCIX Adapters” for the problem area. When the tests are complete, go to step 8.
8. Did the Cryptographic Adapter tests fail?

   If **YES**, go to step 9. If **NO**, go to step 10 on page 3-36.
9. Exchange the FRUs one at a time and rerun the tests to isolate the failure.

   When you repair the problem, go to “Completing the repair” on page 3-37.

   If you cannot isolate the failure, call for assistance.

   Notes:

   a. If you exchange the adapter, verify the configuration of the new FRU. For information, refer to “Trusted Key Entry Workstation configurations” on page 2-48.

   b. If you exchange the adapter, the customer must initialize the new adapter. Refer to:

      - “Loading PCIX TKE adapter card code” on page 2-34
      - “Initializing the PCIX TKE adapter” on page 2-36
      - “Loading the function control vector for the PCIX TKE adapter” on page 2-38

- For additional customization tasks, see Chapter 4, entitled “TKE Workstation Setup and Customization”, the section entitled “Initializing the TKE Cryptographic Adapter” in *Trusted Key Entry PCIX Workstation User's Guide*, SA23-2211-05.

10. Test the TKE Workstation using the procedure in “Testing PCI bus-based consoles” on page 3-17. Select “System Unit” problem area and run the test for “Run all selected”.

    If the tests fail, isolate the problem using the troubleshooting procedures in Chapter 2 of this book. When complete, go to “Completing the repair” on page 3-37.

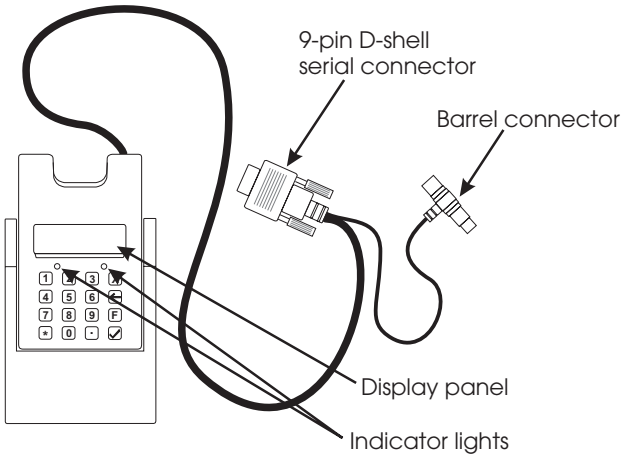
    If the tests do not fail or you cannot isolate the problem, go to step 11.

11. Test the Smart Card Readers by inserting a Smart Card in each reader and invoke the Smart Card Utility Program (SCUP).

    To invoke SCUP:

    - Click on **Trusted Key Entry**.
    - Click on **Smart Card Utility Program 6.0** in the right frame.

    When the Kobil readers are initialized successfully, both indicator lights on each reader will be lit. All information pertaining to the status of the Omnikey reader is displayed on the reader screen only.



End of procedure

Completing the repair

After the repairs have been completed, use this procedure to restore the TKE Workstation to correct operation.

1. Did you exchange the system board or the battery?

   If **YES**, go to step 2. If **NO**, go to step 3.

2. If you have not already done so, configure the system board.

   Refer to “Trusted Key Entry Workstation configurations” on page 2-48. Select **System Unit** configuration area.

3. Did you exchange a PCIX adapter feature card?

   If **YES**, go to step 4. If **NO**, go to step 5.

4. If you have not already done so, verify the adapter’s configuration. Refer to “Trusted Key Entry Workstation configurations” on page 2-48. Select the Configuration Area for the adapter.

   If you exchange the adapter, the customer must initialize the new adapter. Refer to:

   - “Loading PCIX TKE adapter card code” on page 2-34.
   - “Initializing the PCIX TKE adapter” on page 2-36.
   - “Loading the function control vector for the PCIX TKE adapter” on page 2-38.
   - For additional customization tasks, see Chapter 4, **TKE Workstation Setup and Customization**, the section entitled “Initializing the TKE Cryptographic Adapter” in V6.0 of the *Trusted Key Entry PCIX Workstation User's Guide*, SA23-2211–05.

5. Did you exchange the hard disk drive?

   If **YES**, go to step 6. If **NO**, go to step 7.

6. If there are jumpers or tab settings on the new hard drive, ensure they are set the same as the old drive.

   Note: This step copies system licensed internal code and customization information to the new hard disk.

7. Did you exchange the DVD drive?

   If **YES**, go to step 8. If **NO**, go to step 9.

8. If there are jumpers or tab settings on the new DVD drive, ensure they are set the same as the old drive.

   Refer to the defective drive to verify the jumper settings.

9. Use the instructions in “Saving the configuration for PCIX TKE” on page 2-41 to create a BACKUP DVD-RAM.

   When the backup is complete, go to step 11.

10. On the TKE Workstation:
    - Ensure there are no diskettes in the diskette drive.
    - Power the system unit off.
    - Power the system unit on.

    Close the call. For instructions, refer to “Completing the repair.”

    End of procedure

Appendix. Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Adobe is a registered trademark of Adobe Systems Incorporated in the United States, and/or other countries.

Intel is a registered trademark of Intel Corporation or its subsidiaries in the United States and other countries.

Other company, product, or service names may be trademarks or service marks of others.

Electronic emission notices

The following statement applies to this IBM product. The statement for other IBM products intended for use with this product will appear in their accompanying manuals.

Federal Communications Commission (FCC) Statement

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits

are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions contained in the installation manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. IBM is not responsible for any radio or television interference caused by using other than recommended cables and connectors, by installation or use of this equipment other than as specified in the installation manual, or by any other unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Canadian Department of Communications Compliance Statement

This Class A digital apparatus complies with Canadian ICES-003.

Avis de conformlté aux normes du ministère des Communications du Canada

Cet appareil numérique de la classe A est conform à la norme NMB-003 du Canada.

European Union (EU) Electromagnetic Compatibility Directive

This product is in conformity with the protection requirements of EU Council Directive 2004/108/EC on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product, including the fitting of non-IBM option cards.

This product has been tested and found to comply with the limits for Class A Information Technology Equipment according to European Standard EN 55022. The limits for Class equipment were derived for commercial and industrial environments to provide reasonable protection against interference with licensed communication equipment.

Warning: This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

European Community contact:
IBM Technical Regulations
Pascalstr. 100, Stuttgart, Germany 70569
Telephone: 0049 (0) 711 785 1176
Fax: 0049 (0) 711 785 1283
email: tjahn@de.ibm.com

EC Declaration of Conformity (In German)

Deutschsprachiger EU Hinweis: Hinweis für Geräte der Klasse A EU-Richtlinie zur Elektromagnetischen Verträglichkeit

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 89/336/EWG zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten und hält die Grenzwerte der EN 55022 Klasse A ein.

Um dieses sicherzustellen, sind die Geräte wie in den Handbüchern beschrieben zu installieren und zu betreiben. Des Weiteren dürfen auch nur von der IBM empfohlene Kabel angeschlossen werden. IBM übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung der IBM verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung der IBM gesteckt/eingebaut werden.

EN 55022 Klasse A Geräte müssen mit folgendem Warnhinweis versehen werden: ″Warnung: Dieses ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funk-Störungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen zu ergreifen und dafür aufzukommen.″

Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten

Dieses Produkt entspricht dem “Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG)“. Dies ist die Umsetzung der EU-Richtlinie 89/336/EWG in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) vom 18. September 1998 (bzw. der EMC EG Richtlinie 89/336) für Geräte der Klasse A.

Dieses Gerät ist berechtigt, in Übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen.

Verantwortlich für die Konformitätserklärung nach Paragraf 5 des EMVG ist die IBM Deutschland GmbH, 70548 Stuttgart.

Informationen in Hinsicht EMVG Paragraf 4 Abs. (1) 4:

Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022 Klasse A.

update: 2004/12/07

People’s Republic of China Class A Compliance Statement

This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user may need to perform practical actions.

声　明

此为A级产品，在生活环境中，
该产品可能会造成无线电干扰。
在这种情况下，可能需要用户对其
干扰采取切实可行的措施。

Japan Class A Compliance Statement

This is a Class A product based on the standard of the VCCI Council. If this equipment is used in a domestic environment, radio interference may occur, in which case, the user may be required to take corrective actions.

この装置は，クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。　VCCI－A

Korean Class A Compliance Statement

이 기기는 업무용으로 전자파적합등록을 한 기기이오니 판매자 또는 사용자는 이점을 주의하시기 바라며, 만약 잘못 판매 또는 구입하였을 때에는 가정용으로 교환하시기 바랍니다.

Taiwan Class A Compliance Statement

Warning: This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user will be required to take adequate measures.

警告使用者:
這是甲類的資訊產品，在
居住的環境中使用時，可
能會造成射頻干擾，在這
種情況下，使用者會被要
求採取某些適當的對策。

台灣IBM 產品服務聯絡方式：
台灣國際商業機器股份有限公司
台北市松仁路7號3樓
電話：0800-016-888

Printed in USA

GC28-6862-03

Spine information:

System z Service Guide for TKE Version 6.0 or later