Redbooks Flash

Franck Injey

IBM @server zSeries 990 Cryptographic Coprocessor Configuration

Configuration planning

This Redpaper provides information on the PCI X Cryptographic Coprocessor (PCIXCC) and the PCI Cryptographic Accelerator (PCICA) on a z990 server. We describe cryptographic domains and z990 configuration rules considering the increased number of logical partitions. We review items that should be taken into consideration when planning for non-disruptive installation of PCICA and PCIXCC features.

We describe, step-by-step, how to define and configure cryptographic coprocessors to each logical partition from the Hardware Management Console (HMC). We also show the use of ICSF Coprocessor Management panels.

This Redpaper is intended for IBM systems engineers, consultants, and customers who plan to install zSeries 990 cryptographic features.

Cryptographic domains

Each cryptographic coprocessor has 16 physical sets of registers or queue registers, each set belonging to a *domain*.

- A cryptographic domain index, from 0 to 15, is allocated to a logical partition via the definition of the partition in its image profile; the same domain must also be allocated to the ICSF instance running in the logical partition via the Options Data Set.
- Each ICSF instance accesses only the Master Keys or queue registers corresponding to the domain number, which specified in the image profile at the system Service Element and in its Options Data Set. Each ICSF is seeing a logical crypto coprocessor made of the physical cryptographic engine and the unique set of registers (the domain) allocated to this logical partition.

CPC configuration rules

- The installation of the CP Assist for Cryptographic Functions (CPACF) DES/TDES enablement, feature code 3863, is required to enable the use of PCIXCC and PCICA features. Feature code 3863 enables DES and TDES algorithm on the CPACF (the SHA-1 algorithm is always enabled).
- The z990 allows for up to two PCICA features per I/O cage. This allows for a maximum of six PCICA features or twelve PCICA coprocessors per z990 server.
- The maximum number of PCIXCC features (or cryptographic coprocessors) per I/O cage is four; the maximum number of PCIXCC features per z990 is also four.
- The total number of cryptographic features may not exceed eight per z990 for any combination of PCIXCC and PCICA features.
- In addition, any combination of PCIXCC, PCICA, OSA-Express and FICON™-Express features may not exceed 20 features per I/O cage, or 60 features per z990 server.
- On z990, the PCI X Cryptographic Coprocessor and the PCI Cryptographic Accelerator features do not use CHPIDs from the Logical Channel Subsystem pool, but each cryptographic coprocessor is assigned a PCHID, as follows:
  - One PCHID is assigned per PCIXCC feature.
  - Two PCHIDs are assigned per PCICA feature.
- Table 1 summarizes the Cryptographic feature codes for z990.

Table 1 Cryptographic Feature codes

Feature code	Description
3863	Crypto enablement feature. Prerequisite to use the CPACF, PCIXCC, or PCICA hardware features
0868	PCI X Cryptographic Coprocessor (PCIXCC) feature
0862	PCI Cryptographic Accelerator (PCICA) feature
0886	TKE 4.0 hardware for Token Ring
0889	TKE 4.0 hardware for Ethernet

Planning considerations

- The z990 always operates in LPAR mode. The concept of "dedicated coprocessor" does not apply to PCIXCC or PCICA. PCI Cryptographic Coprocessors are made available to logical partitions as directed by the domain assignment and the candidate list, regardless of the shared or dedicated status given to the CPs in the partition.
- The z990 allows for up to 30 logical partitions to be active concurrently. Each PCIXCC or PCICA coprocessor supports 16 domains. When more than 16 active logical partitions on the z990 require concurrent access to a PCICA or PCI X Cryptographic Coprocessor, the configuration must include at least the following:
  - Two PCI Cryptographic Accelerators in one PCICA feature
  - Two PCI X Cryptographic Coprocessors in two PCIXCC features

Note: More features may be needed to satisfy application performance or availability requirements.

- For availability, more than one feature of any given type, PCICA or PCIXCC, should be installed to avoid a single point of failure.
  - When more than one cryptographic coprocessor is installed on a single feature (PCICA), assignment of multiple coprocessors to one logical partition should be spread across multiple cryptographic features.
  - The use of retained private keys on PCIXCC creates an application single point of failure, since RSA retained private keys cannot be copied or backed up.
- There is an intrusion latch within the PCI X Cryptographic Coprocessor logic which is set any time the feature is removed from the system. If the feature is re-installed, and power is applied, the coprocessor keys and secrets are zeroized and the intrusion latch is reset.

  If a TKE workstation is available, the coprocessor may first be disabled from the TKE workstation before removing the feature from the system. In that case, when the feature is re-installed, the coprocessor keys and secrets are not zeroized, but the intrusion latch is reset and the coprocessor remains in the disabled state. The coprocessor then may be enabled from the TKE and normal operations may resume.

  See *z/OS™ ICSF TKE Workstation User's Guide,* SA22-7524, for more information.
- The definition of domain indexes and cryptographic coprocessor numbers in the Candidate list for each logical partition should be planned ahead to prepare your cryptographic configuration for non-disruptive changes.
  - A change to a logical partition image profile to modify its domain index(es) or Candidate list is disruptive to the partition. It requires a partition deactivation-activation to take effect.
- PCIXCC or PCICA features can be installed concurrently by use of the Nondisruptive Hardware Change[1] task. To dynamically enable use of a new PCIXCC or PCICA coprocessor to a partition requires that:
  - At least one usage domain index be defined to the logical partition.
  - The cryptographic coprocessor number(s) be defined in the partition Candidate list.
- The same usage domain index may be defined more than once across multiple logical partitions. However, the cryptographic coprocessor number coupled with the usage domain index specified must be unique across all active logical partitions.
  - The same cryptographic coprocessor number and usage domain index combination may be defined for more than one logical partition. In such a configuration, only one of the logical partitions can be active at any time. This may be used, for example, to define a configuration for backup situations.
- Newly installed cryptographic features are assigned coprocessor numbers sequentially during the power-on Reset following the installation.
  - However, when a new cryptographic feature is installed concurrently using the Nondisruptive Hardware Change task, it is possible for the installation to select an out-of-sequence coprocessor number from the unused range. In this case, the customer should communicate the desired cryptographic coprocessor number(s) to the IBM® installation team.

    When the task is used to concurrently remove a PCI cryptographic feature, the coprocessor number is automatically freed.

Table 2 on page 4 illustrates a simplified configuration map. Each row identifies a logical partition and each column identifies a cryptographic coprocessor, installed or in plan. Each cell indicates the Usage Domain Index number(s) planned to be assigned to the partition in its image profile (we recommend you work from a spreadsheet).

[1] The Nondisruptive Hardware Change is only available when logged to the Support Element in Service mode.

Table 2 Planning LPARs domain and cryptographic coprocessor

Coprocessor ID	AP0	AP1	AP2	AP3	AP4	AP5	AP6	.../...
Type	PCICA or PCIXCC	PCICA or PCIXCC	PCICA or PCIXCC	PCICA or PCIXCC	PCICA or PCIXCC	PCICA or PCIXCC	PCICA or PCIXCC	
LPAR lp0	0	0				0	0	
LPAR lp1			0	0	0			
LPAR lp2	0	0	0	0				
LPAR lp4	4 14	4 14	4 14	4 14	4 14	4 14	4 14	
LPAR lp5				1	1	1	1	
.../...								

There is a potential conflict when, for a given column, different cells contain the same domain number more than once.

Up to 30 partitions can be defined and active, and each coprocessor has 16 domains. Within a row, the domain index number(s) specified are identical since the domain index applies to all cryptographic coprocessors selected in the partition Candidate list.

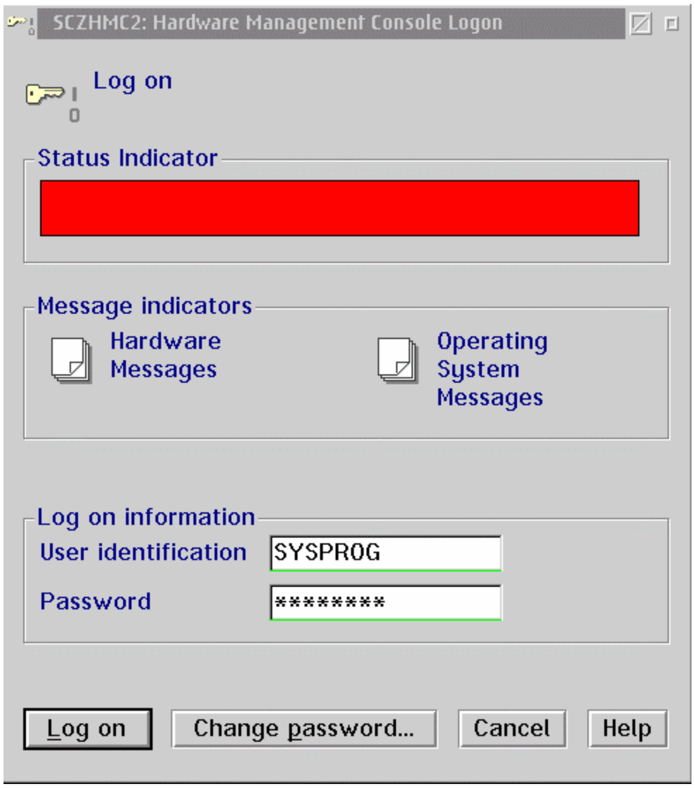
In the example shown in Table 2:

- Both logical partitions lp0 and lp1 use domain 0, but are assigned different cryptographic coprocessors. The combination domain number and cryptographic coprocessor number is unique across partitions. Both partitions lp0 and lp1 can both be active at the same time.
- Logical partition lp4 uses domain 4 and 14. Since no other partition uses the same domain numbers, there is no conflict.
- Logical partition lp5 uses domain 1 and no other partition uses the same domain number. Again, there is no conflict.
- Logical partition lp2 uses domain 0 on the set of cryptographic coprocessors already used by lp0 and lp1. Partition lp2 cannot be active concurrently with lp0 or lp1. However, this may be a valid configuration to cover for backup situations.

LPAR cryptographic definition

The z990 server only operates in LPAR mode. For each logical partition that requires access to the cryptographic coprocessors, either PCICA or PCI XCC, you must customize the partition image profile. This is done from the Hardware Management Console and the Support Element. First, start an HMC session, as shown in the following section.

Start an HMC session


SCZHMC2: Hardware Management Console Logon

User identification: SYSPROG

Password: *********

Figure 1 HMC Logon

1. Sign on to the HMC using the SYSPROG identification, as shown in Figure 1.
2. The initial HMC window is displayed. Open **Groups** from the Views area, and double-click **Defined CPCs** from the Groups Work Area. If multiple CPCs are connected to the HMC, select the one you want to connect to; see Figure 2 on page 6.
3. In the Task list Area, rotate to the CPC Recovery in the Task List.
4. Drag and drop (right mouse click and hold) the selected CPC to Single Object Operations task icon.

   A Single Object Operations Task Confirmation window is displayed. Click **yes** to confirm. The Support Element Workplace session window opens.

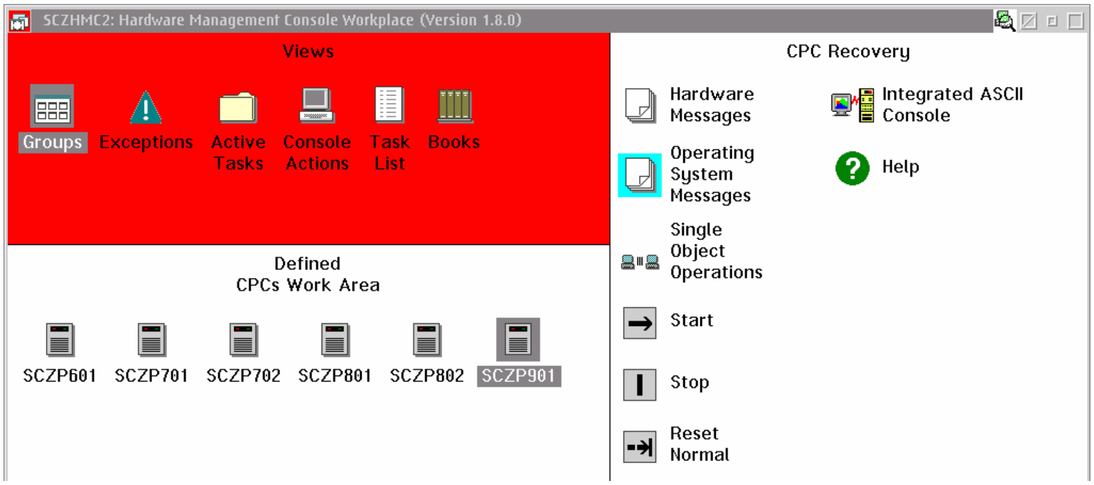
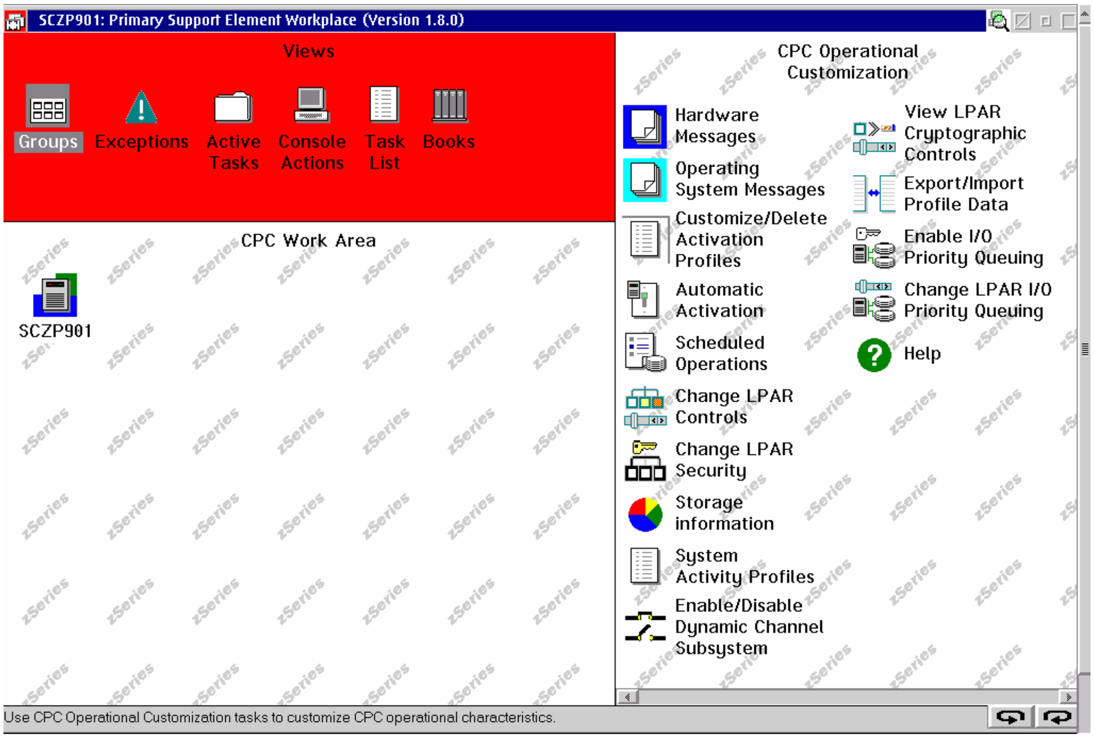


Figure 2 Defined CPCs Work Area and CPC Recovery

CPACF DES/TDES enablement

The z990 crypto enablement feature (#3863) enables DES and TDES algorithms on the CPACF. It is a prerequisite to use the PCIXCC and PCICA features. You can check that the feature is properly installed on your processor from the CPC details window.

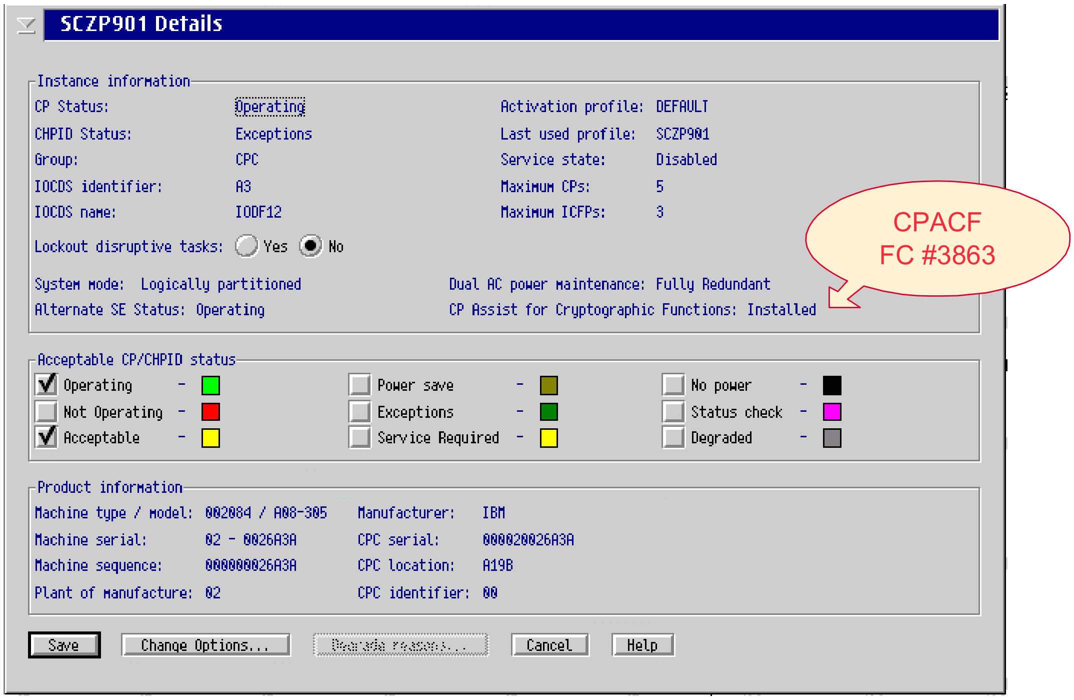

SCZP901: Primary Support Element Workplace (Version 1.8.0)
Views
Groups
Exceptions
Active Tasks
Console Actions
Task List
Books
CPC Work Area
SCZP901
CPC Operational Customization
Hardware Messages
Operating System Messages
Customize/Delete Activation Profiles
Automatic Activation
Scheduled Operations
Change LPAR Controls
Change LPAR Security
Storage information
System Activity Profiles
Enable/Disable Dynamic Channel Subsystem
View LPAR Cryptographic Controls
Export/Import Profile Data
Enable I/O Priority Queuing
Change LPAR I/O Priority Queuing
Help
zSeries

Use CPC Operational Customization tasks to customize CPC operational characteristics.

Figure 3 CPC Work Area and CPC Operational Customization

From the Support Element Workplace shown in Figure 3:

1. From the Views area, open **Groups** and **CPC**.
2. Select the **CPC** icon in the CPC Work Area view and double-click to open the CPC details window shown in Figure 4 on page 7.



SCZP901 Details

Instance information

CP Status: Operating
CHPID Status: Exceptions
Group: CPC
IOCDS identifier: A3
IOCDS name: IODF12
Activation profile: DEFAULT
Last used profile: SCZP901
Service state: Disabled
Maximum CPs: 5
Maximum ICFPs: 3

Lockout disruptive tasks: ○ Yes ● No

System mode: Logically partitioned
Alternate SE Status: Operating
Dual AC power maintenance: Fully Redundant
CP Assist for Cryptographic Functions: Installed

Acceptable CP/CHPID status

☑ Operating - 🟩	□ Power save - 🟫	□ No power - ⬛
□ Not Operating - 🟥	□ Exceptions - 🟩	□ Status check - 🟪
☑ Acceptable - 🟨	□ Service Required - 🟨	□ Degraded - ⬜

Product information

Machine type / model: 002084 / A08-305
Machine serial: 02 - 0026A3A
Machine sequence: 000000026A3A
Plant of manufacture: 02
Manufacturer: IBM
CPC serial: 000020026A3A
CPC location: A19B
CPC identifier: 00

CPACF
FC #3863

Figure 4 CPC Details

3. In the window, verify the CPACF DES/TDES enablement feature. If the window displays `CP Assist for Cryptographic Functions: Installed`, it means that the cryptographic enablement feature code 3863 is installed.

   If the window displays `CP Assist for Cryptographic Functions: Not Installed`, then feature code 3863 is not installed. You may still be able to customize the partition image profiles, but cryptographic functions will not operate.

4. Click **Cancel** to return.

Customize the profiles

The next step is to define in the image profile for each partition where you intend to enable cryptographic operations:

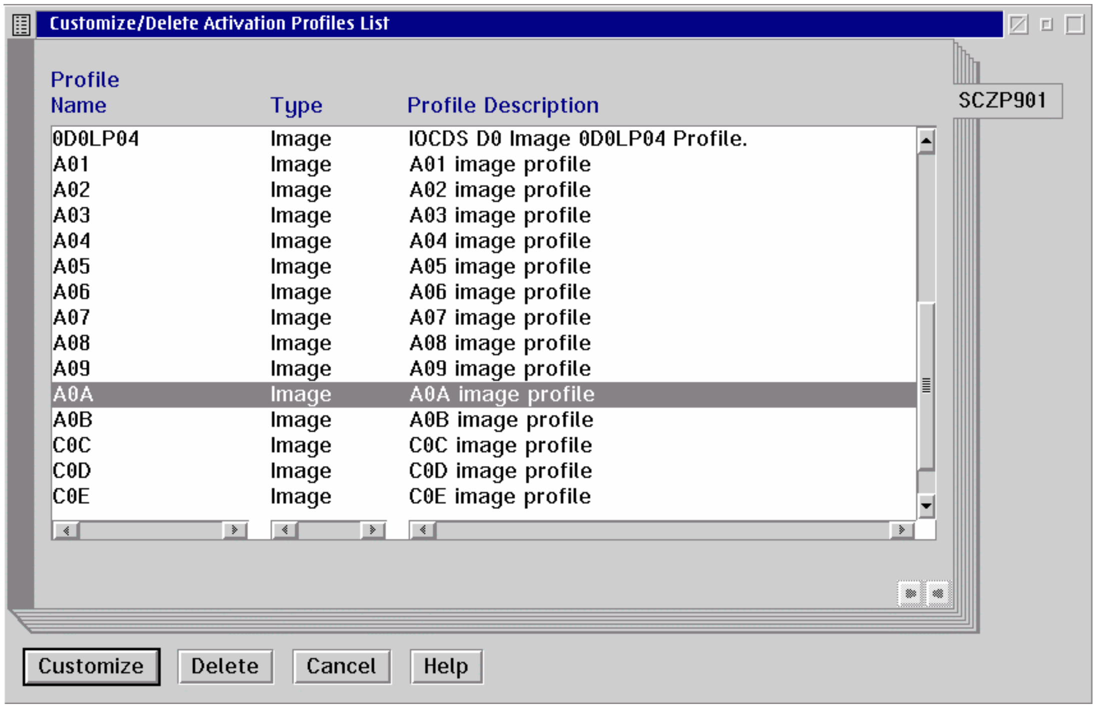
- Its Usage domain index
- Its Control Domain Index
- Its PCI Cryptographic Coprocessor Candidate List
- Its PCI Cryptographic Coprocessor Online List

This is accomplished through the Customize/Delete Activation Profile task.

> **Note:** The Customize/Delete Activation Profile is also available from the HMC Workplace. The scope of the task also depends on the object selected. Whether you decide to work with a CPC object or with an image profile selected from the Image Work Area does not change the result.
>
> In this document we chose use the SE Workplace and selected the CPC object.

From the CPC Work Area, as shown in Figure 3 on page 6:

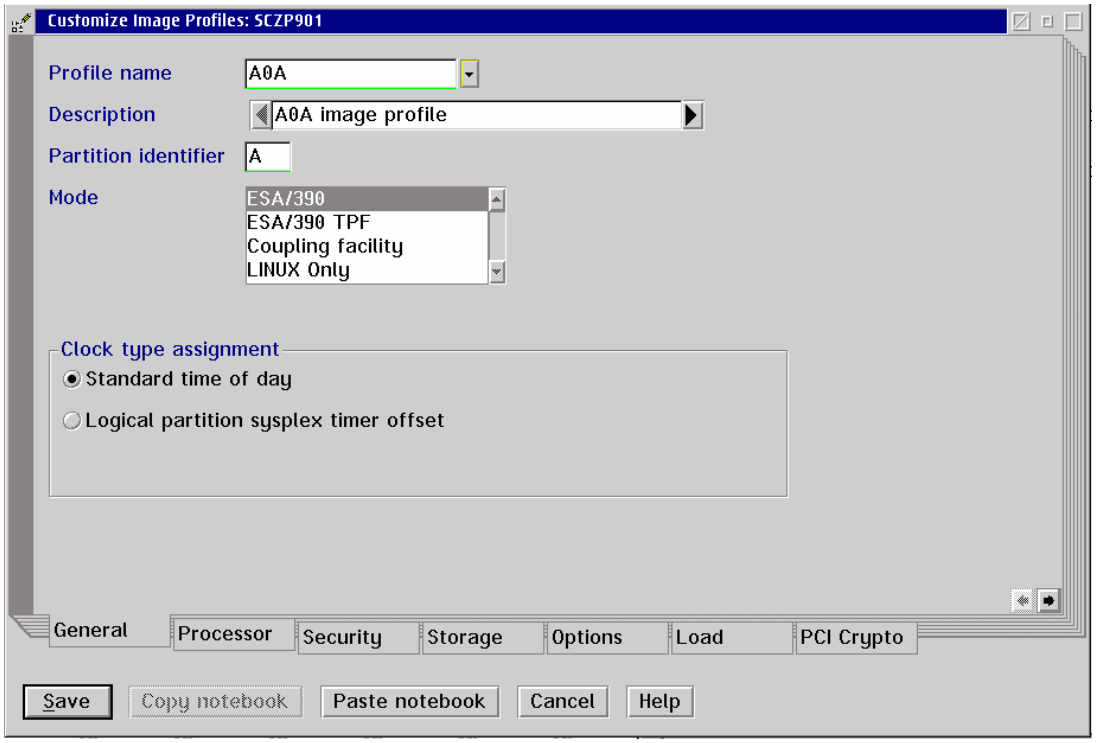
1. In the Task List Work Area, rotate to locate the CPC Operational Customization task.
2. Make sure the **CPC** icon is selected.
3. In the CPC Operational Customization task list, double-click **Customize/Delete Activation Profile**. This opens the notebook shown in Figure 5.



Profile Name	Type	Profile Description
0D0LP04	Image	IOCDS D0 Image 0D0LP04 Profile.
A01	Image	A01 image profile
A02	Image	A02 image profile
A03	Image	A03 image profile
A04	Image	A04 image profile
A05	Image	A05 image profile
A06	Image	A06 image profile
A07	Image	A07 image profile
A08	Image	A08 image profile
A09	Image	A09 image profile
A0A	Image	A0A image profile
A0B	Image	A0B image profile
C0C	Image	C0C image profile
C0D	Image	C0D image profile
C0E	Image	C0E image profile

Figure 5 Customize/Delete Activation Profiles List

4. From the list, select the name of the partition image profile you want to customize and click **Customize**. This brings up the image profile notebook shown in Figure 6 on page 9.



Customize Image Profiles: SCZP901

Profile name A0A

Description A0A image profile

Partition identifier A

Mode
ESA/390
ESA/390 TPF
Coupling facility
LINUX Only

Clock type assignment
● Standard time of day
○ Logical partition sysplex timer offset

Figure 6 Customize Image Profiles - General

5. Click the **PCI Crypto** tab of the image profile. The PCI Crypto window shown in Figure 7 is displayed.

   The definitions can be changed in the image profile, whether or not the logical partition is active. However, the new definitions will not take effect until the next time the partition is activated. Note the following explanations:

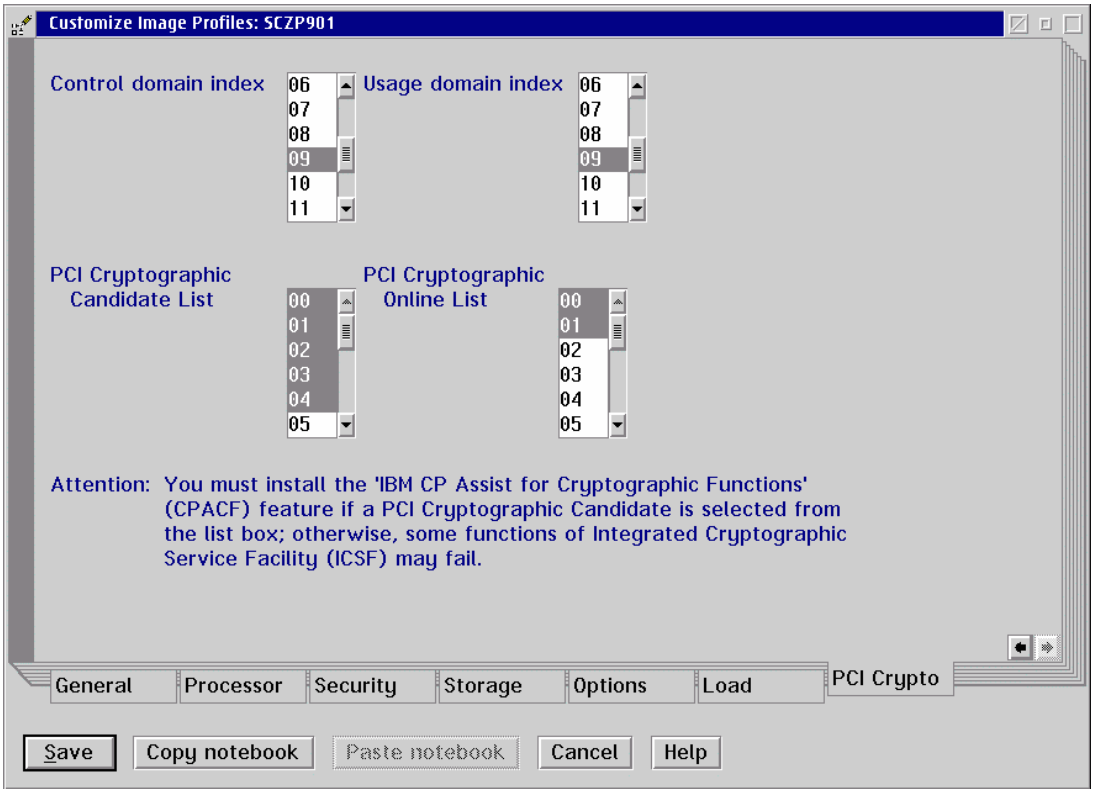
   – Usage domain index

     This identifies the cryptographic coprocessor domain(s) assigned to the partition for all cryptographic coprocessors that are configured on to the partition.

     The number(s) selected should match the domain number(s) entered in the Options dataset when starting this partition's instance of ICSF.

     The same usage domain index can be used by multiple partitions regardless of which LCSS they are defined to, but the combination cryptographic coprocessor number and usage domain index number must be *unique* across all partitions planned to be active at the same time.

     Although it is possible to define duplicate combinations of cryptographic coprocessor number(s) and usage domain index(es), such logical partitions cannot be concurrently active. This is a valid option, for example, for backup configurations.



Control domain index: 06 07 08 09 10 11

Usage domain index: 06 07 08 09 10 11

PCI Cryptographic Candidate List: 00 01 02 03 04 05

PCI Cryptographic Online List: 00 01 02 03 04 05

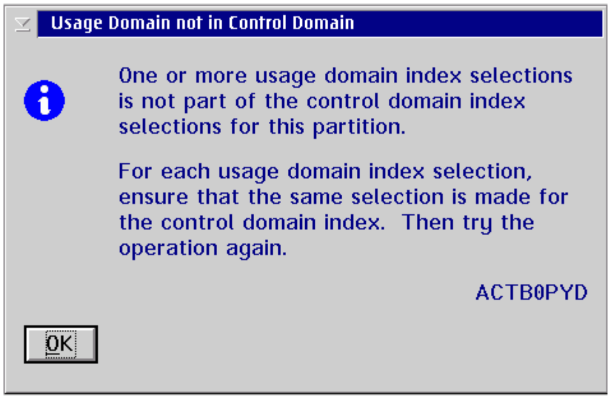
Attention: You must install the 'IBM CP Assist for Cryptographic Functions' (CPACF) feature if a PCI Cryptographic Candidate is selected from the list box; otherwise, some functions of Integrated Cryptographic Service Facility (ICSF) may fail.

Figure 7 Customize Image Profiles - Crypto window definitions

– Control domain index

This identifies the cryptographic coprocessors domain index(es) that can be administered from this logical partition being set up as the TCP/IP host for the TKE.

The control domain index must include the usage domain index specified for the partition. If any selected usage domain index is not part of the control domain index selection, the update is rejected. An error window is displayed (see Figure 8).



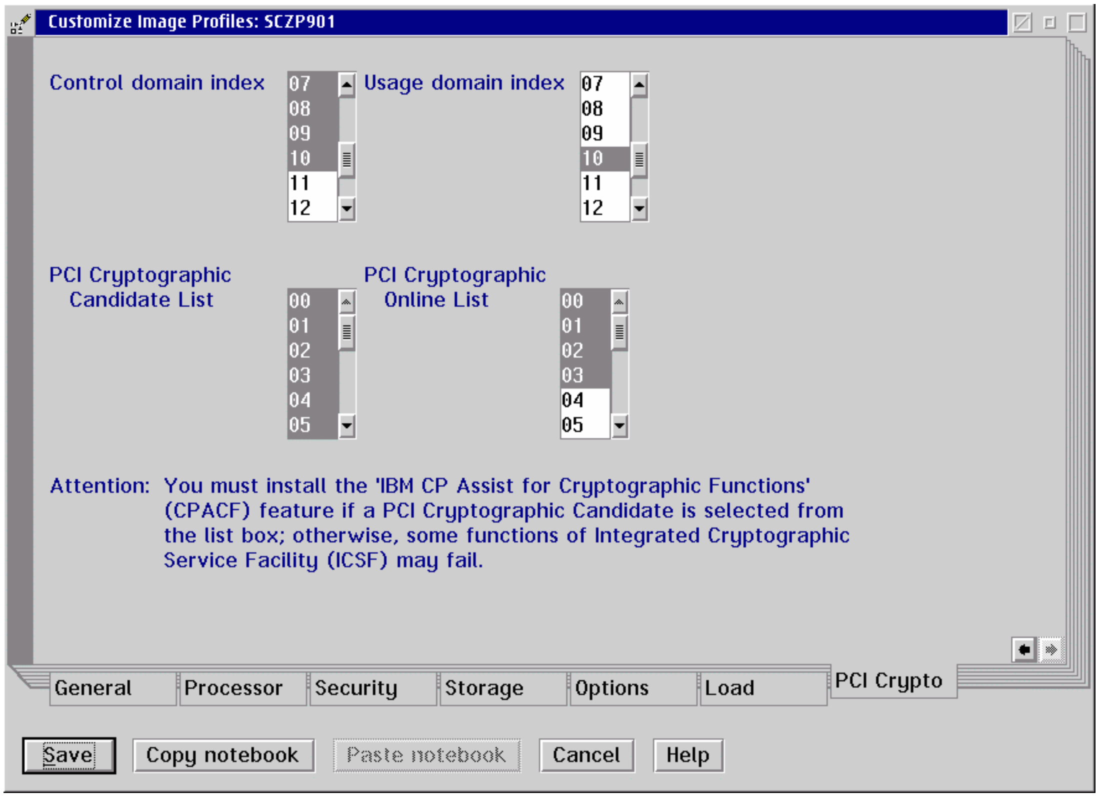
One or more usage domain index selections is not part of the control domain index selections for this partition.

For each usage domain index selection, ensure that the same selection is made for the control domain index. Then try the operation again.

ACTB0PYD

Figure 8 Usage Domain not in Control Domain message

If you are setting up the host TCP/IP in this logical partition to communicate with the TKE, the partition will be used as a path to other domains' Master Keys. Indicate all the Control domains you want to access (including this partition's own control domain) from this partition; refer to Figure 9.



Customize Image Profiles: SCZP901

Control domain index: 07, 08, 09, 10, 11, 12

Usage domain index: 07, 08, 09, 10, 11, 12

PCI Cryptographic Candidate List: 00, 01, 02, 03, 04, 05

PCI Cryptographic Online List: 00, 01, 02, 03, 04, 05

Attention: You must install the 'IBM CP Assist for Cryptographic Functions' (CPACF) feature if a PCI Cryptographic Candidate is selected from the list box; otherwise, some functions of Integrated Cryptographic Service Facility (ICSF) may fail.

Figure 9 Customize Image Profile - Multiple Control domain Indexes

– PCI Cryptographic Coprocessor Candidate List

  This identifies the cryptographic coprocessor numbers that are eligible to be accessed by this logical partition. From the scrollable list, select the coprocessor number(s), from 0 to 15, that identifies the PCIXCC or PCICA Cryptographic Coprocessor to be accessed by this partition.

  When a cryptographic coprocessor number selected in the partition Candidate list is not available to the partition when the partition is activated, either because it is configured off or not installed, no error condition is reported. The cryptographic coprocessor number is ignored and the activation process continues.

  When a new cryptographic coprocessor is installed and its number has been previously selected in the partition Candidate list, it can be dynamically configured on to the partition from the Support Element using the Configure On/Off option in the Crypto Service Operations task list.

  A cryptographic coprocessor number not in the partition Candidate list cannot be configured on to the partition.

– PCI Cryptographic Coprocessor Online List

  This identifies the cryptographic coprocessors numbers that are automatically brought online during logical partition activation. The coprocessor numbers selected in the Online List must also be part of the Candidate List.

  After the next partition activation, installed PCI Cryptographic Coprocessors that are on the partition PCI Cryptographic Candidate list but not on the PCI Cryptographic Online list are in a “configured off” state (Standby). They can be later configured on to the partition from the Support Element by using the Configure On/Off option in Crypto

Service Operations task list (see “Config On/Off from the CPC Work Area” on page 20).

When the partition is activated, no error condition is reported if a cryptographic coprocessor number selected in the partition Online list is not installed. The Cryptographic Coprocessor is ignored and the activation process continues.

When a cryptographic coprocessor number selected in the partition Online list has been previously configured off to the partition, it is automatically configured back on when the partition is next activated.

If the cryptographic coprocessor number and usage domain index combination for the coprocessor selected in the partition Online list is already in use by another active logical partition, activation of the logical partition will fail; see “Logical partition activation” on page 12.

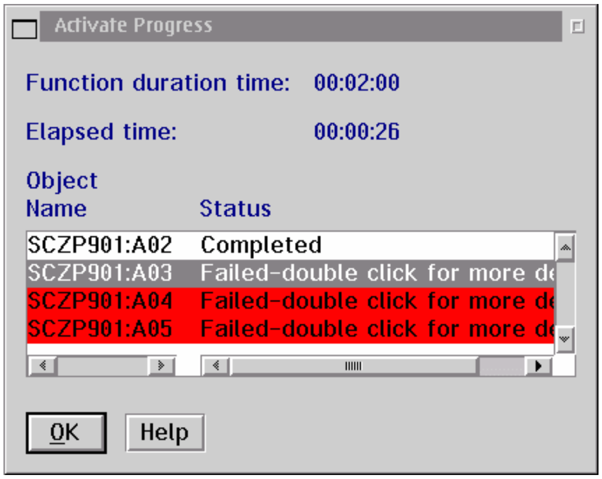
6. When you have completed the PCI Crypto definitions for the partition, click **Save**. This brings you back to the Customize/Delete Activation Profiles List shown in Figure 5 on page 8.

Repeat step 4 through step 6 for each logical partition that needs to be customized for PCICA or PCIXCC operation.

Important: A power-on Reset is not necessary, but the new definitions entered in the partition image profile will not take effect until the next time the partition is activated.

Logical partition activation

If more than one combination of Usage domain Index and PCI Cryptographic Candidate List value(s) is being used, the conflict will only be detected when a partition is activated while another active partition already owns the same combination value. An error message will be issued at the time the partition is activated. This is illustrated in the example shown in Figure 10. In this example, partitions A02, A03, A04, and A05 have conflicting cryptographic definitions. When activation is requested, logical partition A02 activation processes normally. However, activation for logical partitions A03, A04, and A05 fails.


Activate Progress

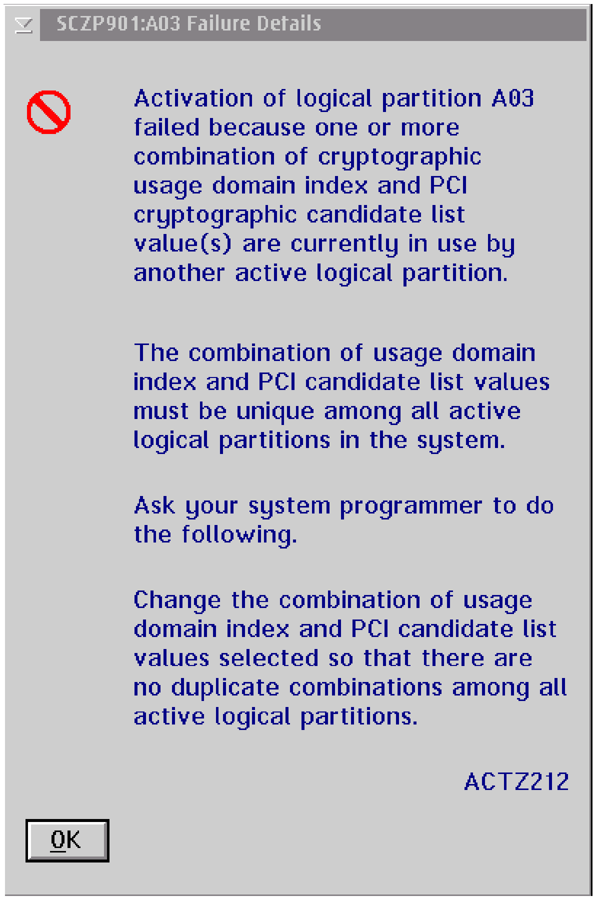
Function duration time: 00:02:00

Elapsed time: 00:00:26

Object Name	Status
SCZP901:A02	Completed
SCZP901:A03	Failed-double click for more de
SCZP901:A04	Failed-double click for more de
SCZP901:A05	Failed-double click for more de

Figure 10 Activate Progress Status

Double-clicking on the message displays the Failure Details window shown in Figure 11 on page 13.



SCZP901:A03 Failure Details

Activation of logical partition A03 failed because one or more combination of cryptographic usage domain index and PCI cryptographic candidate list value(s) are currently in use by another active logical partition.

The combination of usage domain index and PCI candidate list values must be unique among all active logical partitions in the system.

Ask your system programmer to do the following.

Change the combination of usage domain index and PCI candidate list values selected so that there are no duplicate combinations among all active logical partitions.

ACTZ212

Figure 11 Activation Failure details

Log off SE/HMC session

When cryptographic definitions are complete, log off the SE and HMC, as described in the following section.

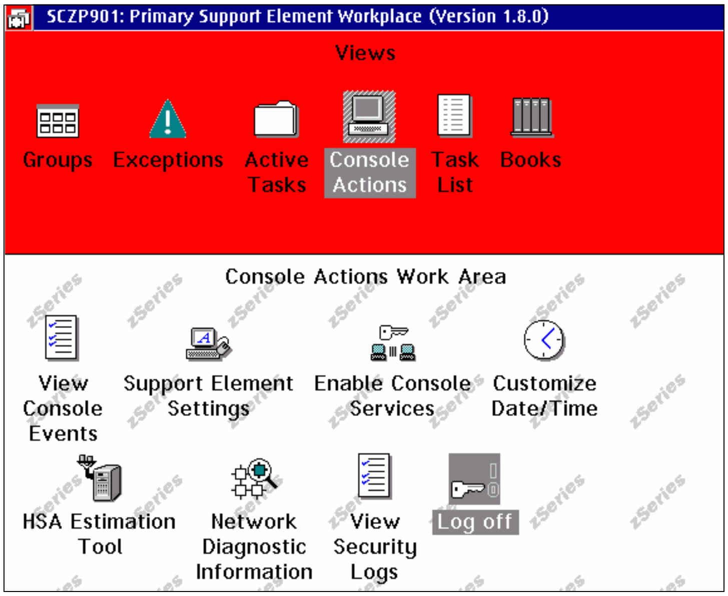


Figure 12 Logoff Support Element

First, log off from the Support Element session.

1. Double-click **Console Actions** (refer to Figure 12 on page 13.)
2. Point to the **Logoff** task and double-click.

Then, log off from the HMC session.

1. In the Views Area, double-click **Console Actions**.
2. Point to the **Logoff** task and double-click.

Configuration using the z990 Support Element

Reconfiguration of a cryptographic coprocessor to a logical partition can be done from the z990 Support Element Workplace.

The ICSF Coprocessor Management panel provides a way to display the status and activate or deactivate a coprocessor; refer to “Activation/Deactivation using ICSF” on page 22.

Important: There is no z/OS command available to display the status or configure On/Off PCICA or PCI X Cryptographic Coprocessors.

From the Support Element, you can display PCI Cryptographic Configuration, view the LPAR cryptographic controls (domain index and Candidate/Online lists for currently active partitions), or configure On/Off a cryptographic coprocessor to a logical partition. These tasks require you to work from the SE Workplace; they are not available from the HMC.

To get the appropriate SE window, log on to the SE directly or via the HMC single object operations task; refer to “Start an HMC session” on page 5.

PCI Cryptographic Management

From the Support Element Workplace:

1. From the Views area, open **Groups** and select the **CPC** object.
2. In the Task List Work Area, rotate to locate the CPC Configuration and locate the PCI Cryptographic Management task; refer to Figure 13.
3. Double-click the PCI Cryptographic Management icon to activate the task.

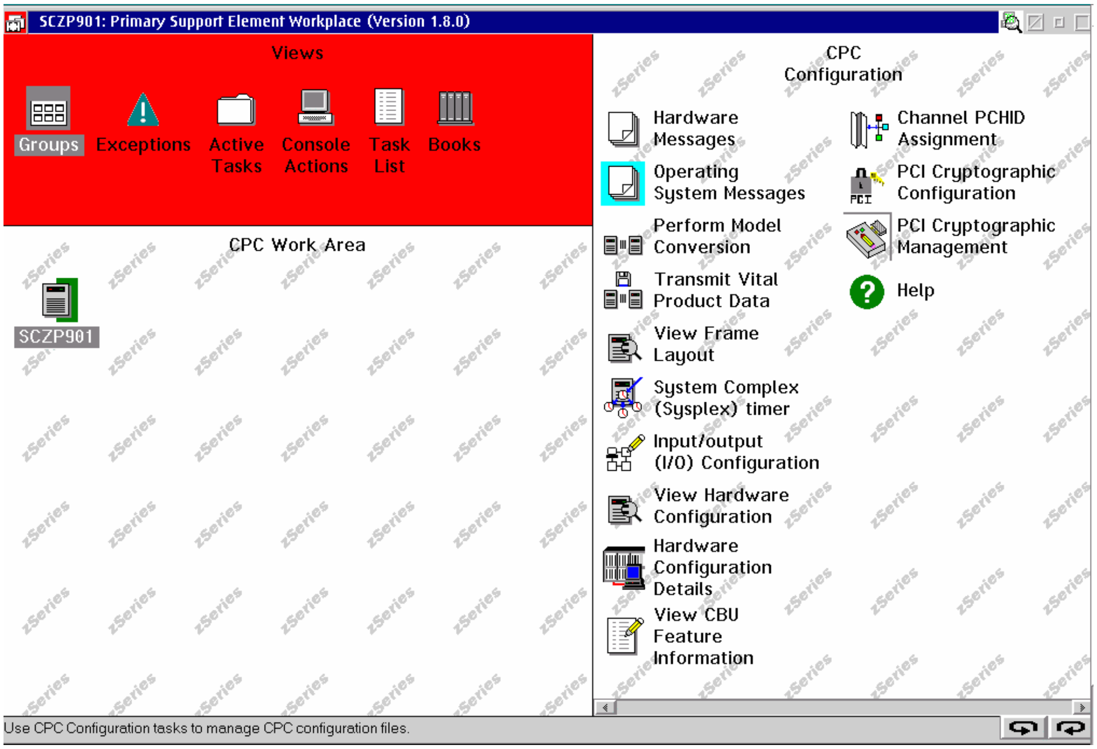
This brings up the PCI Cryptographic Management window shown in Figure 14 on page 16. Use this window to display the installed cryptographic configuration:

- View installed cryptographic features, with current status and assigned PCHID and coprocessor number(s). Each coprocessor in a PCIXCC or PCICA feature is assigned a coprocessor number, in the range 0 to 15, as part of the configuration process. The assignment is made when the feature is installed.

- View coprocessor number(s) that still retain assignment to removed cryptographic features.
- Initiate the release of coprocessor number(s). The relationship should be removed only when a PCI cryptographic feature is permanently removed from the CPC.

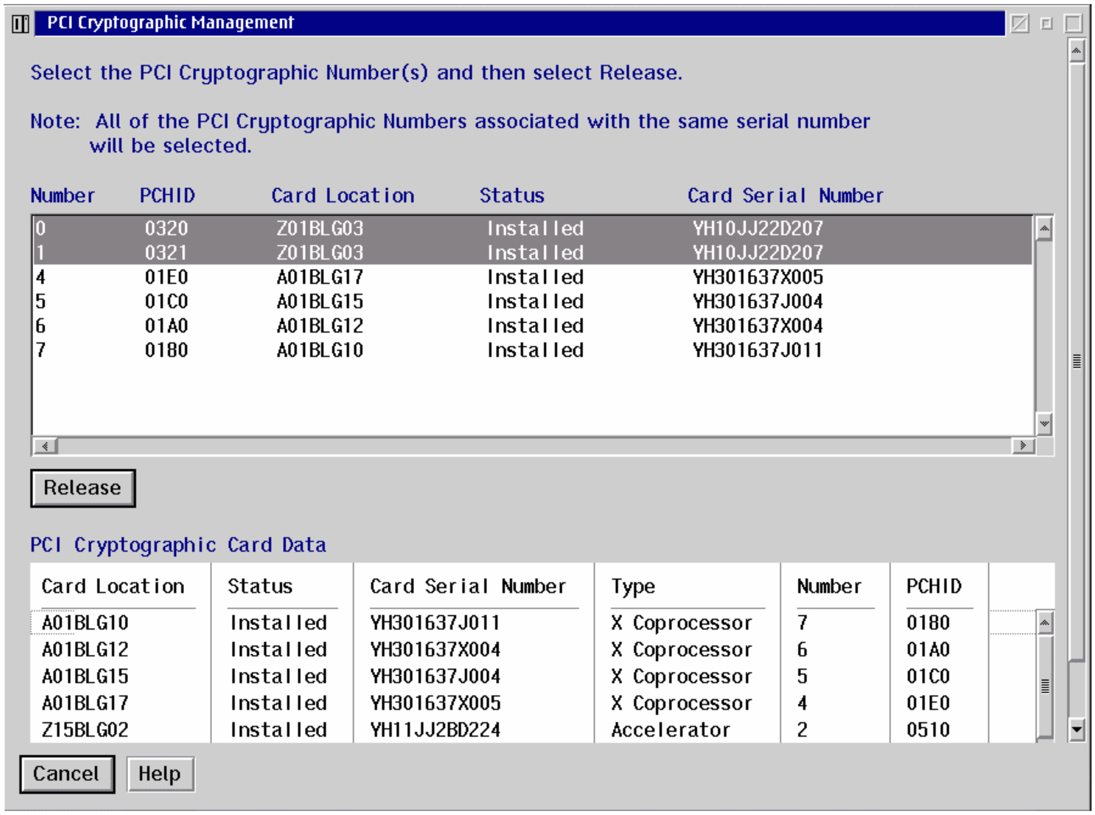
  The release option removes the relationship between a PCI cryptographic feature serial number and the assigned coprocessor number(s). Removing the relationship allows the coprocessor number(s) to be freed, and make it available to be assigned to a new feature serial number.

> **Important:** The coprocessor number is assigned to the feature serial number, *not* to the installed location. If a feature is removed from one location to be reinstalled in another, the coprocessor number(s) assignment remains.


SCZP901: Primary Support Element Workplace (Version 1.8.0)
Views
Groups
Exceptions
Active Tasks
Console Actions
Task List
Books
CPC Work Area
SCZP901
CPC Configuration
Hardware Messages
Operating System Messages
Perform Model Conversion
Transmit Vital Product Data
View Frame Layout
System Complex (Sysplex) timer
Input/output (I/O) Configuration
View Hardware Configuration
Hardware Configuration Details
View CBU Feature Information
Channel PCHID Assignment
PCI Cryptographic Configuration
PCI Cryptographic Management
Help

Use CPC Configuration tasks to manage CPC configuration files.

Figure 13 CPC Work Area - CPC Configuration



Select the PCI Cryptographic Number(s) and then select Release.

Note: All of the PCI Cryptographic Numbers associated with the same serial number will be selected.

Number	PCHID	Card Location	Status	Card Serial Number
0	0320	Z01BLG03	Installed	YH10JJ22D207
1	0321	Z01BLG03	Installed	YH10JJ22D207
4	01E0	A01BLG17	Installed	YH301637X005
5	01C0	A01BLG15	Installed	YH301637J004
6	01A0	A01BLG12	Installed	YH301637X004
7	0180	A01BLG10	Installed	YH301637J011

PCI Cryptographic Card Data

Card Location	Status	Card Serial Number	Type	Number	PCHID
A01BLG10	Installed	YH301637J011	X Coprocessor	7	0180
A01BLG12	Installed	YH301637X004	X Coprocessor	6	01A0
A01BLG15	Installed	YH301637J004	X Coprocessor	5	01C0
A01BLG17	Installed	YH301637X005	X Coprocessor	4	01E0
Z15BLG02	Installed	YH11JJ2BD224	Accelerator	2	0510

Figure 14 PCI Cryptographic Management

View LPAR Cryptographic Controls

To visualize active partitions cryptographic definitions from the SE Workplace:

1. Open **Groups** from the Views area and select **CPC**. Select the **CPC** object.
2. In the task list workarea, rotate to the CPC Operational Customization Task List; see Figure 15.
3. From the task list, select and double-click **View LPAR Cryptographic Controls**. This brings up the window shown on Figure 16 on page 17.

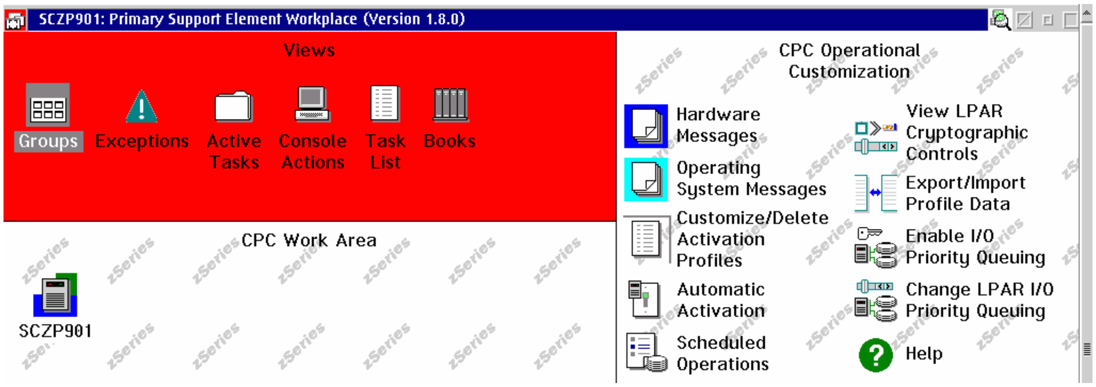
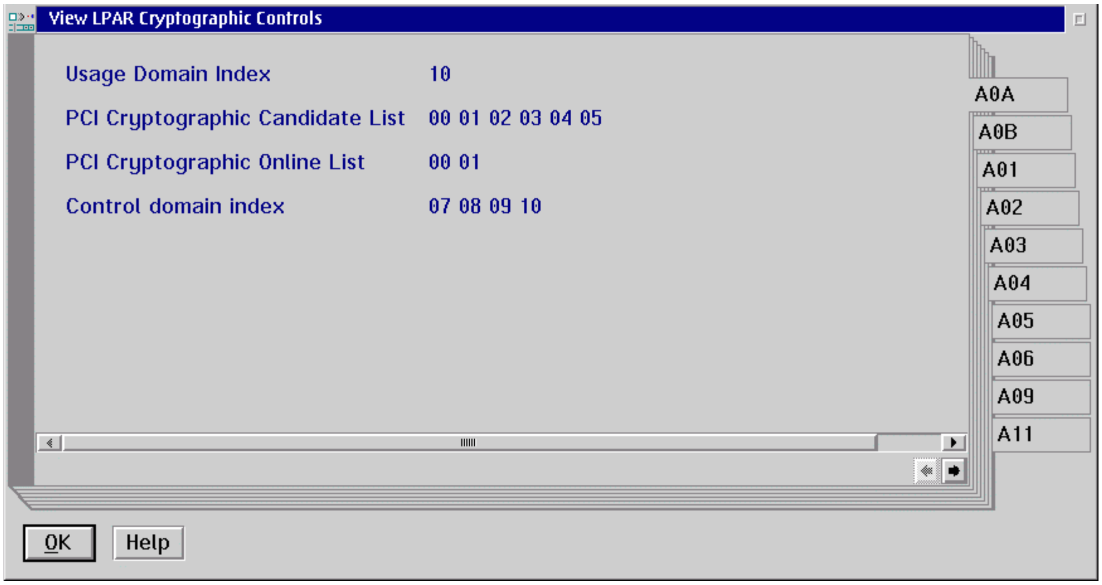

SCZP901: Primary Support Element Workplace (Version 1.8.0)
Views
Groups
Exceptions
Active Tasks
Console Actions
Task List
Books
CPC Work Area
SCZP901
CPC Operational Customization
Hardware Messages
Operating System Messages
Customize/Delete Activation Profiles
Automatic Activation
Scheduled Operations
View LPAR Cryptographic Controls
Export/Import Profile Data
Enable I/O Priority Queuing
Change LPAR I/O Priority Queuing
Help

Figure 15 CPC Operational Customization



Usage Domain Index 10

PCI Cryptographic Candidate List 00 01 02 03 04 05

PCI Cryptographic Online List 00 01

Control domain index 07 08 09 10

Figure 16 View LPAR Cryptographic Controls

The View LPAR Cryptographic Controls window displays the definition of Usage and Control domain indexes, and PCI Cryptographic Candidate and Online lists. Use the tab with the partition name to navigate through the logical partitions. Only active logical partitions are listed.

This display is for information only. You can visualize the definitions, but you cannot change them from this window.

You can modify the cryptographic coprocessor On/Off status using the Configure On/Off task from the Crypto Service Operations task list.

You can apply the Configure On/Off task to the CPC object or to a specific image selected from the Images Work Area.

Config On/Off from the Images Work Area

In this section, we describe the flow using the Images Work Area path. Use this path if you intend to reconfigure only one logical partition image.

From the SE Workplace:

1. In the Task Area, rotate to Crypto Service Operations; refer to Figure 18 on page 19.
2. From Views, select **Groups** -> **Images**.

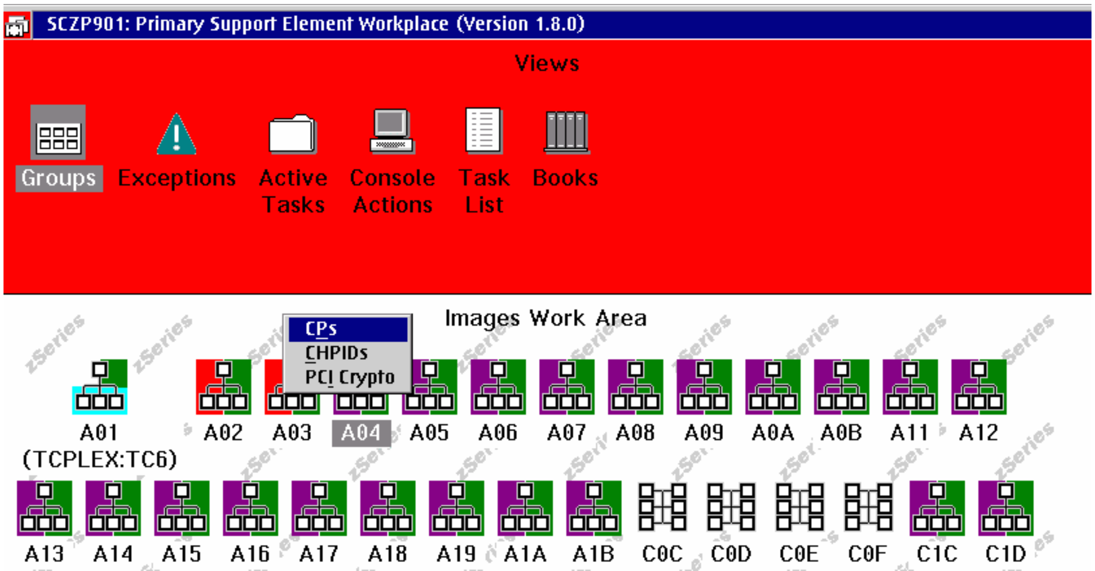


Figure 17 Support Element Workplace - Images Work Area

3. In the Images Work Area, right-click the selected image icon. This brings up the selection menu shown in Figure 17.
4. From the list, select **PCI Crypto**. The PCI Crypto Work Area is displayed; see Figure 18.

Note: When the PCI Crypto Work Area window is accessed from the Images Work Area, the identification displayed below each coprocessor object icon is the cryptographic coprocessor number.

5. From the PCI Crypto Work Area, select the cryptographic coprocessor icon and drag and drop on the Configure On/Off Task. The Configure On/Off window is displayed; see Figure 19 on page 19.

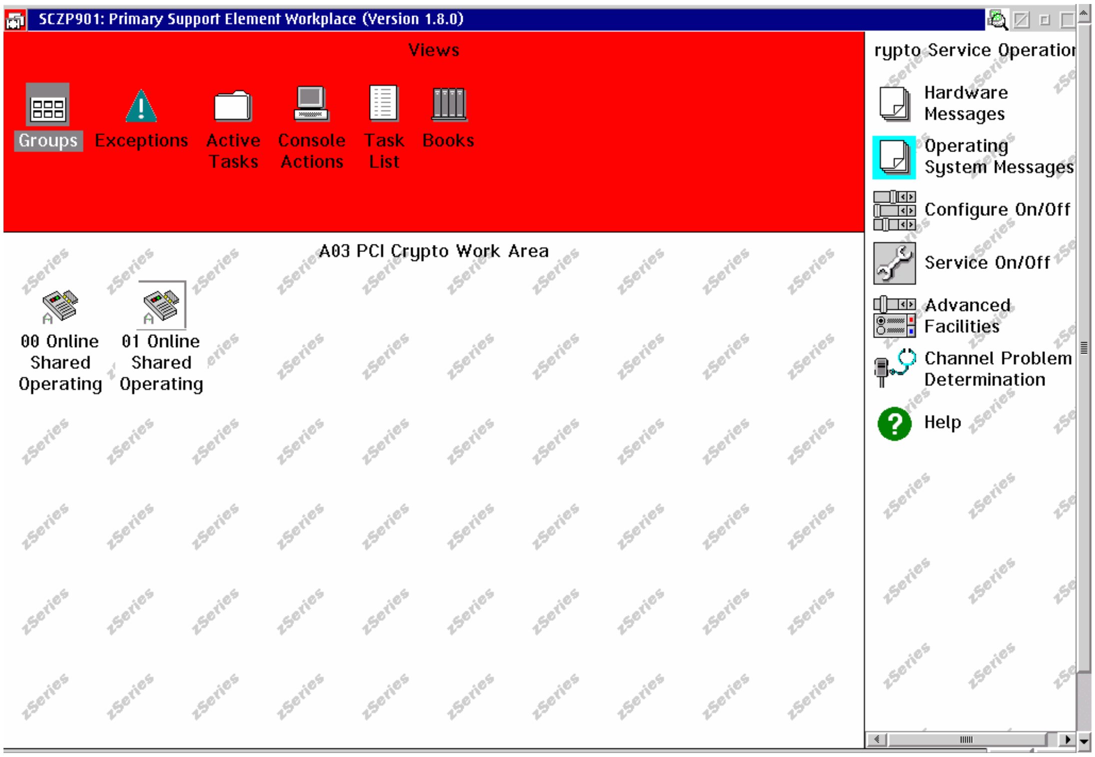
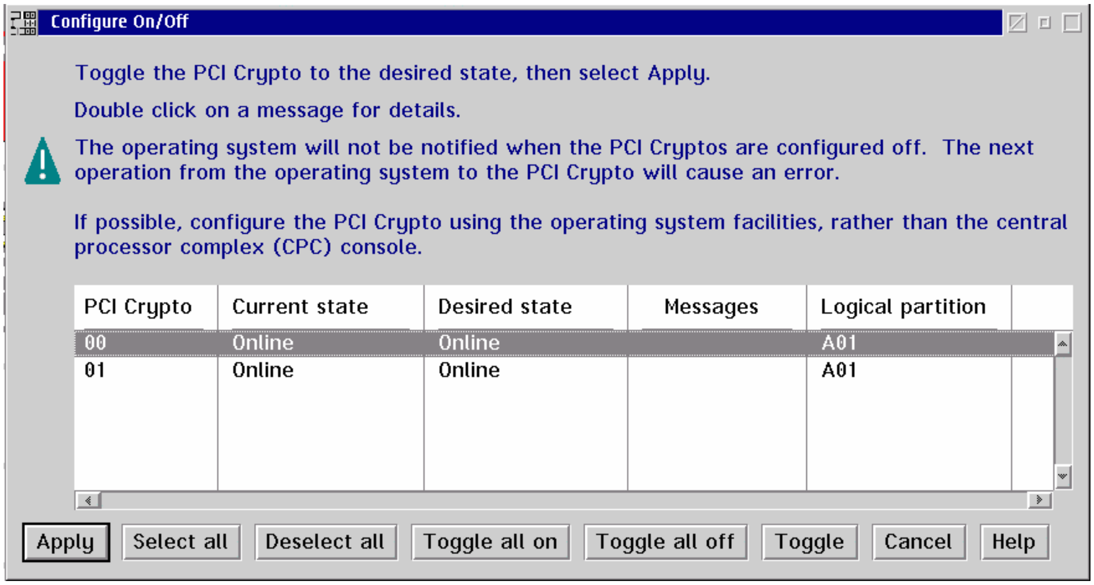


Figure 18 Partition PCI Crypto Work Area



Toggle the PCI Crypto to the desired state, then select Apply.

Double click on a message for details.

The operating system will not be notified when the PCI Cryptos are configured off. The next operation from the operating system to the PCI Crypto will cause an error.

If possible, configure the PCI Crypto using the operating system facilities, rather than the central processor complex (CPC) console.

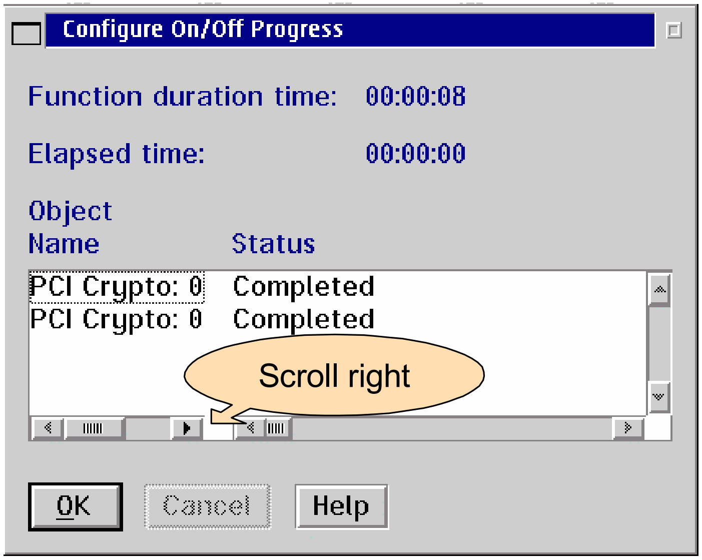
PCI Crypto	Current state	Desired state	Messages	Logical partition
00	Online	Online		A01
01	Online	Online		A01

Figure 19 Support Element Workplace - Configure On/Off

- Select the coprocessor number you want. Use **Toggle** to switch its desired state. Then press **Apply**.

Important: We recommend that you deactivate a coprocessor from the ICSF Coprocessor Management panel before it is configured off from the Support Element. This provides a smooth way to quiesce use of the coprocessor to applications before it is configured off; refer to "Activation/Deactivation using ICSF" on page 22.

A Configure On/Off windows pops up and indicates the progress of the operation, as shown in Figure 20. The visualization of the object name (PCI Crypto identification and partition name) is truncated and you have to scroll to see the full information.



Configure On/Off Progress

Function duration time: 00:00:08

Elapsed time: 00:00:00

Object Name	Status
PCI Crypto: 0	Completed
PCI Crypto: 0	Completed

Figure 20 Support Element Workplace - Configure On/Off Progress

6. When you have completed the reconfiguration, press **Cancel**.
7. Log off the SE and the HMC, as explained in "Log off SE/HMC session" on page 13.

Config On/Off from the CPC Work Area

When using the CPC Work Area, the scope of cryptographic objects displayed will span all defined logical partitions, active or not (but you cannot issue a `Config On/Off` command to a cryptographic coprocessor in an inactive logical partition). Use this path when you want to configure a cryptographic processor across multiple logical partitions.

From the SE Workplace:

1. In the Task Area, rotate to Crypto Service Operations.
2. From Views, select **Groups** -> **CPC**.
3. In the CPC Work Area, right-click the selected CPC icon. This brings up the selection menu shown in Figure 21 on page 21.
4. From the list, select **PCI Crypto**. The PCI Crypto Work Area is displayed, as shown in Figure 22 on page 21.

Note: When the PCI Crypto Work Area window is accessed from the CPC Work Area, the identification displayed below the coprocessor object icon is the PCHID number assigned, not the coprocessor number.

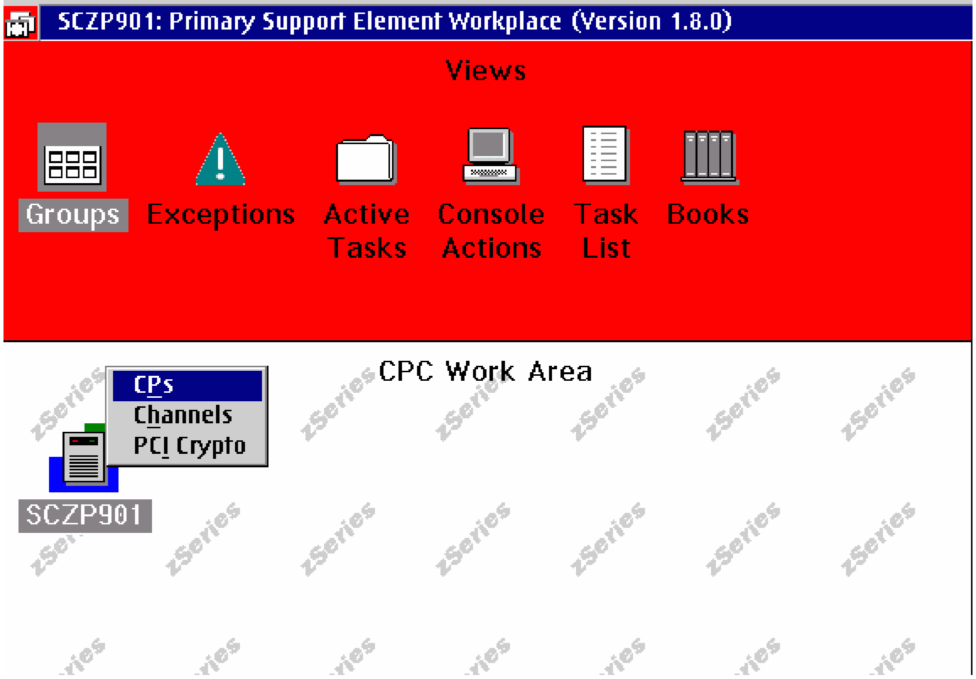


Figure 21 Support Element Workplace - CPC Work Area

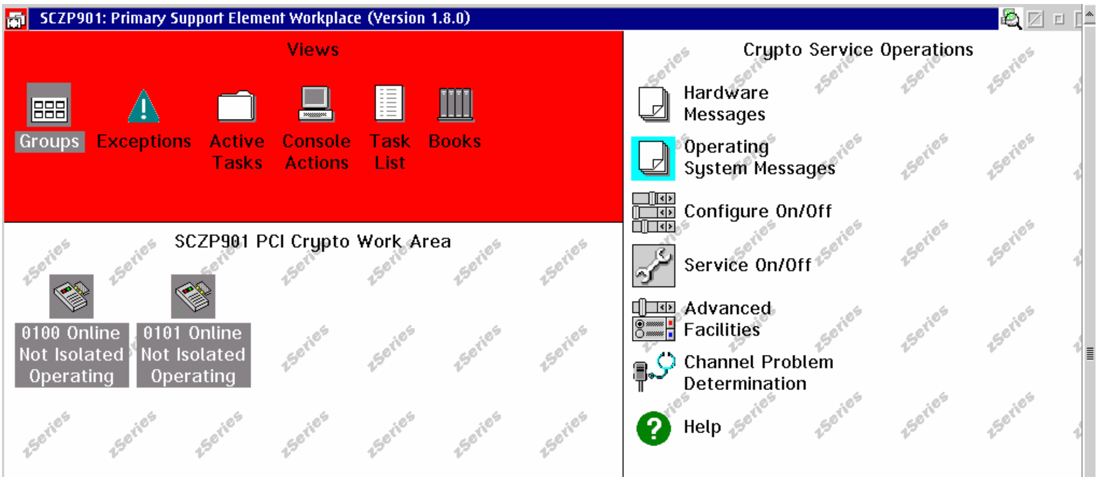
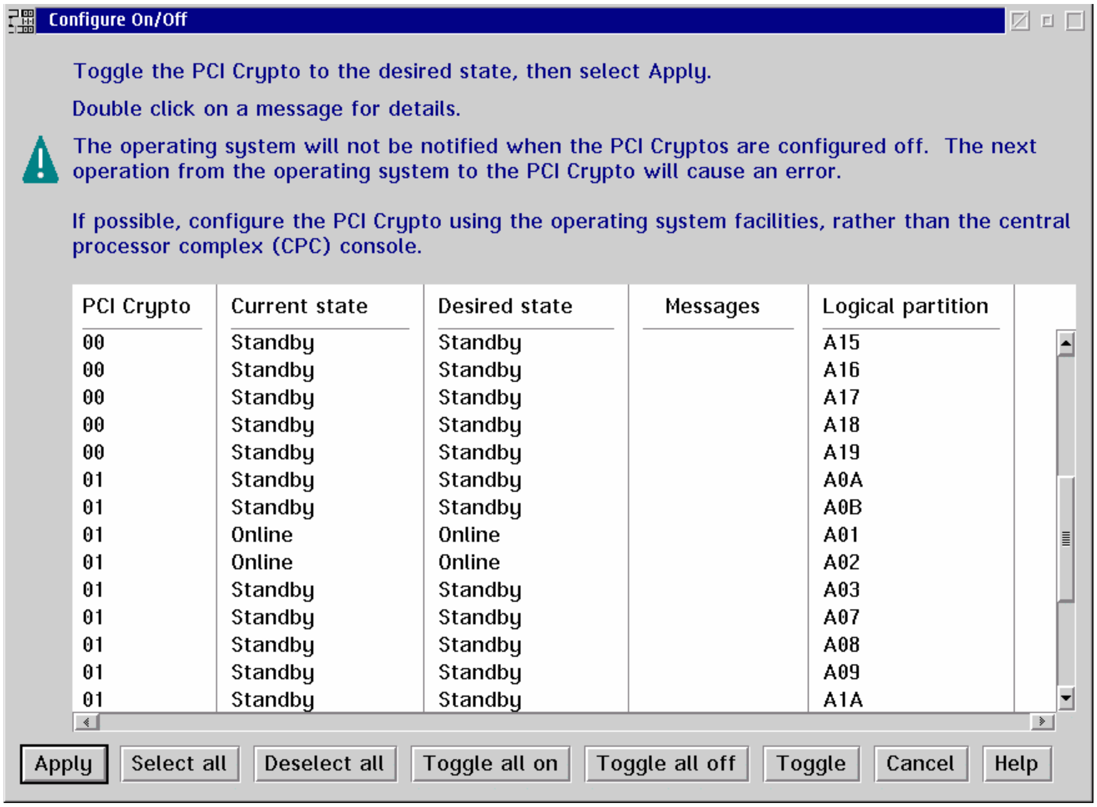

SCZP901: Primary Support Element Workplace (Version 1.8.0)
Views
Groups
Exceptions
Active Tasks
Console Actions
Task List
Books
SCZP901 PCI Crypto Work Area
0100 Online Not Isolated Operating
0101 Online Not Isolated Operating
Crypto Service Operations
Hardware Messages
Operating System Messages
Configure On/Off
Service On/Off
Advanced Facilities
Channel Problem Determination
Help

Figure 22 Support Element Workplace - CPC PCI Crypto Work Area

5. From the PCI Crypto Work Area, select the cryptographic coprocessor icon(s) and drag and drop on the Configure On/Off Task. The Configure On/Off window is displayed; see Figure 23 on page 22.

   Since we are now using the CPC object, all partitions that have the cryptographic coprocessor in their Candidate list are listed, whether active or inactive. The list is sorted by PCI Cryptographic Coprocessor number.

   From the list, select the desired coprocessor/partition and use **Toggle** to change the status of the cryptographic coprocessors. Then press **Apply**.



Toggle the PCI Crypto to the desired state, then select Apply.

Double click on a message for details.

The operating system will not be notified when the PCI Cryptos are configured off. The next operation from the operating system to the PCI Crypto will cause an error.

If possible, configure the PCI Crypto using the operating system facilities, rather than the central processor complex (CPC) console.

PCI Crypto	Current state	Desired state	Messages	Logical partition
00	Standby	Standby		A15
00	Standby	Standby		A16
00	Standby	Standby		A17
00	Standby	Standby		A18
00	Standby	Standby		A19
01	Standby	Standby		A0A
01	Standby	Standby		A0B
01	Online	Online		A01
01	Online	Online		A02
01	Standby	Standby		A03
01	Standby	Standby		A07
01	Standby	Standby		A08
01	Standby	Standby		A09
01	Standby	Standby		A1A

Figure 23 Support Element Workplace - Configure On/Off

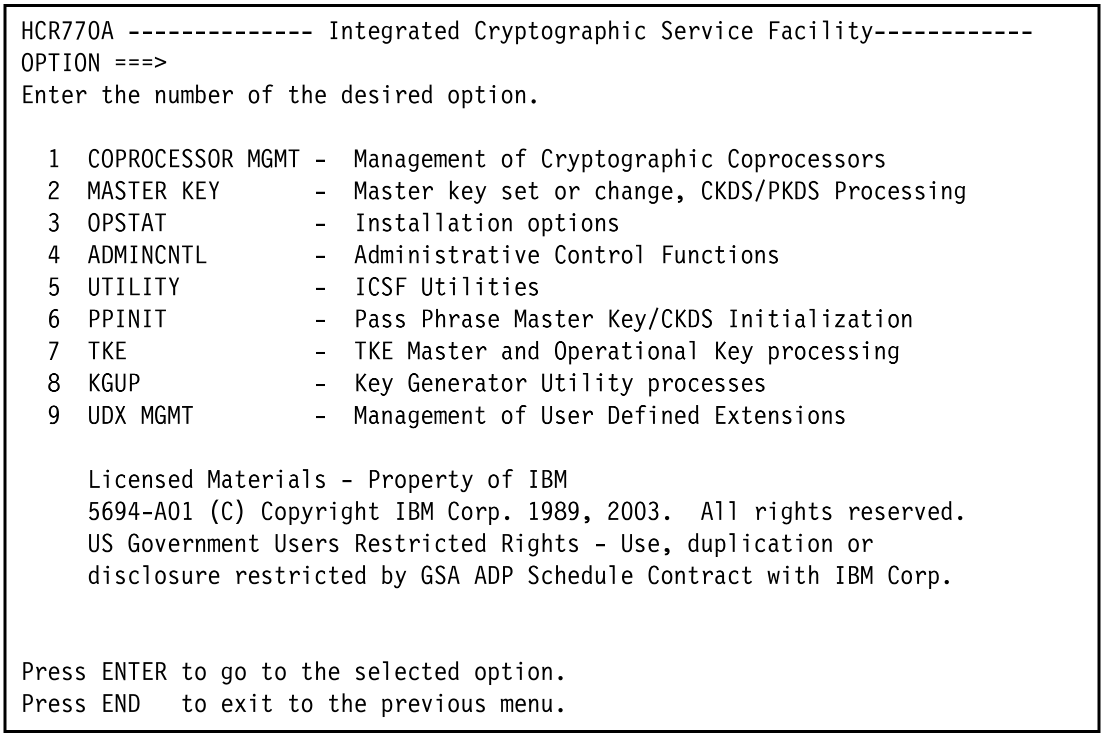
6. When you have completed the reconfiguration, press **Cancel**.
7. Log off the SE and the HMC, as explained in “Log off SE/HMC session” on page 13.

Activation/Deactivation using ICSF

ICSF provides a TSO-ISPF Coprocessor Management panel to display or change the status, Active or Deactivated, of cryptographic coprocessors. This only refers to the coprocessor status to ICSF and has no effect on the Online/Standby hardware status displayed on the z990 Support Element.

From the ICSF main menu (Figure 24 on page 23), select **option 1** to display the ICSF Coprocessor Management panel.

Cryptographic coprocessors that are currently configured on to the partition are displayed on the ICSF Coprocessor Management panel; see Figure 25 on page 23.

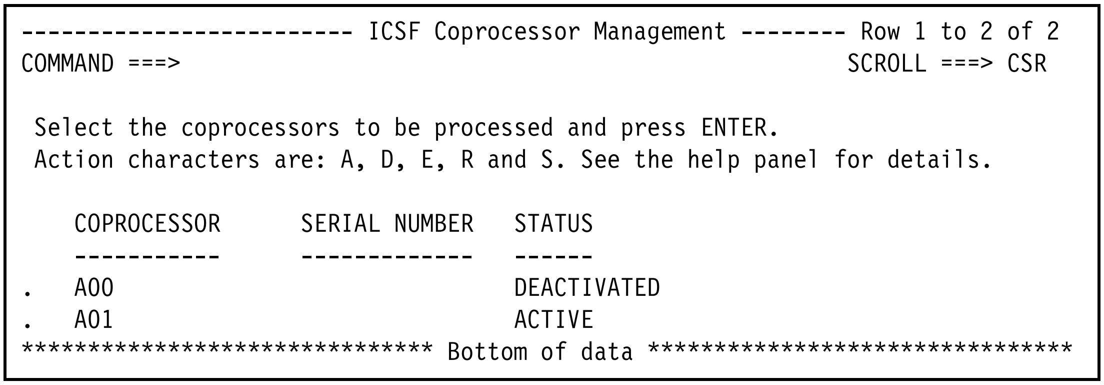


```
HCR770A ------------- Integrated Cryptographic Service Facility-----------
OPTION ===>
Enter the number of the desired option.

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

     Licensed Materials - Property of IBM
     5694-A01 (C) Copyright IBM Corp. 1989, 2003.  All rights reserved.
     US Government Users Restricted Rights - Use, duplication or
     disclosure restricted by GSA ADP Schedule Contract with IBM Corp.


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

Figure 24   Integrated Cryptographic Service Facility Main Panel

In the list, enter action character `A` or `D` to switch a coprocessor status to Active or Deactivated. When a coprocessor is deactivated, it cannot be used by applications.

The Active/Deactivated status set through ICSF Coprocessor Management does not change the Online/Standby status viewed from the z990 Support Element.



```
------------------------- ICSF Coprocessor Management -------- Row 1 to 2 of 2
COMMAND ===>                                                  SCROLL ===> CSR

 Select the coprocessors to be processed and press ENTER.
 Action characters are: A, D, E, R and S. See the help panel for details.

    COPROCESSOR      SERIAL NUMBER   STATUS
    -----------      -------------   ------
.   A00                              DEACTIVATED
.   A01                              ACTIVE
******************************* Bottom of data ********************************
```

Figure 25   ICSF Coprocessor Management

When a coprocessor is configured off to the partition from the SE (Standby status), it is viewed Offline on the ICSF Coprocessor Management panel.

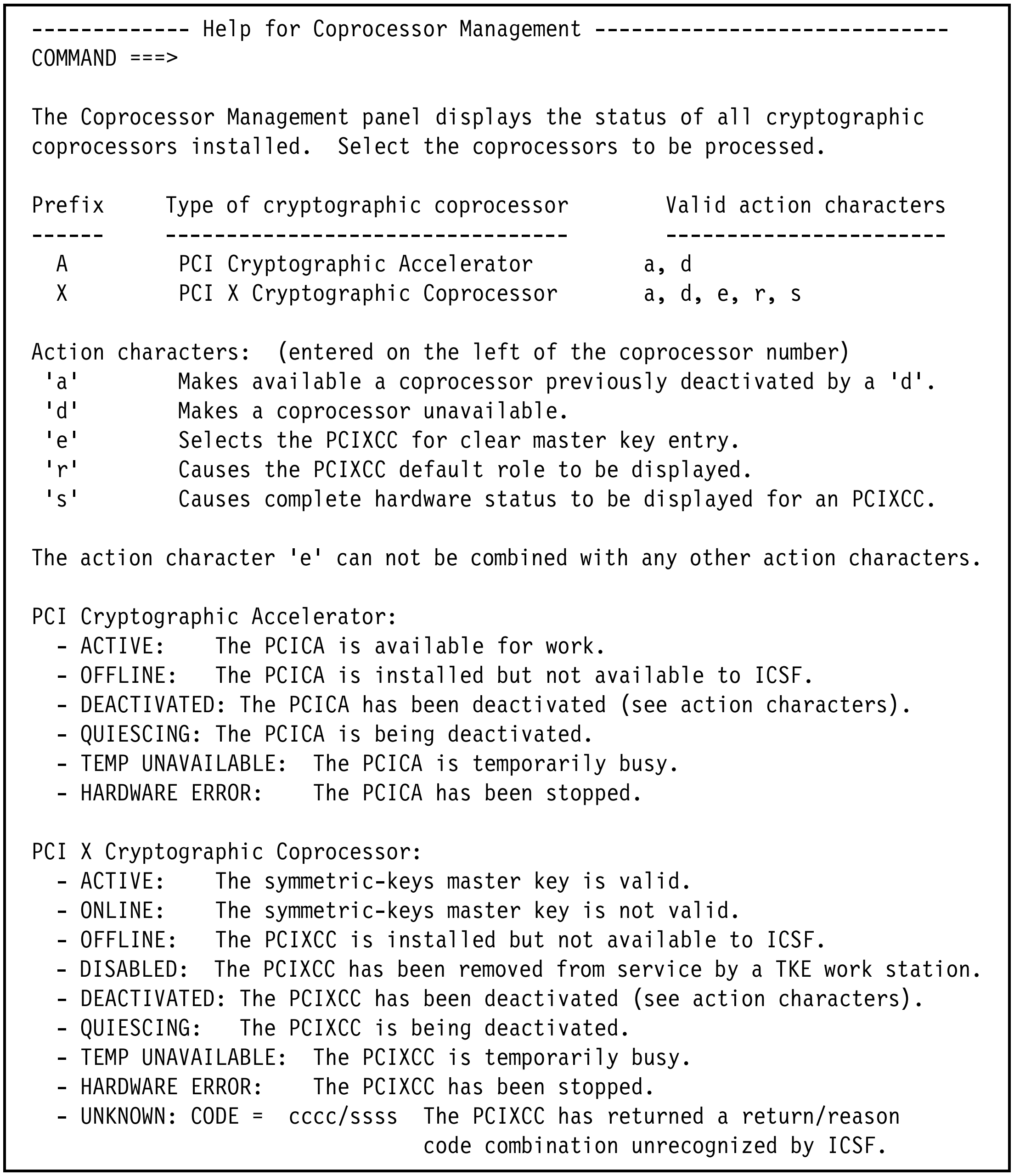
A cryptographic coprocessor becomes visible to ICSF Coprocessor Management when the coprocessor number is part of the partition candidate list *and* the coprocessor is first brought online to the partition

– Either at the time the partition is activated, if the coprocessor is installed and the coprocessor number is part of the partition Online list

– Or when the coprocessor is first configured online to the partition using the Config On/Off task from the SE Workplace

It is recommended to deactivate an *active* coprocessor from the ICSF Coprocessor Management panel before it is configured *off* from the Support Element. If you don't deactivate the coprocessor first before it is configured off from the SE, some jobs may be not rerouted correctly.

Help information for Coprocessor Management, shown in Figure 26, describes valid actions and status displayed for each type of cryptographic coprocessor.



```
------------- Help for Coprocessor Management -----------------------------
COMMAND ===>

The Coprocessor Management panel displays the status of all cryptographic
coprocessors installed.  Select the coprocessors to be processed.

Prefix     Type of cryptographic coprocessor       Valid action characters
------     ---------------------------------       -----------------------
  A         PCI Cryptographic Accelerator         a, d
  X         PCI X Cryptographic Coprocessor       a, d, e, r, s

Action characters:  (entered on the left of the coprocessor number)
 'a'        Makes available a coprocessor previously deactivated by a 'd'.
 'd'        Makes a coprocessor unavailable.
 'e'        Selects the PCIXCC for clear master key entry.
 'r'        Causes the PCIXCC default role to be displayed.
 's'        Causes complete hardware status to be displayed for an PCIXCC.

The action character 'e' can not be combined with any other action characters.

PCI Cryptographic Accelerator:
  - ACTIVE:    The PCICA is available for work.
  - OFFLINE:   The PCICA is installed but not available to ICSF.
  - DEACTIVATED: The PCICA has been deactivated (see action characters).
  - QUIESCING: The PCICA is being deactivated.
  - TEMP UNAVAILABLE:  The PCICA is temporarily busy.
  - HARDWARE ERROR:    The PCICA has been stopped.

PCI X Cryptographic Coprocessor:
  - ACTIVE:    The symmetric-keys master key is valid.
  - ONLINE:    The symmetric-keys master key is not valid.
  - OFFLINE:   The PCIXCC is installed but not available to ICSF.
  - DISABLED:  The PCIXCC has been removed from service by a TKE work station.
  - DEACTIVATED: The PCIXCC has been deactivated (see action characters).
  - QUIESCING:   The PCIXCC is being deactivated.
  - TEMP UNAVAILABLE:  The PCIXCC is temporarily busy.
  - HARDWARE ERROR:    The PCIXCC has been stopped.
  - UNKNOWN: CODE =  cccc/ssss  The PCIXCC has returned a return/reason
                                code combination unrecognized by ICSF.
```

Figure 26 ICSF - Help for Coprocessor Management

Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this Redpaper.

- *z/OS ICSF TKE Workstation User's Guide,* SA22-7524
- *z/OS Integrated Cryptographic Service Facility System Programmer's Guide*, SA22-7520
- *z/OS Integrated Cryptographic Service Facility Messages*, SA22-7523
- *z/OS Integrated Cryptographic Service Facility Administrator's Guide*, SA22-7521

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 give 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.

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.

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.

COPYRIGHT LICENSE:
This information contains sample application programs in source language, which illustrates programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

This document created or updated on September 9, 2003.

Send us your comments in one of the following ways:

- Use the online **Contact us** review redbook form found at:
  ibm.com/redbooks
- Send your comments in an Internet note to:
  redbook@us.ibm.com
- Mail your comments to:
  IBM Corporation, International Technical Support Organization
  Dept. HYJ Mail Station P099
  2455 South Road
  Poughkeepsie, NY 12601-5400 U.S.A.

Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

FICON™
IBM®
z/OS™
Redbooks(logo) ™

The following terms are trademarks of other companies:

Intel, Intel Inside (logos), MMX, and Pentium are trademarks of Intel Corporation in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

SET, SET Secure Electronic Transaction, and the SET Logo are trademarks owned by SET Secure Electronic Transaction LLC.

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