How to setup cryptographic hardware for VSE

VSE in LPAR and under VM

Last formatted on: Friday, December 19, 2008

Joerg Schmidbauer
jschmidb@de.ibm.com

Dept. 3229
VSE Development
IBM Lab Böblingen
Schönaicherstr. 220

D-71032 Böblingen
Germany

Disclaimer

This publication is intended to help VSE system programmers setting up infrastructure for their operating environment. The information contained in this document has not been submitted to any formal IBM test and is distributed AS IS. The information about non-IBM ("vendor") products in this manual has been supplied by the vendor and IBM assumes no responsibility for its accuracy or completeness. The use of this information or the implementation of any of these techniques is a customer responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. While each item may have been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will be obtained elsewhere. Customers attempting to adapt these techniques to their own environments do so at their own risk. Any pointers in this publication to external Web sites are provided for convenience only and do not in any manner serve as an endorsement of these Web sites.

Any performance data contained in this document was determined in a controlled environment, and therefore, the results that may be obtained in other operating environments may vary significantly. Users of this document should verify the applicable data for their specific environment. Reference to PTF numbers that have not been released through the normal distribution process does not imply general availability. The purpose of including these reference numbers is to alert IBM customers to specific information relative to the implementation of the PTF when it becomes available to each customer according to the normal IBM PTF distribution process.

Contents

Changes

Sep 21, 2007 - added disclaimer.
Oct 1, 2007 – added APAR / PTF list
Dec 2008, new functions with z10 and z/VSE 4.2

1 Introduction

This paper describes how access to cryptographic hardware is setup via the Hardware Management Console (HMC) and the Support Element (SE).

Support for cryptographic hardware has been introduced with VSE/ESA 2.7.0 in March 2003 with the PCICA accelerator card. That means RSA operations could be performed via the PCICA card while symmetric algorithms (e.g. DES, TDES, SHA-1, MD5) still had to be executed by the software implementations provided by TCP/IP for VSE/ESA. As a consequence, only the SSL handshaking process and functions like CIALSIGV were hardware accelerated, because only here an RSA operation is performed.

Crypto Express2 and the CPU cryptographic assist feature (CPACF) were then supported by z/VSE 3.1. With the introduction of CPACF also symmetric crypto algorithms were supported by the hardware. In contrast to crypto cards CPACF is not a pluggable adapter card, but is a microcode extension which provides additional processor instructions to perform symmetric crypto functions. So with z/VSE 3.1 onwards the whole SSL process is supported by crypto hardware.

Up to now, z/VSE only supports clear-key cryptography where all kind of keys are stored in the operating system's file system. Cryptographic operations take place in processor main storage, which is of course a possible security leak.

The following hardware and software has been used in the test setup.

- IBM System z9 BC, HMC 2.9.2
- z/VSE 4.1.0 running in an LPAR
- DY46688 / UD53148 for latest crypto service level
- One Crypto Express2 feature assigned to the VSE LPAR
- TCP/IP for VSE/ESA 1.5E as part of z/VSE 4.1 GA version

To show the new functions with z10 and z/VSE 4.2 (Dec 2008), the following setup was used:

- IBM System z10 EC, SE 2.10.1
- z/VSE 4.2.0 running in an LPAR
- Three Crypto Express2 features assigned to the VSE LPAR
- TCP/IP for VSE/ESA 1.5F as part of z/VSE 4.2 GA version

The following section provides an overview of the involved hardware.

2 Hardware Overview

First let's clarify some terms used in this paper:

- A Crypto Express2 *feature* consists of two *cards*, which can be configured in either coprocessor or accelerator mode.
- Older PCI cards like PCIXCC, PCICC, or PCICA were also called *cards.*
- On the HMC panels, cards are called *cryptos*, which is synonym to *crypto device.*
- Each *card* or *crypto device* has a unique *Adjunct Processor* (AP) number or ID, which is used for accessing the card's functionality.

The following sections describe if and how VSE uses the various crypto cards.

2.1 PCICC

The IBM PCI Cryptographic Coprocessor (PCICC) was the first PCI crypto card available for zSeries processors. A PCICC is tolerated since VSE/ESA 2.7, but has never been exploited.

2.2 PCICA

The IBM PCI Cryptographic Accelerator card (PCICA), is supported from VSE/ESA 2.7 onwards to process 512-bit and 1024-bit RSA operations. The card cannot handle 512-bit requests, but TCP/IP uses the 1024-bit format also for 512-bit requests. Although the card can handle 2048-bit requests, this is not exploited by TCP/IP until today. The PCICA is much faster than the PCICC performing RSA operations. A PCICA cannot be plugged into a z9 or z10. You can find more information about the PCICA on

http://www.ibm.com/security/cryptocards/pcica.shtml

2.3 PCIXCC

The PCIX Cryptographic Coprocessor (PCIXCC) feature (#0868) came with the z990 processor. A corresponding “PCIXCA” card was never manufactured. Instead, the Crypto Express2 accelerator mode is the successor of the PCICA card. The PCIXCC is supported with z/VSE 4.1.0 onwards for processing RSA requests with key lengths 512, 1024, and 2048. There is no PTF for z/VSE 3.1.

2.4 Crypto Express2

A Crypto Express2 feature consists of two cards, which can be configured either as coprocessor (CEX2C) or accelerator (CEX2A).

The coprocessor mode can perform many more functions than just RSA: secret-key encryption and decryption support of system master keys, PIN functions, etc. On z/OS many banking applications use CEX2C provided functions via the CCA interface. The CEX2C card is supported by z/VSE 3.1.0 onwards.

The accelerator mode is limited to RSA functions and is about 3 times faster than a coprocessor card performing RSA. The CEX2A mode came later than the CEX2C, so VSE support for CEX2A was included on top of z/VSE 3.1.1 with APAR DY46405

Note: a Crypto Express2 feature can also be used in older processors, like the z890 and z990, but the accelerator mode can only be used on a z9 and z10 BC or EC.

The Crypto Express 2 coprocessor is replacing the z990/z890 PCIX Cryptographic Coprocessor (PCIXCC), which itself was providing a replacement for both the PCICC and the Cryptographic Coprocessor Facility (CCF) of the previous zSeries and 9672 systems.

Systems z9 and z10 allow for up to eight Crypto Express2 features (or sixteen cards) to be installed. More information about the Crypto Express2 feature can be found on:

http://www.ibm.com/systems/z/security/cryptography.html

Figure 1 shows the crypto cards supported by z/VSE 4.1.0 and later.

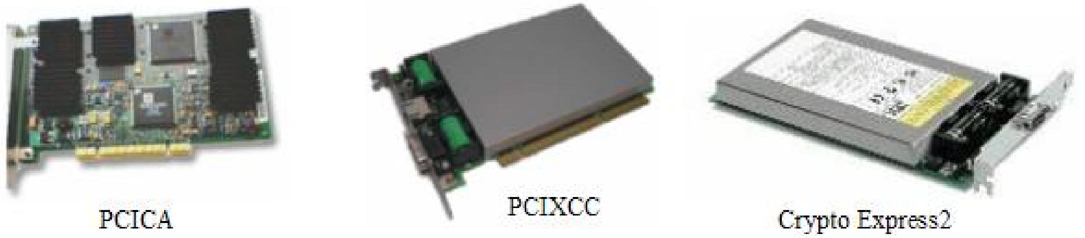


Figure 1: supported crypto cards with z/VSE 4.1.0 and later

2.5 CPACF

CPU Assist for Cryptographic Function (CPACF) is a microcode extension to the processor. It provides additional instructions to perform symmetric algorithms (DES, TDES, and AES) and the SHA hash function with various digest lengths. Also a pseudo random number generator (PRNG) is provided. There is a set of query functions which indicate the availability of particular algorithms dependent on the processor. More information about CPACF can be found on:

http://www.ibm.com/systems/z/security/cryptography.html

The CPACF instructions are described in *the z/Architecture Principles of Operation* manual (chapter 7, General Instructions), which is available online at

http://www.ibm.com/servers/eserver/zseries/zvse/documentation/#vse

Refer to the KM (cipher message) and KMC (cipher message with chaining) instructions.

Note: Feature code #3863 has to be enabled as the prerequisite to use the CPACF functions. The CPACF is enabled using the appropriate “CPACF enablement” diskette. One diskette will enable the CPACF on all the CPUs on each of the nodes in the system.

3 Planning your crypto configuration

On z/OS, coprocessors are exploited for processing specific functions that are only available in coprocessor mode, e.g. PIN verification, RSA key generation etc. On z/VSE, these coprocessor functions are not exploited. z/VSE uses both modes only for processing RSA encryptions and decryptions, which are initiated e.g. during an SSL handshake and by TCP/IP utilities like CIALCREQ and CIALSIGV.

Having one Crypto Express2 feature installed, you would typically configure one AP as coprocessor and one AP as accelerator when running z/OS. When a z/VSE runs on the same machine, you would assign the accelerator card to the VSE LPAR too. On real production systems, Crypto Express2 features are installed in pairs for load balancing and failover reasons, so there would be at least two features installed.

The number of APs is limited to 16 on System z9 and z10. A CEX2C or CEX2A is therefore given an AP number between 0 and 15. Access to an AP is provided through 16 AP queues (cryptographic domains). Each LPAR uses exactly one AP queue in order to send requests to a crypto card.

Figure 2 shows a scenario with several cards getting accessed from different operating systems. The z/OS LPAR has access to APs 1, 2, 3, and 4 via cryptographic domain (AP queue) 0. z/VSE has access to APs 2, 3, 5, and 6 via cryptographic domain 15. This means that z/OS and z/VSE in fact share the crypto devices 2 and 3, but z/OS uses AP queue 0 to enqueue crypto requests to the device while z/VSE uses AP queue 15. The assignment of LPAR3 and LPAR4 is not shown in detail.

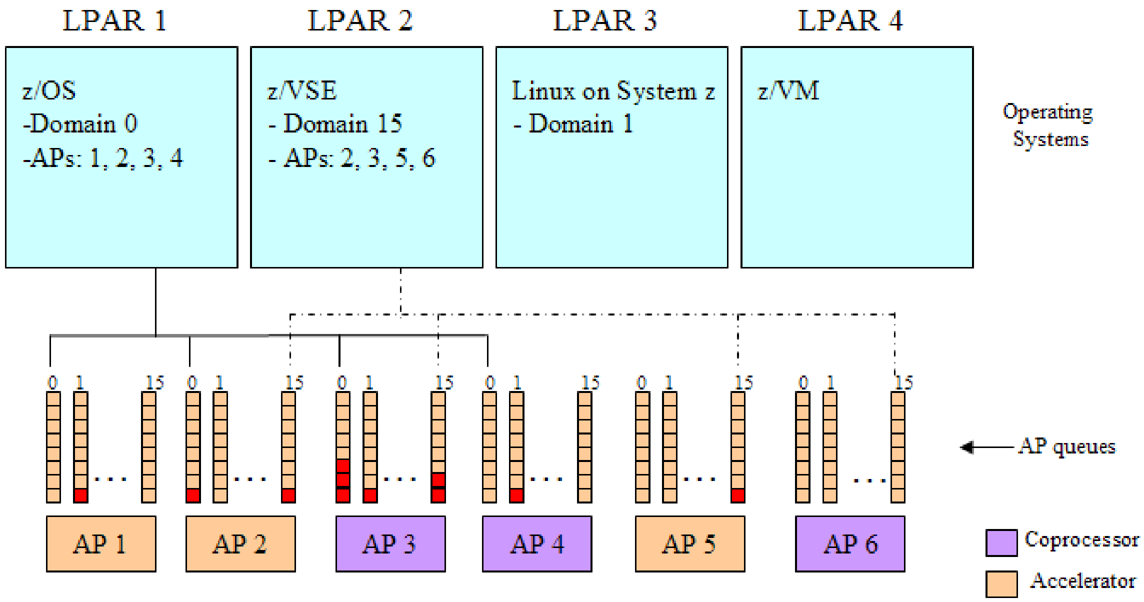


Figure 2: assignment of APs to LPARs

The following chapter shows how to setup access to cryptographic hardware via the Hardware Management Console (HMC) and the Support Element (SE).

4 LPAR cryptographic configuration

Crypto cards and CPACF do not require any hardware configuration in VSE, i.e. they do not have an ADD statement in the IPLPROC and there are no Interactive Interface dialogs to define them. Crypto hardware is sensed during IPL or via operator command and used transparently to applications.

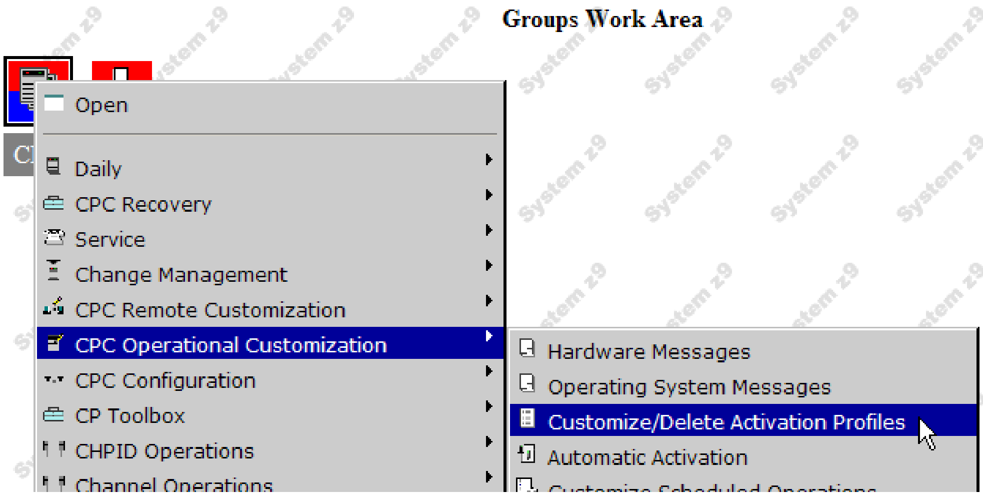
The following sections describe how to view the machine's cryptographic configuration and how to assign crypto devices to a specific LPAR.

4.1 Setting up the cryptographic domain

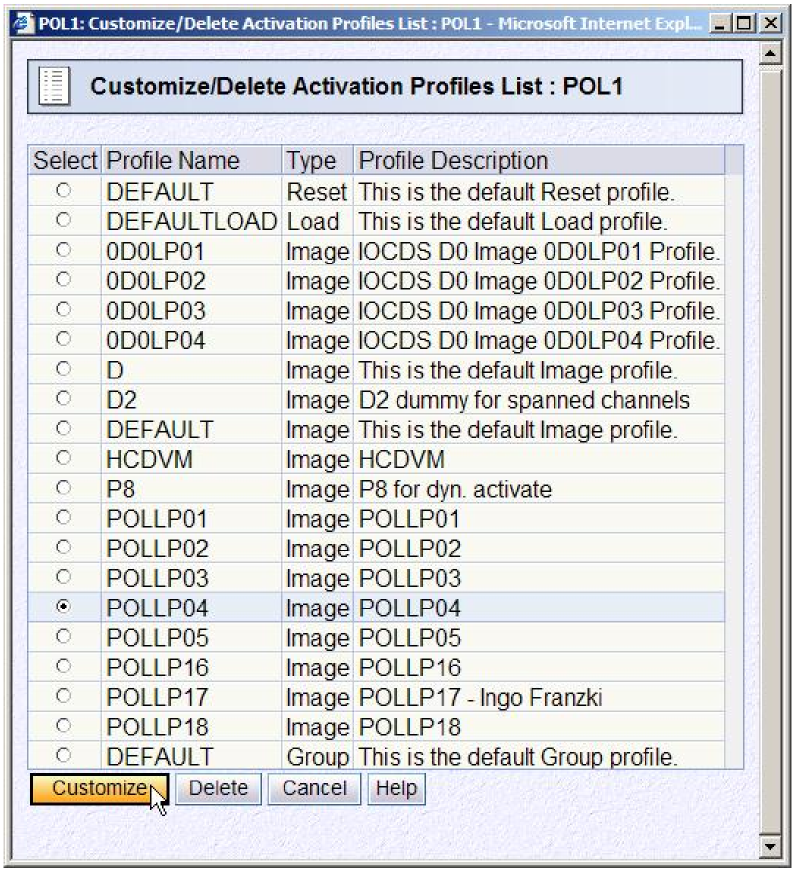
The term *cryptographic domain* is synonym to the term *AP queue* and denotes an input queue provided by a crypto card for receiving requests. Each AP queue can hold up to eight elements until it is full. Setting up the cryptographic domain for an LPAR is the first thing you have to do in order to provide access to crypto cards.

In our first step we get access to the machine's main cryptographic configuration, which is defined in the LPAR activation profile.

After logging on to the Support Element, right-click the CPC icon on the Groups Work Area and select **CPC Operational Customization - Customize/Delete Activation Profiles**.



Select your LPAR and click **Customize**.


POL1: Customize/Delete Activation Profiles List : POL1 - Microsoft Internet Expl...

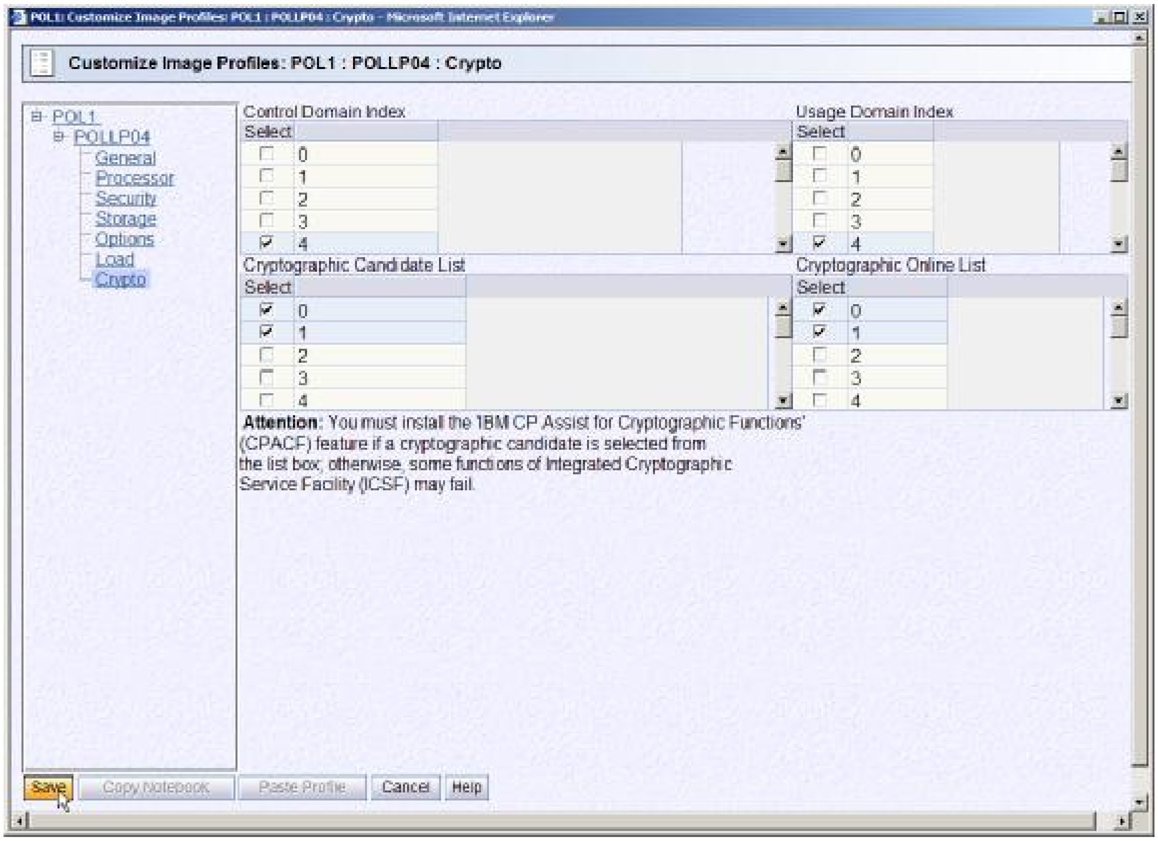
Customize/Delete Activation Profiles List : POL1

Select	Profile Name	Type	Profile Description
○	DEFAULT	Reset	This is the default Reset profile.
○	DEFAULTLOAD	Load	This is the default Load profile.
○	0D0LP01	Image	IOCDS D0 Image 0D0LP01 Profile.
○	0D0LP02	Image	IOCDS D0 Image 0D0LP02 Profile.
○	0D0LP03	Image	IOCDS D0 Image 0D0LP03 Profile.
○	0D0LP04	Image	IOCDS D0 Image 0D0LP04 Profile.
○	D	Image	This is the default Image profile.
○	D2	Image	D2 dummy for spanned channels
○	DEFAULT	Image	This is the default Image profile.
○	HCDVM	Image	HCDVM
○	P8	Image	P8 for dyn. activate
○	POLLP01	Image	POLLP01
○	POLLP02	Image	POLLP02
○	POLLP03	Image	POLLP03
●	POLLP04	Image	POLLP04
○	POLLP05	Image	POLLP05
○	POLLP16	Image	POLLP16
○	POLLP17	Image	POLLP17 - Ingo Franzki
○	POLLP18	Image	POLLP18
○	DEFAULT	Group	This is the default Group profile.

On the next panel select **Crypto**. The following controls are configured here:

Control Domain Index	This identifies the domains that can be administered from this LPAR when it is acting as a TKE host. TKEs are currently not supported by VSE.
Usage Domain Index	The AP queue number which shall be used by this LPAR to access crypto devices.
Cryptographic Candidate List	The AP numbers of the crypto devices that are eligible to be accessed by this LPAR.
Cryptographic Online List	The AP numbers of the crypto devices which are put online at LPAR activation.

In our example, the VSE LPAR has access to crypto devices at AP 0 and AP 1 via AP queue (crypto domain) 4. Both devices are put online at LPAR activation, because they are in the online list.



POL1: Customize Image Profiles: POL1 : POLLP04 : Crypto - Microsoft Internet Explorer

Customize Image Profiles: POL1 : POLLP04 : Crypto

Control Domain Index

Select	
☐	0
☐	1
☐	2
☐	3
☑	4

Usage Domain Index

Select	
☐	0
☐	1
☐	2
☐	3
☑	4

Cryptographic Candidate List

Select	
☑	0
☑	1
☐	2
☐	3
☐	4

Cryptographic Online List

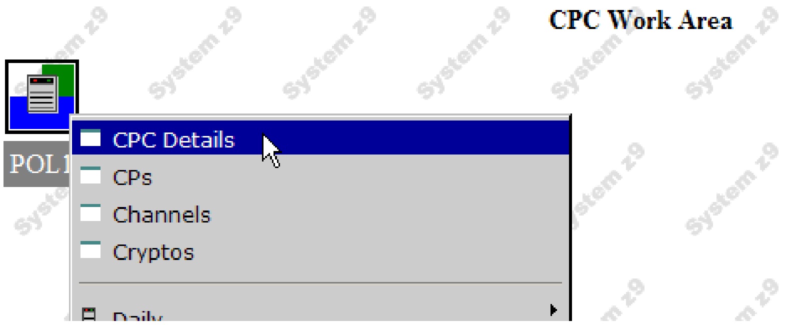
Select	
☑	0
☑	1
☐	2
☐	3
☐	4

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

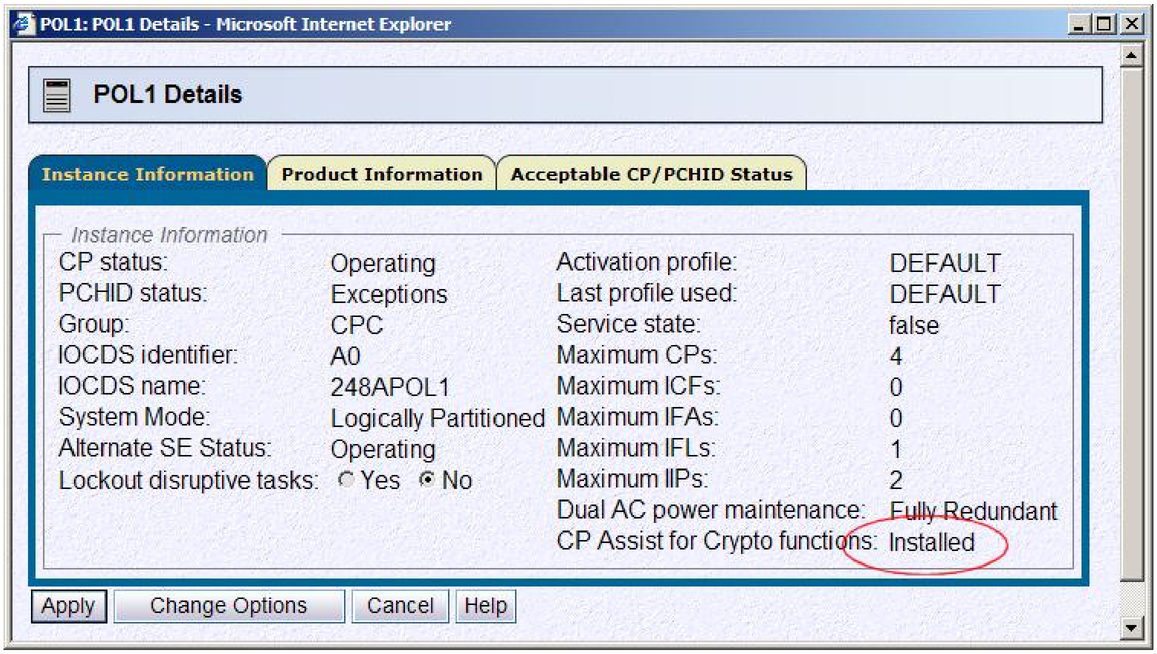
Note: up to a z9 BC or EC you have to restart the LPAR for activating any changes here. The z10 BC and EC processors support dynamic add/remove of crypto devices, refer to chapter 8 on page 23 for details.

4.2 View CPC cryptographic configuration

In our next step we view the cryptographic configuration of the whole machine. On the Primary Support Element Workplace double-click the CPC icon to view its details.



On the CPC details panel you can verify that the CPACF feature is installed.



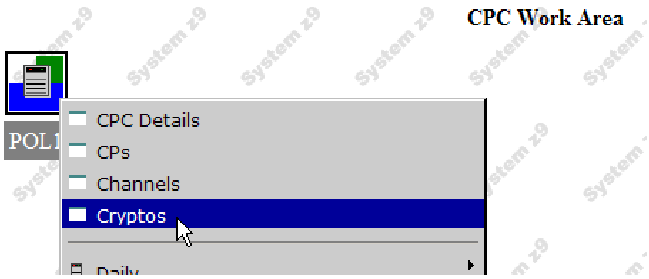
POL1 Details

Instance Information | Product Information | Acceptable CP/PCHID Status

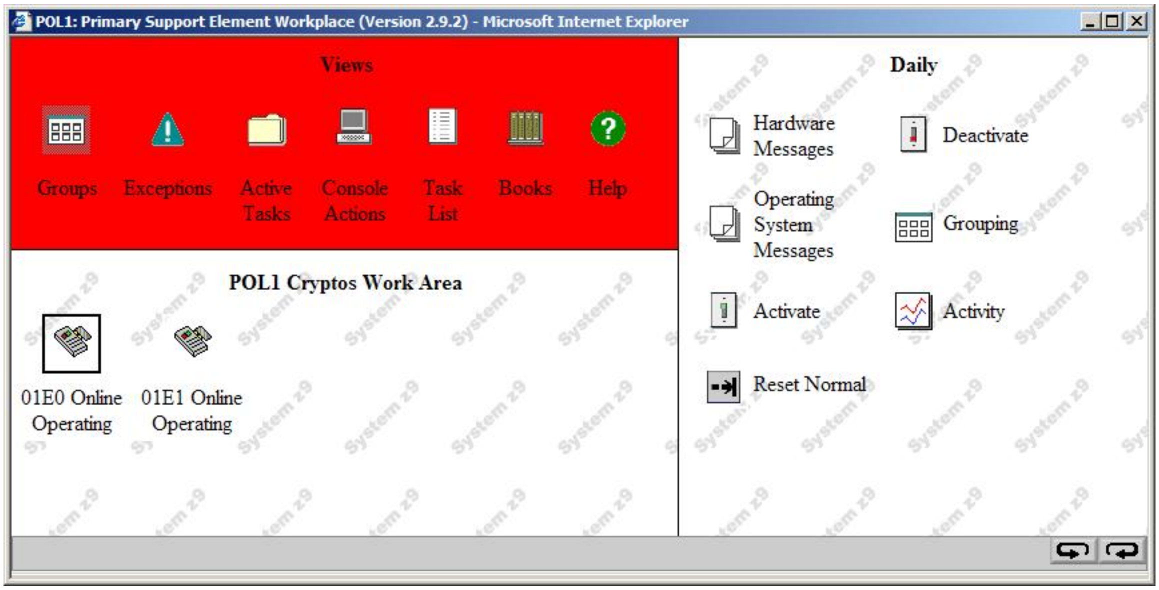
Instance Information

CP status:	Operating	Activation profile:	DEFAULT
PCHID status:	Exceptions	Last profile used:	DEFAULT
Group:	CPC	Service state:	false
IOCDS identifier:	A0	Maximum CPs:	4
IOCDS name:	248APOL1	Maximum ICFs:	0
System Mode:	Logically Partitioned	Maximum IFAs:	0
Alternate SE Status:	Operating	Maximum IFLs:	1
Lockout disruptive tasks:	○ Yes ● No	Maximum IIPs:	2
		Dual AC power maintenance:	Fully Redundant
		CP Assist for Crypto functions:	Installed

Now right-click the CPC icon and select **Cryptos** to display the currently available crypto devices.



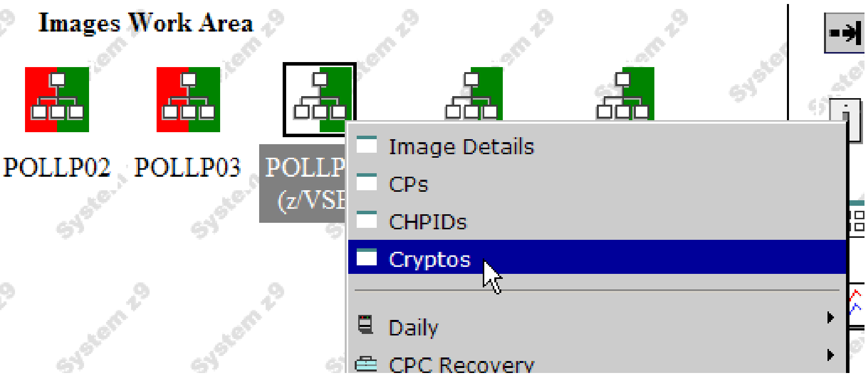
On this machine we have one Crypto Express2 feature with its two APs configured as coprocessors.



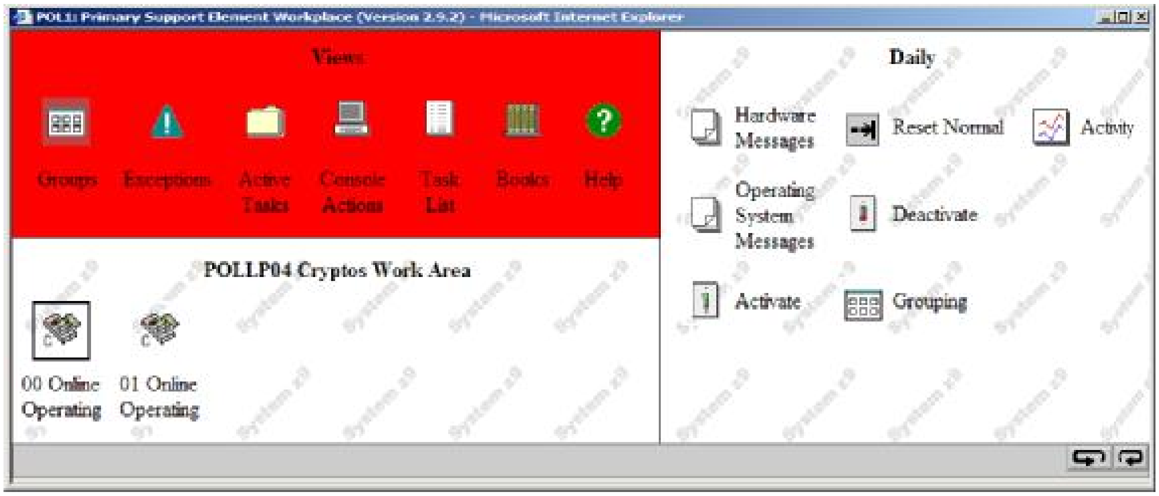
While the above panel shows all crypto cards available on this machine, in the next section we view the crypto cards available from the VSE LPAR.

4.3 View LPAR cryptographic configuration

Right-click the VSE LPAR in the Images Work Area and select **Cryptos**.



The LPAR cryptos work area shows the available crypto devices of this LPAR.



In the next section we will see how VSE senses cryptographic hardware and how crypto related information can be displayed on the operator console.

4.4 The hardware crypto device driver in z/VSE

The VSE crypto device driver runs as a subtask (IJBCRYPT) in the SECSERV job, which runs in partition FB by default as part of the Basic Security Manager. Cryptographic hardware is sensed during IPL when the BSM is initialized. When there are no crypto cards assigned, the device driver finishes processing and the subtask is terminated. When there is at least one usable crypto card available, the device driver keeps running.

Following messages are issued when IPLing VSE with the crypto hardware described in the above sections.

```
FB 0095 1J022I CPU CRYPTOGRAPHIC ASSIST FEATURE AVAILABLE.
FB 0095 1J023I FOUND A CRYPTO EXPRESS2 CARD AT AP 0
FB 0095 1J023I FOUND A CRYPTO EXPRESS2 CARD AT AP 1
FB 0095 1J005I HARDWARE CRYPTO ENVIRONMENT INITIALIZED SUCCESSFULLY.
FB 0095 1J006I USING AP QUEUE 4
```

On a system with CPACF, but no crypto cards, we would get following output.

```
FB 0095 1J022I CPU CRYPTOGRAPHIC ASSIST FEATURE AVAILABLE.
FB 0095 1J017I CRYPTO HARDWARE NOT INSTALLED OR NOT DEFINED.
```

The STATUS command of the SECSERV job can be used to view the device driver status. The below output shows our two coprocessor APs (crypto cards) accessible via AP queue (crypto domain) 4 as configured in section Setting up the cryptographic domain on page 7. As we are running on a z9, CPACF provides the AES algorithm and SHA-256 in addition to DES/TDES, which are available also on older machines.

```
msg fb,data=status=cr
```

```
AR 0015 1I40I  READY
FB 0011 BST223I CURRENT STATUS OF THE SECURITY TRANSACTION SERVER:
FB 0011 ADJUNCT PROCESSOR CRYPTO SUBTASK STATUS:
FB 0011   AP CRYPTO SUBTASK STARTED .......... : YES
FB 0011   MAX REQUEST QUEUE SIZE ............. : 1
FB 0011   MAX PENDING QUEUE SIZE ............. : 1
FB 0011   TOTAL NO. OF AP REQUESTS ........... : 1435
FB 0011   NO. OF POSTED CALLERS .............. : 1435
FB 0011   AP CRYPTO POLLING TIME (1/300 SEC).. : 1
FB 0011   AP CRYPTO TRACE LEVEL .............. : 3
FB 0011   ASSIGNED APS : PCICC / PCICA ....... : 0 / 0
FB 0011                  CEX2C / CEX2A ....... : 2 / 0
FB 0011                  PCIXCC .............. : 0
FB 0011     AP 0 : CEX2C   - ONLINE
FB 0011     AP 1 : CEX2C   - ONLINE
FB 0011   ASSIGNED AP QUEUE (CRYPTO DOMAIN)... : 4
FB 0011 CPU CRYPTOGRAPHIC ASSIST FEATURE:
FB 0011   CPACF AVAILABLE .................... : YES
FB 0011   INSTALLED CPACF FUNCTIONS:
FB 0011     DES, TDES-128, TDES-192
FB 0011     AES-128
FB 0011     SHA-1, SHA-256
FB 0011 END OF CPACF STATUS
```

Other important parameters shown in the above STATUS output are:

- `MAX REQUEST QUEUE SIZE` - the maximum number of RSA requests waiting to be processed by the crypto device driver since its last restart. There can be multiple VSE applications issuing RSA requests simultaneously, even from multiple TCP/IP stacks on the same VSE system. The request queue serializes the requests for processing by the device driver.

- `MAX PENDING QUEUE SIZE` – the maximum number of requests currently being processed by a crypto card. There might be situations where the device driver is under heavy load by incoming new requests so that replies cannot be immediately returned to callers, or a crypto card might be busy so that there is some time interval until a reply can be dequeued.

- `TOTAL NO. OF AP REQUESTS` – the total number of processed RSA requests since the device driver was started.

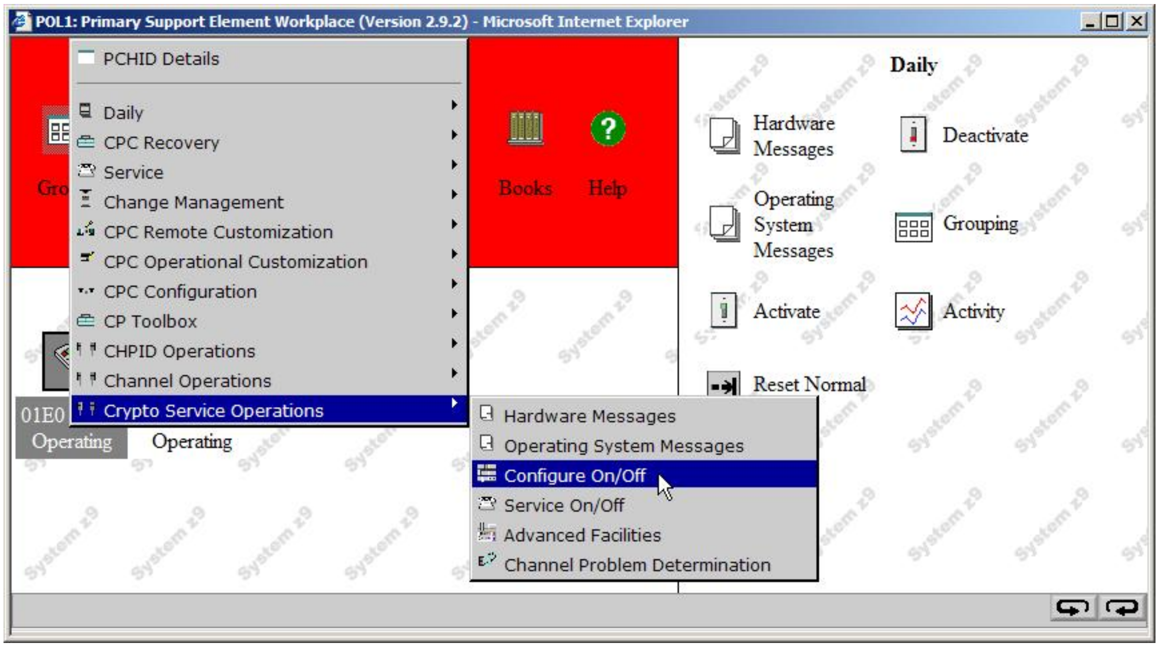
- `NO. OF POSTED CALLERS` – the total number of callers which got back a reply. Normally this value is identical to the above total number of AP requests, except if a reply cannot be delivered, because e.g. the calling application has ended.

- `AP CRYPTO POLLING TIME` – the time interval between enqueuing an RSA request block to a crypto card and the first attempt to dequeue a response. The time interval is specified in 1/300th seconds. The default is 1/300th second. Higher values will decrease CPU load, but increase elapsed job time, lower values will increase CPU load and decrease elapsed job time. See APWAIT command in section VSE Operator commands on page 21 to change this parameter.

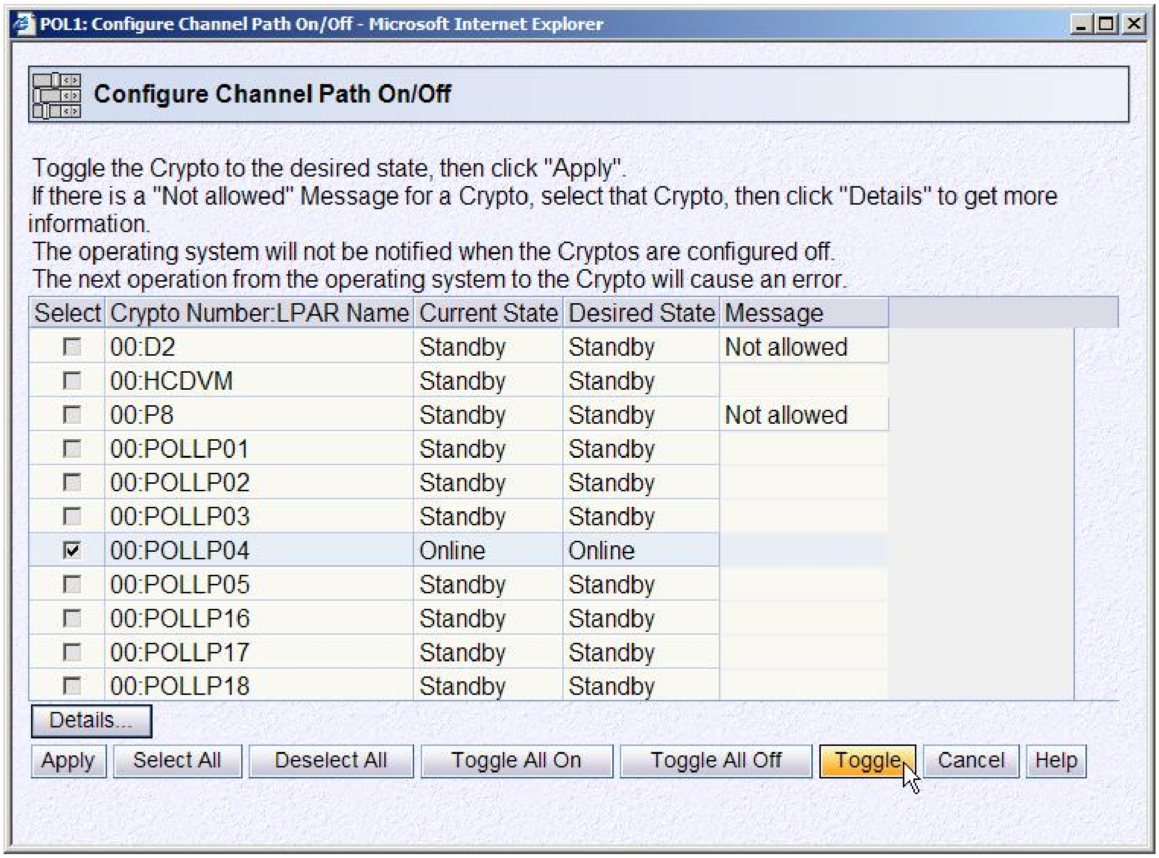
In our next step we will now disable AP number 0.

4.5 Disabling a crypto device

To disable a crypto device, select **Crypto Service Operations** and **Configure On/Off**. This operation will disable the crypto device for this specific LPAR only, i.e. the device might be still online in other LPARs. Therefore the process of enabling or disabling a device is relatively fast, compared to the needed time when activating a device the first time after a machine Power On.



On the **Configure Channel Path On/Off** window select the LPAR for which you want to disable the device, here LPAR4, and press the **Toggle** button.

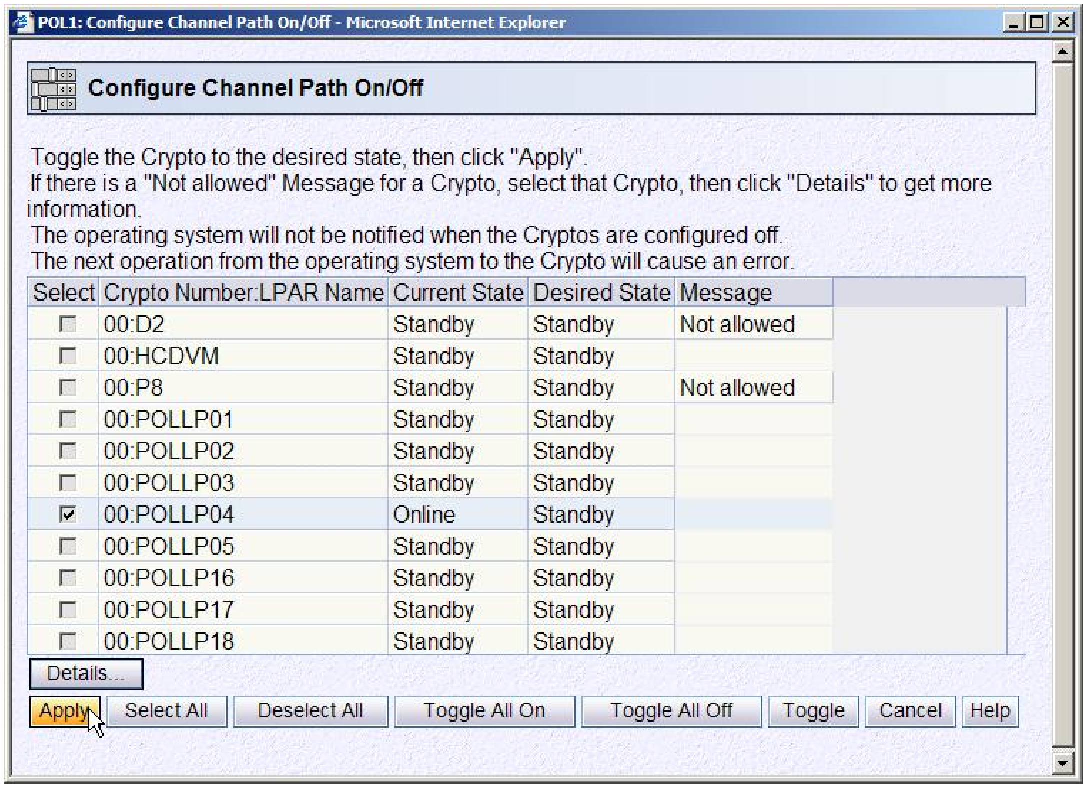


Configure Channel Path On/Off

Toggle the Crypto to the desired state, then click "Apply".
If there is a "Not allowed" Message for a Crypto, select that Crypto, then click "Details" to get more information.
The operating system will not be notified when the Cryptos are configured off.
The next operation from the operating system to the Crypto will cause an error.

Select	Crypto Number:LPAR Name	Current State	Desired State	Message
□	00:D2	Standby	Standby	Not allowed
□	00:HCDVM	Standby	Standby	
□	00:P8	Standby	Standby	Not allowed
□	00:POLLP01	Standby	Standby	
□	00:POLLP02	Standby	Standby	
□	00:POLLP03	Standby	Standby	
☑	00:POLLP04	Online	Online	
□	00:POLLP05	Standby	Standby	
□	00:POLLP16	Standby	Standby	
□	00:POLLP17	Standby	Standby	
□	00:POLLP18	Standby	Standby	

When the desired state has changed to **Standby** click on **Apply**.

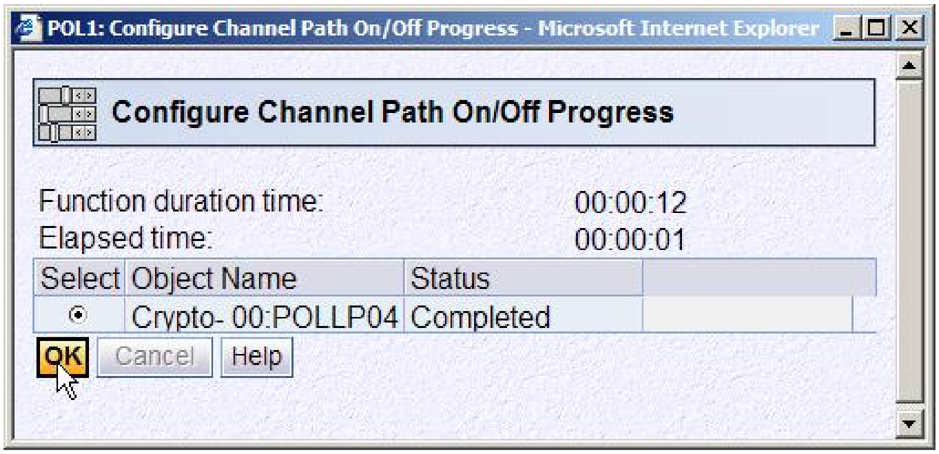


Configure Channel Path On/Off

Toggle the Crypto to the desired state, then click "Apply".
If there is a "Not allowed" Message for a Crypto, select that Crypto, then click "Details" to get more information.
The operating system will not be notified when the Cryptos are configured off.
The next operation from the operating system to the Crypto will cause an error.

Select	Crypto Number:LPAR Name	Current State	Desired State	Message
□	00:D2	Standby	Standby	Not allowed
□	00:HCDVM	Standby	Standby	
□	00:P8	Standby	Standby	Not allowed
□	00:POLLP01	Standby	Standby	
□	00:POLLP02	Standby	Standby	
□	00:POLLP03	Standby	Standby	
☑	00:POLLP04	Online	Standby	
□	00:POLLP05	Standby	Standby	
□	00:POLLP16	Standby	Standby	
□	00:POLLP17	Standby	Standby	
□	00:POLLP18	Standby	Standby	

After the operation has completed, press **OK** to leave the Configure Channel Path window.



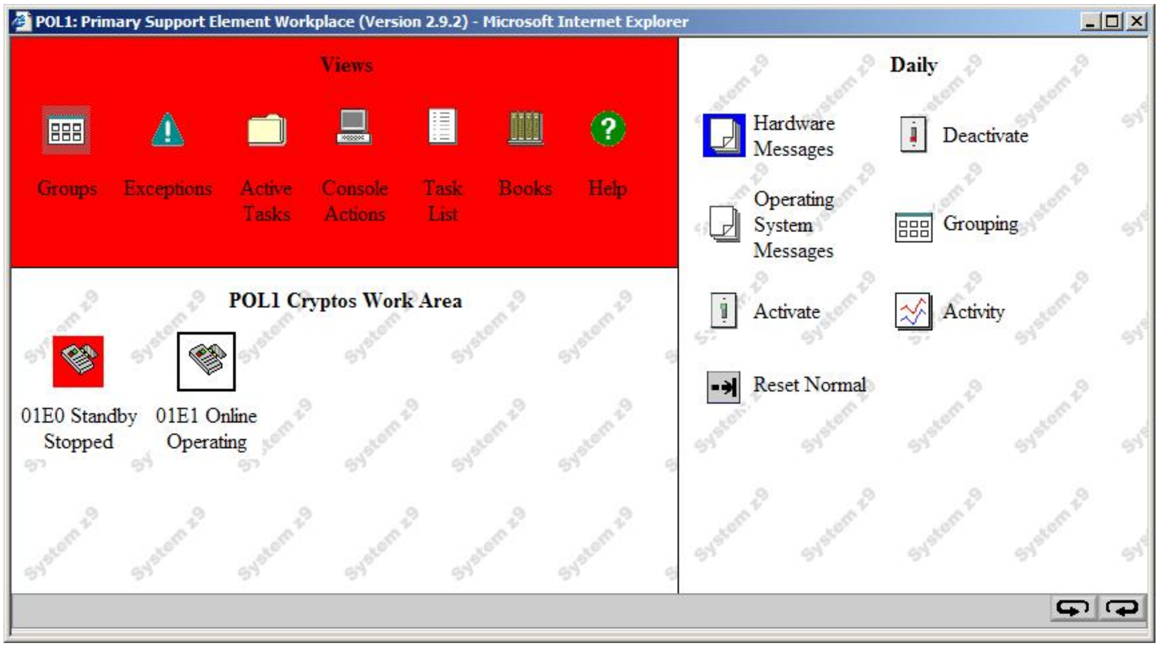
POL1: Configure Channel Path On/Off Progress - Microsoft Internet Explorer

Configure Channel Path On/Off Progress

Function duration time: 00:00:12
Elapsed time: 00:00:01

Select	Object Name	Status
●	Crypto- 00:POLLP04	Completed

The device is now displayed as stopped.



POL1: Primary Support Element Workplace (Version 2.9.2) - Microsoft Internet Explorer

You may now issue the APSENSE command to refresh the crypto configuration in VSE.

```
msg fb,data=apsense
AR 0015 1I40I  READY
FB 0095 1J022I CPU CRYPTOGRAPHIC ASSIST FEATURE AVAILABLE.
FB 0095 1J023I FOUND A CRYPTO EXPRESS2 CARD AT AP 1
FB 0095 1J031I HARDWARE CRYPTO ENVIRONMENT REFRESHED.
```

The STATUS output now shows only one remaining usable AP.

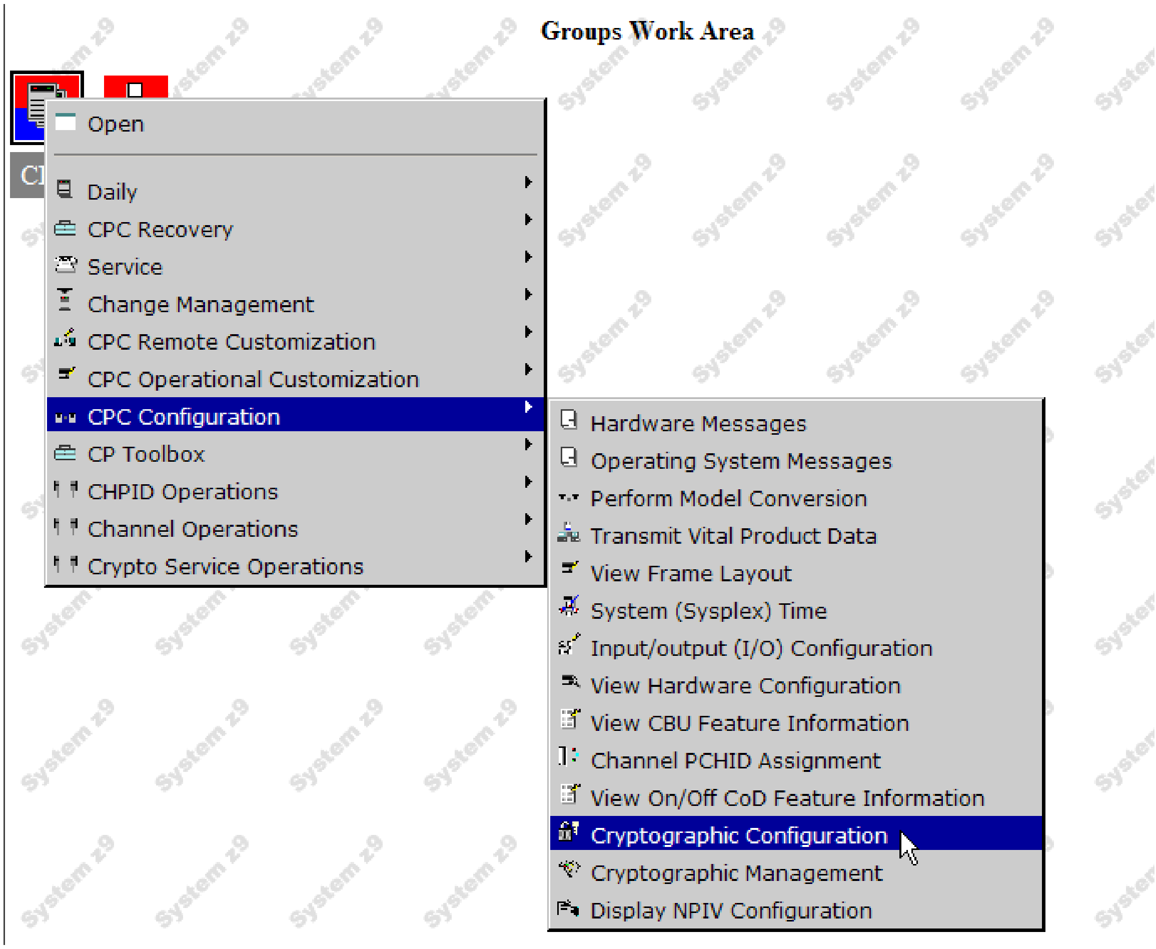
```
msg fb,data=status=cr
…
FB 0011   ASSIGNED APS : PCICC / PCICA ....... : 0 / 0
FB 0011                  CEX2C / CEX2A ....... : 1 / 0
FB 0011                  PCIXCC .............. : 0
FB 0011     AP 1 : CEX2C   - ONLINE
FB 0011   ASSIGNED AP QUEUE (CRYPTO DOMAIN)... : 4
```

In the next section we will reconfigure the stopped coprocessor as accelerator.

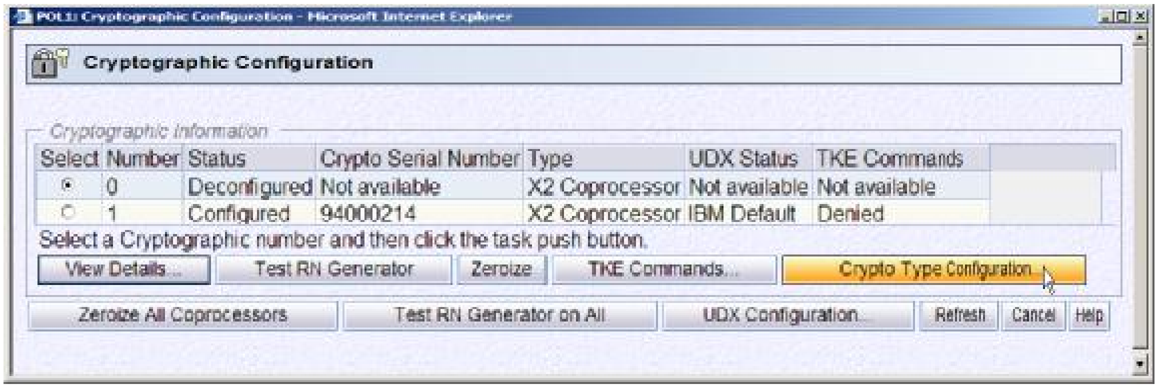
4.6 Reconfiguration as accelerator

Reconfiguring a coprocessor to an accelerator or vice versa requires the device to be first put offline in all LPARs that have access to it, because the mode change affects the physical device itself. In accelerator mode all internal resources of the card are used for making RSA operations faster. You can expect a performance gain of factor 3 with the accelerator mode.

Now let’s change the mode of AP 0 to an accelerator. Double-click **Groups- CPC**. Select the CPC icon. In the **CPC configuration** view on the right select **Cryptographic Configuration**.


Groups Work Area
Open
Daily
CPC Recovery
Service
Change Management
CPC Remote Customization
CPC Operational Customization
CPC Configuration
CP Toolbox
CHPID Operations
Channel Operations
Crypto Service Operations
Hardware Messages
Operating System Messages
Perform Model Conversion
Transmit Vital Product Data
View Frame Layout
System (Sysplex) Time
Input/output (I/O) Configuration
View Hardware Configuration
View CBU Feature Information
Channel PCHID Assignment
View On/Off CoD Feature Information
Cryptographic Configuration
Cryptographic Management
Display NPIV Configuration

Double-click the target Crypto coprocessor and click **Crypto Type Configuration**.



POL1: Cryptographic Configuration - Microsoft Internet Explorer

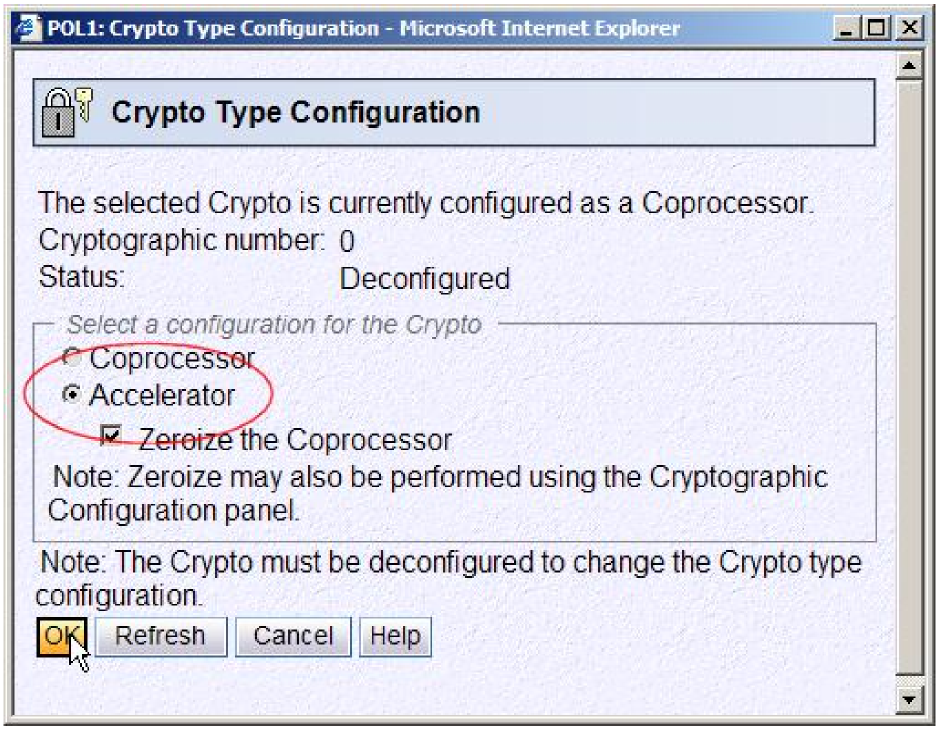
Cryptographic Configuration

Cryptographic Information

Select	Number	Status	Crypto Serial Number	Type	UDX Status	TKE Commands
●	0	Deconfigured	Not available	X2 Coprocessor	Not available	Not available
○	1	Configured	94000214	X2 Coprocessor	IBM Default	Denied

Select a Cryptographic number and then click the task push button.

On the Crypto Type Configuration panel select **Accelerator**.



POL1: Crypto Type Configuration - Microsoft Internet Explorer

Crypto Type Configuration

The selected Crypto is currently configured as a Coprocessor.

Cryptographic number: 0

Status: Deconfigured

Select a configuration for the Crypto

○ Coprocessor

● Accelerator

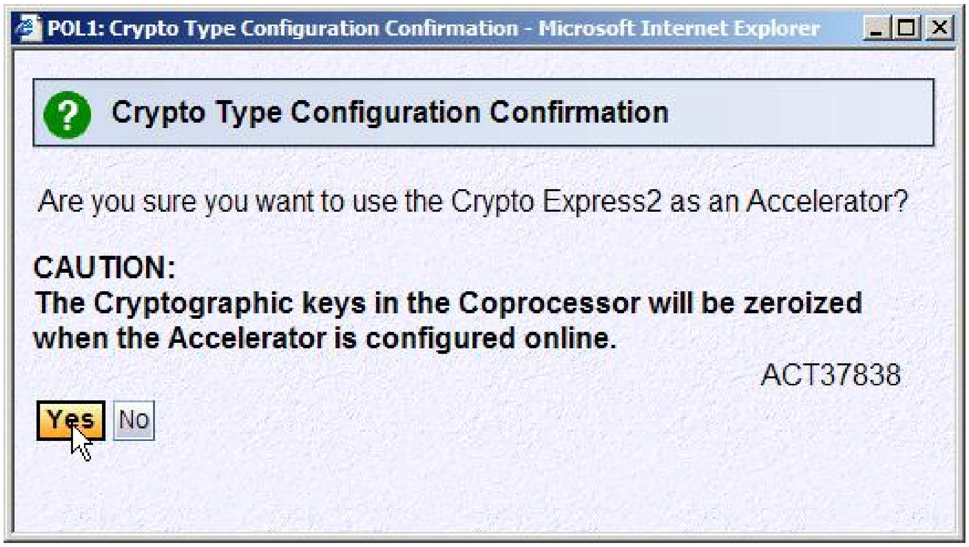
☑ Zeroize the Coprocessor

Note: Zeroize may also be performed using the Cryptographic Configuration panel.

Note: The Crypto must be deconfigured to change the Crypto type configuration.

Press **OK**.

For z/VSE you can ignore the following warning, because z/VSE does not support secret keys stored in the cryptographic hardware. For z/OS you should be aware that stored secret keys are lost when performing the reconfiguration.


POL1: Crypto Type Configuration Confirmation - Microsoft Internet Explorer
Yes
No

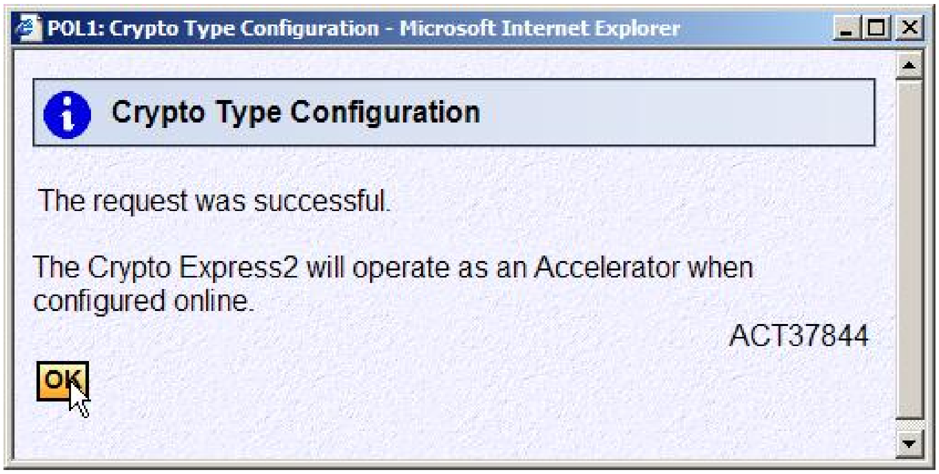
Crypto Type Configuration Confirmation

Are you sure you want to use the Crypto Express2 as an Accelerator?

CAUTION:
The Cryptographic keys in the Coprocessor will be zeroized when the Accelerator is configured online.

ACT37838

Click on **Yes** to continue.


POL1: Crypto Type Configuration - Microsoft Internet Explorer
OK

Crypto Type Configuration

The request was successful.

The Crypto Express2 will operate as an Accelerator when configured online.

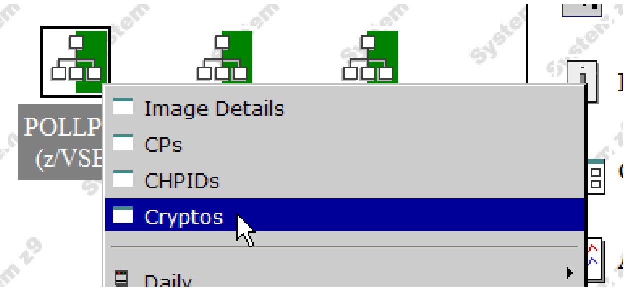
ACT37844

Click **OK**.

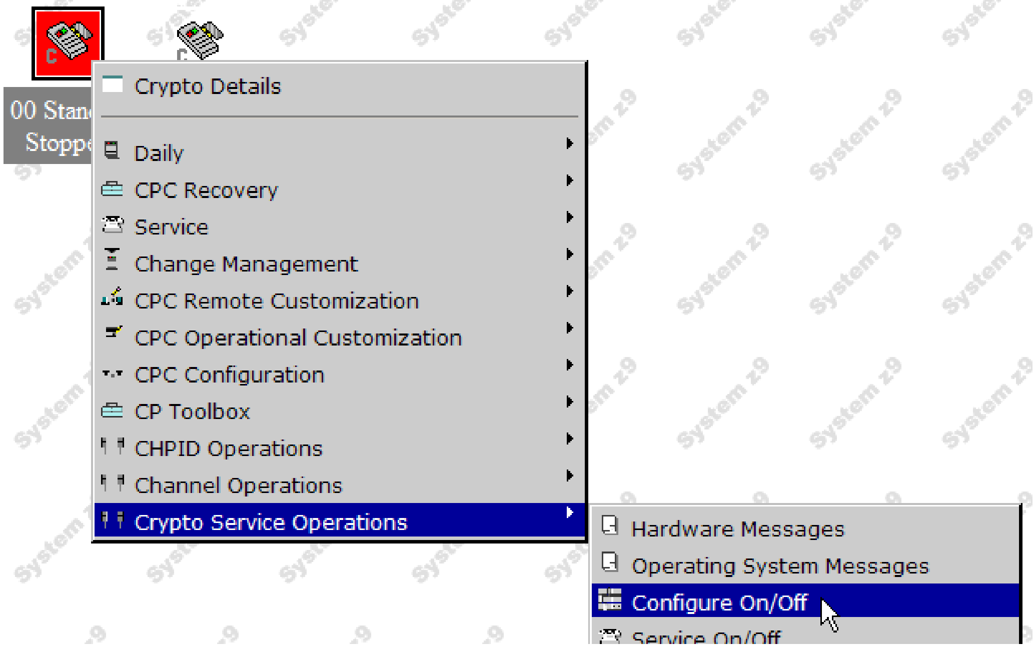
You can now leave the **Crypto Type Configuration** box by pressing Cancel. Also leave the **Cryptographic Configuration** box with Cancel, because all operations are now performed.

4.7 Enable the device after the mode change

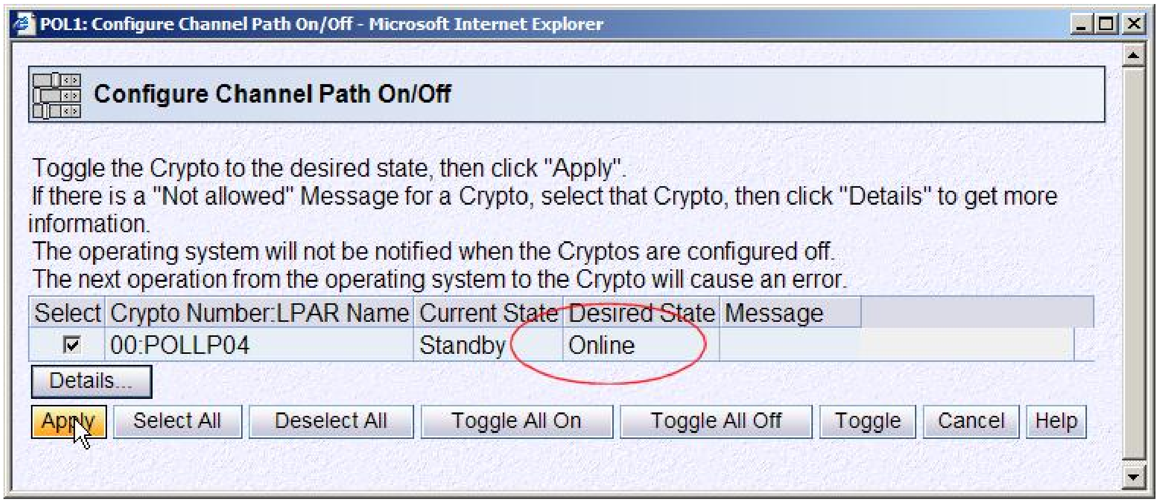
To enable the device in accelerator mode, go to Images, right-click your VSE LPAR and select Cryptos.



Select **Crypto Service Operations** and **Configure On/Off**.



Toggle the device state and press **Apply**.

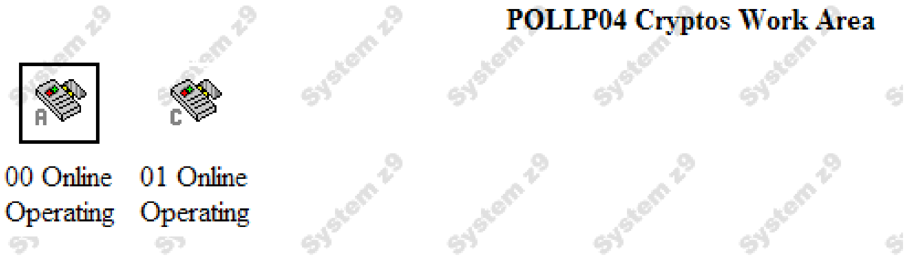

POL1: Configure Channel Path On/Off - Microsoft Internet Explorer

Configure Channel Path On/Off

Toggle the Crypto to the desired state, then click "Apply".
If there is a "Not allowed" Message for a Crypto, select that Crypto, then click "Details" to get more information.
The operating system will not be notified when the Cryptos are configured off.
The next operation from the operating system to the Crypto will cause an error.

Select	Crypto Number:LPAR Name	Current State	Desired State	Message
☑	00:POLLP04	Standby	Online	

After the device has initialized again, it’s now usable as accelerator. The device initialization process may take several minutes, because the device is now physically initialized.



To reflect the mode change in VSE, you issue the APSENSE command.

```
msg fb,data=apsense
AR 0015 1I40I  READY
FB 0095 1J022I CPU CRYPTOGRAPHIC ASSIST FEATURE AVAILABLE.
FB 0095 1J023I FOUND A CRYPTO EXPRESS2 CARD AT AP 0
FB 0095 1J023I FOUND A CRYPTO EXPRESS2 CARD AT AP 1
FB 0095 1J031I HARDWARE CRYPTO ENVIRONMENT REFRESHED.
```

The STATUS command then shows the new hardware configuration.

```
msg fb,data=status=cr
…
FB 0011   ASSIGNED APS : PCICC / PCICA ....... : 0 / 0
FB 0011                  CEX2C / CEX2A ....... : 1 / 1
FB 0011                  PCIXCC .............. : 0
FB 0011     AP 0 : CEX2A   - ONLINE
FB 0011     AP 1 : CEX2C   - ONLINE
FB 0011   ASSIGNED AP QUEUE (CRYPTO DOMAIN)... : 4
…
```

AP 0 is now usable by z/VSE as accelerator.

4.8 APARs and PTFs

Following APARs / PTFs should be applied.

APAR	PTF	Date	Release	Description
DY46681	UD53140	Apr 2007	z/VSE 3.1.2	Crypto refresh for z/VSE 3.1
DY46688	UD53148	June 2007	z/VSE 4.1.0	Crypto refresh for z/VSE 4.1

There are currently no PTFs for z/VSE 4.2.

5 VSE Operator commands

The VSE crypto device driver runs as a subtask (IJBCRYPT) in the SECSERV job, which runs in partition FB by default as part of the Basic Security Manager. Crypto related operator commands are issued in the same way as BSM Security Server commands via

```
MSG FB,DATA=command
```

You can get a list of available crypto related operator commands via the SECSERV help command.

```
msg fb,data=help
AR 0015 1I40I  READY
FB 0011 BST221I POSSIBLE SECURITY SERVER COMMANDS ARE:
...
FB 0011   STATUS=MAIN|PS|DB|CR : SHOWS SELECTED STATUS
...
FB 0011 HARDWARE CRYPTO COMMANDS:
FB 0011   APWAIT=NN ...........: SET AP CRYPTO POLLING TIME (0..99)
FB 0011   APSENSE .............: START SENSING OF CRYPTO HARDWARE
FB 0011   APTRACE=N ...........: SET AP CRYPTO TRACE LEVEL (0..3)
```

The commands are described in the z/VSE V4R1 Administration book, which is available online at

http://www.ibm.com/servers/eserver/zseries/zvse/documentation/#vse

The following chapter gives some brief information about crypto support when running under VM.

Refer to chapter 9 on page 29 for updates that came with z/VSE 4.2.

6 Running under VM

When running under VM, crypto hardware assigned to the VM LPAR is not automatically available for guest systems. Even when there are no crypto cards, we need a CRYPTO directory statement for getting access to CPACF. Of course, the CPACF availability itself depends on the activation of hardware feature code #3863.

You can use the CMS command q crypto to query the hardware crypto settings:

```
q crypto
00: Processor 00 Crypto Unit 0 usable
00: Processor 01 Crypto Unit 1 usable
00: There is no user enabled for PKSC Modify
00: All users with directory authorization are enabled for key entry
00: Crypto Adjunct Processor is installed
```

In this example, there are two crypto *cards*, which might belong to one Crypto Express2 feature installed on the machine.

You can use the *q virtual crypto* CP-command to query the hardware crypto settings for the VSE guest system:

```
* cp q virtual crypto
AR 0015 No CAM or DAC Crypto Facilities defined
AR 0015 AP 0E Queue 13 shared
AR 0015 1I40I  READY
```

In this example, crypto device 0E (14) is available via AP queue 13 in this particular VSE system.

Notes:

- VM hides older PCICC and PCIXCC cards from guest systems if newer cards, like PCICA or CEX2A are also available. Also, when more than one card of the same type is assigned to the VM LPAR, VM shows only one card to its guest systems and does the load balancing itself.
- The above command only queries the availability of *crypto cards*. It does not provide any information about the availability of CPACF.

A domain is assigned to one particular VM guest e.g. via

```
CRYPTO DOMAIN 5
```

VM virtualizes the assignment of AP queue numbers for guest systems, so it is normal for the VSE guest to see a different queue number each time it is IPLed. Although there are only 16 crypto domains available, VM assigns domain numbers in the range from 0 to 63 to VM guests.

For more details about HW-crypto support in z/VM refer to “CP Planning and Administration, SC24-6083” on

http://www.vm.ibm.com/pubs/hcsg0b01.pdf

7 Available algorithms and key lengths

Following table shows the dependencies of encryption algorithms to the System z hardware.

Algorithm	z890/z990	System z9 BC or EC	System z10 BC or EC
MD5	yes (*)	yes (*)	yes (*)
SHA-1	yes	yes	Yes
SHA-224	-	yes	Yes
SHA-256	-	yes	Yes
SHA-384	-	-	Yes
SHA-512	-	-	Yes
DES	yes	yes	Yes
TDES	yes	yes	Yes
AES-128	yes (*)	yes	Yes
AES-192	yes (*)	yes (*)	Yes
AES-256	yes (*)	yes (*)	Yes
RSA	yes (**)	yes (**)	yes (**)
(*) algorithm available as software implementation in TCP/IP for VSE/ESA 1.5E or higher (**) requires TCP/IP for VSE/ESA 1.5E or higher. 2048 bit keys require a PCIXCC or Crypto Express2			

Table 1: hardware accelerated crypto functions

8 Updates with z10 BC and EC

One major improvement with the z10 processor is new functionality to add and remove crypto cards to/from an LPAR without the need for restarting the LPAR. As a consequence, the operating system running in the LPAR needs not to be re-IPLed.

To summarize:

- Up to a z9, all crypto related definitions are static for the lifetime of an LPAR. Any changes require the reactivation of the LPAR.
- With the z10 new APs can be added to an LPAR (or removed from it) without the need for reactivating the LPAR. It is also possible to dynamically change the AP queue number.

However, there are some prerequisites.

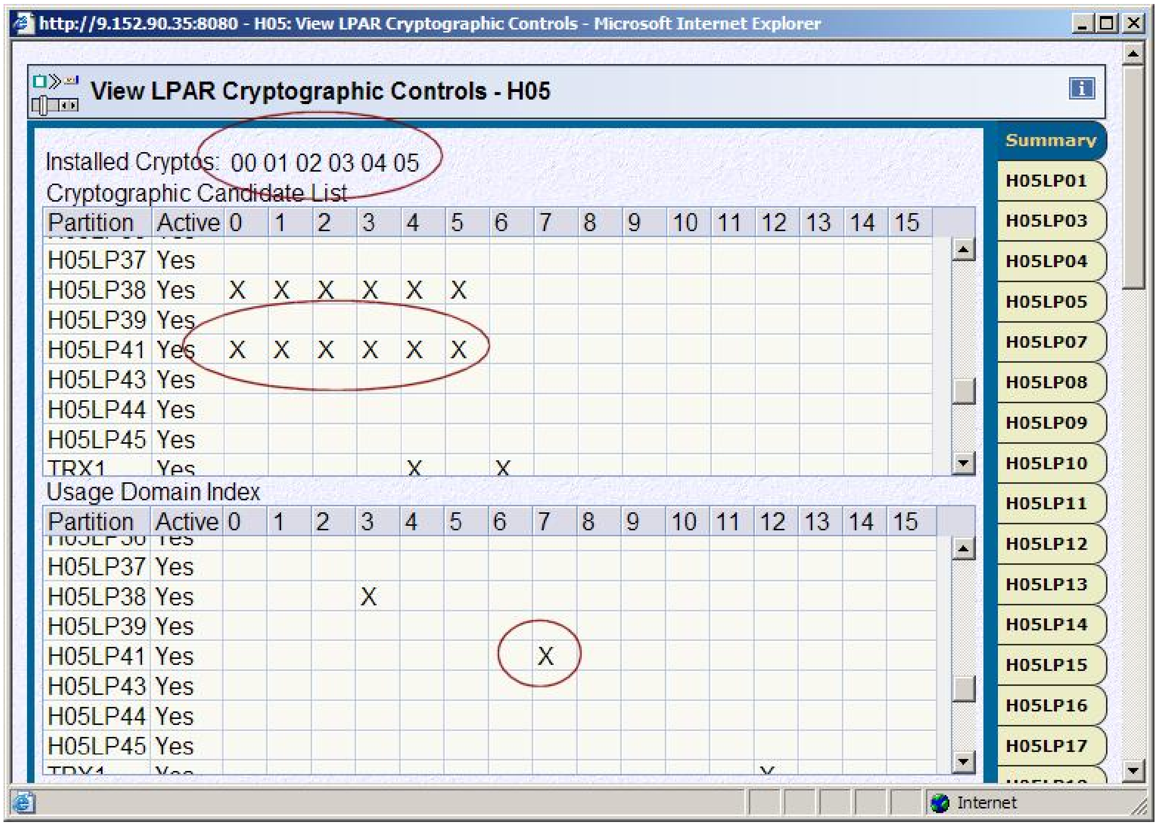
- Candidate AP queues (domains) cannot be removed if they are online.
- Candidate APs cannot be added, if the configuration would conflict with another active LPAR definition. This means that a combination of AP number and AP queue number must be unique, because it is not allowed that two active LPARs use the same AP and AP queue number.

The new functionality is primarily intended for

- Dynamically adding a crypto to an LPAR for the first time
- Dynamically adding a crypto to an existing LPAR already using crypto
- Dynamically removing a crypto from an LPAR when it's no more needed

There are several new SE panels for the z10. For example, a new summary panel for the LPAR cryptographic controls.

Select CPC – CPC Operational Customization – View LPAR Cryptographic Controls.



View LPAR Cryptographic Controls - H05

Installed Cryptos: 00 01 02 03 04 05

Cryptographic Candidate List

Partition	Active	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
H05LP37	Yes																
H05LP38	Yes	X	X	X	X	X	X										
H05LP39	Yes																
H05LP41	Yes	X	X	X	X	X	X										
H05LP43	Yes																
H05LP44	Yes																
H05LP45	Yes																
TRX1	Yes					X		X									

Usage Domain Index

Partition	Active	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
H05LP37	Yes																
H05LP38	Yes				X												
H05LP39	Yes																
H05LP41	Yes								X								
H05LP43	Yes																
H05LP44	Yes																
H05LP45	Yes																
TRX1	Yes													X			

The panel shows six installed *cryptos* (crypto cards or APs), which means that a total of three Crypto Express2 features are installed. The VSE system runs in LPAR 41 and has all cryptos assigned in the candidate list. The assigned AP queue (crypto domain) is 7.

Note: This machine is a z10 EC, so all crypto cards are part of a Crypto Express2 feature with two APs each. On a z10 BC it would be possible to have one or more single-port Crypto Express2 features with only one AP. These single-port crypto features are specially designed for the z9 and z10 BC machines and require less space in the IO cage.

The following sections describe how to dynamically remove and add a crypto device.

8.1 Performing a dynamic remove

The following steps are necessary to dynamically remove a crypto device from an LPAR.

1. On the Operating System all work (crypto requests) for the AP, which will be removed, need to be quiesced. On VSE you can use the APREM command (z/VSE 4.2) to disable the AP from use by VSE.

   ```
   msg fb,data=aprem ap=3
   AR 0015 1I40I  READY
   FB 0011 1J026I AP 3 DISABLED SUCCESSFULLY.
   ```

   The output of the STATUS=CR command now shows the AP as disabled by operator. It will now not be used to process any further crypto requests. Requests that are already in the AP queue will still be processed until the AP queue is empty.

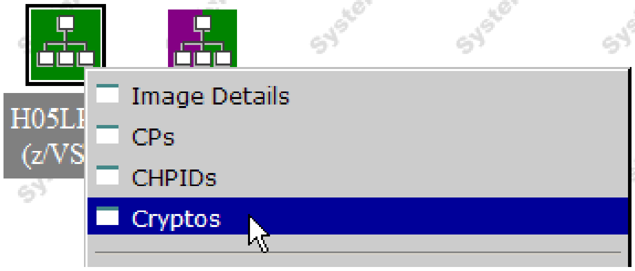
   ```
   msg fb,data=status=cr
   ...
   FB 0011   ASSIGNED APS : PCICC / PCICA ....... : 0 / 0
   FB 0011                  CEX2C / CEX2A ....... : 4 / 2
   FB 0011                  PCIXCC ............. : 0
   FB 0011     AP 0 : CEX2A   - ONLINE
   FB 0011     AP 1 : CEX2A   - ONLINE
   FB 0011     AP 2 : CEX2C   - ONLINE
   FB 0011     AP 3 : CEX2C   - DISABLED BY OPER
   FB 0011     AP 4 : CEX2C   - ONLINE
   FB 0011     AP 5 : CEX2C   - ONLINE
   FB 0011   ASSIGNED AP QUEUE (CRYPTO DOMAIN)... : 7
   ...
   ```

2. You can now use the APQUE command to show the number of pending requests for each AP. When the number of pending requests is zero for the previously disabled device, it is safe for configuring off. You may enter the APQUE command repeatedly until the device shows a zero count.

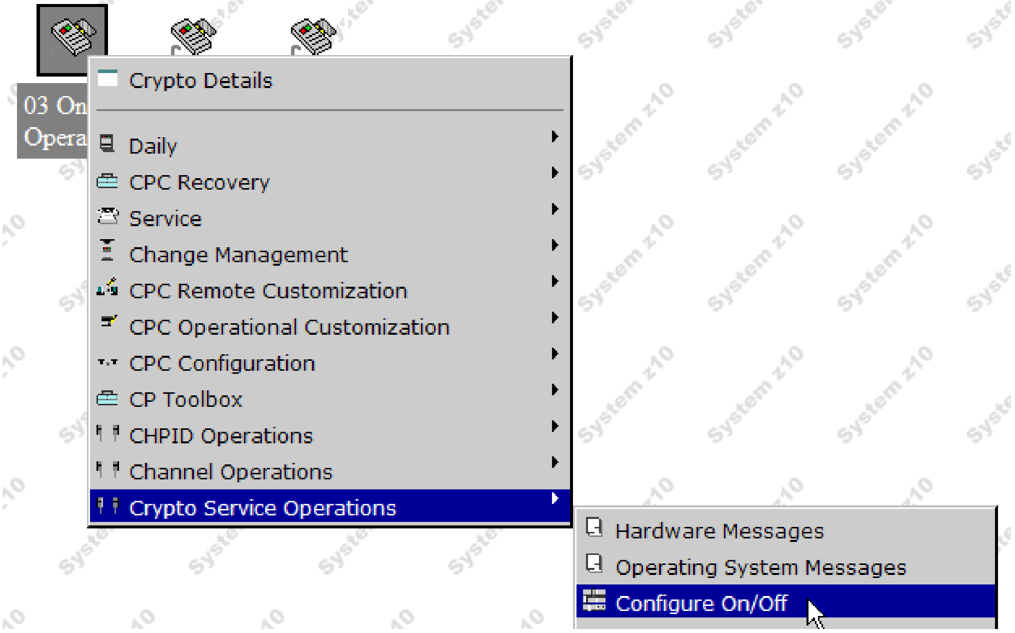
   ```
   msg fb,data=apque
   AR 0015 1I40I  READY
   FB 0011 1J045I NUMBER OF REQUESTS BEING PROCESSED BY AP QUEUE 7:
   FB 0011   AP 0 : 0
   FB 0011   AP 1 : 0
   FB 0011   AP 2 : 0
   FB 0011   AP 3 : 0
   ...
   ```

3. On the SE you have to configure Off the AP for this LPAR (manual action on SE panel), then use the Change LPAR Cryptographic Controls panel to finally remove the AP.

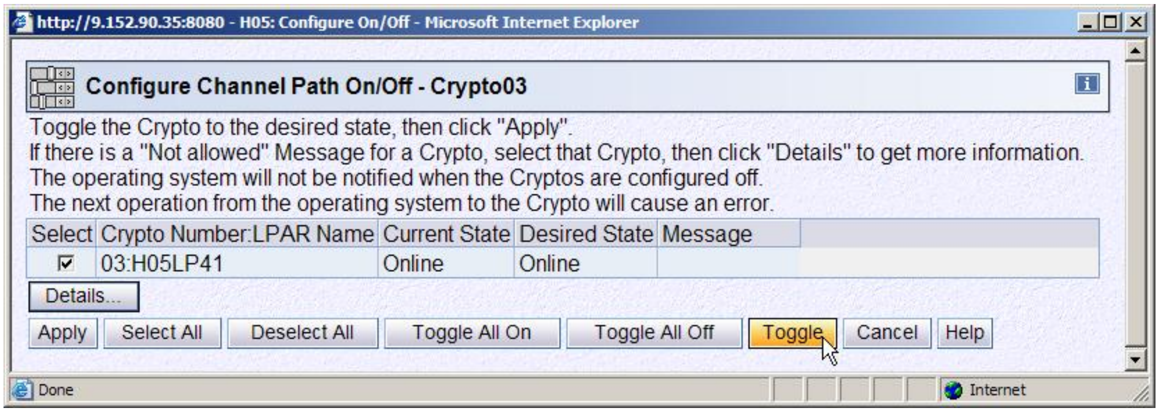
   Right-click the VSE LPAR icon and select Cryptos.



   Right-click the previously disabled crypto device and select Crypto Service Operations – Configure On/Off.



   You will be prompted with a warning, saying that this task is disruptive. Press **Yes** to continue.



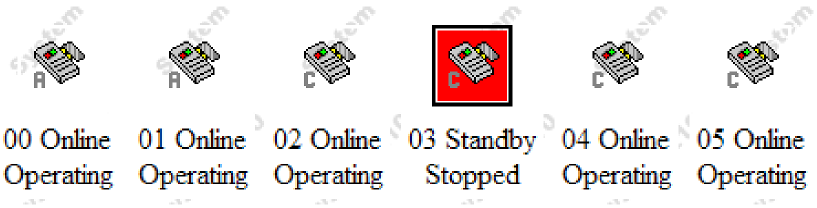
http://9.152.90.35:8080 - H05: Configure On/Off - Microsoft Internet Explorer

Configure Channel Path On/Off - Crypto03

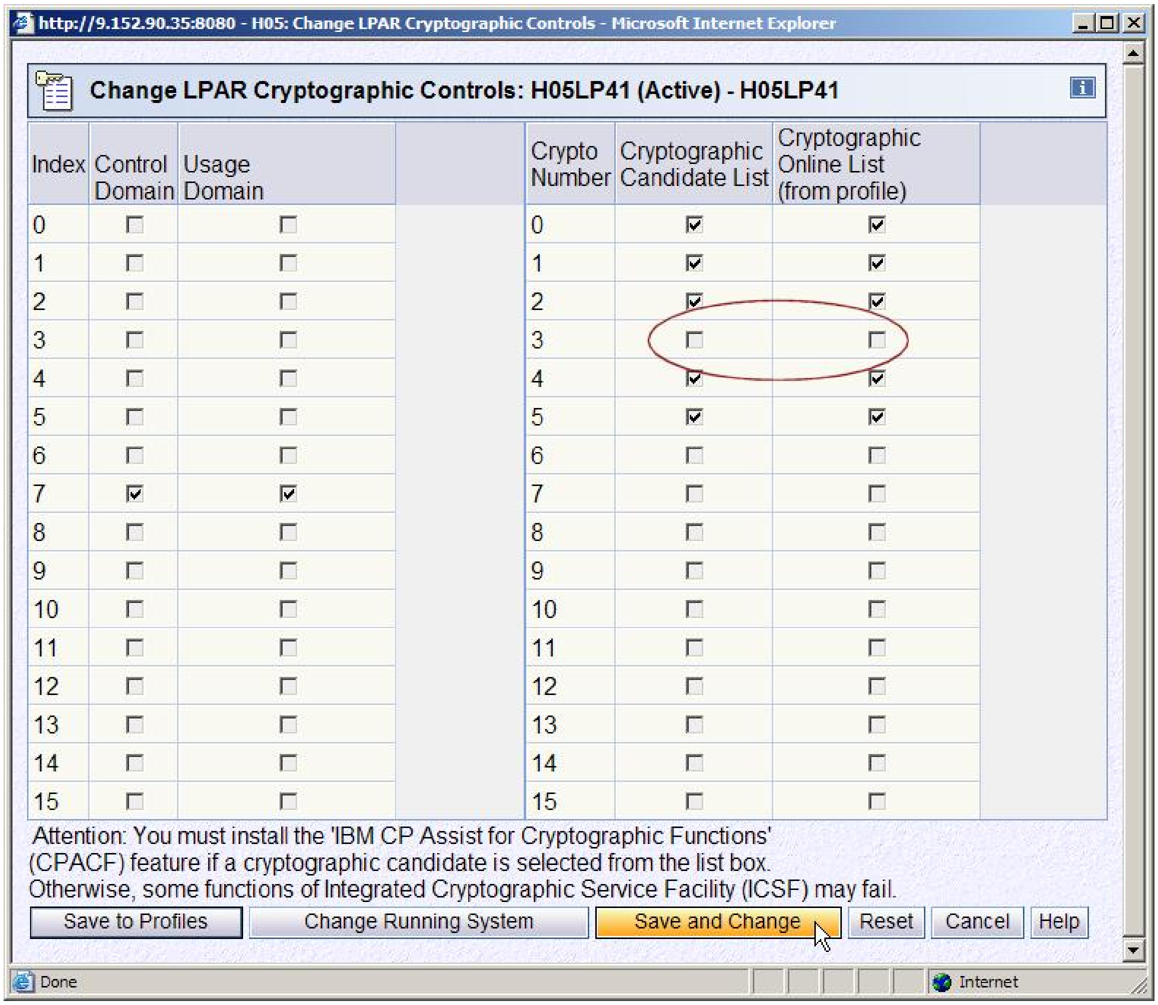
Toggle the Crypto to the desired state, then click "Apply".
If there is a "Not allowed" Message for a Crypto, select that Crypto, then click "Details" to get more information.
The operating system will not be notified when the Cryptos are configured off.
The next operation from the operating system to the Crypto will cause an error.

Select	Crypto Number:LPAR Name	Current State	Desired State	Message
☑	03:H05LP41	Online	Online	

Mark the checkbox and press **Toggle**. Then press **Apply**. The device is now displayed as Stopped.



Right-click the VSE LPAR icon and select CPC Operational Configuration – Change LPAR Cryptographic Controls.

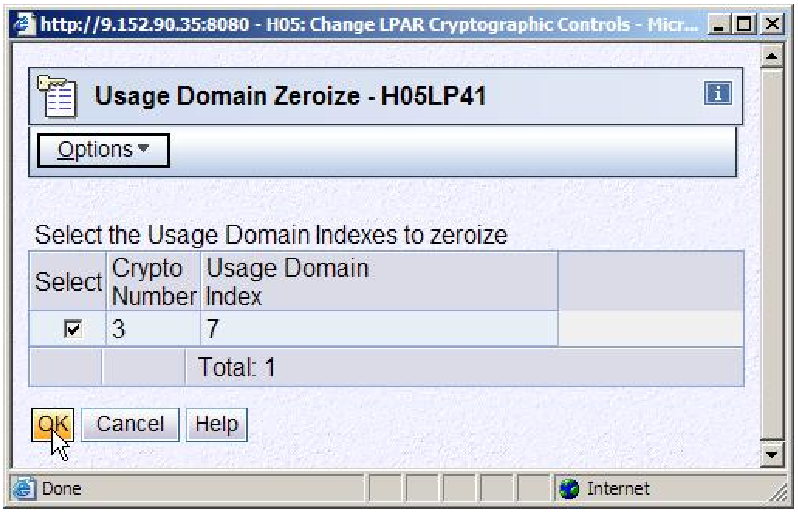

http://9.152.90.35:8080 - H05: Change LPAR Cryptographic Controls - Microsoft Internet Explorer

Change LPAR Cryptographic Controls: H05LP41 (Active) - H05LP41

Index	Control Domain	Usage Domain	Crypto Number	Cryptographic Candidate List	Cryptographic Online List (from profile)
0	□	□	0	☑	☑
1	□	□	1	☑	☑
2	□	□	2	☑	☑
3	□	□	3	□	□
4	□	□	4	☑	☑
5	□	□	5	☑	☑
6	□	□	6	□	□
7	☑	☑	7	□	□
8	□	□	8	□	□
9	□	□	9	□	□
10	□	□	10	□	□
11	□	□	11	□	□
12	□	□	12	□	□
13	□	□	13	□	□
14	□	□	14	□	□
15	□	□	15	□	□

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

Deselect the AP from the online and candidate list and press **Save and Change**. As VSE does not support secret keys, therefore a domain zeroize is not necessary. However, if you are using this device also from a z/OS system, be careful with deleting secret keys.



http://9.152.90.35:8080 - H05: Change LPAR Cryptographic Controls - Micr...

Usage Domain Zeroize - H05LP41

Options ▾

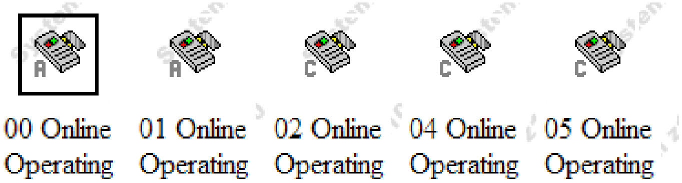
Select the Usage Domain Indexes to zeroize

Select	Crypto Number	Usage Domain Index
☑	3	7
		Total: 1

OK Cancel Help

Press **OK**.

The list of cryptos now shows the remaining APs only. AP 3 has been removed.



4. On VSE, perform a re-sensing of the crypto environment. AP 3 is no more recognized.

```
msg fb,data=apsense
AR 0015 1I40I  READY
FB 0095 1J022I CPU CRYPTOGRAPHIC ASSIST FEATURE AVAILABLE.
FB 0095 1J023I FOUND A CRYPTO EXPRESS2 CARD AT AP 0
FB 0095 1J023I FOUND A CRYPTO EXPRESS2 CARD AT AP 1
FB 0095 1J023I FOUND A CRYPTO EXPRESS2 CARD AT AP 2
FB 0095 1J023I FOUND A CRYPTO EXPRESS2 CARD AT AP 4
FB 0095 1J023I FOUND A CRYPTO EXPRESS2 CARD AT AP 5
FB 0095 1J031I HARDWARE CRYPTO DEVICE DRIVER REFRESHED.
```

The STATUS command now shows the remaining APs.

```
msg fb,data=status=cr
...
FB 0011     AP 0 : CEX2A   - ONLINE
FB 0011     AP 1 : CEX2A   - ONLINE
FB 0011     AP 2 : CEX2C   - ONLINE
FB 0011     AP 4 : CEX2C   - ONLINE
FB 0011     AP 5 : CEX2C   - ONLINE
FB 0011   ASSIGNED AP QUEUE (CRYPTO DOMAIN)... : 7
...
```

Now the AP 3 is free for reconfiguration to another LPAR.

8.2 Performing a dynamic add

This section shows how to dynamically add a new crypto device to the VSE LPAR. The following steps have to be performed.

1. On the SE use ‘Change LPAR Cryptographic Controls’ Panel to add an AP to a Logical Partition. The AP appears as Standby/Stopped in the Logical Partitions work area.

   Right-click the VSE LPAR icon and select CPC Operational Configuration – Change LPAR Cryptographic Controls.

2. On the SE perform Configure On of the previously added AP for the LPAR.

   Right-click the VSE LPAR icon and select Cryptos. Then right-click the newly added crypto device and select Crypto Service Operations – Configure On/Off.

3. On VSE perform a re-sensing of the crypto environment with the APSENSE operator command, which will sense all crypto devices, including CPACF.

4. After this step, the new AP can be used by VSE.

9 Updates with z/VSE 4.2

With z/VSE 4.2, several new crypto operator commands have been introduced, mainly to support the dynamic add/remove crypto functionality of the z10, but also to display some more statistics about recently processed crypto functions.

As described in chapter 5 on page 21 you can display a list of available commands on the operator console. Following output shows the commands available with z/VSE 4.2.

```
msg fb,data=?
AR 0015 1I40I  READY
FB 0011 BST221I POSSIBLE SECURITY SERVER COMMANDS ARE:
...
FB 0011 HARDWARE CRYPTO COMMANDS:
FB 0011   APBUSY=NN ...........: SET AP CRYPTO WAIT ON BUSY (0..99)
FB 0011   APRETRY=NN ..........: SET AP CRYPTO RETRY COUNT (0..99)
FB 0011   APREM AP=nn .........: REMOVE (DISABLE) A CRYPTO DEVICE
FB 0011   APADD AP=nn .........: ADD (ENABLE) A DISABLED DEVICE
FB 0011   APQUE ...............: SHOW STATUS OF ASSIGNED AP QUEUE
FB 0011   APHIST ..............: SHOW HISTORY OF PROCESSED REQUESTS
FB 0011   APWAIT=NN ...........: SET AP CRYPTO POLLING TIME (0..99)
FB 0011   APSENSE .............: START SENSING OF CRYPTO HARDWARE
FB 0011   APTRACE=N ...........: SET AP CRYPTO TRACE LEVEL (0..3)
```

For more details and usage examples refer to the z/VSE V4R2 Administration guide, chapter 38 “Implementing Hardware Cryptographic Support”, section “Using Hardware Crypto Commands”.

10 More information

You can find more information on these Web pages.

CryptoCards, IBM eServer Cryptographic Hardware Products
http://www.ibm.com/security/cryptocards/index.shtml

IBM PCI Cryptographic Accelerator (PCICA)
http://www.ibm.com/security/cryptocards/pcica.shtml

IBM Crypto Express2 (CEX2)
http://www.ibm.com/systems/z/security/cryptography.html

CP Assist for Cryptographic Function (CPACF)
http://www.ibm.com/systems/z/security/cryptography.html

IBM Security Products - Overview
http://www.ibm.com/security/products/

Redbook: z9-109 Crypto and TKE V5 Update, SG24-7123
http://www.redbooks.ibm.com/abstracts/sg247123.html?Open

Redbook: IBM zSeries 990 Cryptographic Coprocessor Configuration, REDP-3747
http://www-ibm.com/servers/eserver/zseries/zvse/documentation/security.htm

CP Planning and Administration, SC24-6083
http://www.vm.ibm.com/pubs/hcsg0b01.pdf

VSE Documentation
http://www.ibm.com/servers/eserver/zseries/zvse/documentation/