

Linux on Z and Crypto Express Cards



Andy Hartman, Senior Consultant

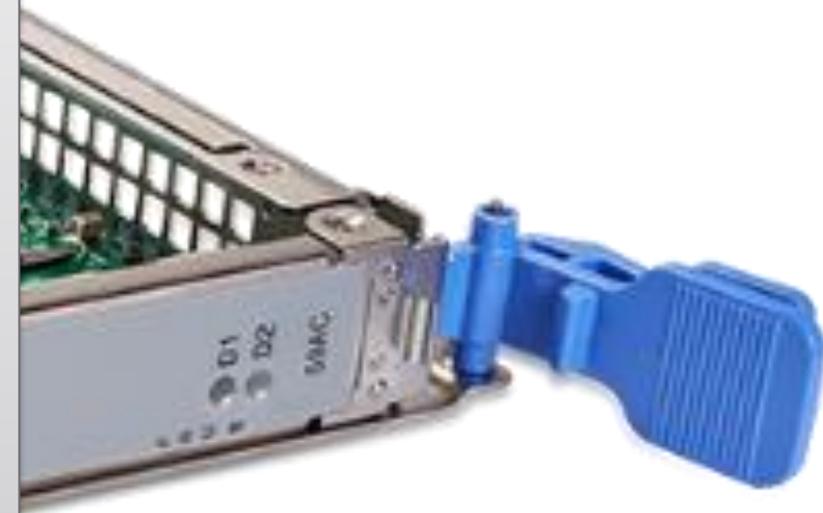
andy.hartman@mainline.com

440.785.4890

The Technology Partner for Business Results

Agenda

- What is Pervasive Encryption , CPACF and Crypto Express Cards
 - How to Implement Crypto Express Cards with Linux on z
 - Configure Crypto Express as an Accelerator
 - Configure z/VM to use the Crypto Express Cards
 - Configure Linux Guests to use the Crypto Express Cards
 - How to Measure Crypto Express Usage
 - From Linux
 - From the HMC
- Demo
 - Show processing offloaded by using the Crypto Cards
- Q&A



What Is Pervasive Encryption

- IBM Pervasive Encryption for Linux on IBM z covers several areas
- Data in Flight – SSL/TLS communications to and from the Linux system are encrypted
- Data at Rest – Partitions and File Systems can be encrypted so they cannot be used except when opened with the correct security key
- Secure Service Containers (SSC) - This allows a special LPAR to run that has been hardened and prevents access except through approved API's and secures data in flight , data at rest and provides for a secure boot process, signed images , encrypted dumps etc.
- There are several Hyper Protect offerings available that take advantage of the SSC technology

Crypto Express Cards And CPACF

- CPACF (CP Assist for Cryptographic Functions) are a set of instructions and a coprocessor on each IFL or GP processor used to process cryptographic requests
- No charge feature code 3863 is required to be activated
- Automatically virtualized and shared across all LPARs
- Scales as you grow, add more IFLs , you get more CPACF's
- Supports encryption and decryption using AES,TDES and DES for example as well as supporting SHA
- Provides very fast symmetric cryptographic functions
- Provides protected keys for encryption and decryption
- Provides the encryption and decryption of data at rest and z/VM encrypted paging

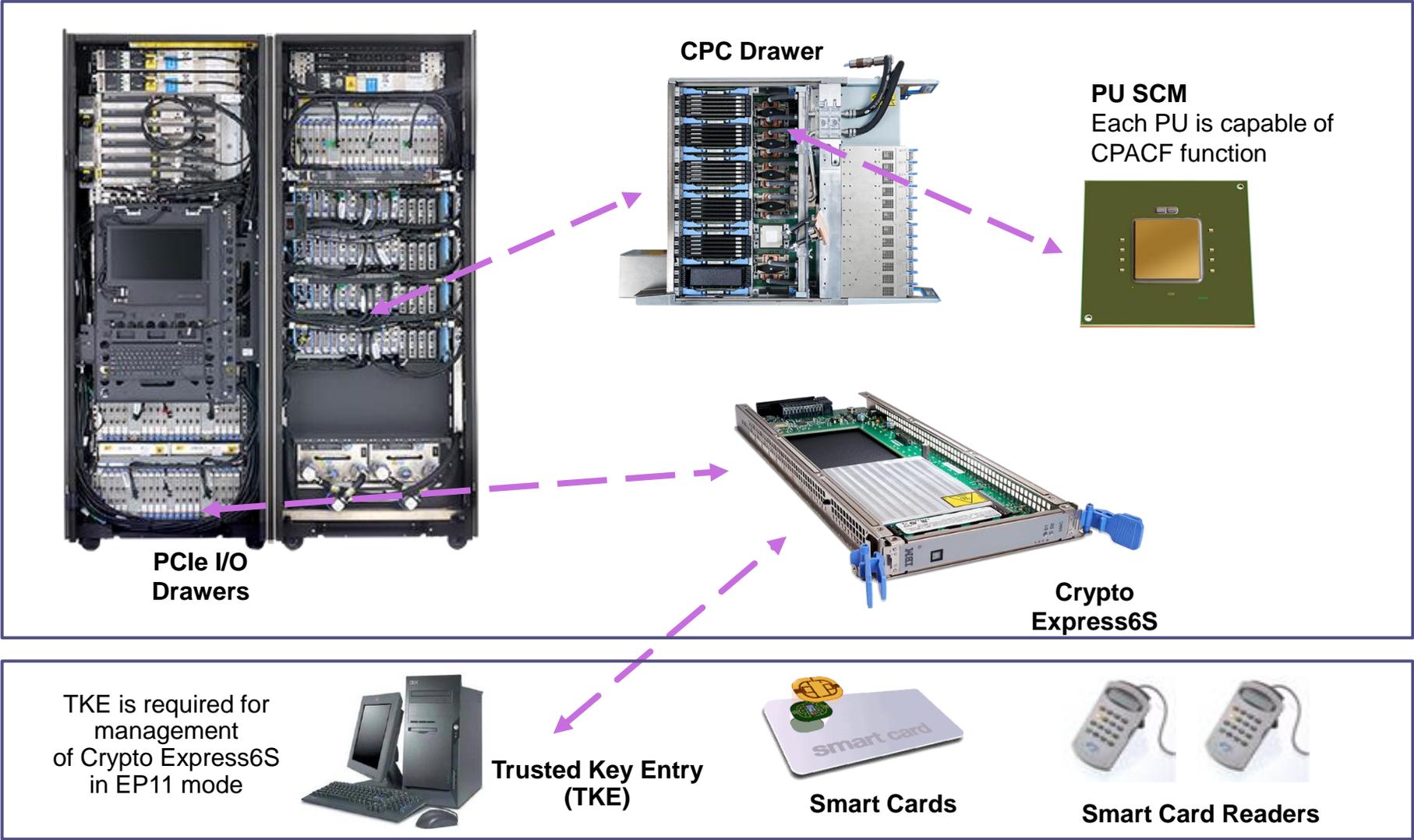
Crypto Express Cards And CPACF

- Crypto Express Cards are physical PCIe I/O cards that provide various cryptographic functions
- Up to 30 2 port cards can be configured on one z15 T01 / Minimum of 2 initially / 1 or more after initial order – Up to 20 2 port cards for a z15 T02 / Up to 16 1 port features can be supported on a z15/T01 or T02
- Each card supports either 40 or 85 domains depending on if it's installed on z15 T02 or z15 T01
- Domains are assigned to LPARs / All active LPARs must have unique domain assignments
- Crypto Express Cards provide offloading of certain cryptographic functions reducing CPU utilization
 - Secure IBM Common Cryptographic Architecture (CCA) coprocessor – provides FIPS 140-2 Level 4 certification – Used for secure key functions
 - Secure IBM Enterprise PKCS #11 Coprocessor – used to meet different industry requirements – Requires a TKE Workstation
 - Accelerator – used for public key and private key cryptography – Used in SSL/TLS processing

Crypto Express Cards And CPACF

- Multiple cards may be required depending on your configuration
 - Performance
 - Multiple Accelerators and Coprocessors for redundancy or separation of workloads
 - When used as CCA coprocessors for encrypting data at rest domains need to be dedicated to a z/VM guests , Linux or KVM LPARs
- Crypto Express Cards provide hardware security module (HSM) which is a tamper resistant/responding repository for various types of master keys used for encryption and decryption
- Crypto express cards require that the Central Processor Assist for Cryptographic Function (CPACF) be enabled on your IBM z (this is a feature that is ordered with your system)

What are Crypto Express Cards



How to Implement Crypto Express Cards with Linux on z

- Sign into the Support Element from the HMC – Single Object Operations
- HMC / Tasks Index / Single Object Operations

The screenshot displays the IBM Hardware Management Console (HMC) interface. The browser address bar shows the URL: <https://10.0.10.86/hmc/connects/mainuiFrameset.jsp>. The page title is "HMC1: Hardware Management Console Workplace (Version 2.14.1) - Mozilla Firefox".

The main content area is titled "Tasks Index" and contains a table of tasks. A mouse cursor is hovering over the "Single Object Operations" task. The table has the following columns: Name, Permitted Objects, Count, and Description.

Name	Permitted Objects	Count	Description
Remote Service	Systems	0	Customize remote service information for selected systems
Report a Problem		0	Report problem and request service for console
Report a Problem	Systems	0	Report problem and request service for selected system
Reset Clear	Partitions	1	Perform resets clear of selected images
Reset Normal	Partitions	0	Perform resets normal of selected images
Retrieve Backup or Upgrade Data	Systems	0	Retrieve backup or upgrade data
Retrieve Internal Code	Systems	0	Retrieve internal code change levels for all systems
Service Status	Systems	0	Set service status of selected system
Set Power Cap	BladeCenters, Blades, Systems	0	Set Power Cap
Set Power Saving	BladeCenters, Blades, Systems	0	Enable your system to use less power
Shutdown or Restart		1	Restart the application or shutdown/restart the console
Single Object Operations	Systems	29	Log on to selected object's console
Single Step Change Internal Code		0	Manage console's internal code change levels in a single step
Single Step Internal Code Changes	Systems	0	Manage internal code change levels for selected systems in a single step
Start	Systems	0	Start Dynamic Partition Manager systems
Start	Partitions	0	Start Dynamic Partition Manager partitions
Start All Processors	Partitions	0	Start all processors for selected partitions
Stop	Systems	0	Stop Dynamic Partition Manager systems
Stop	Partitions	0	Stop Dynamic Partition Manager partitions
Stop All Processors	Partitions	0	Stop all processors for selected partitions
System Details	Systems	2	Displays information about a system
System Information	Systems	3	Display internal code change information for selected systems
System Input/Output Configuration Analyzer	Systems	0	System Input/Output Configuration Analyzer
Tip of the Day		0	Display tips for using the console
Toggle Lock	BladeCenters, Blades, Ensemble, Managed VM, Partitions, Systems, Virtual Servers	0	Toggle Lock
Transmit Console Service Data		0	Send console's CSD
Transmit Service Data	Systems	0	Send service data for selected system
Transmit Vital Product Data		0	Send console's VPD before hardware upgrade
Transmit Vital Product Data	Systems	0	Send system's VPD before hardware upgrade
User Management		0	Manage users, user roles, password rules, LDAP server definitions, user templates, and user patterns
Users and Tasks		1	View the logged on users and the tasks they are running
User Settings		1	Customize the appearance of the workplace
View Console Events		0	Display the event log of the operations and activities

The status bar at the bottom of the page shows "Status: Exceptions and Messages" and "Total: 119 Filtered: 119".

How to Implement Crypto Express Cards with Linux on z

- Check that the CPACF feature is enabled on your processor
- Click on System Management / CPU Serial No. / System Details at the bottom

The screenshot displays the IBM Support Element web interface in a Mozilla Firefox browser window. The browser title is "P00298A8: Primary Support Element Workplace (Version 2.14.1) - Mozilla Firefox". The address bar shows the URL "https://10.0.10.86:9950/hmc/connects/mainuiFrameset.jsp". The page header includes "IBM Support Element" and navigation options like "SEARCH", "FAVORITES", and "SooSysprog". The main content area is titled "P00298A8 Details - P00298A8" and features several tabs: "Instance Information", "Product Information", "Acceptable CP/PCHID Status", "Energy Management", and "Security". The "Instance Information" tab is active, showing a list of system parameters and their values. At the bottom of the page, there are buttons for "OK", "Apply", "Change Options...", "Cancel", and "Help". A status bar at the very bottom indicates "Transferring data from 10.0.10.86..." and provides contact information: "www.mainline.com | 866.490.MAIN(6246)".

Instance Information	Product Information	Acceptable CP/PCHID Status	Energy Management	Security
Group:			CPC	
CP status:			Operating	
Channel status:			Exceptions	
Crypto status:			Channel acceptable	
Alternate SE status:			Operating	
Activation profile:			DEFAULT	
Last profile used:			DEFAULT	
IOCDS identifier:			A3	
IOCDS name:			OSA Chan	
System mode:			Logically Partitioned	
Service state:			false	
Number of CPs:			6	
Number of CBPs:			0	
Number of ICFs:			0	
Number of IFLs:			5	
Number of zIIPs:			1	
Dual AC power maintenance:			Fully Redundant	
CP Assist for Crypto functions:			Installed	
Licensed Internal Code security mode:			Monitor	
Lock out disruptive tasks:			<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	

How to Implement Crypto Express Cards with Linux on z

- Support Element / Cryptos

The screenshot displays the IBM Support Element web interface. The browser address bar shows the URL `10.0.10.86:9950/hmc/connects/mainuiFrameset.jsp`. The page title is "IBM Support Element". The breadcrumb navigation indicates the current location is "System Management > P00298A8 > Cryptos".

The main content area features a table with the following columns: Select, PCHID, ID, Status, State, Location, and Type. The table contains two rows of data:

Select	PCHID	ID	Status	State	Location	Type
<input type="checkbox"/>	011C	00	Operating	Online	A14B-LG10	Crypto Express6S
<input type="checkbox"/>	013C	01	Operating	Online	A14B-LG20	Crypto Express6S

Below the table, the status summary reads: "Max Page Size: 500 Total: 2 Filtered: 2 Selected: 0".

The left sidebar contains a navigation menu with the following items: Welcome, System Management, P00298A8, Processors, Channels, Cryptos, Partitions, Custom Groups, SE Management, Service Management, and Tasks Index. The "Cryptos" item is currently selected.

At the bottom of the interface, there is a "Tasks: Cryptos" section and a "Status: Exceptions" indicator.

How to Implement Crypto Express Cards with Linux on z

- Support Element / Tasks Index / Filter 'crypt'

The screenshot shows the IBM Support Element interface. The browser title is "P00298A8: Primary Support Element Workplace (Version 2.14.1) - Mozilla Firefox". The URL is "https://10.0.10.86:9950/hmc/connects/mainuiFrameset.jsp". The page header includes "IBM Support Element", a search bar, and "SooSysprog". The left sidebar shows a navigation tree with "System Management" expanded to "P00298A8", and "Cryptos" selected. The main content area is titled "Tasks Index" and shows a table of tasks filtered by "crypt".

Name	Permitted Objects	Count	Description
Change LPAR Cryptographic Controls	Partitions	4	Change LPAR Cryptographic Controls
Crypto Details	Logical Adapters	1	Displays information about a Crypto
Cryptographic Configuration	System	4	Cryptographic Configuration
Cryptographic Management	System	2	Cryptographic Management
Query Channel/Crypto Configure Off/On Pending	System	1	Query Channel/Crypto Configure Off/On Pending
View LPAR Cryptographic Controls	System	1	View LPAR Cryptographic Controls

Total: 116 Filtered: 6

Status: Exceptions

Transferring data from 10.0.10.86...

How to Implement Crypto Express Cards with Linux on z

- Click on Crypto Configuration / Review the Crypto Type / Note the Crypto Type Configuration
- Cancel to return to the Tasks Index

IBM Support Element

Home Cryptographic Configurat... X

Cryptographic Configuration - P00298A8

Cryptographic Information

Select	Number	Status	Crypto Serial Number	Type	Operating mode	TKE Commands
<input checked="" type="radio"/>	00	Configured	YH1093AAAT96	CEX6S CCA Coprocessor	Default	Denied
<input type="radio"/>	01	Configured	YH1093AAAUTC	CEX6S Accelerator	Default	Not supported

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

[View Details...](#) [Test RNG/CIS](#) [Zeroize](#) [Domain Management...](#) [TKE Commands...](#) [Crypto Type Configuration...](#)

[Zeroize All](#) [Test RNG/CIS on All](#) [UDX Configuration...](#) [Refresh](#) [Cancel](#) [Help](#)

Transferring data from 10.0.10.86...

How to Implement Crypto Express Cards with Linux on z

- Systems Management / Cryptos
- PCHID's need to be in Standby to change from CCA to Accelerator Mode

System Management > P00298A8 > Cryptos

Select	PCHID	ID	Status	State	Location	Type
<input type="checkbox"/>	011C	00	Operating	Online	A14B-LG10	Crypto Express6S
<input type="checkbox"/>	013C	01	Operating	Online	A14B-LG20	Crypto Express6S

Max Page Size: 500 Total: 2 Filtered: 2 Selected: 0

Tasks: Cryptos

Status: Exceptions

Transferring data from 10.0.10.86...

How to Implement Crypto Express Cards with Linux on z

- Systems Management / Cryptos / Select the Cards / Configure On/Off
- Select Actions / Select All / Select Toggle All Standby

The screenshot shows the IBM Support Element interface for configuring crypto express cards. The page title is "Configure On/Off - PCHID011C". The interface includes a navigation bar with "Home" and "Configure On/Off - PCHI..." tabs. Below the navigation bar, there is a toolbar with icons for actions like "Select Action" and "Filter". The main content area displays a table with the following data:

Select	PCHID	ID	LPAR Name	Current State	Desired State	Message
<input checked="" type="checkbox"/>	011C	00	AH	Online	Online	
<input checked="" type="checkbox"/>	011C	00	AH2	Online	Online	

Page 1 of 1 Total: 2 Filtered: 2 Displayed: 2

Buttons: OK, Cancel, Help

How to Implement Crypto Express Cards with Linux on z

- Systems Management / Cryptos / Configure On/Off
- PCHID shows Stopped – Remember this is disruptive to anyone using this card/cards

P00298A8: Primary Support Element Workplace (Version 2.14.1) - Personal - Microsoft Edge

Not secure | <https://10.0.10.86:9950/hmc/connects/mainuiFrameset.jsp>

IBM Support Element

SEARCH FAVORITES SooSysprog

Home

System Management > P00298A8 > Cryptos

Cryptos Topology

Select	PCHID	ID	Status	State	Location	Type
<input type="checkbox"/>	011C	00	Stopped	Standby	A14B-LG10	Crypto Express6S
<input type="checkbox"/>	013C	01	Stopped	Standby	A14B-LG20	Crypto Express6S

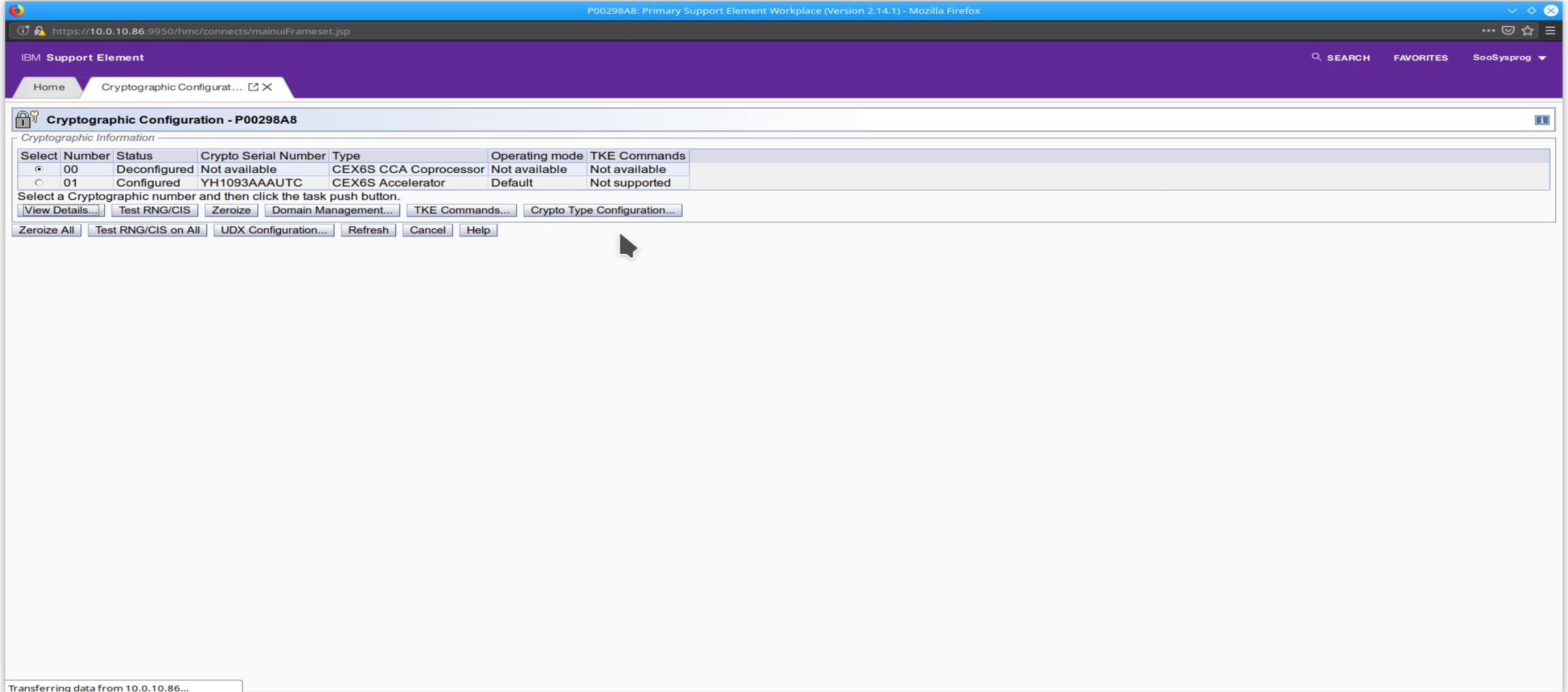
Max Page Size: 500 Total: 2 Filtered: 2 Selected: 0

Tasks: Cryptos

Status: Exceptions and Messages

How to Implement Crypto Express Cards with Linux on z

- Systems Management / Tasks Index / Crypto Configuration
- Card Number shows Deconfigured – Remember this is disruptive to anyone using this card



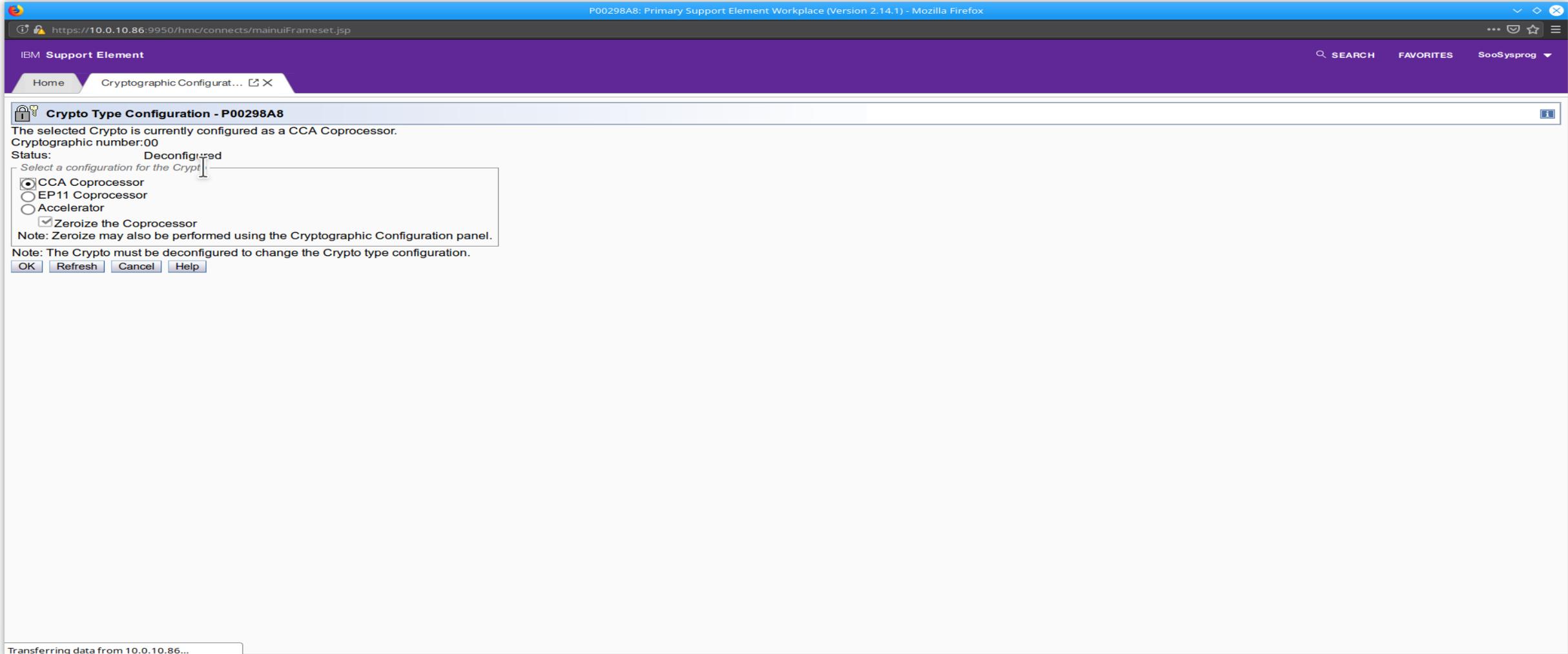
The screenshot shows the IBM Support Element interface for Cryptographic Configuration. The browser address bar indicates the URL is <https://10.0.10.86:9950/hmc/connects/mainuiFrameset.jsp>. The page title is "Cryptographic Configuration - P00298A8". Below the title, there is a section for "Cryptographic Information" containing a table with the following data:

Select	Number	Status	Crypto Serial Number	Type	Operating mode	TKE Commands
<input checked="" type="radio"/>	00	Deconfigured	Not available	CEX6S CCA Coprocessor	Not available	Not available
<input type="radio"/>	01	Configured	YH1093AAAUTC	CEX6S Accelerator	Default	Not supported

Below the table, there is a instruction: "Select a Cryptographic number and then click the task push button." followed by several buttons: "View Details...", "Test RNG/CIS", "Zeroize", "Domain Management...", "TKE Commands...", and "Crypto Type Configuration...". At the bottom of the interface, there are additional buttons: "Zeroize All", "Test RNG/CIS on All", "UDX Configuration...", "Refresh", "Cancel", and "Help".

How to Implement Crypto Express Cards with Linux on z

- Systems Management / Tasks Index / Crypto Configuration
- Select Accelerator / Uncheck or check the Zeroize the Coprocessor



The screenshot displays the IBM Support Element web interface. The browser address bar shows the URL `https://10.0.10.86:9950/hmc/connects/mainuiFrameset.jsp`. The page title is "Crypto Type Configuration - P00298A8". The status is "Deconfigured". The cryptographic number is "00". The configuration options are:

- CCA Coprocessor
- EP11 Coprocessor
- Accelerator
- Zeroize the Coprocessor

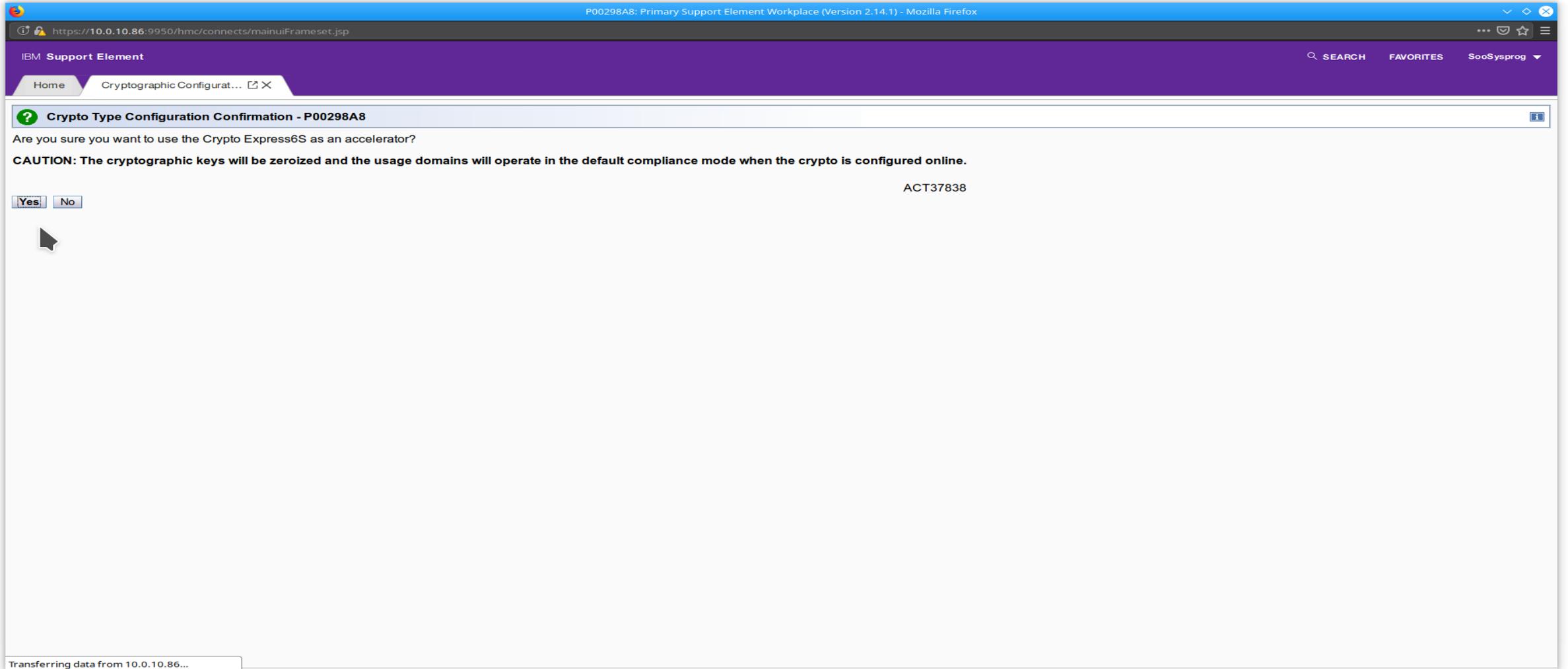
Note: Zeroize may also be performed using the Cryptographic Configuration panel.

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

Buttons: OK, Refresh, Cancel, Help

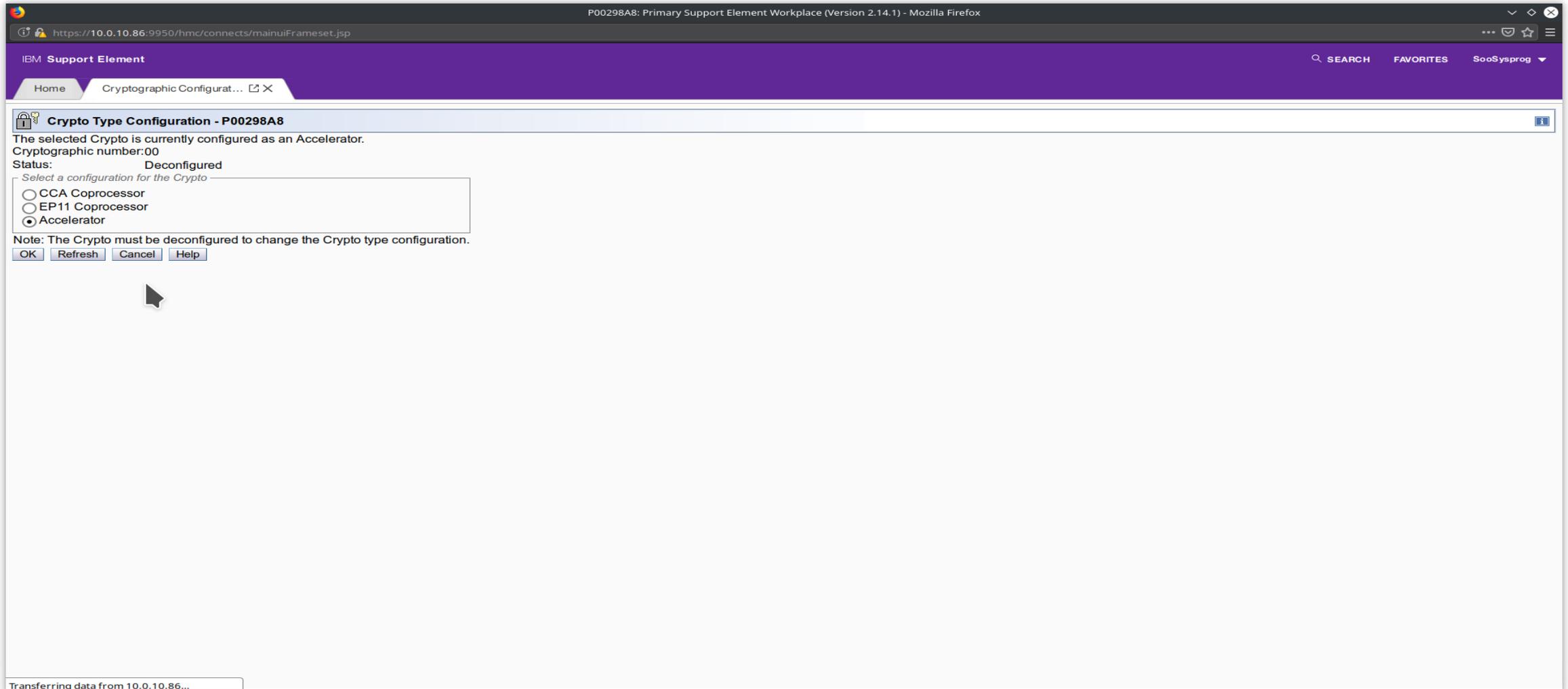
How to Implement Crypto Express Cards with Linux on z

- Select Accelerator / Then select Yes on the screen below /
- This will wipe out any keys you have stored on this card – make sure you select the correct card
- If you unchecked the zeroized box then the keys will NOT be removed



How to Implement Crypto Express Cards with Linux on z

- This shows the card has been changed to an Accelerator
- Select Cancel to return to the Crypto Configuration Screen / Select Cancel or close the tab



How to Implement Crypto Express Cards with Linux on z

- This shows the card has been changed to an Accelerator
- Select Cancel to return to the Tasks Index or Close the Crypto Config tab

The screenshot displays the IBM Support Element Cryptographic Configuration interface for P00298A8. The browser address bar shows the URL: https://10.0.10.86:9950/hmc/connects/mainuiFrameset.jsp. The page title is "Cryptographic Configuration - P00298A8".

The main content area is titled "Cryptographic Information" and contains a table with the following data:

Select	Number	Status	Crypto Serial Number	Type	Operating mode	TKE Commands
<input checked="" type="radio"/>	00	Deconfigured	Not available	CEX6S Accelerator	Not available	Not supported
<input type="radio"/>	01	Configured	YH1093AAAUTC	CEX6S Accelerator	Default	Not supported

Below the table, there is a instruction: "Select a Cryptographic number and then click the task push button." followed by a row of buttons: "View Details...", "Test RNG/CIS", "Zeroize", "Domain Management...", "TKE Commands...", and "Crypto Type Configuration...".

At the bottom of the interface, there is another row of buttons: "Zeroize All", "Test RNG/CIS on All", "UDX Configuration...", "Refresh", "Cancel", and "Help".

A status bar at the bottom left indicates "Transferring data from 10.0.10.86...".

How to Implement Crypto Express Cards with Linux on z

- Systems Management / Cryptos
- PCHID will show as stopped/standby - Select the PCHID / Tasks / Channel Operations / Configure On/Off

The screenshot displays the IBM Support Element web interface. The breadcrumb navigation shows 'System Management > P00298A8 > Cryptos'. The main content area features a table with columns for 'PCHID', 'ID', 'Status', 'State', 'Location', and 'Type'. Two rows are visible: one for PCHID 011C (ID 00, Stopped, Standby, A14B-LG10, Crypto Express6S) and one for PCHID 013C (ID 01, Operating, Online, A14B-LG20, Crypto Express6S). A mouse cursor is positioned over the PCHID 011C row. Below the table, a 'Tasks: Cryptos' section is visible. The left sidebar contains a navigation tree with categories like 'System Management', 'Processors', 'Channels', 'Cryptos', 'Partitions', 'AH', 'AH2', 'BP', 'IT', 'MP', 'PS', and 'TA'. The bottom status bar shows 'Status: Exceptions' and a progress indicator for 'Transferring data from 10.0.10.86...'.

Select	PCHID	ID	Status	State	Location	Type
<input type="checkbox"/>	011C	00	Stopped	Standby	A14B-LG10	Crypto Express6S
<input type="checkbox"/>	013C	01	Operating	Online	A14B-LG20	Crypto Express6S

How to Implement Crypto Express Cards with Linux on z

- Systems Management / Cryptos / Configure On/Off
- Select Action – Toggle All Online / Press Ok

IBM Support Element

Home Configure On/Off - PCHL... X

Configure On/Off - PCHID011C

Select Action Filter

Select	PCHID	ID	LPAR Name	Current State	Desired State	Message
<input checked="" type="checkbox"/>	011C	00	AH	Standby	Online	
<input checked="" type="checkbox"/>	011C	00	AH2	Standby	Online	

Page 1 of 1 Total: 2 Filtered: 2 Displayed: 2

OK Cancel Help

Read 10.0.10.86

How to Implement Crypto Express Cards with Linux on z

- Systems Management / Cryptos
- This screen will show initializing then online when the card is ready to use

The screenshot displays the IBM Support Element interface for system management. The main content area shows a table of Cryptos for system P00298A8. The table has columns for Select, PCHID, ID, Status, State, Location, and Type. Two rows are visible: one for PCHID 011C (ID 00) which is in an 'Initializing' state, and another for PCHID 013C (ID 01) which is in an 'Operating' state. Below the table, there are sections for 'Tasks: 011C' and 'Crypto Service Operations'.

Select	PCHID	ID	Status	State	Location	Type
<input checked="" type="checkbox"/>	011C	00	Initializing	Online	A14B-LG10	Crypto Express6S
<input type="checkbox"/>	013C	01	Operating	Online	A14B-LG20	Crypto Express6S

Tasks: 011C

Channel Operations

- Advanced Facilities
- Channel Problem Determination
- Configure On/Off
- Service On/Off
- Show LED

Crypto Service Operations

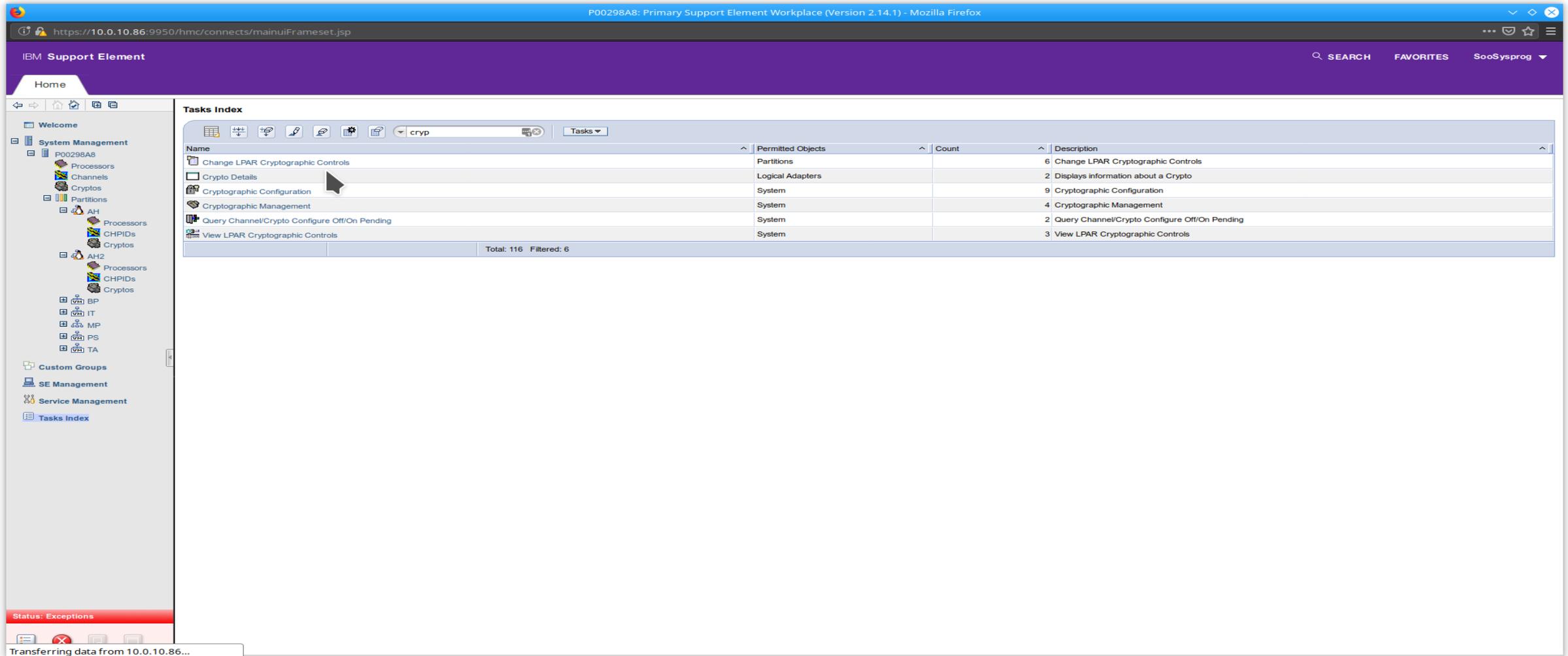
- Advanced Facilities
- Channel Problem Determination
- Configure On/Off
- Service On/Off
- Show LED

Status: Exceptions

Transferring data from 10.0.10.86...

How to Implement Crypto Express Cards with Linux on z

- Systems Management / Tasks Index / Filter for Crypt / Select Change LPAR Crypto Controls
- This will allow you to assign crypto domains/indexes to your partitions



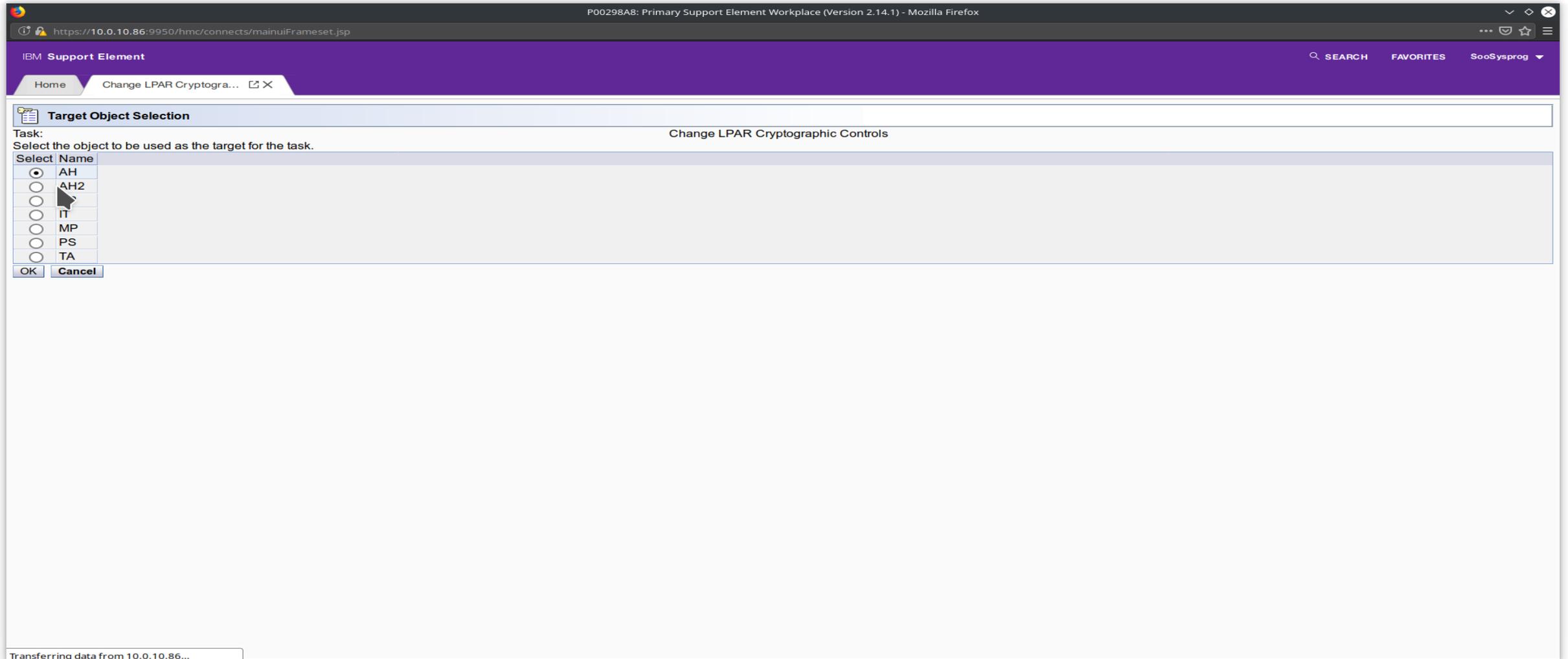
The screenshot displays the IBM Support Element web interface. The browser address bar shows the URL `https://10.0.10.86:9950/hmc/connects/mainuiFrameset.jsp`. The page title is "P00298A8: Primary Support Element Workplace (Version 2.14.1) - Mozilla Firefox". The interface includes a navigation menu on the left with categories like "System Management", "Processors", "Channels", "Cryptos", "Partitions", "AH", "AH2", "BP", "IT", "MP", "PS", and "TA". The main content area is titled "Tasks Index" and shows a table of tasks filtered by "crypt". The table has columns for Name, Permitted Objects, Count, and Description. The tasks listed are:

Name	Permitted Objects	Count	Description
Change LPAR Cryptographic Controls	Partitions	6	Change LPAR Cryptographic Controls
Crypto Details	Logical Adapters	2	Displays information about a Crypto
Cryptographic Configuration	System	9	Cryptographic Configuration
Cryptographic Management	System	4	Cryptographic Management
Query Channel/Crypto Configure Off/On Pending	System	2	Query Channel/Crypto Configure Off/On Pending
View LPAR Cryptographic Controls	System	3	View LPAR Cryptographic Controls

At the bottom of the table, it indicates "Total: 116 Filtered: 6". A status bar at the bottom left shows "Status: Exceptions" and a message "Transferring data from 10.0.10.86...".

How to Implement Crypto Express Cards with Linux on z

- Select the partition you wish to configure
- This will need to be done for each partition you wish to configure



How to Implement Crypto Express Cards with Linux on z

- Explained on the next Slide

The screenshot shows the IBM Support Element web interface. The browser address bar displays the URL `https://10.0.10.86:9950/hmc/connects/mainuiFrameset.jsp`. The page title is "Change LPAR Cryptographic Controls: AH (Active) - AH".

The interface includes a navigation bar with "Home" and "Change LPAR Cryptogra..." tabs. Below the navigation bar, there are two main sections: "Assigned Domains" and "Assigned Cryptos".

Assigned Domains

Select	Index	Control	Control and Usage
<input type="checkbox"/>	0		✓
<input type="checkbox"/>	2		✓

Assigned Cryptos

Select	Number	Candidate	Candidate and Online
<input type="checkbox"/>	0		✓
<input type="checkbox"/>	1		✓

Attention: You must install the '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.

Buttons: Save and Change, Save to Profiles, Change Running System, Reset, Cancel, Help

Transferring data from 10.0.10.86...

How to Implement Crypto Express Cards with Linux on z

- This screen allows you to choose your index (must be unique for active partitions)
- This screen allows you to choose which crypto cards are used
- The Save and Change button , dynamically changes the configuration and saves these setting in your LPAR image profile under the crypto tab
- This screen shows I selected Control and Usage – allowing me to use these indexes and Candidate and Online giving me access to these two crypto cards
- You can select one or more Indexes for each LPAR and Crypto Card, you may want to select more than one index per LPAR if you are planning to dedicate resources to specific users for example

How to Implement Crypto Express Cards with Linux on z

- System Management / Partitions / Customize Delete Activation Profiles
- This shows the Activation Profile for the AH partition after the previous step was complete

The screenshot displays the IBM Support Element web interface for configuring image profiles. The browser address bar shows the URL `https://10.0.10.86:9950/hmc/connects/mainuiFrameset.jsp`. The page title is "Customize Image Profiles: AH : AH : Crypto".

Assigned Domains

Select	Index	Control	Control and Usage
<input type="checkbox"/>	0		✓
<input type="checkbox"/>	2		✓

Assigned Cryptos

Select	Number	Candidate	Candidate and Online
<input type="checkbox"/>	0		✓
<input type="checkbox"/>	1		✓

Attention: You must install the '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.

Buttons at the bottom: Cancel, Save, Copy Profile, Paste Profile, Assign Profile, Help.

How to Implement Crypto Express Cards with Linux on z

- Systems Management / Tasks Index / Filter for Crypt / Select View LPAR Crypto Configuration
- This will allow you to see all the crypto cards and indexes for all partitions

The screenshot displays the IBM Support Element web interface. The browser address bar shows the URL `https://10.0.10.86:9950/hmc/connections/mainuiFrameset.jsp`. The page title is "P00298A8: Primary Support Element Workplace (Version 2.14.1) - Mozilla Firefox". The interface includes a navigation menu on the left with categories like "System Management", "Processors", "Channels", "Cryptos", "Partitions", "AH", "AH2", "BP", "IT", "MP", "PS", and "TA". The main content area is titled "Tasks Index" and features a search filter set to "crypt". Below the filter is a table with the following data:

Name	Permitted Objects	Count	Description
Change LPAR Cryptographic Controls	Partitions	7	Change LPAR Cryptographic Controls
Crypto Details	Logical Adapters	2	Displays information about a Crypto
Cryptographic Configuration	System	9	Cryptographic Configuration
Cryptographic Management	System	5	Cryptographic Management
Query Channel/Crypto Configure Off/On Pending	System	2	Query Channel/Crypto Configure Off/On Pending
View LPAR Cryptographic Controls	System	4	View LPAR Cryptographic Controls

At the bottom of the table, it indicates "Total: 116 Filtered: 6". A mouse cursor is pointing at the "View LPAR Cryptographic Controls" task. The bottom status bar shows "Status: Exceptions" and "Transferring data from 10.0.10.86..."

How to Implement Crypto Express Cards with Linux on z

- Systems Management / Tasks Index / Filter for Crypt / Select View LPAR Crypto Configuration
- This will show you if you have any conflicts

IBM Support Element

View LPAR Cryptographic Controls - P00298A8

Installed Crypto Express5S: NONE
Installed Crypto Express6S: 00 01

Cryptographic Candidates

Partition	Active	Crypto Numbers	Conflicts
AH	Yes	0-1	
AH2	Yes	0-1	
BP	Yes		
IT	Yes	1	
MP	Yes		
PS	Yes		

Usage Domain Indexes

Partition	Active	Indexes	Conflicts
AH	Yes	0, 2	
AH2	Yes	3-4	
BP	Yes		
IT	Yes	1	
MP	Yes		
PS	Yes		

Close Refresh Help

Transferring data from 10.0.10.86...

How to Implement Crypto Express Cards with Linux on z

- Z/VM 7.1 does not require an IPL to recognize a new crypto card – RSU 2001 – APAR – VM66266
- Z/VM 6.4 requires and IPL to see changes to crypto hardware
- I'm using CRYPTO APVIRT for the accelerator cards which is fine for clear key acceleration
- Use CRYPTO APDEDICATED if you need specific resources for specific guests for performance etc.
- When using APVIRT z/VM will dynamically choose which crypto resources to use
- When using APVIRT Linux configurations will always show only one crypto card , even though 2 or more may be in use to satisfy the requests
- The CRYPTO APVIRT can be placed in the user's directory or in a common profile if all the Linux guests will use the crypto cards

How to Implement Crypto Express Cards with Linux on z

- Z/VM setup crypto express definitions in the system config file
- System Config File

```
/*  
/* CRYPTOGRAPHIC CO-PROCESSORS AND ACCELERATORS */  
*/
```

```
AHZVMM01: BEGIN  
    CRYPTO APVIRT AP 0 DOMAIN 0 2  
    CRYPTO APVIRT AP 1 DOMAIN 0 2  
/* ENCRYPT PAGING ON ALG AES256 */  
    ENCRYPT PAGING REQUIRED ALG AES256  
AHZVMM01: END
```

```
AHZVMM02: BEGIN  
    CRYPTO APVIRT AP 0 DOMAIN 3 4  
    CRYPTO APVIRT AP 1 DOMAIN 3 4  
/* ENCRYPT PAGING ON ALG AES256 */  
    ENCRYPT PAGING REQUIRED ALG AES256  
AHZVMM02: END
```

AP – equates to crypto card number | Domain equates to Index number from the hardware configuration earlier

How to Implement Crypto Express Cards with Linux on z

- Z/VM setup crypto express definitions in the Linux directory statements

- AHUBCRPT DIRECT

```
USER AHUBCRPT XXXXXXXX 4G 12G G
```

```
INCLUDE LNXDFLT
```

```
CPU 0
```

```
CPU 1
```

```
CPU 2
```

```
CPU 3
```

```
CRYPTO APVIRT
```

```
*
```

```
* IP ADDRESS - 10.0.10.196
```

```
*
```

```
* 0100 - DASDA1 SWAP DEFINED IN SWAPGEN EXEC
```

```
* 0101 - DASDB1 SWAP DEFINED IN SWAPGEN EXEC
```

```
*
```

```
MDISK 0200 3390 1 END AHB701 MR READPASS WRITPASS MULTPASS
```

AHUBBASE does not contain the crypto entry since it doesn't use the crypto express cards

How to Implement Crypto Express Cards with Linux on z

- Z/VM Query Crypto Express cards available for use

Q CRYPTO

Crypto Adjunct Processor Instructions are installed - OR - Crypto Adjunct Processor Instructions are not installed

Ready; T=0.01/0.01 15:44:33

q crypto domain users

AP 000 CEX6A Domain 000 operational online shared
AP 000 CEX6A Domain 002 operational online shared
AP 001 CEX6A Domain 000 operational online shared
AP 001 CEX6A Domain 002 operational online shared

Shared-Crypto Users:

AHUBCRPT

Ready; T=0.01/0.01 10:16:12

q crypto domain users

AP 000 CEX6A Domain 000 operational online shared
AP 000 CEX6A Domain 002 operational online shared
AP 001 CEX6A Domain 000 operational online shared
AP 001 CEX6A Domain 002 operational online shared

There are no shared-crypto users.

Ready; T=0.01/0.01 10:17:57

How to Implement Crypto Express Cards with Linux on z

- AHUBCRPT – Ubuntu 20.04

```
andy@ahubcrpt:~$ sudo apt upgrade
```

```
andy@ahubcrpt:~$ sudo apt upgrade
```

```
Reading package lists... Done
Building dependency tree
Reading state information... Done
```

```
.
Adding #2: IPL section 'old'
Preparing boot device: dasda (0200).
Done.
```

```
sudo apt install openssh-client openssh-server openssl openssl-ibmca libica3 libica-utils
```

Openssh-client , openssh-server and openssl are usually already installed by default

zcrypt is part of the device drivers for IBM z and installed by default

Make a copy of openssl.cnf in /etc/ssl

Modify the openssl.cnf file in /etc/ssl to use the ibmca engine

Add the following two lines to the openssl.cnf file right after the HOME line near the top of the file

```
# Line inserted to use ibmca
```

```
openssl_conf = openssl_def
```

Append /usr/share/doc/openssl-ibmca/examples/openssl.cnf.sample to the end of the openssl.cnf file

Comment out the line open_conf =

Completely shut down the Linux guest and bring it back up to enable the changes

How to Implement Crypto Express Cards with Linux on z

- AHRHCRPT – RHEL 8.2

```
[root@ahrhcrpt card01]# dnf upgrade
```

```
Updating Subscription Management repositories.
```

```
Red Hat Enterprise Linux 8 for IBM z Systems - AppStream (RPMs)
```

```
769 B/s | 4.5 kB 00:05
```

```
Red Hat Enterprise Linux 8 for IBM z Systems - BaseOS (RPMs)
```

```
744 B/s | 4.0 kB 00:05
```

```
Dependencies resolved.
```

```
Nothing to do.
```

```
Complete!
```

```
dnf install libica openssl-ibmca openssl openssl
```

openssl and openssl are usually already installed by default

zcrypt is part of the device drivers for IBM z and installed by default

Make a copy of openssl.cnf in /etc/pki/tls

Modify the openssl.cnf file in /etc/pki/tls to use the ibmca engine

Add the following two lines to the openssl.cnf file right after the HOME line near the top of the file

```
# Line inserted to use ibmca
```

```
openssl_conf = openssl_def
```

Append /usr/share/doc/openssl-ibmca/openssl.cnf.sample.s390x to the end of the openssl.cnf file

Comment out any other openssl_conf = statements and their directives

Completely shutdown the Linux guest and bring it back up to enable the changes

How to Implement Crypto Express Cards with Linux on z

- AHSLCRPT – SLES 15 SP 1

```
ahslcrpt:~ # zypper update
```

```
Refreshing service 'Basesystem_Module_15_SP1_s390x'.
```

```
Refreshing service 'SUSE_Linux_Enterprise_Server_15_SP1_s390x'.
```

```
zypper
```

```
Core libraries or services have been updated.
```

```
Reboot is required to ensure that your system benefits from these updates.
```

```
zypper install openssh openssl openssl-ibmca libica3 libica-tools
```

openssh and openssl are usually already installed by default

zcrypt is part of the device drivers for IBM z and installed by default

Make a copy of openssl.cnf in /etc/ssl

Modify the openssl.cnf file in /etc/ssl to use the ibmca engine

Add the following two lines to the openssl.cnf file right after the #RANDFILE line near the top of the file

```
# Line inserted to use ibmca
```

```
openssl_conf = openssl_def
```

Append /usr/share/doc/packages/openssl-ibmca/openssl.cnf.sample to the end of the openssl.cnf file

Completely shut down the Linux guest and bring it back up to enable the changes

How to Measure Crypto Express Usage

- `Vmcp q v crypto` – shows virtual cryptographic card available to this Linux guest

```
root@ahubcrpt:~# vmcp q v crypt
AP 001 CEX6A Domain 001 shared online
```

This only shows 1 but VM will use all available crypto cards to satisfy the requests

- `ls /sys/devices/ap/cardxx` - shows various files associated with the virtual crypto card

```
root@ahubcrpt:~# ls /sys/devices/ap/card01/
01.0001      depth  hwtype  modalias  pendingq_count  request_count  subsystem  uevent
ap_functions  driver  load    online   raw_hwtype     requestq_count  type
```

- `cat /sys/devices/ap/card01/request_count`

```
root@ahubcrpt:~# cat /sys/devices/ap/card01/request_count
21179
```

How to Measure Crypto Express Usage

Icainfo – Display cryptographic functions supported by libica

```
andy@ahubcrpt:~$ icainfo
```

```
    Cryptographic algorithm support
```

```
-----
```

function	hardware		software
	dynamic	static	
SHA-1	no	yes	yes
SHA-224	no	yes	yes
SHA-256	no	yes	yes
SHA-384	no	yes	yes
.			
RSA ME	yes	no	no
RSA CRT	yes	no	no
.			

```
-----
```

```
No built-in FIPS support.
```

– Lszcrypt -V – Displays available cryptographic cards and requests

```
andy@ahubcrpt:~$ lszcrypt -V
```

```
CARD.DOMAIN TYPE MODE STATUS REQUESTS PENDING HWTYPE QDEPTH FUNCTIONS DRIVER
```

```
-----
```

01	CEX6A Accelerator	online	21179	0	12	08 -MC-A-NF-	cex4card
01.0001	CEX6A Accelerator	online	21179	0	12	08 -MC-A-NF-	cex4queue

How to Measure Crypto Express Usage

- Icastats – Shows statistics for hardware and software cryptography used by the libica functions

```
root@ahubcrpt:~# icastats
```

function	hardware			software		
	ENC	CRYPT	DEC	ENC	CRYPT	DEC
SHA-1	126520			0		
SHA-224	0			0		
SHA-256	540257			0		
SHA-384	0			0		
SHA-512	151			0		
RSA-ME	12104			0		
RSA-CRT	9075			0		
AES XTS	0	0		0	0	
AES GCM	33142		18090	0		0

How to Measure Crypto Express Usage

- Systems Management / Monitors Dashboard

IBM Hardware Management Console

Home

Systems Management

Systems | Partitions | Topology

Select	Name	Status	Activation Profile	Last Used Profile	SE IP Address	Machine Type - Model	Machine Serial
<input type="radio"/>	P00298A8	Operating	DEFAULT	DEFAULT	fe80::210:6fff:fe23:9184%eth1	3907 - ZR1	0000200298A8
<input type="radio"/>	Unmanaged Systems						

Max Page Size: 500 Total: 2 Filtered: 2 Selected: 0

Tasks: Systems Management

Grouping | Manage System Time | Monitors Dashboard | New Partition

Status: Exceptions and Messages

How to Measure Crypto Express Usage

- Click on Details

IBM Hardware Management Console

Home Monitors Dashboard

Monitors Dashboard

Last refresh time: 02:37:46 PM Date: 08/06/19 Time zone: UTC-04:00 [Pause Refresh](#)

Overview

Select	Name	Status	Type	Machine Type - Model	Processor Usage(%)	I/O Usage(%)	Power Consumption (kW) (Btu/hr)	Ambient Temperature (°C) (°F)
<input type="checkbox"/>	P00298A8	Operating	CPC	3907 - ZR1	2	0	1.444 4927	25.7 78.26

Page 1 of 1 Max Page Size: 100 Total: 1 Filtered: 1 Displayed: 1 Selected: 0

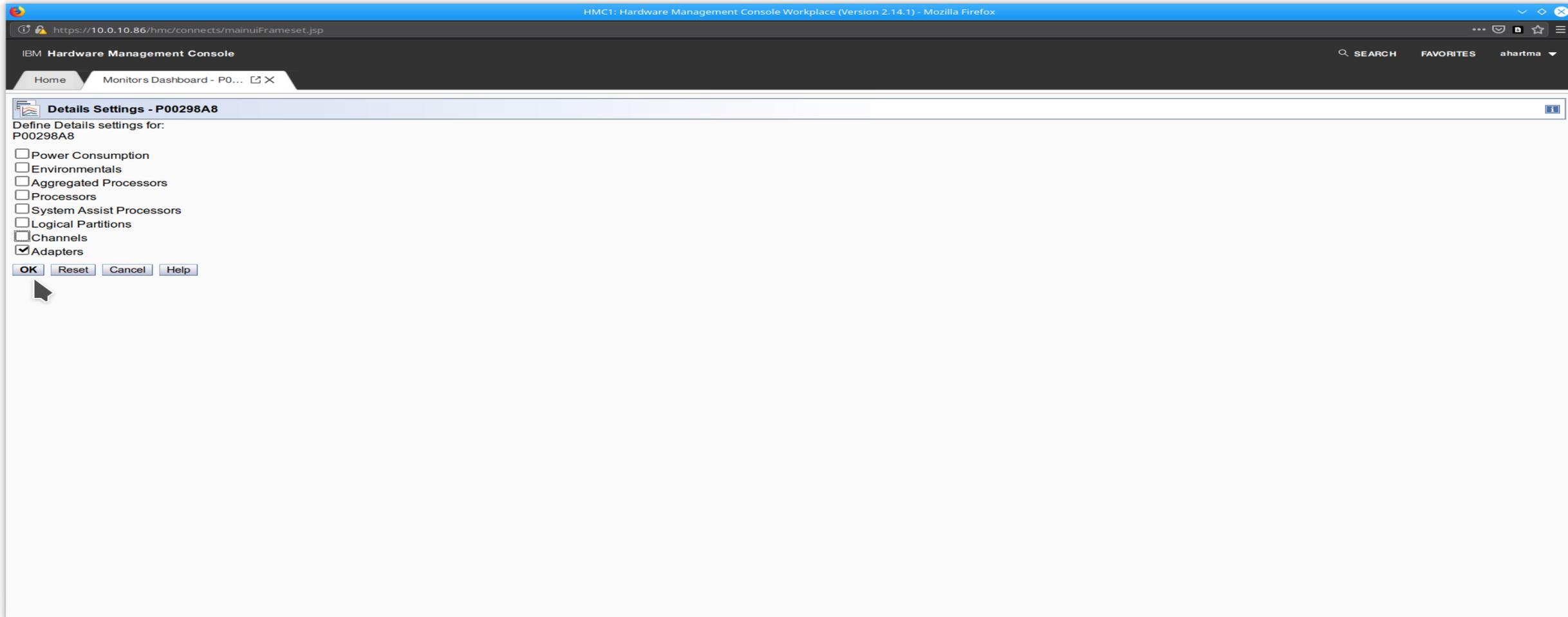
Details

P00298A8

Close Help

How to Measure Crypto Express Usage

- Select Adapters and Click OK



How to Measure Crypto Express Usage

- Select both adapters / Select Start History from Select Action Drop Down
- It will start two new tabs one for each adapter

The screenshot displays the IBM Hardware Management Console (HMC) interface. The browser address bar shows the URL `https://10.0.10.86/hmc/connects/mainuiFrameset.jsp`. The page title is "HMC1: Hardware Management Console Workplace (Version 2.14.1) - Mozilla Firefox". The main content area is titled "Monitors Dashboard" and includes a "Last refresh time: 02:44:45 PM Date: 08/06/19 Time zone: UTC-04:00" and a "Pause Refresh" button.

The "Overview" section shows a table with the following data:

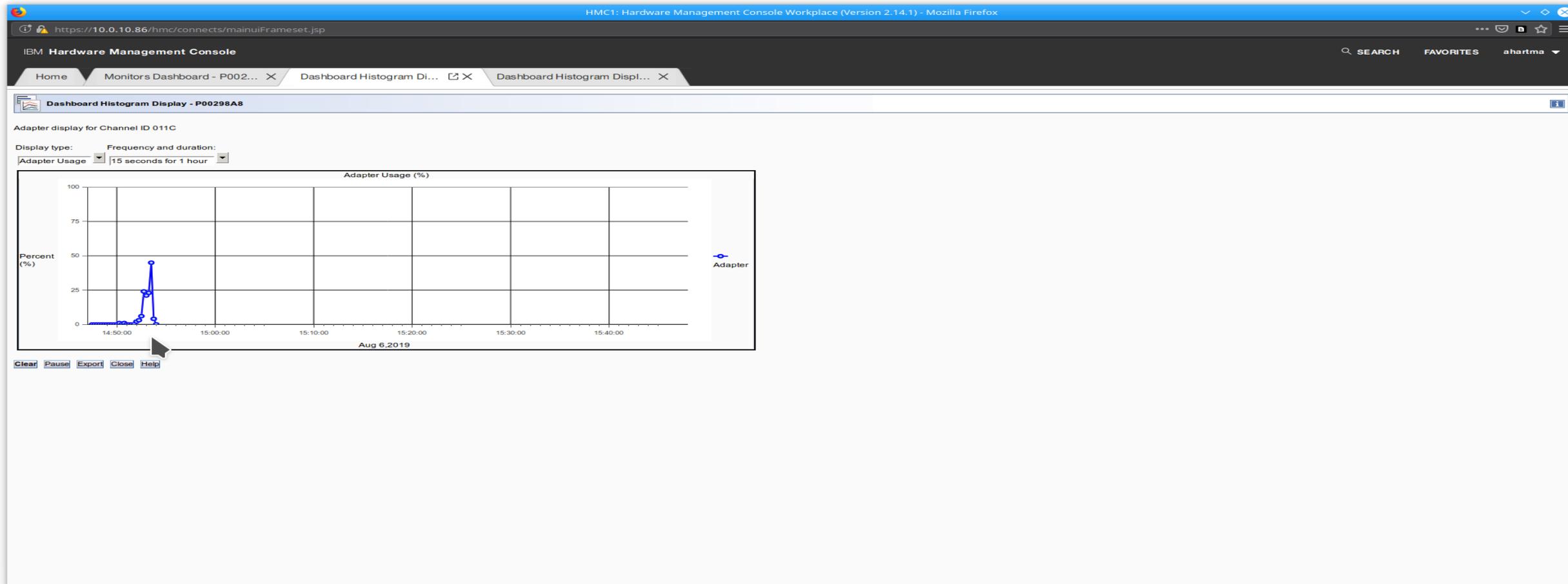
Select	Name	Status	Type	Machine Type - Model	Processor Usage(%)	IO Usage(%)	Power Consumption (W) (Suhu)	Ambient Temperature (°C) (°F)
<input type="checkbox"/>	P00298A8	Operating	CPC	3907 - ZR1	2	0	1.442 4920	25.7 78.26

The "Details" section shows the "Adapters" view for P00298A8. The table below shows the selected adapters:

Select	Channel #	Type	Adapter Usage(%)
<input checked="" type="checkbox"/>	011C	Crypto (ID = 0)	0
<input checked="" type="checkbox"/>	013C	Crypto (ID = 1)	0

How to Measure Crypto Express Usage

- Both tabs will look the same – each is used evenly



Show Processing
Offloaded By Using The
Crypto Cards

DEMO

Show Processing Offloaded By Using The Crypto Cards

ab -n 3000 -c 50 -Z DHE-RSA-AES128-SHA <https://10.0.10.194/> - No CPACF/ No Crypto Express

ab -n 3000 -c 50 -Z DHE-RSA-AES128-SHA <https://10.0.10.196/> - CPACF / Crypto Express

-n 3000 = number of requests to perform during the benchmark

-c 50 = number of requests to perform at the same time

-Z = Encryption suite used for the benchmark

DHE = key exchange via Diffie Hellman

RSA = authentication algorithm

AES128 = bulk encryption algorithm

SHA = hashing algorithm

- Different Cipher Suites will have different affects on CPU utilization – this one showed around a 60-70% utilization without crypto cards / Less than 1% CPU utilization with crypto cards
- Different distributions and releases can affect how the cpu and crypto cards are utilized
- Choose your Cipher Suites based on your specific needs

Show Processing Offloaded By Using The Crypto Cards

```
andy@DESKTOP-T02VH7C:~$ ab -n 3000 -c 50 -Z DHE-RSA-AES128-SHA https://10.0.10.194/  
This is ApacheBench, Version 2.3 <$Revision: 1843412 $>  
Copyright 1996 Adam Twiss, Zeus Technology Ltd, http://www.zeustech.net/  
Licensed to The Apache Software Foundation, http://www.apache.org/
```

```
Benchmarking 10.0.10.194 (be patient)  
Completed 300 requests  
Completed 600 requests  
Completed 900 requests  
Completed 1200 requests  
Completed 1500 requests  
Completed 1800 requests  
Completed 2100 requests  
Completed 2400 requests  
Completed 2700 requests  
Completed 3000 requests  
Finished 3000 requests
```

```
Server Software:    Apache/2.4.41  
Server Hostname:    10.0.10.194  
Server Port:        443  
SSL/TLS Protocol:   TLSv1.2,DHE-RSA-AES128-SHA,4096,128  
Server Temp Key:    DH 4096 bits
```

```
Document Path:      /  
Document Length:    10918 bytes
```

Show Processing Offloaded By Using The Crypto Cards

Concurrency Level: 50
Time taken for tests: 164.189 seconds
Complete requests: 3000
Failed requests: 0
Total transferred: 33576000 bytes
HTML transferred: 32754000 bytes
Requests per second: 18.27 [#/sec] (mean)
Time per request: 2736.481 [ms] (mean)
Time per request: 54.730 [ms] (mean, across all concurrent requests)
Transfer rate: 199.70 [Kbytes/sec] received

Connection Times (ms)

	min	mean[+/-sd]	median	max
Connect:	355	2199 594.6	2292	4402
Processing:	57	491 354.7	376	2657
Waiting:	55	287 292.6	147	1844
Total:	430	2690 639.2	2722	6805

Percentage of the requests served within a certain time (ms)

50%	2722
66%	2915
75%	3029
80%	3124
90%	3354
95%	3604
98%	3915
99%	4230
100%	6805 (longest request)

What are Crypto Express Cards

```
andy@ahubbase:~$ sar -u 10 1000
```

```
Linux 5.4.0-33-generic (ahubbase.s390.mainline.com) 06/10/2020 _s390x_ (4 CPU)
```

	CPU	%user	%nice	%system	%iowait	%steal	%idle
01:00:31 PM	all	0.00	0.00	0.00	0.00	0.00	100.00
01:00:41 PM	all	44.61	0.00	0.15	0.00	0.55	54.69
01:00:51 PM	all	58.29	0.00	0.02	0.00	0.50	41.19
01:01:01 PM	all	68.47	0.00	0.15	0.00	0.62	30.76
01:01:11 PM	all	63.24	0.00	0.07	0.00	0.60	36.09
01:01:21 PM	all	61.07	0.00	0.12	0.00	0.52	38.28
01:01:31 PM	all	60.63	0.00	0.07	0.00	0.52	38.77
01:01:41 PM	all	68.92	0.00	0.17	0.00	0.62	30.28
01:01:51 PM	all	67.29	0.00	0.12	0.00	0.55	32.04
01:02:01 PM	all	63.70	0.00	0.10	0.00	0.55	35.66
01:02:11 PM	all	63.02	0.00	0.10	0.00	0.52	36.36
01:02:21 PM	all	62.19	0.00	0.05	0.00	0.57	37.19
01:02:31 PM	all	60.19	0.00	0.10	0.00	0.57	39.14
01:02:41 PM	all	60.11	0.00	0.12	0.00	0.60	39.17
01:02:51 PM	all	67.73	0.00	0.17	0.00	0.60	31.50
01:03:01 PM	all	67.82	0.00	0.07	0.00	0.60	31.51
01:03:11 PM	all	71.54	0.00	0.10	0.00	0.67	27.69
01:03:21 PM	all	26.34	0.00	0.02	0.00	0.17	73.46
01:03:31 PM	all	0.00	0.00	0.05	0.00	0.00	99.95

```
Average: all 54.51 0.00 0.09 0.00 0.49 44.90
```

WITHOUT CPACF OR CRYPTO EXPRESS CARDS

```
ab -n 3000 -c 50 -Z DHE-RSA-AES128-SHA https://10.0.10.194/
```

Show Processing Offloaded By Using The Crypto Cards

```
andy@DESKTOP-T02VH7C:~$ ab -n 3000 -c 50 -Z DHE-RSA-AES128-SHA https://10.0.10.196/  
This is ApacheBench, Version 2.3 <$Revision: 1843412 $>  
Copyright 1996 Adam Twiss, Zeus Technology Ltd, http://www.zeustech.net/  
Licensed to The Apache Software Foundation, http://www.apache.org/
```

```
Benchmarking 10.0.10.196 (be patient)  
Completed 300 requests  
Completed 600 requests  
Completed 900 requests  
Completed 1200 requests  
Completed 1500 requests  
Completed 1800 requests  
Completed 2100 requests  
Completed 2400 requests  
Completed 2700 requests  
Completed 3000 requests  
Finished 3000 requests
```

```
Server Software:    Apache/2.4.41  
Server Hostname:   10.0.10.196  
Server Port:       443  
SSL/TLS Protocol:  TLSv1.2,DHE-RSA-AES128-SHA,2048,128  
Server Temp Key:   DH 2048 bits
```

```
Document Path:     /  
Document Length:   10918 bytes
```

Show Processing Offloaded By Using The Crypto Cards

Concurrency Level: 50
Time taken for tests: 32.172 seconds
Complete requests: 3000
Failed requests: 0
Total transferred: 33576000 bytes
HTML transferred: 32754000 bytes
Requests per second: 93.25 [#/sec] (mean)
Time per request: 536.200 [ms] (mean)
Time per request: 10.724 [ms] (mean, across all concurrent requests)
Transfer rate: 1019.18 [Kbytes/sec] received

Connection Times (ms)

	min	mean[+/-sd]	median	max
Connect:	197	323 149.4	298	1751
Processing:	57	201 167.9	128	1339
Waiting:	54	108 72.8	81	1046
Total:	262	524 237.2	435	2319

Percentage of the requests served within a certain time (ms)

50%	435
66%	582
75%	635
80%	652
90%	737
95%	982
98%	1320
99%	1528
100%	2319 (longest request)

What are Crypto Express Cards

```
root@ahubcrpt:~# sar -u 10 1000
```

```
Linux 5.4.0-33-generic (ahubcrpt)    06/10/2020    _s390x_ (4 CPU)
```

01:15:02 PM	CPU	%user	%nice	%system	%iowait	%steal	%idle
01:15:12 PM	all	0.10	0.00	0.10	0.00	0.17	99.63
01:15:22 PM	all	0.60	0.00	0.45	0.00	0.94	98.01
01:15:32 PM	all	0.67	0.00	0.45	0.00	0.92	97.97
01:15:42 PM	all	0.55	0.00	0.42	0.00	0.77	98.26
01:15:52 PM	all	0.00	0.00	0.00	0.00	0.00	100.00
01:16:02 PM	all	0.00	0.00	0.02	0.00	0.00	99.98
01:16:12 PM	all	0.00	0.00	0.00	0.00	0.00	100.00
01:16:22 PM	all	0.00	0.00	0.02	0.00	0.00	99.98

```
Average:    all    0.24    0.00    0.18    0.00    0.35    99.22
```

WITH CPACF AND CRYPTO EXPRESS CARDS

```
ab -n 3000 -c 50 -Z DHE-RSA-AES128-SHA https://10.0.10.196
```

Show Processing Offloaded By Using The Crypto Cards

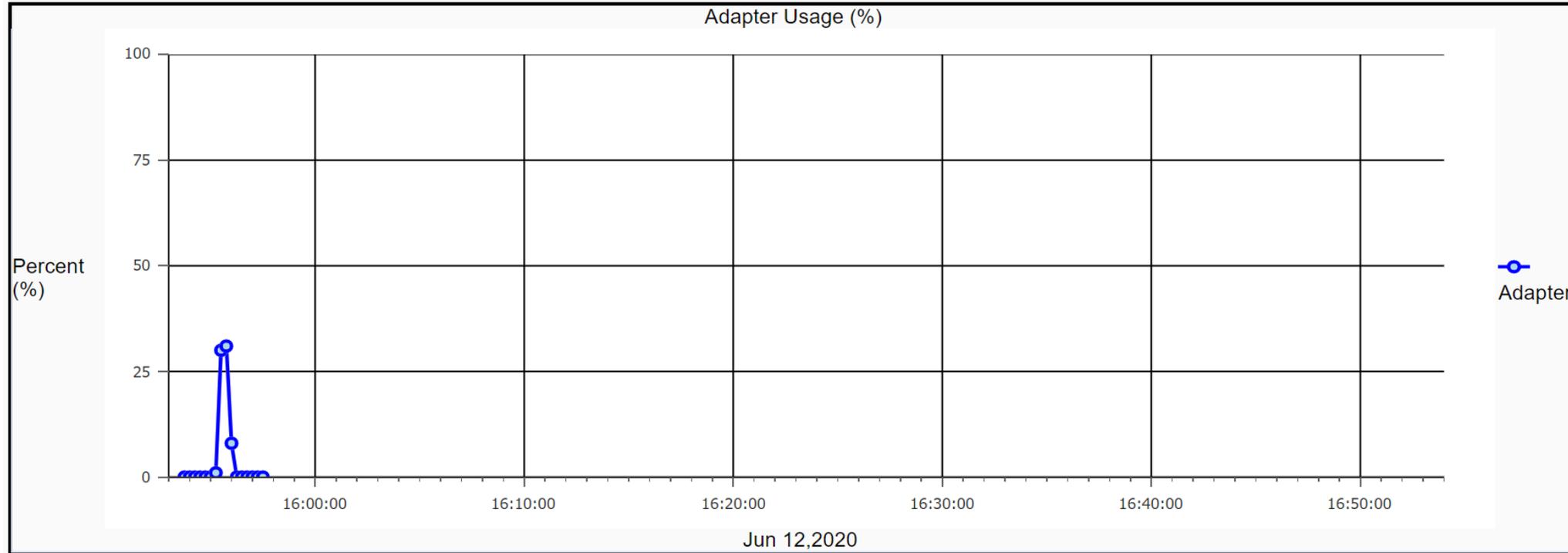
15:53 plus time period



Dashboard Histogram Display - P00298A8

Adapter display for Channel ID 013C

Display type: Adapter Usage
Frequency and duration: 15 seconds for 1 hour



Clear Pause Export Close Help

Show Processing Offloaded By Using The Crypto Cards

15:53 plus time period



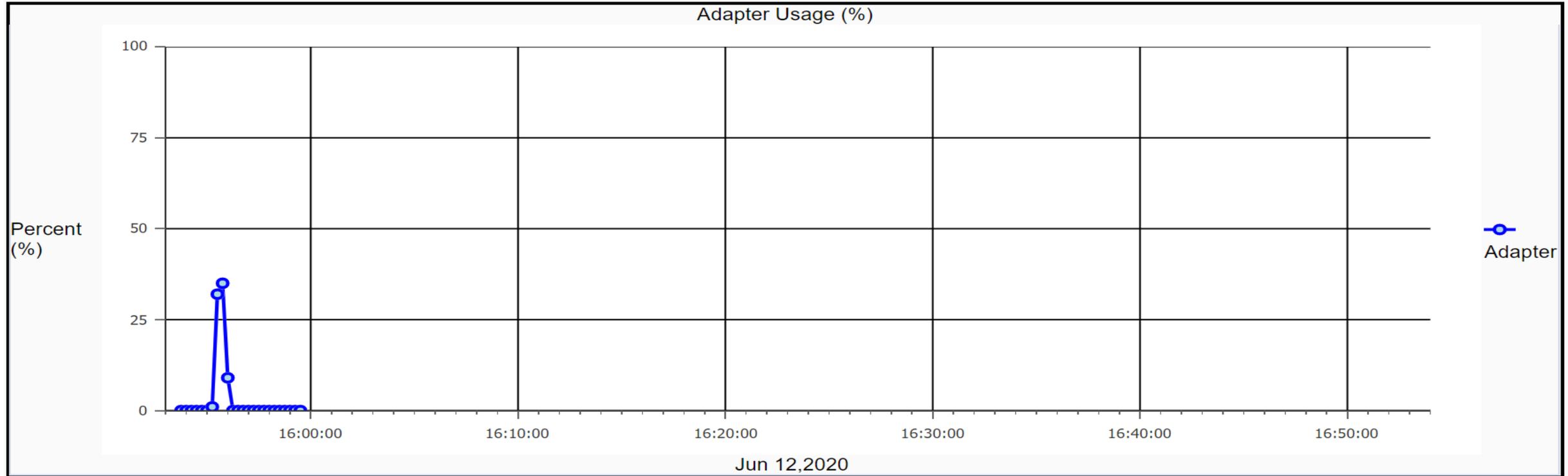
Dashboard Histogram Display - P00298A8

Adapter display for Channel ID 011C

Display type: Frequency and duration:

Adapter Usage

15 seconds for 1 hour



Clear Pause Export Close Help

How to Implement Crypto Express Cards with Linux on z

References

- Z15 Technical Guide
 - <http://www.redbooks.ibm.com/abstracts/sg248851.html?Open>
- Z15 Configuration Setup
 - <http://www.redbooks.ibm.com/abstracts/sg248860.html>
- Cryptographic hardware support for IBM Z and IBM LinuxONE
 - https://www.ibm.com/support/knowledgecenter/en/linuxonibm/liaaf/sec_hw_supp.html
- Hardware cryptographic support of IBM z Systems for OpenSSH in RHEL 7.2 and SLES 12 SP1 - Older
 - http://www.vm.ibm.com/devpages/spera/MG_OpenSSH.pdf
- Hardware cryptographic support for IBM Z and IBM LinuxONE with Ubuntu Server - Older
 - https://people.canonical.com/~fheimes/MG_HWCrypto_with_Ubuntu_on_z.pdf
- **New** – z/VM 7.1 CP Planning and Administration Guide – Chapter 5
 - <http://www.vm.ibm.com/library/710pdfs/71627104.pdf>
- KVM and Virtual Guest Setup for Crypto Express
 - https://www.ibm.com/support/knowledgecenter/en/linuxonibm/com.ibm.Linux.z.lxhq/lxhq_c_welcome.html
- Linux Setup for Crypto Express when install directly into and LPAR
 - <https://www.ibm.com/support/knowledgecenter/en/linuxonibm/liaab/icwhatsnew.html>
- Running Docker Containers on IBM Z with Crypto Express
 - https://www.ibm.com/support/knowledgecenter/en/linuxonibm/com.ibm.Linux.z.ldvd/ldvd_c_welcome.html
- SSL/TLS Cipher Suites – Nice overview of cipher suites
 - <https://www.thesslstore.com/blog/cipher-suites-algorithms-security-settings/>

Conclusion

- Your company's data is one of your most important assets and needs to be protected
- Data in flight is a critical part of this protection
- By using Crypto Express cards you can significantly reduce the consumption of processor resources while providing the ability to service a great number of SSL/TLS sessions used in web serving for example
- Different cipher suites will have different results – you can choose which ciphers and protocols are used for your websites
- I discussed and demonstrated the Crypto Express Card configured as an Accelerator, but remember that these cards can do much more and can be configured to satisfy many different types of security needs
- If you don't have crypto cards on your system and you want to test out various cipher suites and Linux configurations , Mainline can work with you to set up demonstrations using our system to show what the possible benefits would be for adding crypto express cards to your installation



Questions?



Mainline

The Technology Partner for Business Results