



IBM

zSeries

Vanguard Session J5

May 10, 2005

Ernie Nachtigall CISSP;CISA

Using the z890/z990 Encryption Facilities

ON DEMAND BUSINESS™

Trademarks

The following are trademarks of the International Business Machines Corporation in the United States and/or other countries.

AIX*	Database 2	e-business logo*	MVS	Resource Link
AIX/ESA*	DB2*	e((logo)server*	MVS/DFP	RMF
C/MVS	DB2 Connect	ESCON	MVS/ESA	S/390*
C/370	developerWorks*	FICON*	OS/2*	S/390 Parallel Enterprise Server
CICS*	DFSMS/MVS*	ibm.com*	OS/2 WARP*	WebSphere*
CICS/ESA*	DFSMSdftp	IBMLink	OS/390*Parallel Sysplex*	z/Architecture
CICS/MVS*	DFSMSdss	MQSeries*	Processor Resource/Systems Manager	z/OS*
COBOL/370	DFSMSHsm	Multiprise*	PR/SM	z/VM*
			RACF*	zSeries*

* Registered trademarks of IBM Corporation

The following are trademarks or registered trademarks of other companies.

Linux is a registered trademark of Linus Torvalds

Java and all Java-related trademarks and logos are trademarks of Sun Microsystems, Inc., in the United States and other countries

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

Microsoft, Windows and Windows NT are registered trademarks of Microsoft Corporation.

SET and Secure Electronic Transaction are trademarks owned by SET Secure Electronic Transaction LLC.

* All other products may be trademarks or registered trademarks of their respective companies.

Notes:

Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.

IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.

All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.

This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.

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

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

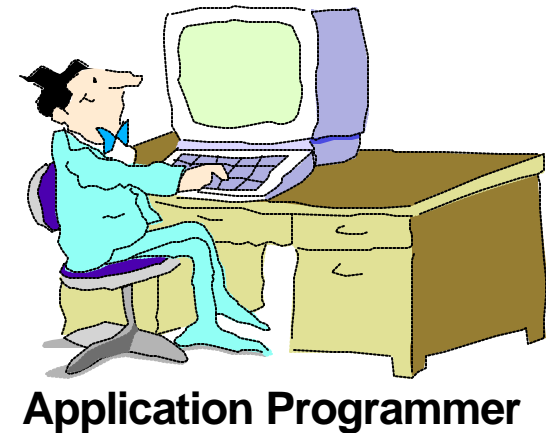
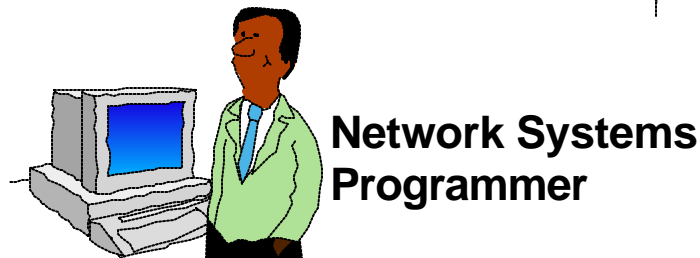
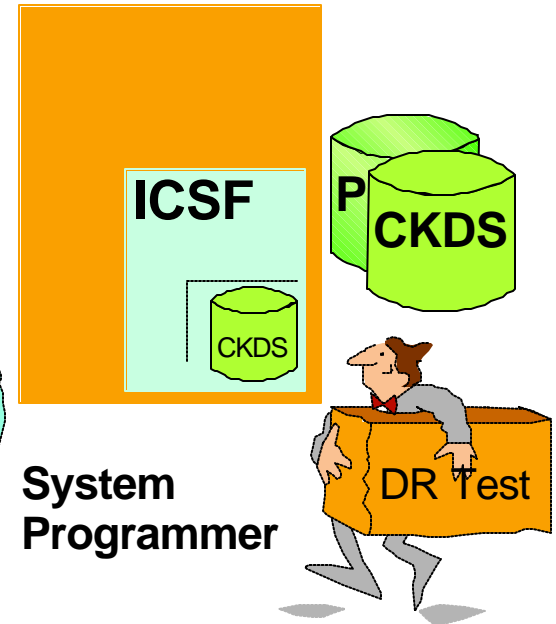
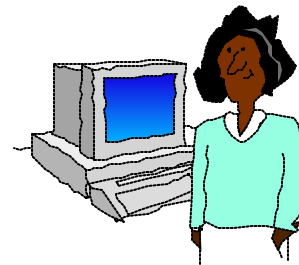
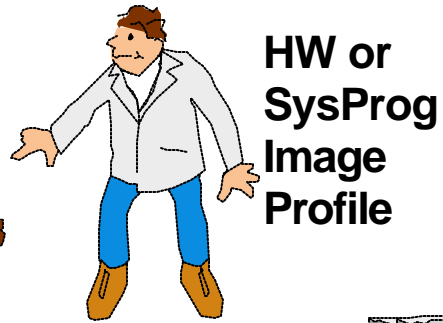
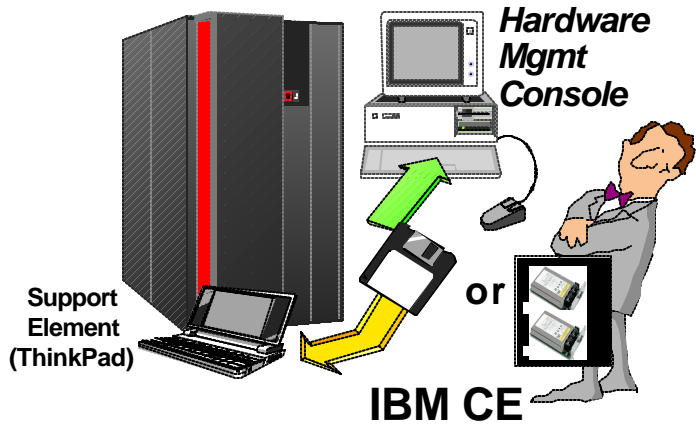
Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

brief BIO

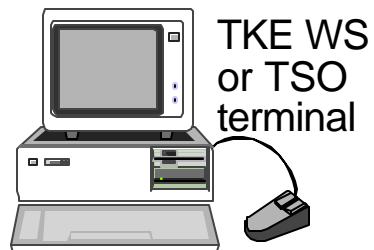
Ernest has been involved in the banking I/T area since 1970 and in cryptography since 1971. He has been involved with or assisted in authoring teller, 3270, ABM, POS, CSPIN applications and is self-taught in COBOL;C;BASIC;PLI;PL/X and ASM.

Since 1988 he has been involved in the design, coding and support of various cryptographic implementations (IBM 3624, 4700, 4730, 4780, 4753, PCF, CUSP, ICSF, Racal/Zaxus/Thales, Atalla, Eracom). Currently, he is the IBM Crypto Regional Designated Specialist for the Americas northern region and works closely with the Washington Systems Center security team.

MainFrame Crypto Installation: Welcome to the Party



TKE or ICSF Administrator



S/390 and zSeries Crypto Solution

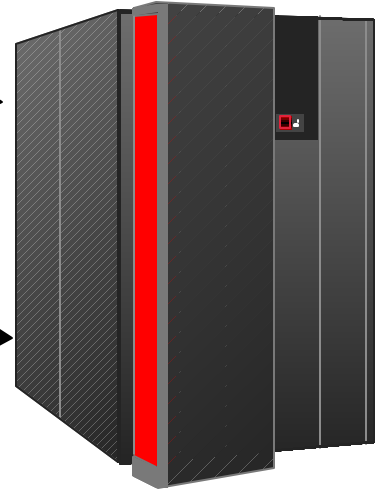
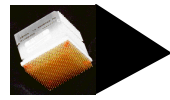
S/390 z800

z890 z990

Peripheral z900
 Component Interconnect
 Crypto Coprocessor
 PCICC/PCICA



Crypto Coprocessor
 Facility CCF



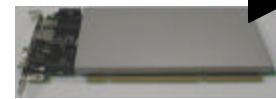
FC3863 CPACF
 clear key



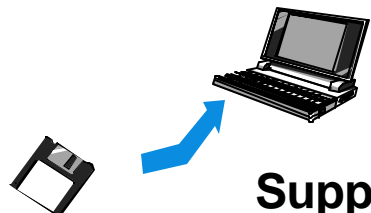
PCICA



PCIxCC
 no PCICC



PCIxCC
 CEX2C
 z890 z990



Support Element

Trusted Key Entry



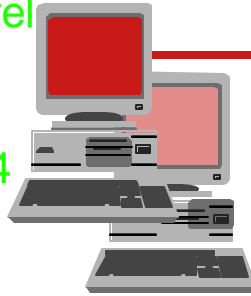
4758 Card

TKE Support Based on ICSF Version Release

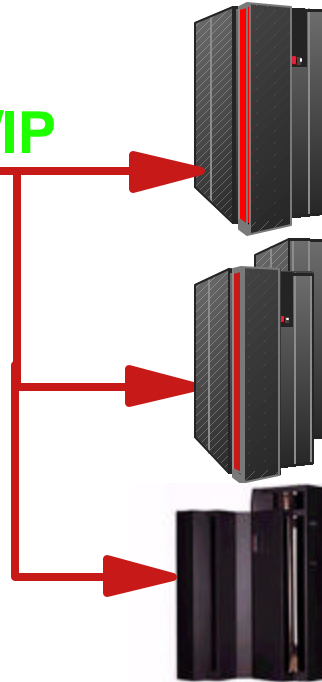
TKE workstation V3

TKE code level 3.0

4758 card
OS/2 Warp 4
no Personal Security Card



TCP/IP



S/390 **G5-G6** with **PCICC**
ICSF 2.3 needed (OS/390 Rel.9)

S/390 - **G3 to G6** w/o **PCICC**
ICSF 2.1,2.2 (APAR needed) or
ICSF 2.3 (OS/390 2.9 or higher)

zSeries - **with or without PCICC**
z/OS ICSF
PCICA
All



TKE workstation V4

Trusted Key Entry

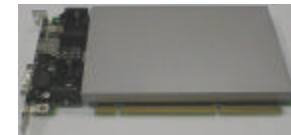
4758 Card



TCP/IP



z890/z990 HCR770A HCR770B
HCR7720



PCIXCC
CEX2C
z890 z990

Clear Key Crypto (CPACF)

High Speed Symmetric Algorithms imbedded in each CP
available via ICSF as API's (CSNBSYD/CSNBSYE) or as new operation codes (OP CODES)

"SOFTWARE ENCRYPTION" with algorithm code in hardware

DES TDES SHA-1 (MD5 and AES via ICSF)

Encryption/Decryption keys are clear (not encrypted) in user address space

typically not appropriate or allowed for sensitive processing such as VISA, MasterCard, INTERAC, LINK

can be mitigated to offer certain in-house functions

file archive to tape

ICSF user defined functions, keys in clear in the ICSF address space only

Specifically designed for WEB

(SSL/TLS/TN3270/FIREWALL) type applications, short duration applications, throw-away key values

z890/z990 vs z900 Base Crypto: Clear vs Secure

z890/z990 Base Crypto

*Central Processor Assist for Cryptographic Function (CPACF)
Requires hardware setup, configuration data load, ICSF active
Does Not require Master Key Loading*

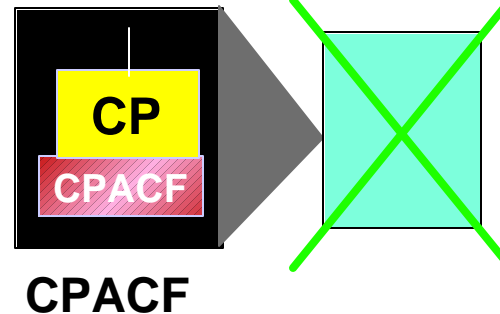
z800/z900 Base Crypto

*Cryptographic Coprocessor Facility (CCF)
Requires hardware setup, configuration data load, ICSF active
Requires Master Key Loading*

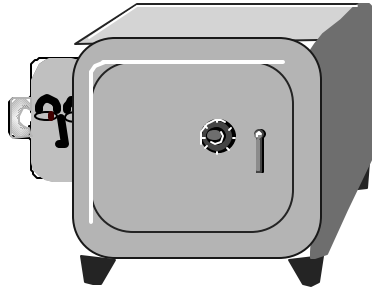


CCF

MK SMK	AUX KMMK
MK SMK	AUX KMMK
:	:
MK SMK	AUX KMMK



Secure Key Operations & Clear Key Operations



Secure operation implies that the interruption of the activity will not expose any unprotected key value.

Previous IBM crypto products including software require secure key usage

Key Value Protection?

Actual value used in cryptographic algorithm is also encrypted or securely protected from view

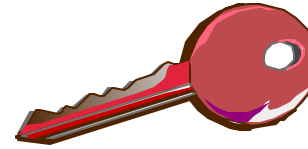
Level of protection

Actual key value is not exposed to view or copy once imported into a cryptographic system

Actual key value is protected until use is required.

Actual key value is restored and used for cryptographic operation within crypto system

z990 Cryptographic Hardware



Base Crypto - Central Processor Assist for Cryptographic Function (CPACF)

Performs clear key encrypt/decrypt, MAC and SHA-1 hashing

Feature Code 3863 Required to obtain Configuration Data

No feature code to indicate crypto hardware

Accelerator for SSL - PCI Cryptographic Accelerator (PCICA)

Performs decrypt/encrypt of pre-master secret during handshake

Handles same throughput rate per card as on z900, approx. (2100 handshakes per second)

CPACF and Feature Code 3863 required

May Require Software updates

For SSL users - no exploitation of crypto hardware for SSL handshake performance improvements without ordering PCICA, PCIXCC or CEX2C!!!!

z990 Cryptographic Hardware . . .

Trusted Key Entry Workstation (TKE) V4

Cannot be ordered without PCIXCC selection

TKE V4 MCL is Feature Code 0853

Only TKE V3 Workstations can be upgraded by MCL

Cannot be used unless ICSF HCR770A (HCR770B HCR7720)

Only for Master Key Entry

Entry for Application Keys not supported when TKE is on z990 unless TKE 4.1

TKE 4.2 adds Smart Card reader/writer

Secure Key Support - PCIXCC CEX2C

Performs most functions allowed on CCF and PCICC (based on ICSF APIs supported)

Requires ICSF HCR770A/HCR770B/HCR7720 - Web Deliverable name of z990 Cryptographic Support



CCF

MK

SMK

AUX

KMMK

Sym

Asym

NSym

NAsym

OSym

OAsym



PCICC



PCIXCC/CEX2C

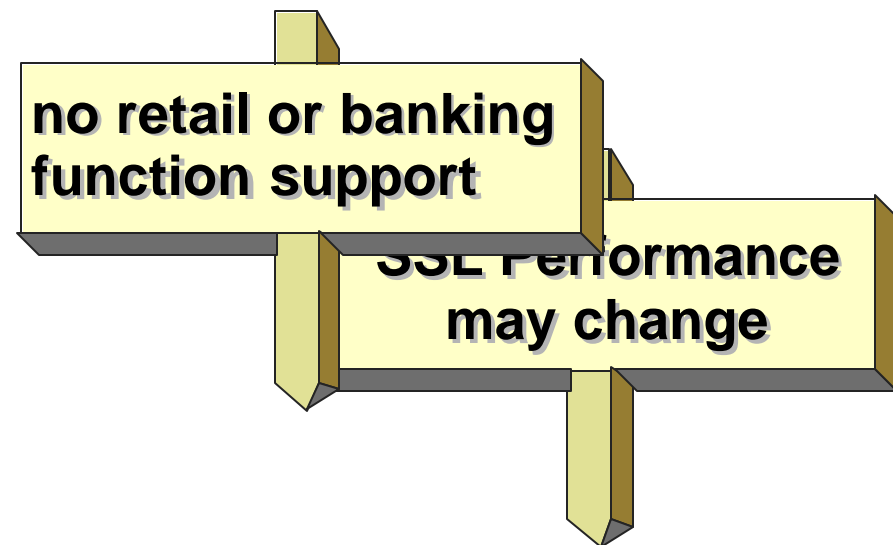
Clear vs Secure Has Meaning on z890/z990

With CPACF

- No protected key values used with API
- CSNBSYE/SYD
 - ▶ for data privacy
 - ▶ DES / TDES / (AES)
- CSNBECO/CSNBDCO
 - ▶ for data privacy
 - ▶ DES - ECB; no chaining
- SHA-1 and (MD5)
- Utility based functions
- No Performance Support with Handshake

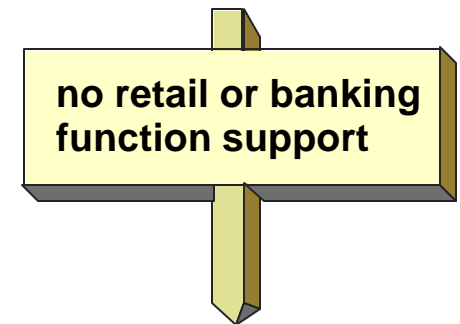
With PCICA

- CSNDPKE/PKD
 - ▶ to provide acceleration during SSL handshake
- No Hardware Acceleration for Client Authentication



Clear vs Secure Has Meaning on z890/z990 . . .

- TKE Required to comply with dual key part entry and no exposure of key parts within network during entry
 - ▶ TKE 4.1+ required for application key entry
 - ▶ else
 - Need to have a z900/z800, 9672, or 7060 for this
- PCIXCC Required to support
 - ▶ DUKPT, PIN processing applications
 - ▶ Retained Keys
 - ▶ Secure Application Keys in CKDS or application storage
 - ▶ Any old crypto applications that might be running production
 - PCF/CUSP
 - IDCAMS Repro using ENCIPHER/DECIPHER



Clear vs Secure Has Meaning on z890/z990 . . .

SSL based applications may not have the same performance as on z900/z800 when migrated to z990

Same throughput for the decrypt of premaster secret

Impact may be felt if requiring the SSL optional actions

Server requires temporary RSA key because certificate key length or purpose cannot be used in session

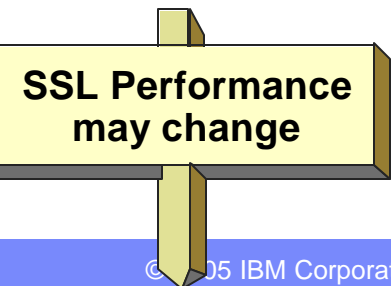
Client Authentication required

Impact is also due to CPACFs not supporting the RSA functions supported on CCFs

Plan for Performance

Expectations from previous benchmarks on non-z990 or on service level objectives

PCICA/CEX2C features may be required to offset CCF loss



z890/z990 in a Sysplex

Generally Sysplex members are on same operating system release level

z/OS with the necessary compatibility code levels may not be available for all systems in the sysplex

*z900, z800, 9672, etc. may be in sysplex and will not be at the same release level
Based on operational usage and specific site considerations this could be an issue*

ICSF might be required to operate at different release levels

TKE 4.1 use on a z890/z990 for all application key entry

Run TKE TP on z990 MK/User key entry when PCIXCC/CEX2C installed

Test all production applications that depend on using the crypto hardware to ensure that nothing surprises you

New OP CODES

5 New Machine Instructions

Documented in z/OS™ 1.5 Principles of Operation (POP)

Never before have crypto instructions been documented
Problem state instructions, as such, can be used directly in
applications without going through ICSF.

Instruction Names and Mnemonics

Cipher Message (KM)

Cipher Message with Chaining (KMC)

Compute Intermediate Message Digest (KIMD)

Compute Last Message Digest (KLMD)

Compute Message Authentication Code (KMAC)

CPACF Enabled

Instance information










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

Lockout disruptive tasks: Yes No

System mode: Logically partitioned
Alternate SE Status: Operating

Dual AS power maintenance: Fully Redundant
CP Assist for Cryptographic Functions: Installed

Acceptable CP/CHPID status

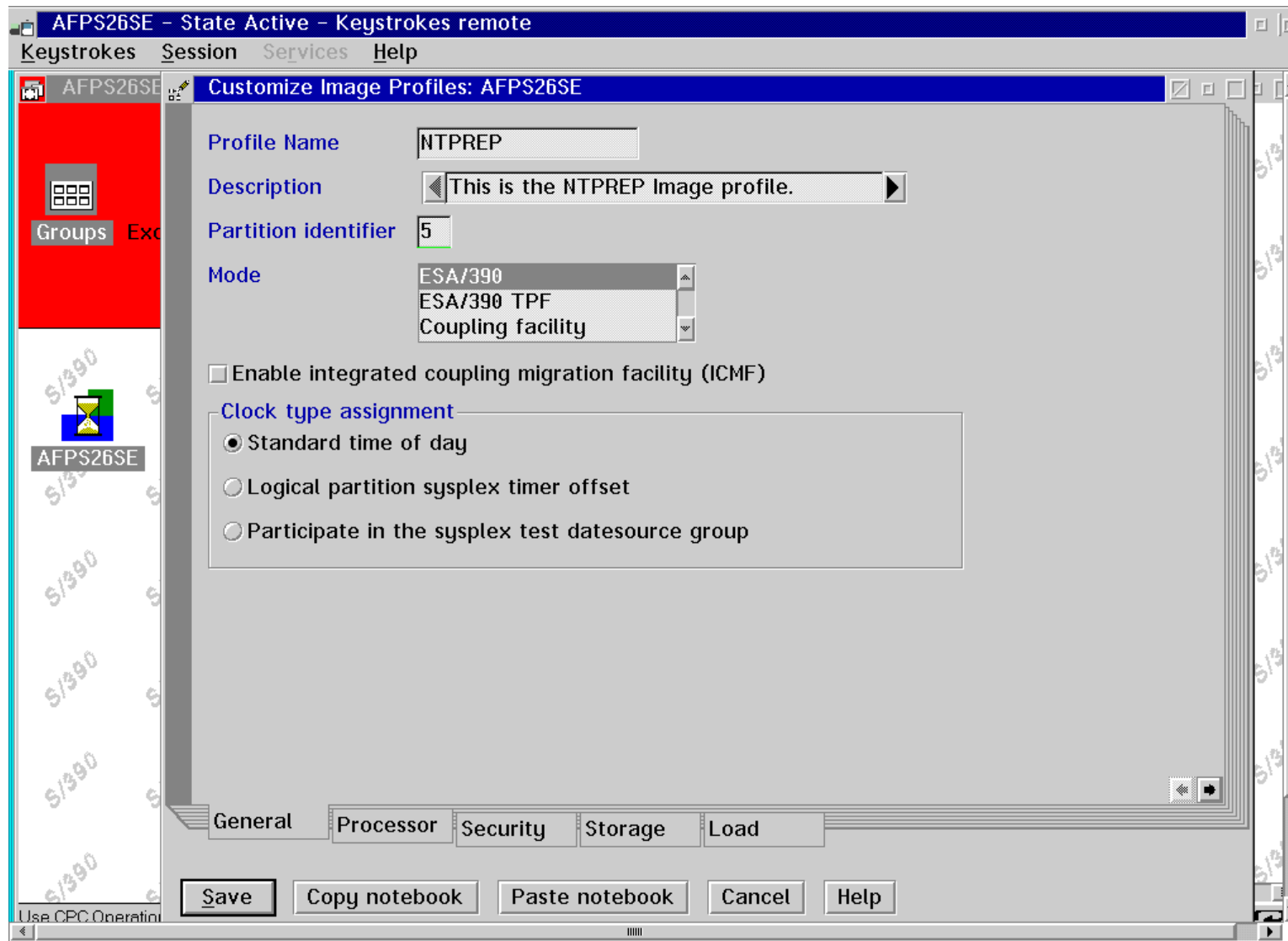
<input checked="" type="checkbox"/> Operating - 	<input type="checkbox"/> Power save - 	<input type="checkbox"/> No power - 
<input type="checkbox"/> Not Operating - 	<input type="checkbox"/> Exceptions - 	<input type="checkbox"/> Status check - 
<input checked="" type="checkbox"/> Acceptable - 	<input type="checkbox"/> Service Required - 	<input type="checkbox"/> Degraded - 

Product information

Machine type / model:	002084 / A08-385	Manufacturer:	IBM
Machine serial:	02 - 0026A3A	CPC serial:	000020026A3A
Machine sequence:	000000026A3A	CPC location:	A19B
Plant of manufacture:	02	CPC identifier:	00

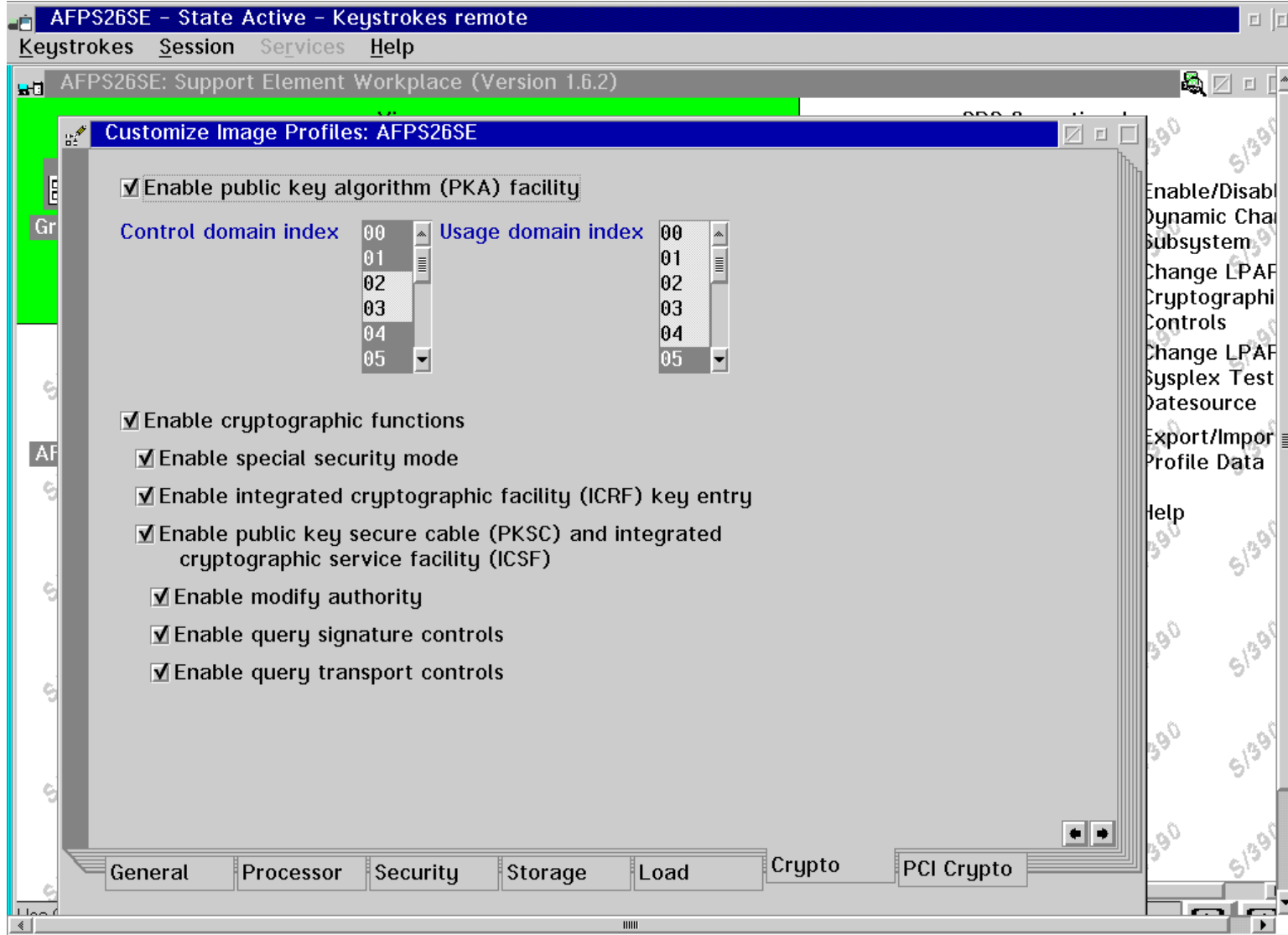
Save Change Options... Diagnose Messages... Cancel Help

Profile Customization



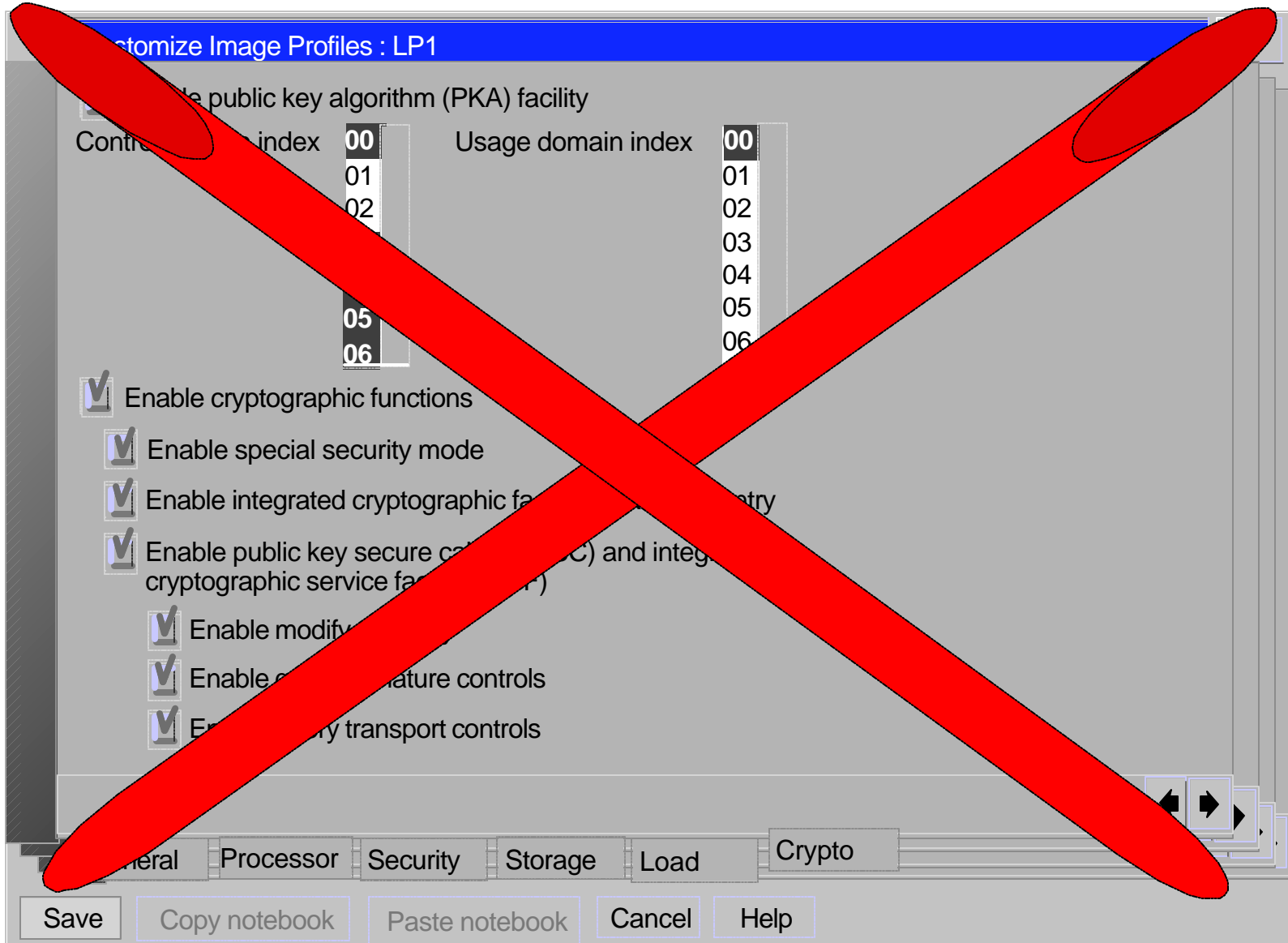
Original chart provided courtesy of ITSO.

Domain Associations



Original chart provided courtesy of ITSO.

Defining Coprocessor Characteristics



LPAR DEFINITION PCI TAB

Customize Image Profiles: P00ESIM2

Control domain index: 00, 01, 02, 03, 04, 05

Usage domain index: 00, 01, 02, 03, 04, 05

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

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

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

General | Processor | Security | Storage | Options | Load | PCI Crypto

Save | Copy notebook | Paste notebook | Cancel | Help

Installation Setup

- Install FMID HCR7708
- Install Feature 3863 (CPACF)
 - ▶ does not replace 08x5. Pre-req for PCI adapters
- Install WEB download HCR770A (HCR770B/HCR7720)
- Add libraries to LNKLST
 - ▶ csf.scsfmod0 (authorized)
 - ▶ cee.sceerun
- Add CSFDAUTH and CSFDPKDS to IKJTSOxx in AUTHPGM and AUTHTSF also CSFTTKE if using TKE
- Create CKDS and PKDS Create ICSF PROC
- Create ICSF INIT Params
- Install ICSF ISPF panels
- Start ICSF
- Install Master Keys
- Check www.ibm.com/support/techdocs/atmastr.nsf search on crypto for hints, tips, tools, free software



HCR770A ----- Integrated Cryptographic Service Facility-----

OPTION ==>

Enter the number of the desired option.

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

Licensed Materials - Property of IBM

5694-A01 (C) Copyright IBM Corp. 1989, 2003. All rights reserved.

US Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Press ENTER to go to the selected option

----- ICSF Coprocessor Management ----- Row 1 to 6 of 6
COMMAND ==> SCROLL ==> PAGE

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

COPROCESSOR	SERIAL NUMBER	STATUS
-----	-----	-----
. A00		ACTIVE
. A01		ACTIVE
. A02		ACTIVE
. A03		ACTIVE
. E04	93002173	ACTIVE
. F05	93002184	ACTIVE
. X06	93001166	ACTIVE
. X07	93001449	ACTIVE
***** Bottom of data *****		

COMMAND ==>

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

Prefix	Type of cryptographic coprocessor	Valid action characters
-----	-----	-----
A	PCI Cryptographic Accelerator	a, d
E	Crypto Express2 Coprocessor	a, d, e, k, r, s
F	Crypto Express2 Coprocessor	a, d
X	PCI X Cryptographic Coprocessor	a, d, e, r, s

Action characters: (entered on the left of the coprocessor number)

- 'a' Makes available a coprocessor previously deactivated by a 'd'.
- 'd' Makes a coprocessor unavailable.
- 'e' Selects the PCIXCC/CEX2C for clear master key entry.
- 'k' Selects the PCIXCC/CEX2C for DES operational key load.
- 'r' Causes the PCIXCC/CEX2C default role to be displayed.
- 's' Causes complete hardware status to be displayed for an PCIXCC/CEX2C.

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

The action character 'k' may be specified on only one coprocessor.

F3 = END HELP

----- ICSF - Coprocessor Hardware Status -----

COMMAND ==>

SCROLL ==>

CRYPTO DOMAIN: 3

REGISTER STATUS	COPROCESSOR X06	COPROCESSOR X07	
		More:	+
Crypto Serial Number	: 93001166	93001449	
Status	: ACTIVE	ACTIVE	
Symmetric-Keys Master Key			
New Master Key register	: EMPTY	EMPTY	
Verification pattern	:		
Hash pattern	:		
	:		
Old Master Key register	: EMPTY	EMPTY	
Verification pattern	:		
Hash pattern	:		
	:		
Current Master Key register	: VALID	VALID	
Verification pattern	: E9572EFFDAA14AA8	E9572EFFDAA14AA8	
Hash pattern	: DD20A717C842FC0C	DD20A717C842FC0C	
	: 5D018950FEB7F9B4	5D018950FEB7F9B4	
Asymmetric-Keys Master Key			
New Master Key register	: EMPTY	EMPTY	
Hash pattern	:		
	:		
Old Master Key register	: VALID	VALID	
Hash pattern	: AB519EF52BAC4855	AB519EF52BAC4855	
	: A8F15364996604B6	A8F15364996604B6	
	:		
Current Master Key register	: VALID	VALID	
Hash pattern	: AB519EF52BAC4855	AB519EF52BAC4855	
	: A8F15364996604B6	A8F15364996604B6	

Press ENTER to refresh the hardware status display.

----- ICSF Coprocessor Management ----- Row 1 to 6 of 6
COMMAND ==> SCROLL ==> PAGE

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

COPROCESSOR	SERIAL NUMBER	STATUS
-----	-----	-----
. A00		ACTIVE
. A01		ACTIVE
. A02		ACTIVE
. A03		ACTIVE
. E04	93002173	ACTIVE
. F05	93002184	ACTIVE
. X06	93001166	ACTIVE
. X07	93001449	ACTIVE
***** Bottom of data *****		

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

	COPROCESSOR	SERIAL NUMBER	STATUS
	-----	-----	-----
.	A00		ACTIVE
.	A01		ACTIVE
.	A02		ACTIVE
.	A03		ACTIVE
.	E04	93002173	ACTIVE
.	F05	93002184	ACTIVE
e	X06	93001166	ACTIVE
e	X07	93001449	ACTIVE

***** Bottom of data*****

----- ICSF - Clear Master Key Entry -----

COMMAND ==>

Symmetric-keys new master key register : EMPTY

Asymmetric-keys new master key register : EMPTY

Specify information below

Key Type ==> sym-mk (SYM-MK, ASYM-MK)

Part ==> first (RESET, FIRST, MIDDLE, FINAL)

Checksum ==> 3f

Key Value ==> 0123456789abcdef

==> fedcba9876543210

==> 0000000000000000 (ASYM-MK only)

Press ENTER to process.

Press END to exit to the previous menu.

----- ICSF - Master Key Management -----

OPTION ===>

Enter the number of the desired option.

- 1 INIT/REFRESH CKDS - Initialize a Cryptographic Key Data Set or activate an updated Cryptographic Key Data Set
- 2 SET MK - Set a DES/symmetric-keys master key
- 3 REENCIPHER CKDS - Reencipher the CKDS prior to changing the DES master key
- 4 CHANGE MK - Change the DES/symmetric-keys master key and activate the reenciphered CKDS
- 5 INITIALIZE PKDS - Initialize or update a PKDS Cryptographic Key Data Set header record
- 6 REENCIPHER PKDS - Reencipher the PKA Cryptographic Key Data Set
- 7 ACTIVATE PKDS - Activate the PKDS after it has been reenciphered
- 8 REFRESH CACHE - Refresh the PKDS Cache if enabled

Press ENTER to go to the selected option.

Press END to exit to the previous menu.

----- ICSF - Status Display ----- Row 1 to 25 of 95

COMMAND ==>

Enabled access control points from the default role for X06 domain 3

Access Control Manager - Read role

Authorize UDX

Clear Key Import/Multiple Clear Key Import

Clear New ASYM Master Key Register

Clear New SYM Master Key Register

Clear PIN Encrypt

Clear PIN Generate - GBP

Clear PIN Generate - Interbank

Clear PIN Generate - VISA PVV

Clear PIN Generate - 3624

Clear PIN Generate Alternate - VISA PVV

Clear PIN Generate Alternate - 3624 Offset

Combine ASYM Master Key Parts

Combine SYM Master Key Parts

Control Vector Translate

Cryptographic Variable Encipher

Data Key Export

Data Key Export - Unrestricted

Data Key Import

Data Key Import - Unrestricted

Decipher

Digital Signature Generate

Digital Signature Verify

Diversified Key Generate - single length or same halves

Diversified Key Generate - CLR8-ENC

----- ICSF - Administrative Control Functions -- Row 1 to 4 of 4
COMMAND ==> SCROLL ==> PAGE

Active CKDS: CSF.Z990DEC.CKDS

Active PKDS: CSF.Z990DEC.PKDS

To change the status of a control, enter the appropriate character
(E - ENABLE, D - DISABLE) and press ENTER.

FUNCTION	STATUS
-----	-----
. Dynamic CKDS Access	ENABLED
. PKA Callable Services	DISABLED
. PKDS Read Access	DISABLED
. PKDS Write, Create, and Delete Access	DISABLED

***** Bottom of data *****

----- ICSF - Installation Option Display -- Row 1 to 12 of 12

COMMAND ===>

SCROLL ===> PAGE

Active CKDS: CSF.Z990DEC.CKDS

Active PKDS: CSF.Z990DEC.PKDS

OPTION		CURRENT VALUE
-----		-----
CHECKAUTH	RACF check authorized callers	NO
COMPAT	Allow CUSP/PCF compatibility	NO
DOMAIN	Current domain index or usage domain index	3
KEYAUTH	Key Authentication in effect	NO
CKTAUTH	CKT Authentication in effect	NO
SSM	Allow Special Secure Mode	YES
TRACEENTRY	Number of trace entries active	1000
USERPARM	User specified parameter data	USERPARM
REASONCODES	Source of callable services reason codes	ICSF
PKDSCACHE	PKDS Cache size in records	64
WAITLIST	Source of CICS Wait List if CICS installed	default

***** Bottom of data *****

Removed Interfaces

Support for DSA signatures and key generation.

Support for ANSI x9.17 services (offset and notarization), and associated key types.

Support for Ciphertext_translate(CSNBCTT).

Support for German Bank Pool - Pin Offset

Support for CSFUDK - use CSNBDKG instead.

Support for CDMF (40 bit encryption)

Sample CIPHER Throughputs

Totally unscientific, empirical, but consistent results

Other work being performed on server

z800 2 CCF processors, LPAR with 2 CP's

z990 B16 LPAR with 2 CP's

2 PCIxCC adapters

4 PCICA adapters (not used)

FILCRYPT - read a file

start job timer

block n records

start cipher timer

encipher n records

stop cipher timer

save shortest/longest times and data size ciphered

write x records to output using fixed block records

stop job timer

FIDCRYPT - recover the file

same processes as FILCRYPT

CAN OVERLAP BUFFERS!!!

Sample CIPHER Throughputs ...cont

z800 Encipher, TDES 24 byte key

1011004 records; 80 bytes each; 80,880,320 bytes

one record at a time about 80 bytes per encipher call

Elapsed clock time: 212.853190 seconds

Cipher time (ICSF): 198.632159 seconds

Average cipher time: 0.000196 seconds

Sample CIPHER Throughputs ...cont

z800 Decipher, TDES 24 byte key

1107953 records (includes control/padding); 80,880,320 bytes recovered

one record at a time, about **72** bytes per decipher call

Elapsed clock time: 228.881434 seconds

Cipher time (ICSF): **213.202982** seconds

Average cipher time: 0.000192 seconds

z800 Decipher, TDES 24 byte key

1107953 records (includes control/padding); 80,880,320 bytes recovered

12237 records at a time, about **978928** bytes per decipher call

Elapsed clock time: 20.064974 seconds

Cipher time (ICSF): **5.348829** seconds

Average cipher time: 0.064443 seconds

Sample CIPHER Throughputs ...cont

z990 (PCIxCC) Encipher, TDES 24 byte key
1011004 records; 80 bytes each; 80,880,320 bytes
one record at a time about 80 bytes per encipher call
Elapsed clock time: 1953.168870 seconds
Cipher time (ICSF): 1950.324934 seconds
Average cipher time: 0.001929 seconds

z800 Encipher, TDES 24 byte key
1011004 records; 80 bytes each; 80,880,320 bytes
one record at a time about 80 bytes per encipher call
Elapsed clock time: 212.853190 seconds
Cipher time (ICSF): 198.632159 seconds
Average cipher time: 0.000196 seconds

Sample CIPHER Throughputs ...cont

z990 (PCIxCC) Decipher, TDES 24 byte key
1107953 records (includes control/padding); 80,880,320
bytes recovered

one record at a time, about **72** bytes per decipher call

Elapsed clock time: 2138.434733 seconds

Cipher time (ICSF): **2133.420225** seconds

Average cipher time: 0.001925 seconds

z990 (PCIxCC) Decipher, TDES 24 byte key
1107953 records (includes control/padding); 80,880,320
bytes recovered

12237 records at a time, about **978928** bytes per decipher
call

Elapsed clock time: 44.783924 seconds

Cipher time (ICSF): **32.060308** seconds

Average cipher time: 0.386268 seconds

Sample CIPHER Throughputs ...cont

z990 (ICSF Clear key) Encipher, TDES 24 byte key
1011004 records; 80,880,320 bytes
one record at a time, about **80** bytes per encipher call

Elapsed clock time: 19.151577 seconds

Cipher time (ICSF): **12.598216** seconds

Average cipher time: 0.000012 seconds

z990 (ICSF Clear key) Encipher, TDES 24 byte key
1011004 records; 80,880,320 bytes
12237 records at a time, about **986960** bytes per encipher call

Elapsed clock time: 15.384605 seconds

Cipher time (ICSF): **0.509520** seconds

Average cipher time: 0.006213 seconds

Sample CIPHER Throughputs ...cont

z990 (native CPACF Clear key) Encipher, TDES 24 byte key

1011004 records; 80,880,320 bytes

one record at a time, about **80** bytes per encipher call

Elapsed clock time: 11.020412 seconds

Cipher time (CP): **1.105856** seconds

z990 (Native CPACF Clear key) Encipher, TDES 24 byte key

1011004 records; 80,880,320 bytes

12237 records at a time, about **986960** bytes per encipher call

Elapsed clock time: 13.656816 seconds

Cipher time (CP): **0.545292** seconds

	z800 Cipher Time (seconds)	z800 Clock Time (seconds)	z990 Cipher Time (seconds)	z990 Clock Time (seconds)	CPACF Clear Key Cipher Time	CPACF Clear Key Clock Time
72 Byte Records	198.632159	212.853190	1950.324934	1953.168870	1.105856 523 Mbyte 8.765327 seconds	11.020412 523 Mbyte 114.764597 seconds
980,000 Byte Records	5.348829	20.064974	32.060308 523 Mbyte 210 seconds	44.783924 523 Mbyte 318 seconds	0.545292 523 Mbyte 3.269381 seconds	13.656816 523 Mbyte 106.562428 seconds

z990 CIPHER Reference

CIPHZ990 - How To Use The New CPACF Crypto Functions

<http://www-1.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/PRS821>

CALCPACF: Callable Routine To Invoke z990 CPACF Crypto Functions

<http://www-1.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/PRS822>

References

- **ATS TechDocs Web Site**
 - <http://www-1.ibm.com/support/techdocs/atmastr.nsf>
 - ▶ search on CRYPTO
- **IBM Web Libraries**
 - <http://www-1.ibm.com/servers/eserver/zseries/zos/bkserv/>
 - http://www-1.ibm.com/servers/eserver/zseries/library/online_pubs.html
 - <http://www-1.ibm.com/servers/eserver/zseries/library/whitepapers/>
 - <http://app-06.www.ibm.com/servers/resourcelink>
 - ▶ z990
 - <http://publib-b.boulder.ibm.com/Redbooks.nsf/RedpaperAbstracts/redp3747.html?Open>
 - http://www-1.ibm.com/servers/eserver/zseries/zos/downloads/index.html#z990_compatibility/
 - ▶ HCR770A HCR770B HCR7720
 - http://www-1.ibm.com/servers/eserver/zseries/security/pdf/Web_GA2_Crypto_Rel_121203.pdf
- **Standards**
 - <http://www.ietf.org/>
 - <http://csrc.nist.gov/cryptval/140-1/1401val.htm>
 - <http://www.rsasecurity.com/rsalabs/standards/>
- **Free Stuff**
 - <http://www.infosecuritymag.com/>
 - <http://www.scmagazine.com/index2.html>
 - <http://www.counterpane.com/crypto-gram.html>

Questions?

