Linux for zSeries VSE
Dorint-Hotel 24.-26.Oktober 2005

IBM

IBM zSeries

(G12)

Verwendung von Crypto Prozessoren auf zSeries und System z9

GSE Herbsttagung 2005 in Garmisch-Partenkirchen

24.-26.Oktober 2005

Dr. Manfred Gnirss
gnirss@de.ibm.com
TMCC Böblingen
IBM Deutschland Entwicklung GmbH

Arthur Winterling
winterling@de.ibm.com
zServer Software System Evaluation
IBM Deutschland Entwicklung GmbH

ON DEMAND BUSINESS™

Trademarks

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

AIX*
CICS*
DB2*
e-business logo*
Enterprise Storage Server*
ESCON*
FICON
FlashCopy*
GDPS*
HyperSwap
IBM*
IBM eServer*
IBM logo*
NetView*
OS/390*
Parallel Sysplex*
S/390*
Sysplex Timer*
Tivoli*
TotalStorage*
z/OS*
z/VM*
zSeries*

* Registered trademarks of IBM Corporation

The following are trademarks or registered trademarks of other companies.

Intel is a trademark of the Intel Corporation in the United States and other countries.
Java and all Java-related trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc., 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.
UNIX is a registered trademark of The Open Group in the United States and other countries.

* 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.

This presentation and the claims outlined in it were reviewed for compliance with US law. Adaptations of these claims for use in other geographies must be reviewed by the local country counsel for compliance with local laws.

G12 – Verwendung von Crypto Prozessoren / SSL Verschlüsselung im VM/VSE

Dr. Manfred Gnirss, Arthur Winterling, IBM Böblingen

Krypthographische Verfahren sind eine Möglichkeit Informationen vor unberechtigtem Zugriff zu schützen. Leider sind die üblicherweise benutzten Verfahren relativ aufwendig und belasten die Systeme stark. Deshalb existieren eine Reihe von Spezialprozessoren, die dazu dienen, die Last der Systeme zu reduzieren, die krypthographischen Operationen sicher auszuführen und deren Bearbeitung zu beschleunigen. In diesem Vortrag wird ein Überblick über die verschiedenen Hardware Unterstützungen für Krypthographie auf zSeries gegeben und ihre Einsatzmöglichkeiten in unterschiedlichen Umgebungen besprochen

Agenda

- **Introduction**
- **zSeries and System z9 Crypto: Hardware Support**
- **zSeries and System z9 Crypto: Enabling Crypto Hardware**
- **Crypto Hardware Performance**
- **Hardware Crypto Support for z/VSE**
- **SSL Support for z/VM**
- **Linux for zSeries and System z9: Hardware Crypto Support**
- **Access to Crypto Hardware in z/OS**
- **Check HW Crypto**
- **Summay**

Introduction

Encryption of Data –
A Business Imperative

- Businesses are proactively focusing on securing customer and business data
  - Increasing regulatory requirements driving need for security of data for audit and compliance
  - Recent events highlight impact of loss/theft of removable data
  - Requirements for tighter security driving need for encryption of data

The Power of Mainframe Encryption

Helping to reduce risk across your value-net

Helping to protect data over the Internet

Helping to protect data leaving your enterprise

Customer objectives:

- Only intended party is allowed to decrypt
- Availability of the keys and decryption services when you need them

Protect archived data

Encryption and Decryption

- Symmetric encryption (same key for encrypt and decrypt)
  - Problem is key exchange!
  - Relatively fast algorithms
- Asymmetic encryption (key-pair, one key for encrypt and one for decrypt – Public-Private Key)
  - No exchange of secret key via unsecure methods necessary!
  - Relatively slow algorithms (expensive, high CPU load)

Encryption and Decryption . . .

- Crypto in Software: Performance depends on CPU capacity.
- Crypto Support with specialized hardware:
  - Benefit better performance/throughput
  - Faster specialized HW and/or Off-loading from CPU
  - CPACF: DES, TDES, SHA-1, SHA-256, AES
  - PCI-Cryptofeatures, PCICC, PCICA, PCIXCC, CEX2x: RSA (and other ...)

zSeries and System z9 Crypto Hardware Support

System z9 and zSeries Cryptographic Technology

- Continue to provide flexible Secure Sockets Layer (SSL) acceleration
- Continue to provide competitive symmetric performance in a security-rich environment
- Provide integration of Crypto features via ICSF
- Focus on required certifications and open standards
- Continue to improve performance
  - Each Crypto Express2 feature on a System z9, with both adapters configured as accelerators is designed to provide up to 6000* SSL handshakes per second

z900/z800 – Dec. 2000/ May 2002
2 Chips on CEC Board -
CMOS7s+ PCICC/PCICA (10/01)

G6 – June 1999
2 Chips on Processor
MCM - CMOS5x +
PCICC (6/99)

G5 – Sept. 1998
2 Chips on Processor
MCM - CMOS5x +
PCICC (6/99)

G4 – Sept. 1997
SCMs on Planar
Board - CMOS5x

G3 – June, 1997
SCMs on Planar
Board - CMOS5x

z9-109 – Planned for Sept, 2005
Crypto Express2

z990/z890 – January 2005
Crypto Express2

z890 – May 2004
PCIXCC/PCICA

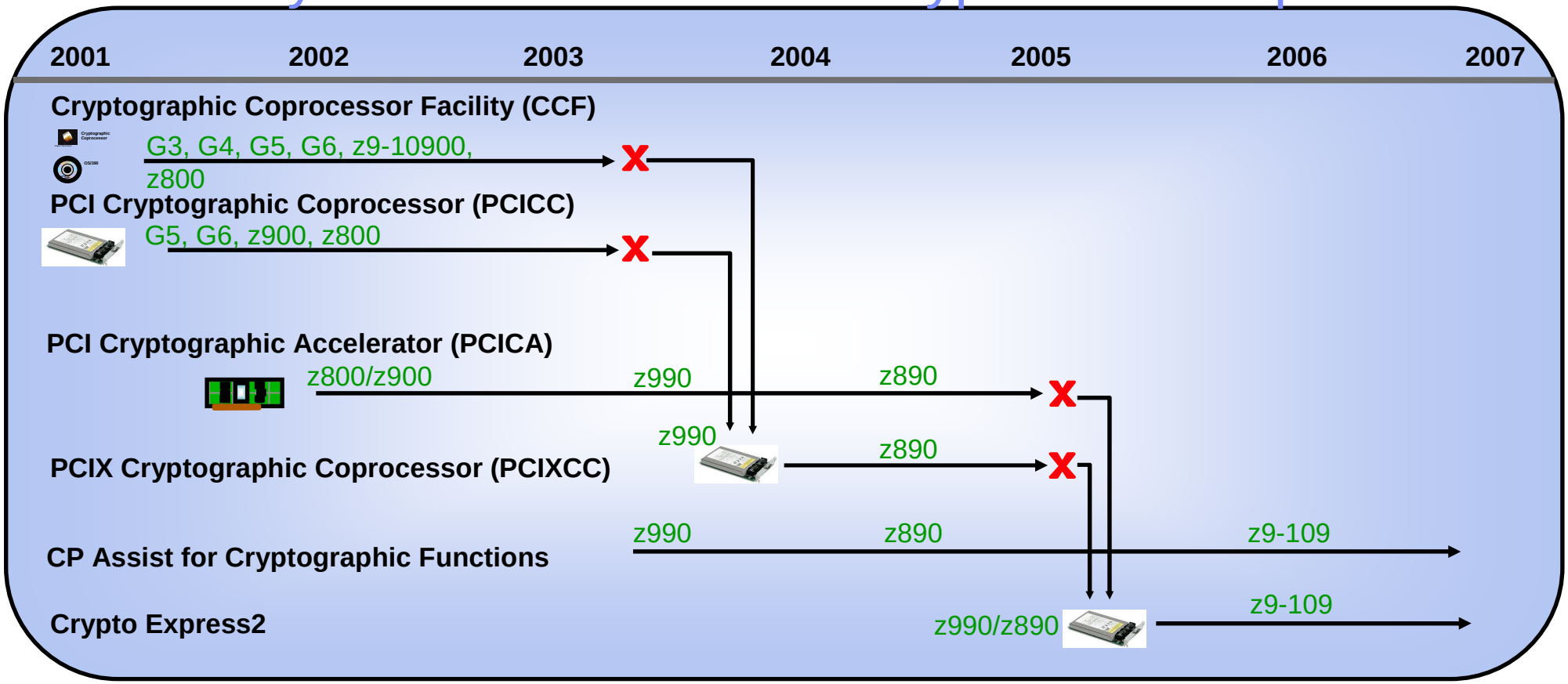
z990 - September 2003
PCIXCC

z990 - June 2003
CPACF/PCICA

z900/z800 – Dec. 2000/ May 2002
2 Chips on CEC Board -
CMOS7s+ PCICC/PCICA (10/01)

*These measurements are examples of the maximum transactions/second achieved in a lab environment with no other processing occurring and do not represent actual field measurements. Details available upon request.

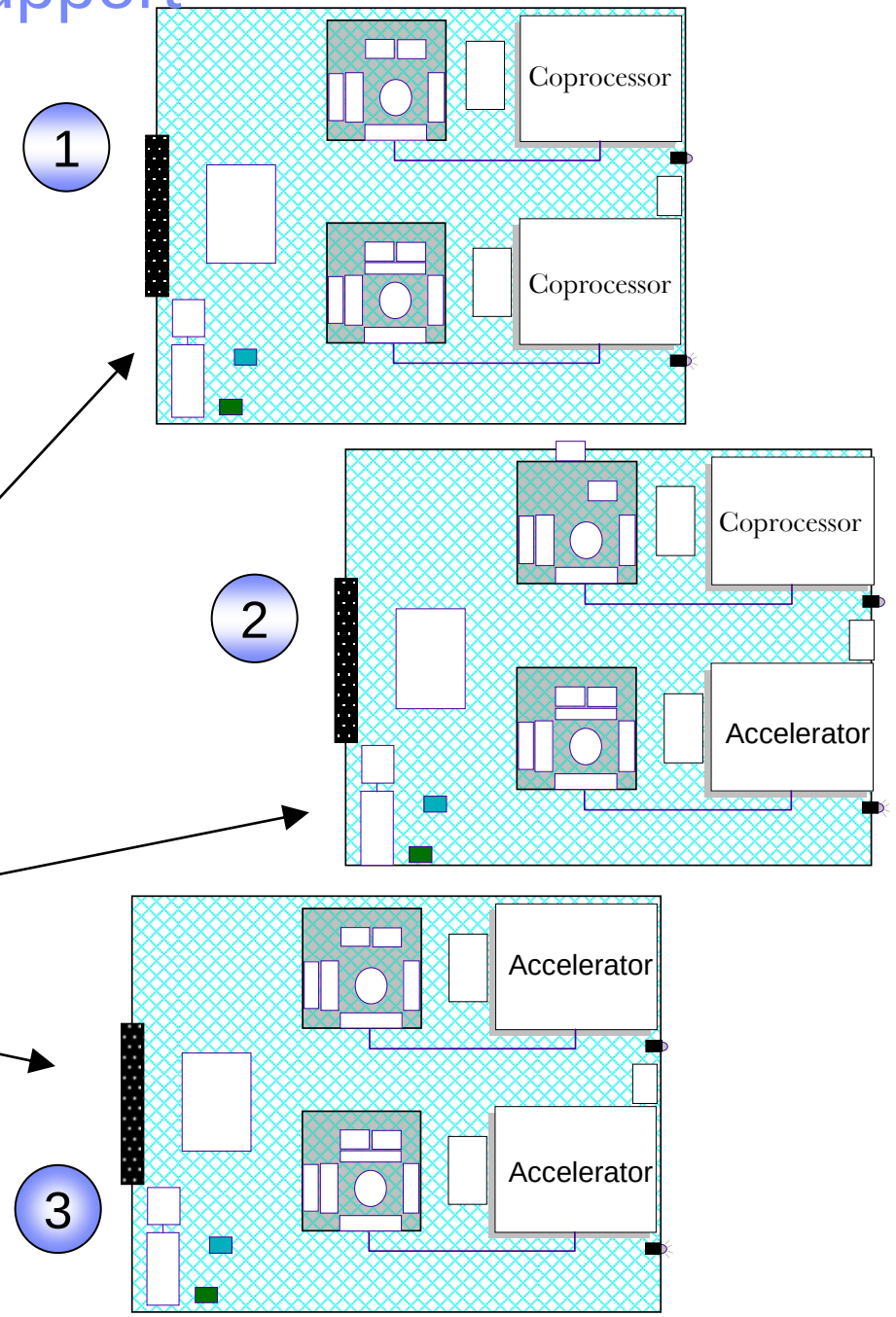
System z9 and zSeries Crypto Roadmap



- Cryptographic Coprocessor Facility – Supports “Secure key” cryptographic processing
- PCICC Feature – Supports “Secure key” cryptographic processing
- PCICA Feature – Supports “Clear key” SSL acceleration
- PCIXCC Feature – Supports “Secure key” cryptographic processing
- CP Assist for Cryptographic Function allows “Clear key” crypto functions from any CP/IFL
- Crypto Express2 – Combines function and performance of PCICA and PCICC

z9-109 Cryptographic Support Summary

- **CP Assist for Cryptographic Function (CPACF)**
  - Standard on every CP and IFL
  - Supports DES, TDES and SHA-1
  - New to z9-109
    - Advanced Encryption Standard (AES)
    - Secure Hash Algorithm – 256 (SHA-256)
    - Pseudo Random Number Generation (PRNG)
- **Crypto Express2**
  - Two configuration modes
    - Coprocessor (default)
      - Designed for Federal Information Processing Standard (FIPS) 140-2 Level 4 certification
    - Accelerator (configured from the HMC)
  - Three configuration options
    - Default set to Coprocessor
- **TKE workstation with 5.0 level of LIC**
  - Supports configurable Crypto Express2 feature
  - New Graphical User Interface (GUI)
  - Smart Card Reader

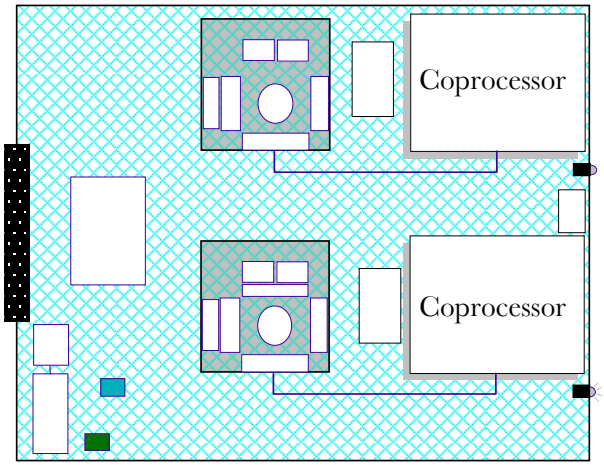


z9-109 CPACF Support

- **CP Assist for Cryptographic Function (CPACF)**
  - Available on every CP & IFL
  - High performance clear key symmetric encryption/decryption
    - Advanced Encryption Standard (AES) – 128-bit
    - Triple DES / DES
    - Requires no charge enablement feature
  - High performance clear key hashing
    - Secure Hash Algorithm (SHA)-256
    - SHA-1
    - Shipped enabled on all systems
  - High performance Pseudo Random Number Generator (PRNG)
    - Requires no charge enablement feature
  - Called via ICSF API or Problem State Instructions
- **CPACF Enabler Feature**
  - No additional charge export control feature
  - Required to enable AES, DES/TES, and PRNG - FC3863 with PoR (SHA-1 and SHA-256 are always enabled)
  - Required to order Crypto Express2

z9-109 Cryptographic Coprocessor

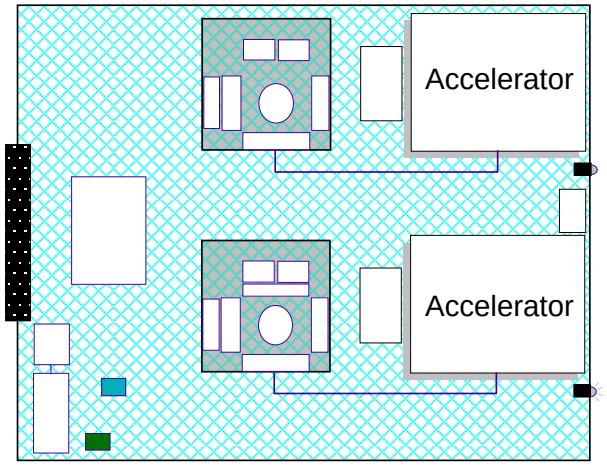
- **Crypto Express2 Coprocessor**
  - Default configuration for Crypto Express2 feature
    - Provides ‘secure-key’ and ‘public key’ functionality
  - Scalable - 0 to 8 features
    - Minimum purchase increment is two
  - Configurable
    - 0, 1, or 2 coprocessors per feature
    - Individually by PCIX adapter
  - Current applications expected to run without change
  - Connection to STI interface; no external cables
  - Fully programmable, User Defined Extensions (UDX) support
  - Designed for FIPS 140-2 Level 4 Certification
  - Trusted Key Entry (TKE) 5.0 support
    - Supports Crypto Express2 coprocessor
    - Smart Card Reader support
  - PCIXCC cannot be carried forward to z9-109
    - Replaced by Crypto Express2 Coprocessor



Note: A TKE workstation is required to manage Crypto Express2 features WHEN configured as a coprocessor

z9-109 Cryptographic Accelerator

- **Crypto Express2 Accelerator**
  - Non-default configuration for Crypto Express2 feature
    - Configured from the HMC
    - Provides SSL acceleration functions
  - Scalable - 0 to 8 features
    - Minimum purchase increment is two
  - Configurable
    - 0, 1, or 2 accelerators per feature
    - Individually by PCIX adapter
  - Hardware acceleration for Secure Sockets Layer (SSL transactions)
  - High performance public key (RSA) acceleration
  - Connection to STI interface; no external cables
  - PCICA cannot be carried forward to z9-109
    - Replaced by Crypto Express2 Accelerator



PCI Cryptographic Accelerator (PCICA)

There is no microprocessor subsystem. The overall operation control, including command decoding, is implemented in the hardware. The main components of the IBM PCI Cryptographic Accelerator feature are five IBM Ultra Cypher cryptographic engines that perform the following

Functions

- RSA (modular exponentiation) with data key lengths up to 2048 bits
- Special RSA functions up to 2048 bits
- DES, TDES, SHA-1 and MAC functions

Designed for maximum Secure Socket Layer (SSL) acceleration.

API

- CCA on z/OS (clear key RSA only)
- PKCS #11

Platforms (SSL acceleration)

- z800/z900 and z890/z990 with z/OS, VSE/ESA 2.7 or Linux for zSeries

System z9 and zSeries Crypto features over time

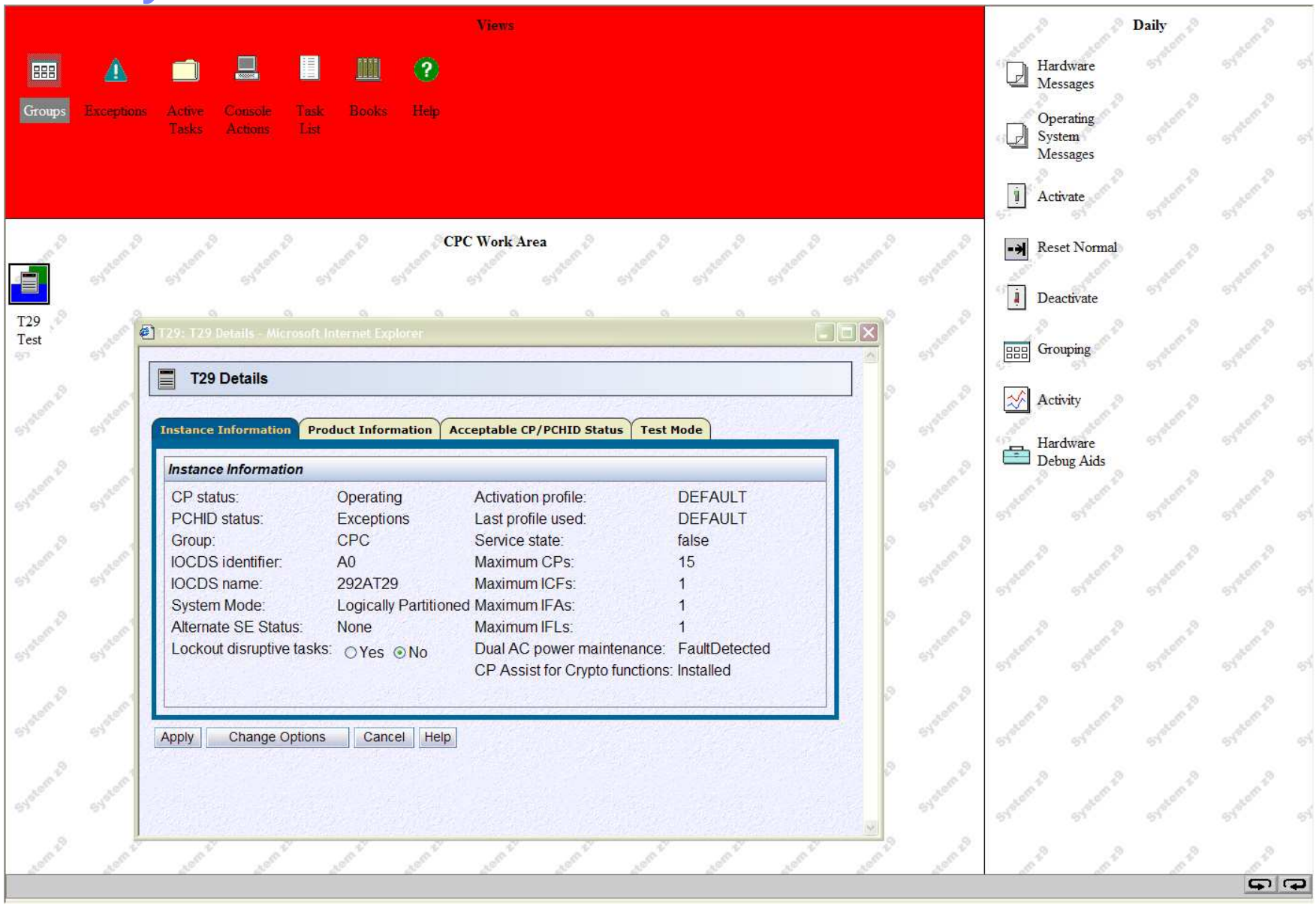
Feature	Feature Name	G5/G6	z900	z990	z9-109
0860	**PCICC**	**06/99**	**N/A**	**N/A**	**N/A**
0861	**PCICC replaces 0860**	**N/A**	**12/00**	**N/A**	**N/A**
0862	**PCICA**	**N/A**	**10/01**	**X**	**N/A**
0868	**PCIXCC replaces 0861**	**N/A**	**N/A**	**X**	**N/A**
0863	**Crypto Express2 replaces 0862 and 0868**	**N/A**	**N/A**	**X**	**X**

X = Available on a new build or an upgrade/MES.

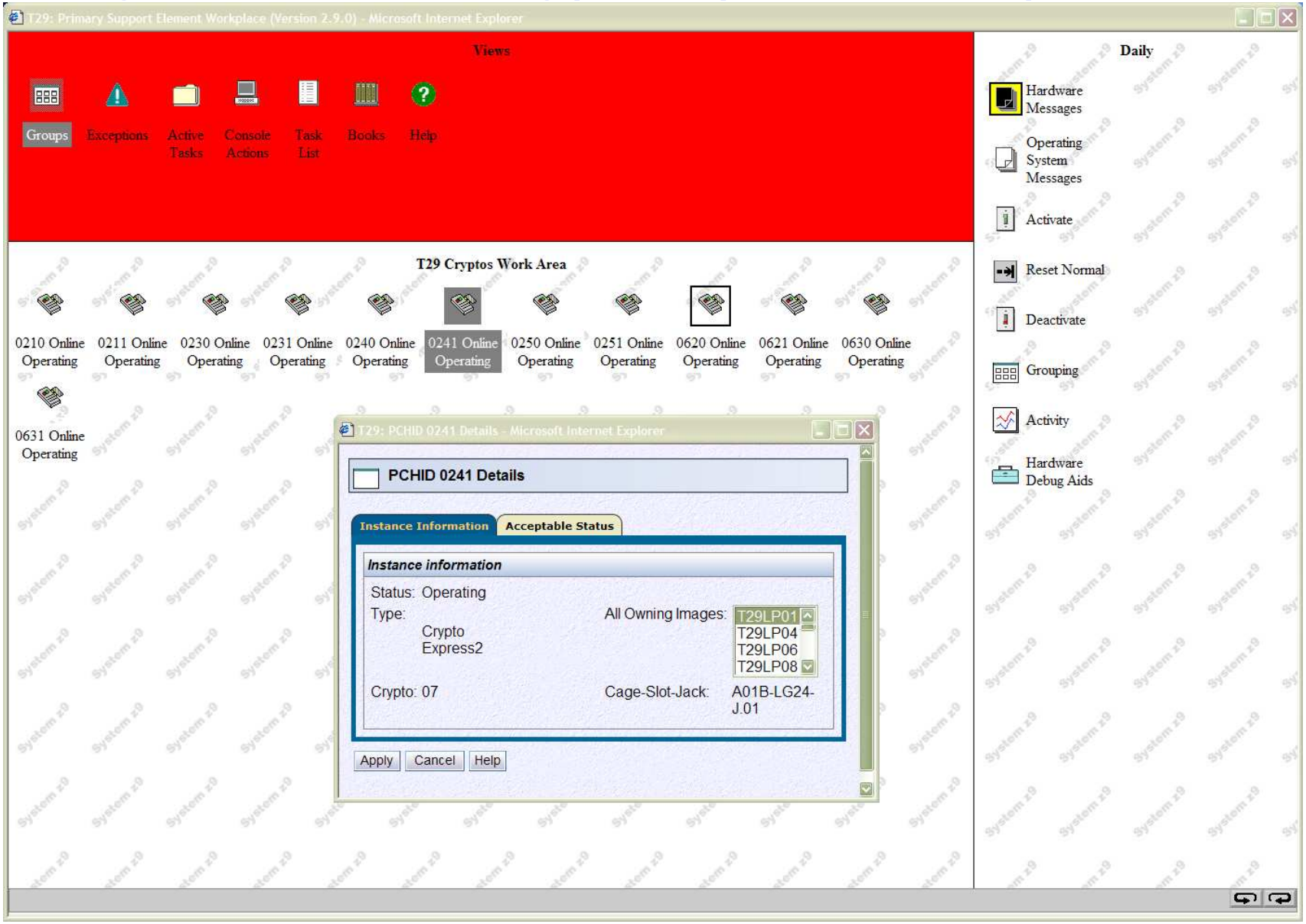
0862 and 0868 not available on z990 since January 28, 2005.

zSeries and System z9
Enabling Crypto Hardware

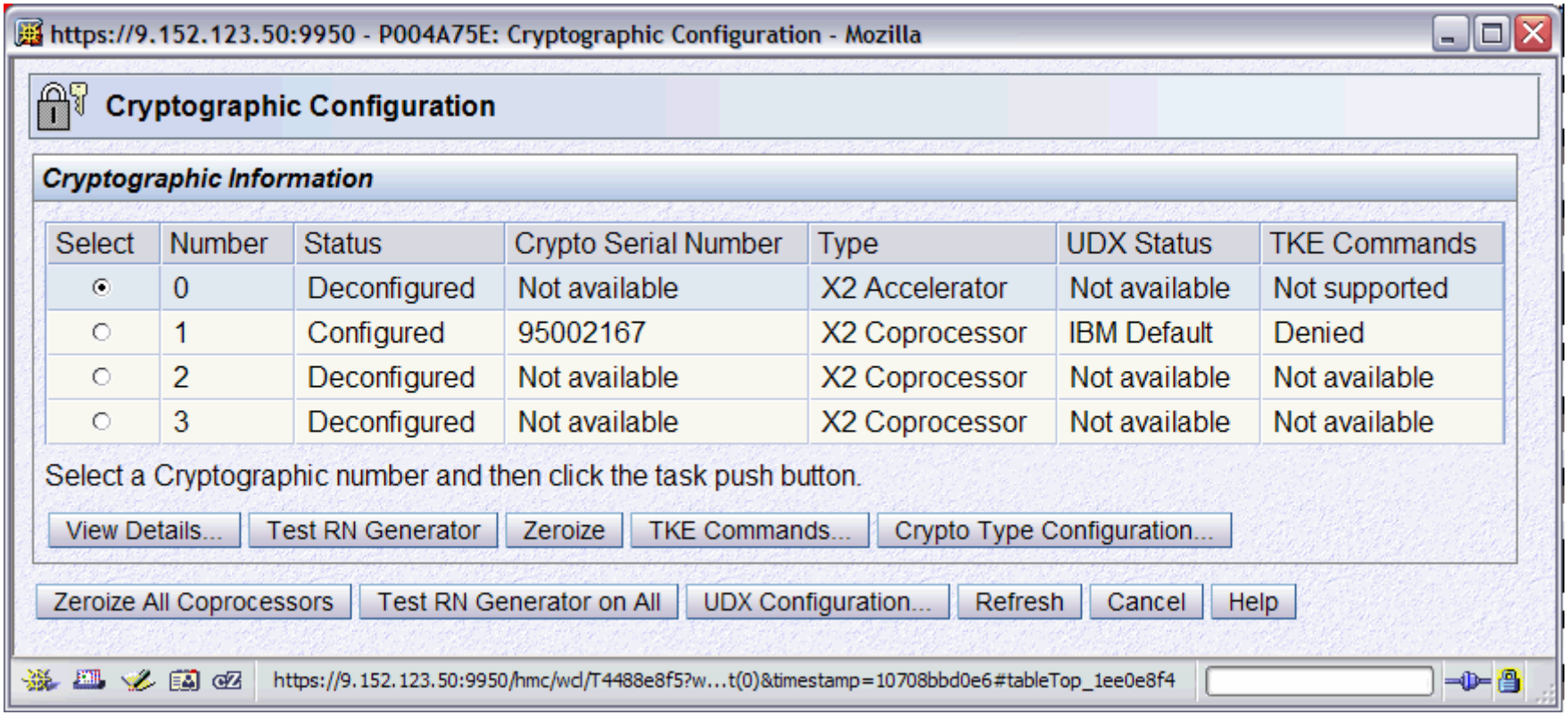
System z9 with enabled CPACF



System z9 with CryptoExpress 2 Adapter

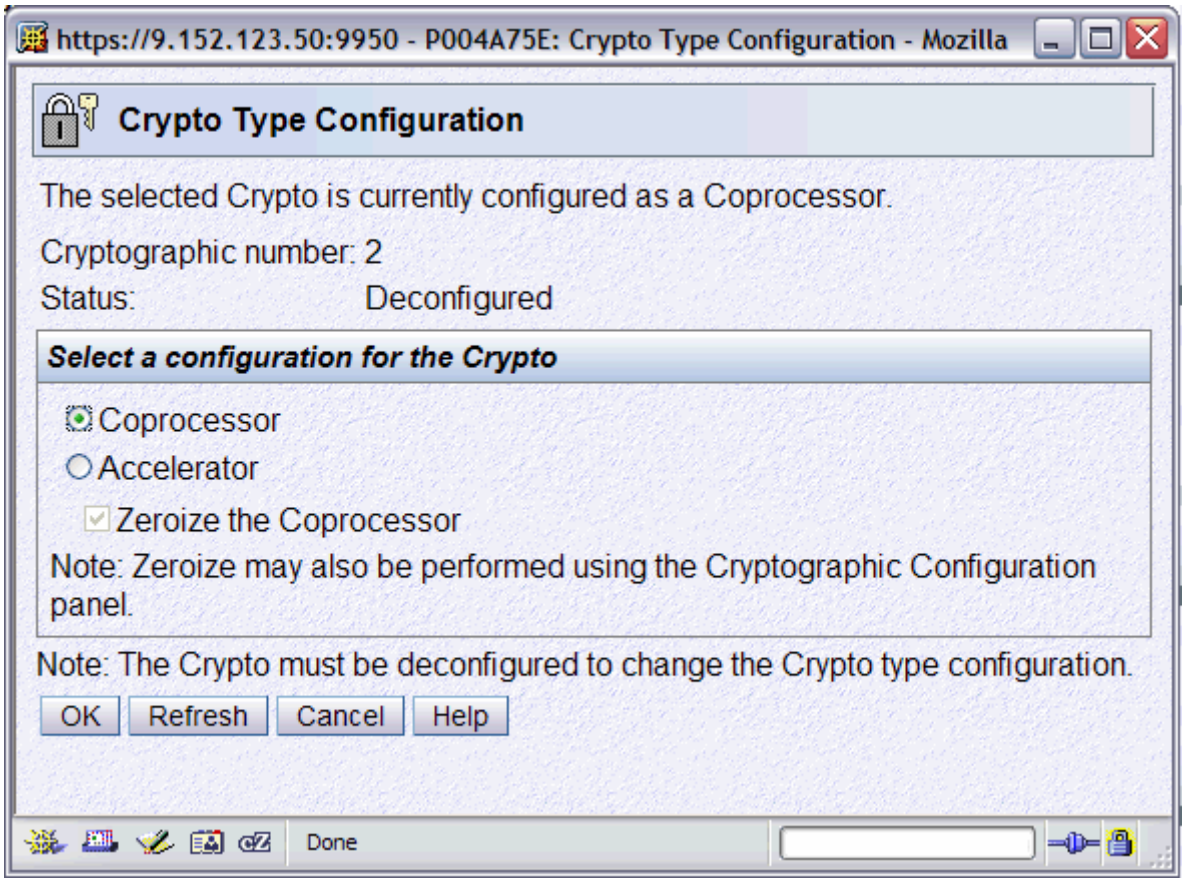


System z9: CryptoExpress 2 Configuration



Select	Number	Status	Crypto Serial Number	Type	UDX Status	TKE Commands
◉	0	Deconfigured	Not available	X2 Accelerator	Not available	Not supported
○	1	Configured	95002167	X2 Coprocessor	IBM Default	Denied
○	2	Deconfigured	Not available	X2 Coprocessor	Not available	Not available
○	3	Deconfigured	Not available	X2 Coprocessor	Not available	Not available

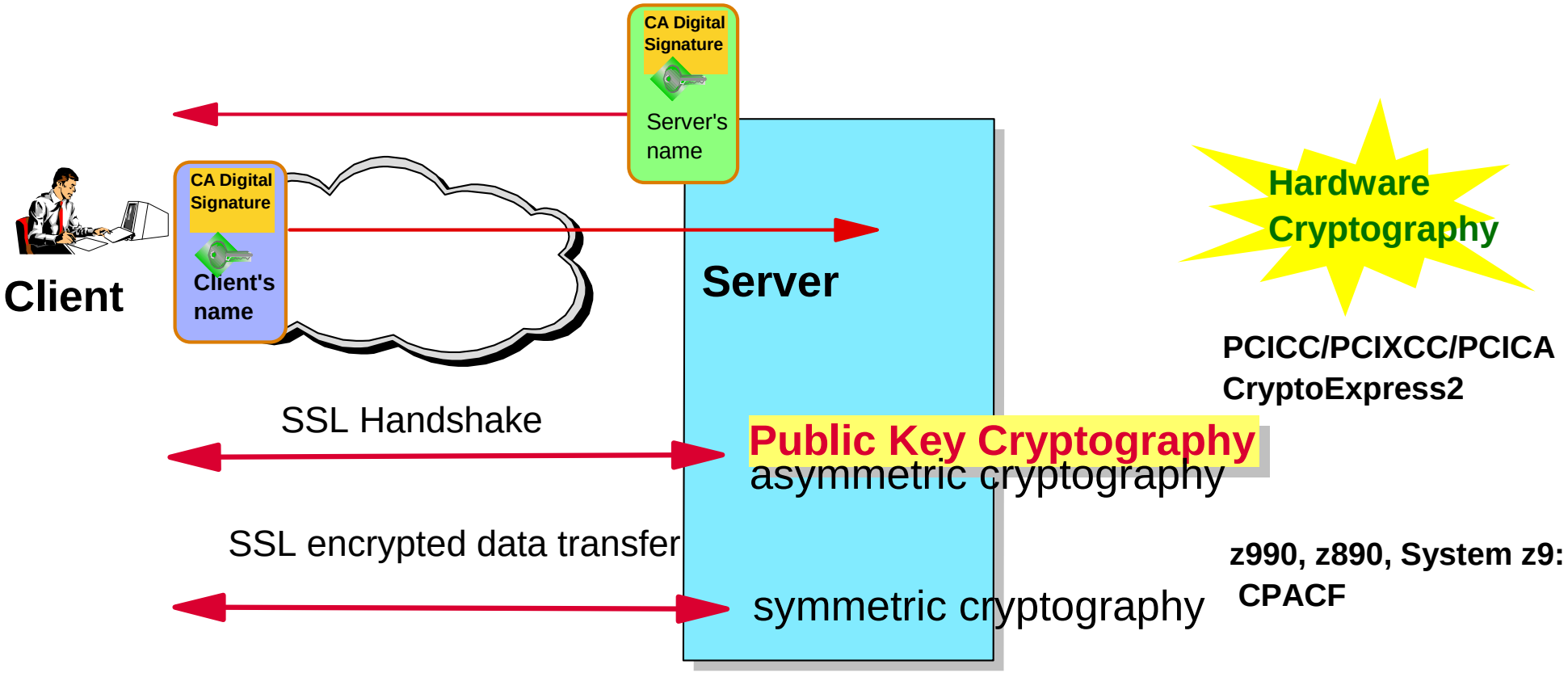
System z9: CryptoExpress 2 Configuration . . .



Crypto Hardware Performance

Hardware Support for Secure Socket layer (SSL) Protocol

Secure Socket Layer is a communications protocol, developed by Netscape, for client/server secure socket communications



Cryptography

- Hardware
  - Asymmetric
    - RSA handshake
      - PCICC with ~200 handshakes/second/card
      - PCICA with ~1000 handshakes/second/card
      - PCIXCC with ~ 1000 handshakes/second/card
      - CEX2C with ~ 1000 handshakes/second/card
      - CEX2A with ~ 3000 handshakes/second/card

HW- Performance

www.ibm.com/servers/eserver/zseries/security/cryptography.html

z990 Figures:

One CPACF: 400+MB/sec DES, 160+MB/secT-DES, 350+MB/sec SHA-1

Crypto Express 2 (Coprocessor Mode – CEX2C)

DES – 4KB blocks = 5.2 MB/sec for one CEX2C feature
T-DES – 4KB blocks = 4.8 MB/sec
MAC – 4KB blocks = 4.8 MB/sec
DSG (CRT – 1024-bit) = 2200/sec

SSL handshakes
PKD-CRT 1024-bit = 2100/sec

System z9 Figures:

Crypto Express 2 (Accelerator Mode – CEX2A)

SSL handshakes
PKD-CRT 1024-bit = 6000/sec for one feature with two CEX2A

Driving the coprocessors with Linux for zSeries

For all Linux Open SSL measurements the following applies:
•Linux Kernel Level: 2.4.19
•Open SSL Code Level: 0.9.6E
•z90Crypt Level: 1.1.2
•No Client Authentication

Linux native in LPAR

Caching SID	Handshake	# of CPs	ETR	Utilization %
no	Software	4	208	99.9
no	8 Cryp.Acc.Cards	4	6,703	99.5
no	12 Cryp.Acc.Cards	16	13,068	55.1

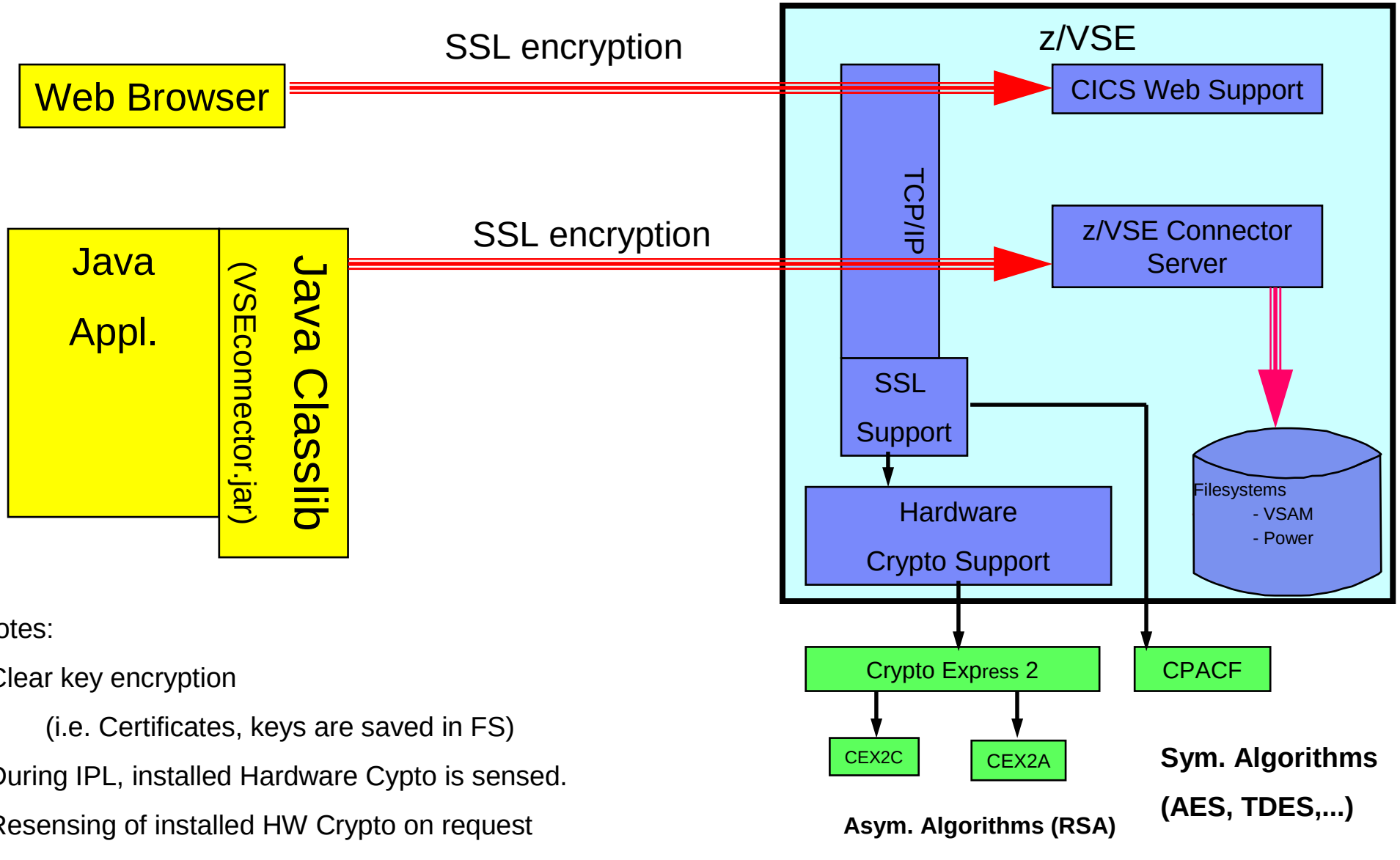
For all Linux Open SSL measurements the following applies:
- Linux running native on 2084-304
- Linux System Level: SLES8 SP4
- Linux Kernel Level: 2.4.21-266
- Open SSL Code Level: 0.9.7a
- z990Crypt Level: 1.3.2
- No Client Authentication

Caching SID	Handshake	Cipher	ETR	CPU Util. %
no	Software	RC4,MD5	202	99.99
no	4 PCIXCC Feat.	RC4,MD5	4,630	83.55
no	2 CEX2C Feat.	RC4,MD5	4,320	80.06
no	4 CEX2C Feat.	RC4,MD5	5,697	99.89

z990 Crypto performance figures at www.ibm.com/servers/eserver/zseries/security/cryptography.html

SSL Support for z/VSE

Hardware Crypto Support in z/VSE



Notes:

- Clear key encryption

  (i.e. Certificates, keys are saved in FS)
- During IPL, installed Hardware Cypto is sensed.
- Resensing of installed HW Crypto on request

Get HW-Crypto Status in z/VSE

```
SYSTEM:  z/VSE                z/VSE 3.1          TURBO (01)        USER:   SYS
                                                                   TIME:   14:54:38

BG 0001 1Q34I   BG WAITING FOR WORK
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 .......... : 5
FB 0011   NO. OF POSTED CALLERS ............. : 5
FB 0011   AP CRYPTO WAIT TIME ............... : 7
FB 0011   AP CRYPTO TRACE LEVEL ............. : 0
FB 0011   NO. OF AVAIL. APQS: PCICC / PCICA .. : 0 / 0
FB 0011                       CEX2C / CEX2A .. : 1 / 2
FB 0011     AP 0 : CEX2C   - ONLINE
FB 0011     AP 2 : CEX2A   - ONLINE
FB 0011     AP 9 : CEX2A   - ONLINE
FB 0011   AP CRYPTO DOMAIN ................... : 6
FB 0011 CPU CRYPTOGRAPHIC ASSIST FEATURE:
FB 0011   CPACF AVAILABLE .................... : YES
FB 0011   INSTALLED CPACF FUNCTIONS:
FB 0011     DES, TDES-128, TDES-192, SHA-1
FB 0011     AES-128
FB 0011     SHA-256
FB 0011 END OF CPACF STATUS
```

System z9 with
CPACF enabled
And Crypto Express 2

Get HW-Crypto Status in z/VSE

```
SYSTEM:  z/VSE                z/VSE 3.1         TURBO (01)       USER:   JSCH
VM USER ID:  VSER20                                              TIME:   15:01:44
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 ......... : NO
FB 0011   MAX REQUEST QUEUE SIZE ............ : -
FB 0011   MAX PENDING QUEUE SIZE ............ : -
FB 0011   TOTAL NO. OF AP REQUESTS .......... : -
FB 0011   NO. OF POSTED CALLERS .............. : -
FB 0011   AP CRYPTO WAIT TIME ................ : -
FB 0011   AP CRYPTO TRACE LEVEL .............. : -
FB 0011   NO. OF AVAIL. APQS: PCICC / PCICA .. : - / -
FB 0011                       CEX2C ......... : -
FB 0011   AP CRYPTO DOMAIN ................... : -
FB 0011 CPU CRYPTOGRAPHIC ASSIST FEATURE:
FB 0011   CPACF AVAILABLE .................... : NO
```

zSeries with
CPACF not enabled
No Crypto Features

Get HW-Crypto Status in z/VSE

Resensing of installed hardware Crypto:

```
msg fb,data=apsense
AR 0015 1I40I  READY
FB 0095 ADJUNCT PROCESSOR HW CRYPTO ENVIRONMENT REFRESHED.
```

SSL Support for z/VM

Secure Socket Layer (SSL) Support in z/VM

SSL support between a remote client and z/VM TCP/IP server is provided via a SSL server.

The SSL server is a special Linux machine only for this purpose.

The SSL server manages the certificate database and handles encryption and decryption of data

3 Steps:
- Install and configure SSL server (Linux)
- Configure TCP/IP
- Test configuration

Secure Socket Layer (SSL) Support in z/VM . . .

TCP/IP for VM Secure Socket Layer (SSL) Server Configuration Information and Requirements

http://www.vm.ibm.com/related/tcpip/vmsslinf.html

For z/VM 4.4 to z/VM – z/VM 5.1:

The z/VM SSL server implementation is supported on **specific Linux distributions**, for which **specific Linux IUCV driver support** is also required.
Supported distributions, requisite IUCV patches, and the z/VM-supplied SSL RPM packages for each distribution are listed in the table that follows.

SUSE Kernel Version	Required Patches	Linux RPM Package File	z/VM-Supplied RPM File
2.4.19 (**SLES-8**) †	Not Applicable	vmssld-1.24.19-1.rpm	VMSLDSB RPMBIN

(†) 31-bit version **only**

File transfer and installation instructions: see RPM Fackage File.

Check also for detailed information about service updates for the z/VM SSL Server (APARs/PTFs)

Secure Socket Layer (SSL) Support in z/VM . . .

Configure sslserv virtual machine

z/VM 5.1 TCP/IP Planning and cutomization - SC24-6125
Chapter 23: Configuring the SSL Server

SSL Server Configuration Steps

1. Install the appropriate VMSSL Linux Red Hat Package Manager (RPM) package
2. Update the PROFILE TCPIP file
3. Update the DTCPARMS file for the SSL server
4. Update the ETC SERVICES file

Set up the certificate database

Secure Socket Layer (SSL) Support in z/VM . . .

TCP/IP SSL Server – Configuration
Certificate Testing Examples, Hints and Tips

http://www.vm.ibm.com/related/tcpip/tcsslcfx.html

- SSL capable client, like
  - IBM Personal Communications (commonly referred to as "PCOM") Telnet client
  - BlueZone Telnet client
  - BlueZone FTP client
  - Netscape browser (HTTP and FTP protocols)

- Certificat (USEFUL COMMAND. SSLADMIN9
  - Self-signed certificate
  - Certificate signed by a CA (free test certificates available)

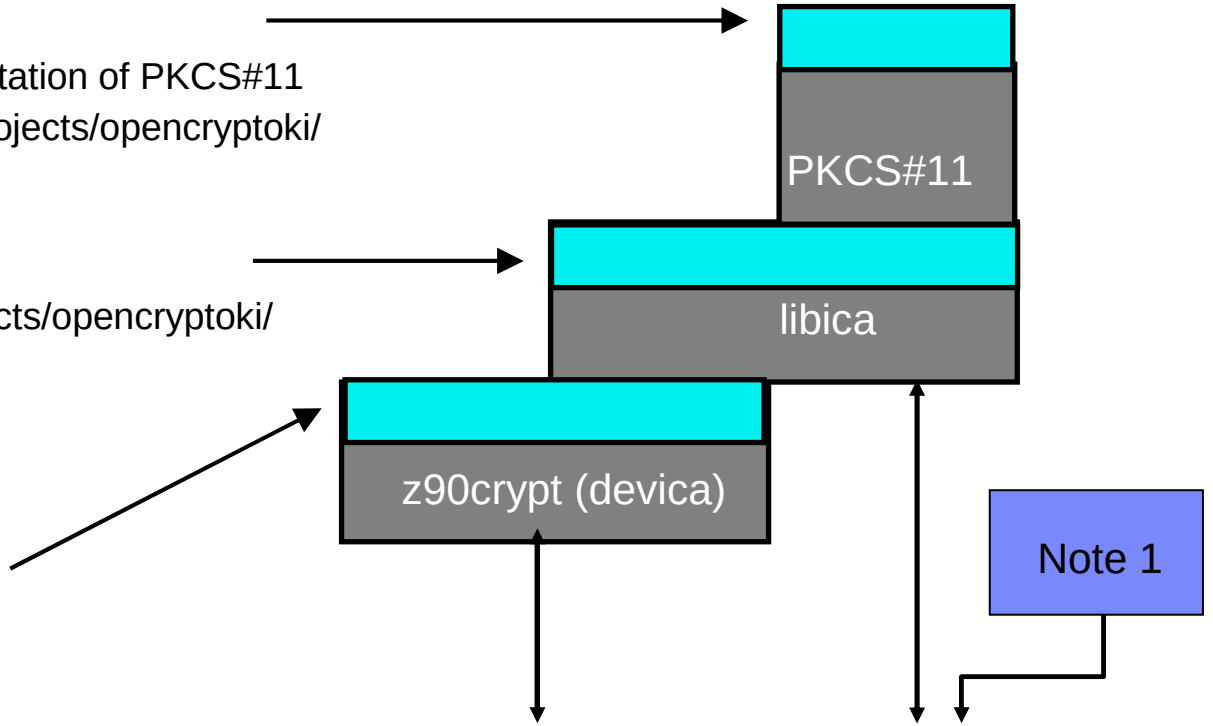
- Send and store also certificate to client

Linux for zSeries and System z9 Hardware Crypto Support

Crypto APIs With Linux For zSeries and System z9

OpenCryptoki is openSource implematation of PKCS#11
Information: http://sourceforge.net/projects/opencryptoki/

Information: http://sourceforge.net/projects/opencryptoki/



z90crypt API
- hdw status check
- random number generation
- RSA decryption (modular/CRT exponentiation)
- quiescing

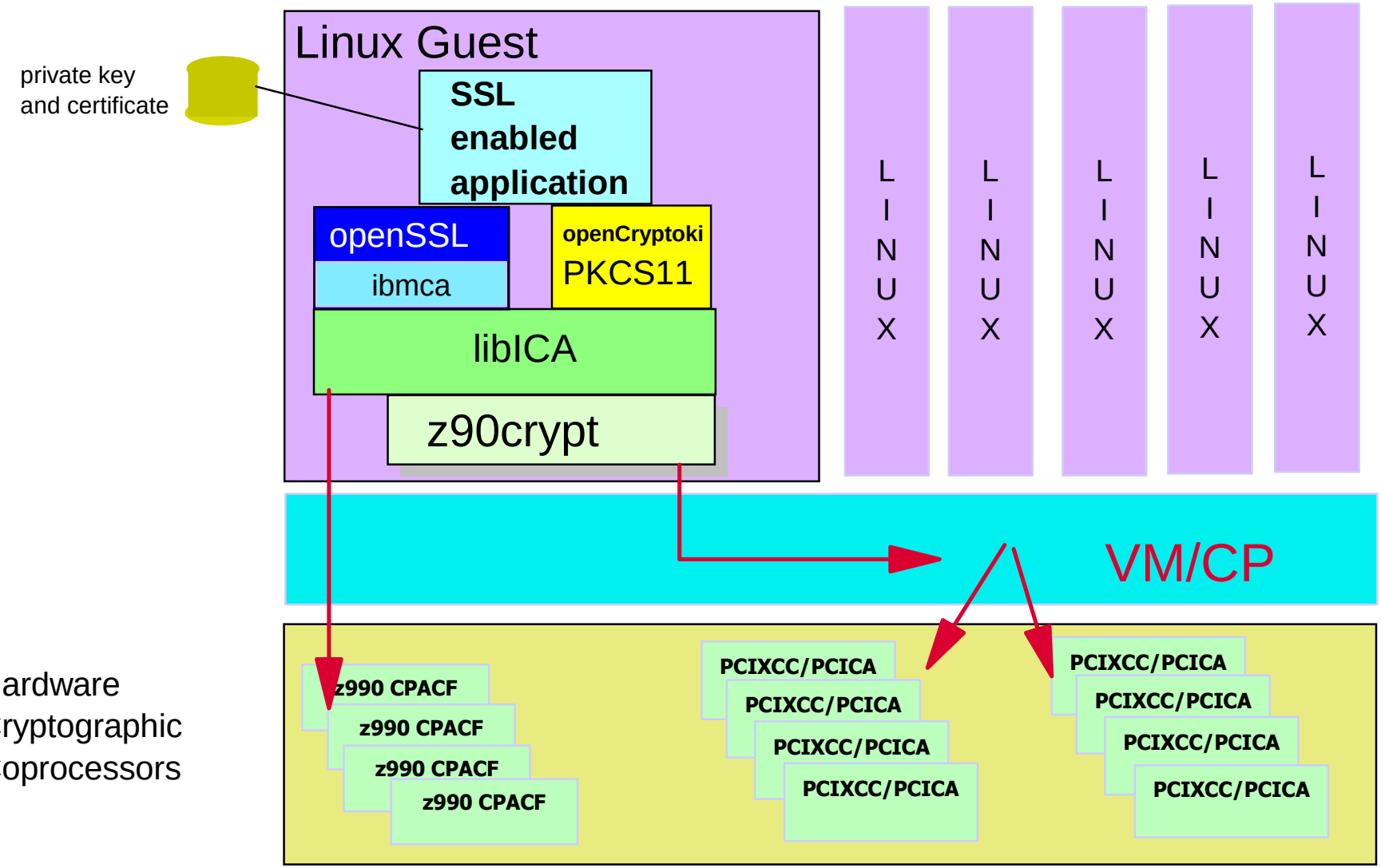
PCI hardware crypto
(PCIXCC, PCICA, Crypto Express2)

CPACF
(z990, z890, System z9)

Known exploiters
- Libica: openSSL, …
- PKCS#11: IBM WebSphere Application Server, Tivoli Access manager, IBM JDK 1.4, …

Note 1: Kernel 2.6 invokes directly the CPACF for IPSec VPN, …

Linux access to cryptographic hardware support



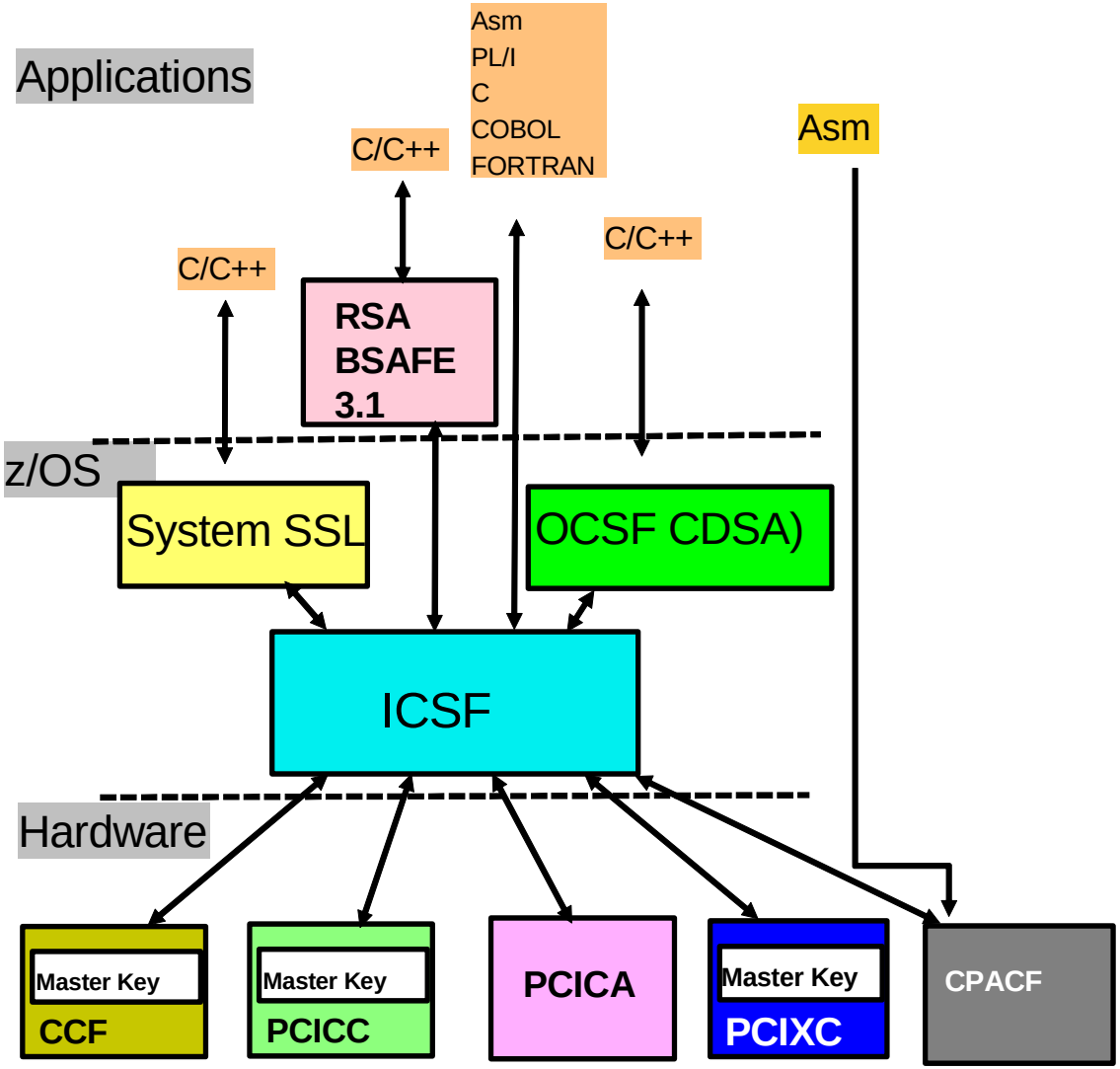
Inkernel Cryptography with Linux kernel 2.6

- Set of modules which provide encryption functions (Linux kernel 2.6)
- IBM provides modules for specific support of zSeries and System z9 for inkernel encryption
- Supported algorithms, see
  /lib/modules/*kernelversion*/kernel/crypto
  /lib/modules/*kernelversion*/kernel/arch/s390/crypto
- **zSeries / System z9 specific modules benefit from CPACF for SHA-1, DES, TDES**
- Examples:
  - IPSEC (for securre communication) – Freeswan (in SuSE SLES9)
  - Disk encryption, encrypted file system with dm-crypt and LUKS
    Transparent access to encrypted data on disk
    dm-crypt is a device-mapper target that provides transparent encryption of block devices using the new Linux 2.6 cryptoapi.
    LUKS Linux unified Keys Setup used for administration of appropriate keys

Note: Requires some configuration setup, if SuSE SLES 9 is not used!
libica is not used for inkernel cryptography

Access to Crypto Hardware in z/OS

Crypto Coprocessors on zSeries with z/OS



- System SSL
  - IBM HTTP Server for z/OS
  - TN3270 Server
  - LDAP Directory Server and LDAP Client
  - FTP Server and Client
  - CICS Transaction Gateway
  - IMS Connect
  - WebSphere AS
  - TAM for Business Integration (MQSeries)
- RACF
- Firewall Technology IPSec (VPN) and IKE (Internet Key Exchange)
- DCE Security Server
- z/OS Kerberos
- Java JCE and JSSE
- Open Cryptographic Services Facility (CDSA APIs)
- BSAFE Toolkit - for applications and subsystems
- IBM Payment Suite e-commerce solutions
- Financial Institution Applications
  - IBM ELS solution
- DKMS (Distributed Key Management System)
- CBT (Crypto Based Transactions) banking solution
- PCF Compatibility Mode
  - VTAM SLE
  - AMS REPRO command

Linux for zSeries and System z9
Check Crypto Hardware

Verify Installation for HW Crypto Support

Load Linux z90crypt device driver

Load the Linux z90crypt device driver with rcz90crypt if not already done.

```
t29lp40:~/crypto/tools # rcz90crypt start
Loading z90crypt module
```

You can check whether z90crypt is loaded using dmesg

Example for Crypto hardware support available:

```
z90crypt: Version 1.3.3 loaded, built on Oct 11 2005 16:46:19
z90crypt: z90main.o ($Revision: 1.31.2.9 $/$Revision: 1.8.2.5 $/$Revision: 1.2.2.4 $)
z90crypt: z90hardware.o ($Revision: 1.19.2.7 $/$Revision: 1.8.2.5 $/$Revision: 1.2.2.4 $)
```

Example for Crypto hardware support not available:

```
z90crypt: Version 1.3.2 loaded, built on Aug 26 2005 00:57:18
z90crypt: z90main.o ($Revision: 1.31.2.8 $/$Revision: 1.8.2.4 $/$Revision: 1.2.2.3 $)
z90crypt: z90hardware.o ($Revision: 1.19.2.6 $/$Revision: 1.8.2.4 $/$Revision: 1.2.2.3 $)
z90crypt: query_online -> Exception testing device 0
z90crypt: helper_scan_devices -> exception taken!
z90crypt: z90crypt_config_task -> Error 34 detected in refresh_z90crypt.
```

Verify Installation for HW Crypto Support . . .

Query status of Linux z90crypt device driver

Example:Status **before** some crypto requesets have been performed

```
t291p40:~ # cat /proc/driver/z90crypt

z90crypt version: 1.3.3
Cryptographic domain: 8
Total device count: 12
PCICA count: 0
PCICC count: 0
PCIXCC MCL2 count: 0
PCIXCC MCL3 count: 0
CEX2C count: 8
CEX2A count: 4
requestq count: 0
pendingq count: 0
Total open handles: 0

Online devices: 1=PCICA 2=PCICC 3=PCIXCC(MCL2) 4=PCIXCC(MCL3) 5=CEX2C 6=CEX2A
           5566555556560000 0000000000000000 0000000000000000 0000000000000000

Waiting work element counts
           0000000000000000 0000000000000000 0000000000000000 0000000000000000

Per-device successfully completed request counts
    00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
    00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
    00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
```

Verify Installation for HW Crypto Support . . .

Query status of Linux z90crypt device driver

Example:Status **after** some crypto requesets have been performed

```
t29lp40:~/crypto/tools # cat /proc/driver/z90crypt

z90crypt version: 1.3.3
Cryptographic domain: 8
Total device count: 12
PCICA count: 0
PCICC count: 0
PCIXCC MCL2 count: 0
PCIXCC MCL3 count: 0
CEX2C count: 8
CEX2A count: 4
requestq count: 0
pendingq count: 0
Total open handles: 0


Online devices: 1=PCICA 2=PCICC 3=PCIXCC(MCL2) 4=PCIXCC(MCL3) 5=CEX2C 6=CEX2A
            5566555556560000 0000000000000000 0000000000000000 0000000000000000


Waiting work element counts
            0000000000000000 0000000000000000 0000000000000000 0000000000000000


Per-device successfully completed request counts
    00000BF2 00000BDB 00000A7E 00000A4E 00000BDE 00000BD4 00000BBE 00000BB0
    00000896 00000A23 00000889 000009F2 00000000 00000000 00000000 00000000
    00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
```

Verify Installation for HW Crypto Support . . .

Test OpenSSL with HW cryptography provided with engine ibmca

Example:OpenSSL with engine ibmca for RSA

```
t29lp40:~/crypto/tools # openssl speed rsa1024 -engine ibmca
engine "ibmca" set.
Doing 1024 bit private rsa's for 10s: 1000 1024 bit private RSA's in 0.00s
Doing 1024 bit public rsa's for 10s: 1000 1024 bit public RSA's in 0.00s
OpenSSL 0.9.7d 17 Mar 2004
built on: Tue Oct 11 15:42:57 UTC 2005
options:bn(64,64) md2(int) rc4(ptr,int) des(idx,cisc,4,long) aes(partial) blowfish(idx)
compiler: gcc -fPIC -DOPENSSL_THREADS -D_REENTRANT -DDSO_DLFCN -DHAVE_DLFCN_H -DOPENSSL_NO_KRB5 -DB_ENDIAN -DNO_ASM -DMD32_REG_T=int -
DOPENSSL_NO_RC5 -DOPENSSL_NO_IDEA -O2 -fsigned-char -fmessage-length=0 -Wall -fomit-frame-pointer -fno-strict-aliasing -DTERMIO -Wall
-fbranch-probabilities
available timing options: TIMES TIMEB HZ=100 [sysconf value]
timing function used: times
                  sign    verify    sign/s verify/s
rsa 1024 bits   0.0000s   0.0000s 1000000.0 1000000.0
t29lp40:~/crypto/tools #
```

Verify Installation for HW Crypto Support . . .

Test OpenSSL with HW cryptography provided with engine ibmca

Example:OpenSSL with engine ibmca for SHA

```
t29lp40:~/crypto/tools # openssl speed sha -engine ibmca
engine "ibmca" set.
Doing sha1 for 3s on 16 size blocks: 1074895 sha1's in 3.00s
Doing sha1 for 3s on 64 size blocks: 972592 sha1's in 3.00s
Doing sha1 for 3s on 256 size blocks: 878587 sha1's in 3.00s
Doing sha1 for 3s on 1024 size blocks: 643746 sha1's in 3.00s
Doing sha1 for 3s on 8192 size blocks: 185033 sha1's in 3.00s
OpenSSL 0.9.7d 17 Mar 2004
built on: Tue Oct 11 15:42:57 UTC 2005
options:bn(64,64) md2(int) rc4(ptr,int) des(idx,cisc,4,long) aes(partial) blowfish(idx)
compiler: gcc -fPIC -DOPENSSL_THREADS -D_REENTRANT -DDSO_DLFCN -DHAVE_DLFCN_H -DOPENSSL_NO_KRB5 -DB_ENDIAN -DNO_ASM -DMD32_REG_T=int -
DOPENSSL_NO_RC5 -DOPENSSL_NO_IDEA -O2 -fsigned-char -fmessage-length=0 -Wall -fomit-frame-pointer -fno-strict-aliasing -DTERMIO -Wall
-fbranch-probabilities
available timing options: TIMES TIMEB HZ=100 [sysconf value]
timing function used: times
The 'numbers' are in 1000s of bytes per second processed.
type             16 bytes     64 bytes    256 bytes   1024 bytes   8192 bytes
sha1              5732.77k    20748.63k    74972.76k   219731.97k   505263.45k
```

Verify Installation for HW Crypto Support . . .

Test OpenSSL with HW cryptography provided with engine ibmca

Example:OpenSSL with engine ibmca for DES

```
t29lp40:~/crypto/tools # openssl speed des -engine ibmca
engine "ibmca" set.
Doing des cbc for 3s on 16 size blocks: 3548696 des cbc's in 3.00s
Doing des cbc for 3s on 64 size blocks: 967139 des cbc's in 3.00s
Doing des cbc for 3s on 256 size blocks: 246998 des cbc's in 3.00s
Doing des cbc for 3s on 1024 size blocks: 61997 des cbc's in 3.00s
Doing des cbc for 3s on 8192 size blocks: 7785 des cbc's in 3.00s
Doing des ede3 for 3s on 16 size blocks: 1359777 des ede3's in 3.00s
Doing des ede3 for 3s on 64 size blocks: 350043 des ede3's in 3.00s
Doing des ede3 for 3s on 256 size blocks: 88161 des ede3's in 3.00s
Doing des ede3 for 3s on 1024 size blocks: 22071 des ede3's in 3.00s
Doing des ede3 for 3s on 8192 size blocks: 2755 des ede3's in 3.00s
OpenSSL 0.9.7d 17 Mar 2004
built on: Tue Oct 11 15:42:57 UTC 2005
options:bn(64,64) md2(int) rc4(ptr,int) des(idx,cisc,4,long) aes(partial) blowfish(idx)
compiler: gcc -fPIC -DOPENSSL_THREADS -D_REENTRANT -DDSO_DLFCN -DHAVE_DLFCN_H -DOPENSSL_NO_KRB5 -DB_ENDIAN -DNO_ASM -DMD32_REG_T=int -
DOPENSSL_NO_RC5 -DOPENSSL_NO_IDEA -O2 -fsigned-char -fmessage-length=0 -Wall -fomit-frame-pointer -fno-strict-aliasing -DTERMIO -Wall
-fbranch-probabilities
available timing options: TIMES TIMEB HZ=100 [sysconf value]
timing function used: times
The 'numbers' are in 1000s of bytes per second processed.
type             16 bytes     64 bytes    256 bytes   1024 bytes   8192 bytes
des cbc          18926.38k    20632.30k    21077.16k    21161.64k    21258.24k
des ede3          7252.14k     7467.58k     7523.07k     7533.57k     7522.99k
```

Summary

Recommendation

- For data transport and data exchange, please consider seriously usage of cryptographic methods!
- If you have any chance to access crypto hardware support, benefit from performance and throughput increase.
- If you have already some crypto hardware installed, enable it also for usage with Linux for zSeries and System z9
  (If you are using a z890, z990, or System z9 then you can enable the CPACF in any case.)

Questions ?

zSeries and System z9 Integrated Cryptography Appendices

Disabling/Enabling Crypto in Linux

Disabling crypto

For test or trouble shooting purposes, you might want to disable a cryptographic device. You can do this by editing the /proc/driver/z90crypt file with the vi editor. Proceed like this to disable a cryptographic device:

1. Open /proc/driver/z90cryp with vi. You will see several lines including two lines like this:

```
Mask of online devices: 1 means PCICA, 2 means PCICC
    2200000000000000 0000000000000000 0000000000000000 0000000000000000
```

The lower line represents the physical arrangement of the cryptographic devices with digits 1 and 2 representing PCICA and PCICC cards, respectively.

2. Overwrite the digit that represents the card you want to disable with a character d. To disable the card in the second position or our example overwrite the second 2:

```
Mask of online devices: 1 means PCICA, 2 means PCICC
    2d00000000000000 0000000000000000 0000000000000000 0000000000000000
```

3. Close and save /proc/driver/z90cryp. Confirm that you want to save your changes even if the content of the file has changed since you opened it.

Disabling/Enabling Crypto in Linux

To enable a disabled device proceed like this:

1. Open /proc/driver/z90cryp with vi. You will see two lines like this:

```
Mask of online devices: 1 means PCICA, 2 means PCICC
    2d000000000000000 0000000000000000 0000000000000000 0000000000000000
```

   Each d in the second line represents the disabled device. In our example, the device in the second position has been disabled.

2. Overwrite the d that represents the device you want to enable with an e:

```
Mask of online devices: 1 means PCICA, 2 means PCICC
    2e000000000000000 0000000000000000 0000000000000000 0000000000000000
```

3. Close and save /proc/driver/z90cryp. Confirm that you want to save your changes even if the content of the file has changed since you opened it. The device driver replaces the e with the digit for the actual device.

Linux for zSeries Cryptography Bibliography

Linux for zSeries Device Drivers and Installation Commands –
Linux kernel 2.6 – October 2005 stream

ftp://www6.software.ibm.com/software/developer/linux390/docu/l26cdd00.pdf

openCryptoki docs
http://sourceforge.net/projects/opencryptoki/
http://www-128.ibm.com/developerworks/security/library/s-pkcs/index.html

IBM zSeries 990 Cryptographic Coprocessor Configuration
http://www.redbooks.ibm.com/redbooks/pdfs/sg246310.pdf

zSeries Crypto Guide Update
http://www.redbooks.ibm.com/redbooks/pdfs/sg246870.pdf

Processor Resource/Systems Manager Planning Guide - SB10-7036

z/VM CP Planning and Administration Version 5 Release 1.0 - SC24-6083

z/VM Directory Maintenance Facility Tailoring and Administration Guide - SC24-6084

z/OS Integrated Cryptographic Service Facility Overview - SA22-7519

Linux for zSeries Cryptography Bibliography

Linux on IBM zSeries and S/390: Best Security Practices - SG24-7023

z/VM 5.1 TCP/IP Planning and cutomization - SC24-6125