z/VSE Live Virtual Class Series

Overview of cryptography and enhancements on z/VSE 4.3

Joerg Schmidbauer

jschmidb@de.ibm.com

March, 2011

Trademarks

Trademarks

The following are trademarks of the International Business Machines Corporation in the United States and/or other countries. For a complete list of IBM Trademarks, see www.ibm.com/legal/copytrade.shtml: AS/400, DBE, e-business logo, ESCO, eServer, FICON, IBM, IBM Logo, iSeries, MVS, OS/390, pSeries, RS/6000, S/30, VM/ESA, VSE/ESA, Websphere, xSeries, z/OS, zSeries, z/VM

The following are trademarks or registered trademarks of other companies

Lotus, Notes, and Domino are trademarks or registered trademarks of Lotus Development Corporation
Java and all Java-related trademarks and logos are trademarks of Sun Microsystems, Inc., in the United States and other countries
LINUX is a registered trademark of Linux Torvalds
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.
Intel is a registered trademark of Intel Corporation
* 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.

References in this document to IBM products or services do not imply that IBM intends to make them available in every country.

Any proposed use of claims in this presentation outside of the United States must be reviewed by local IBM country counsel prior to such use.

The information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

Agenda

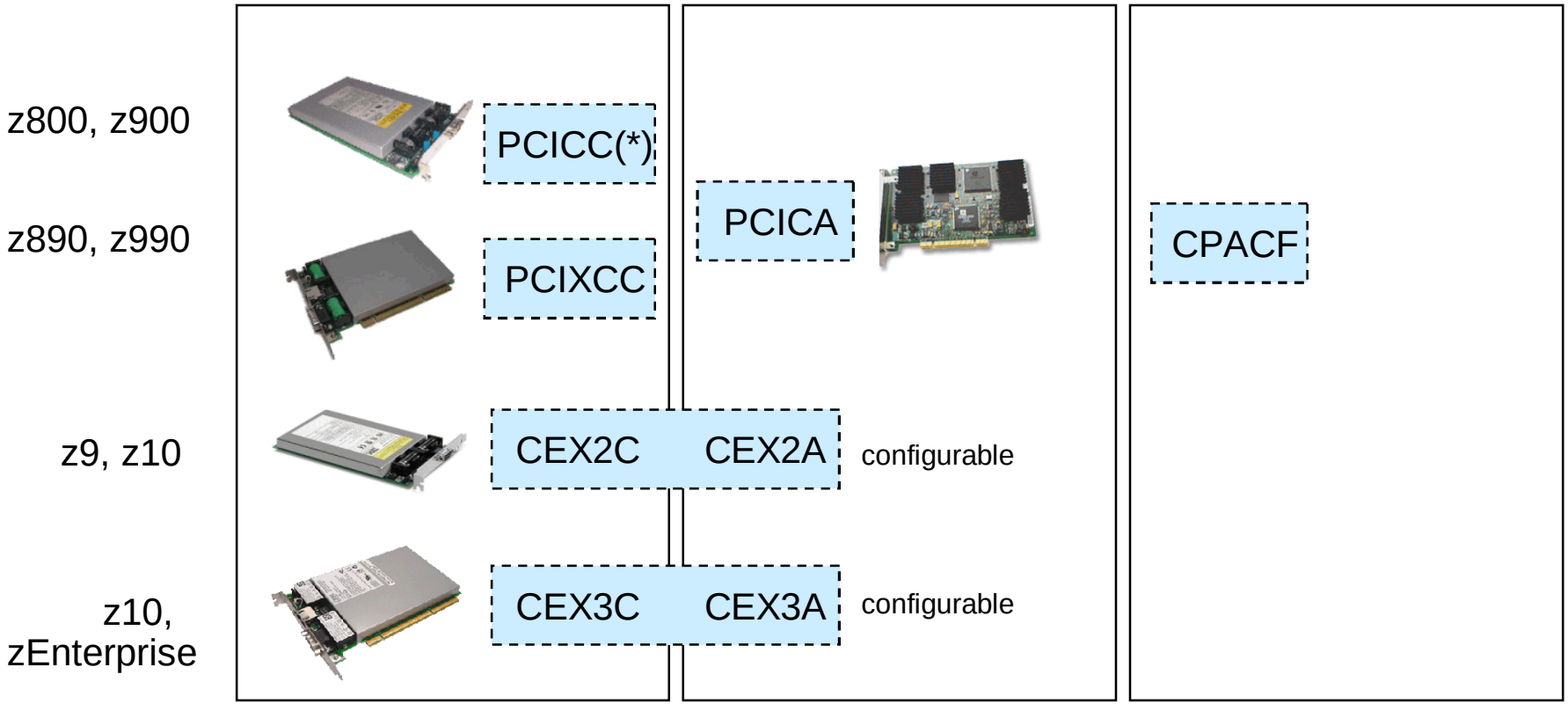
- **Overview of cryptographic support in VSE**
  - Crypto hardware
  - HMC/SE view
  - Crypto device driver
- **Enhancements with VSE 4.3**
  - Device driver
  - TCP/IP for VSE/ESA
  - Keyman/VSE
  - VSE Navigator

Overview of cryptographic support in VSE

Crypto hardware - overview

- **System z provides two types of cryptographic hardware:**
  - Crypto cards
    - Pluggable PCI cards
    - Provide RSA encryption/decryption
    - Provide secure key functions (not supported by VSE, mainly used on z/OS)
  - CPU Assist for cryptographic functions (CPACF)
    - On-board crypto functions (feature code #3863)
    - One separate crypto chip per CP
    - Provides symmetric crypto algorithms (DES, Triple-DES, AES) and hashing (SHA-1, SHA-2)
    - Set of instructions, documented in the Principles of Operation book

Crypto hardware - evolution

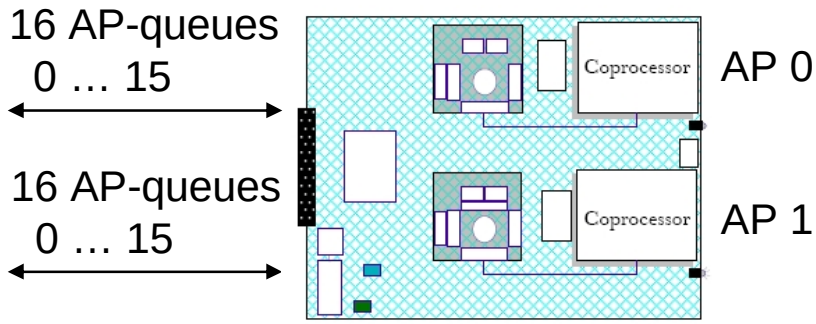


(*) PCICC was never supported by VSE

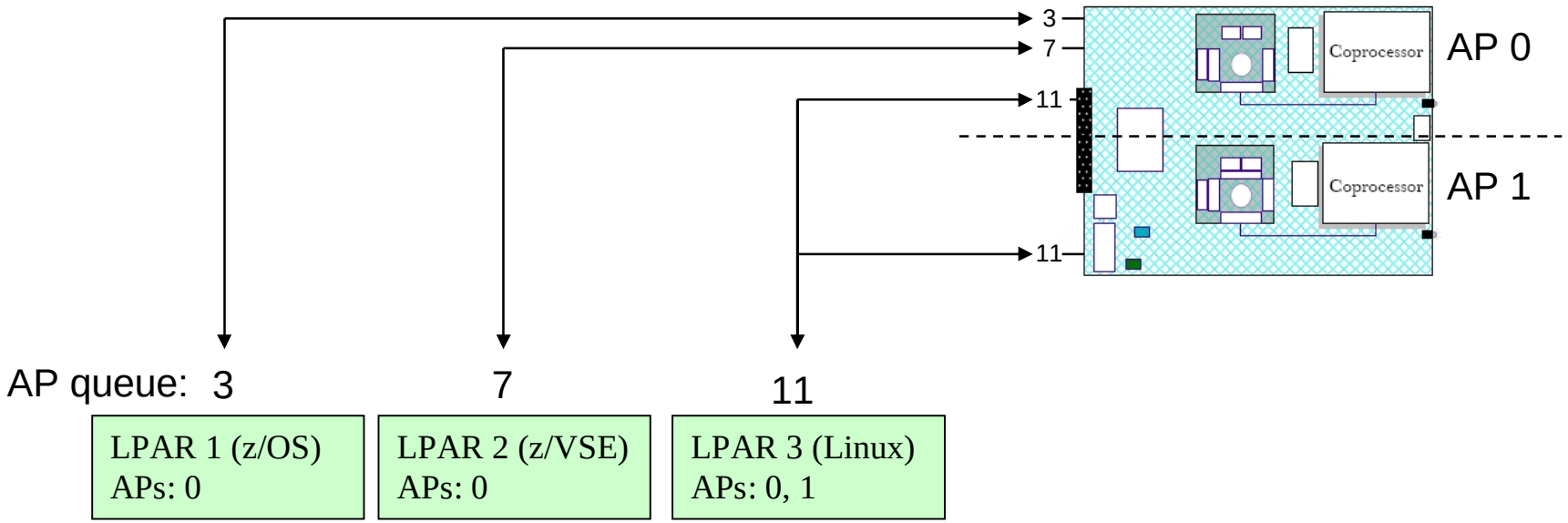
Crypto hardware - terms

- **AP: Adjunct processor**
  - A cryptographic processor on a crypto card
- **AP-queue (= cryptographic domain index)**
  - An input/output queue to/from an AP

Example:
- Crypto card with 2 APs



Crypto hardware - AP Assignment to LPARs

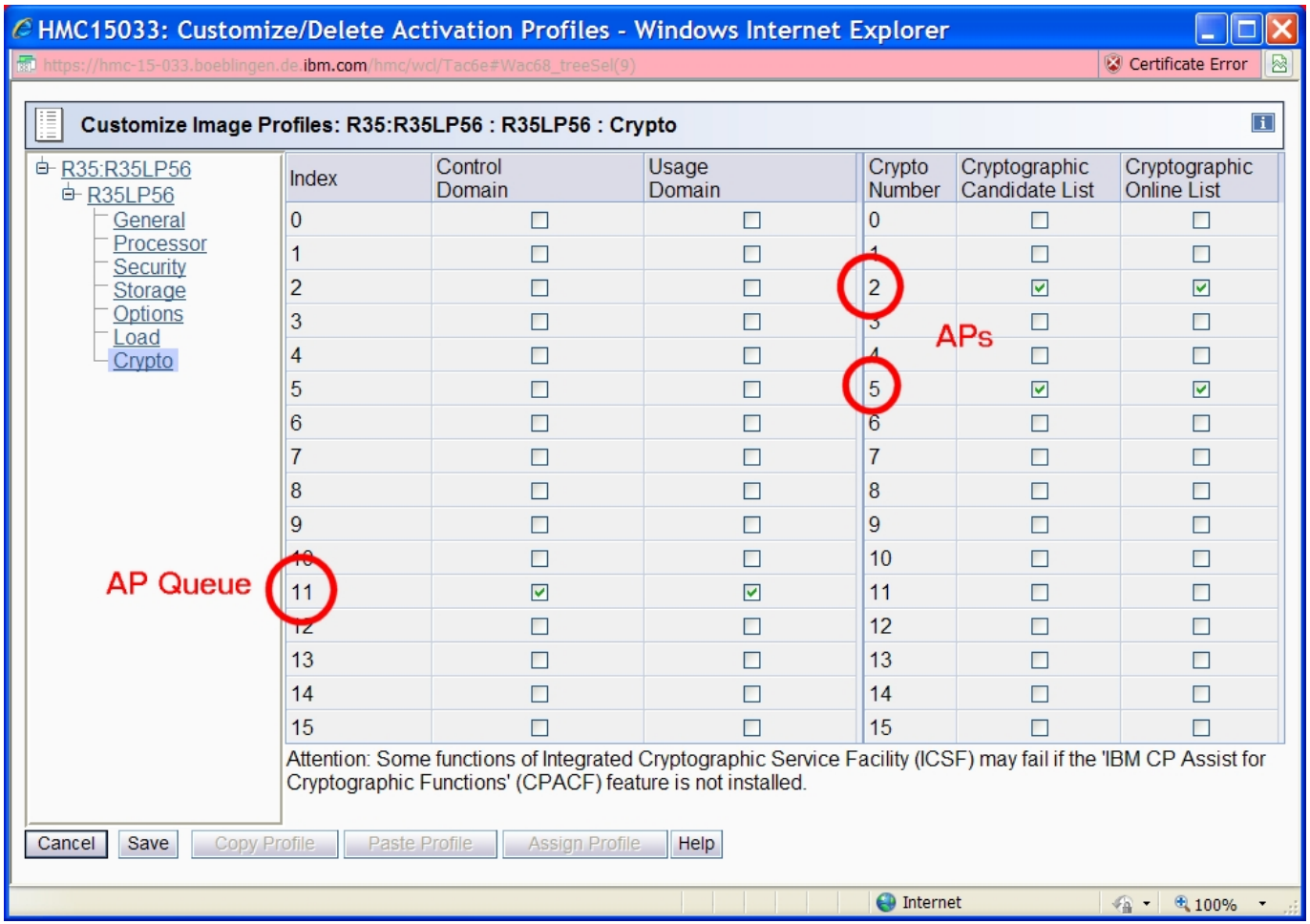


Each LPAR can use exactly 1 AP queue (cryptographic domain)

Each AP can serve up to 16 LPARs

Configuration via HMC / SE panels

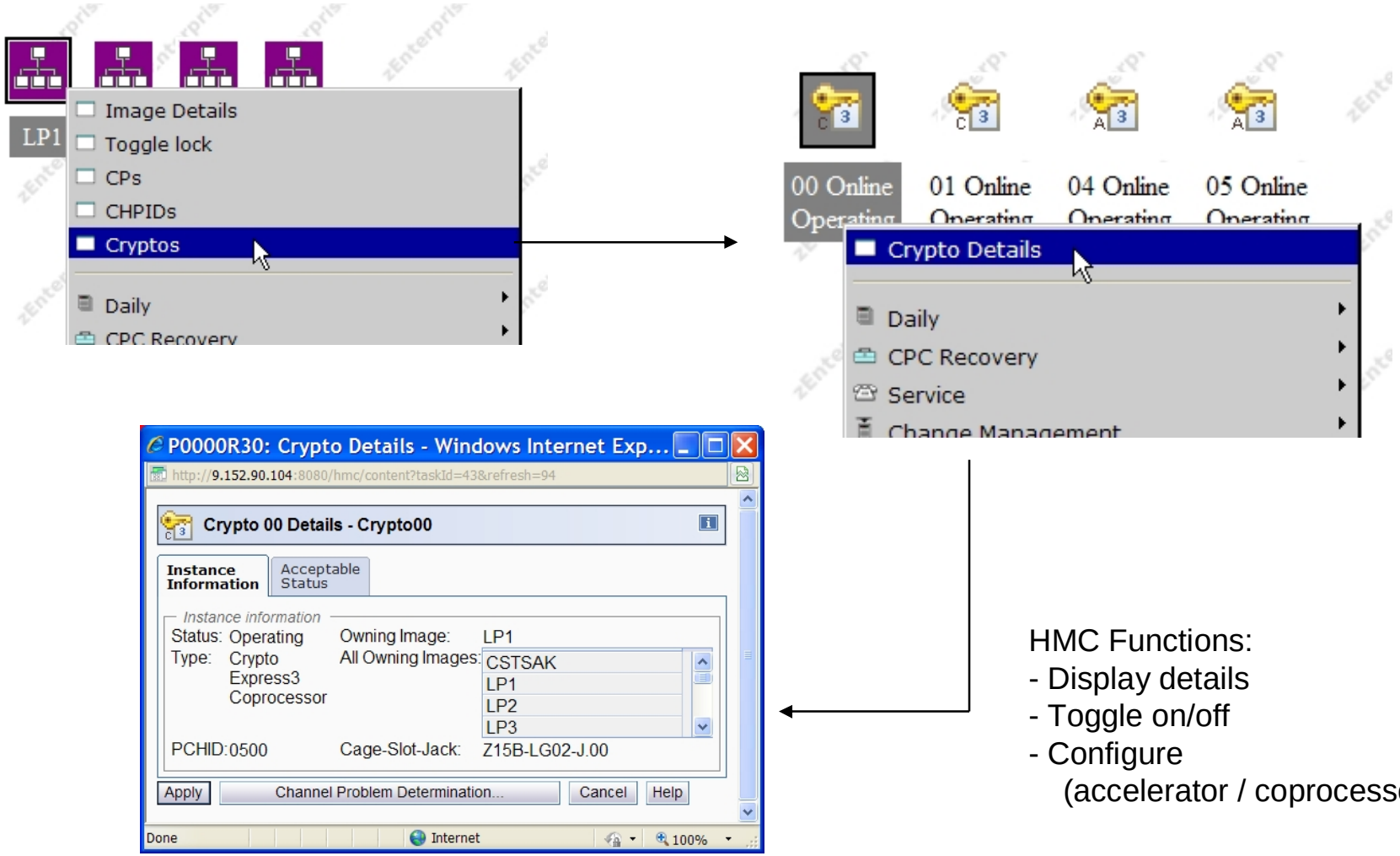
Crypto hardware - HMC/SE view



Assign APs and AP-queue to an LPAR

(Picture taken from a z196)

Crypto cards view on HMC/SE



HMC Functions:
- Display details
- Toggle on/off
- Configure
  (accelerator / coprocessor)

Crypto hardware - supported RSA key lengths per card

RSA key length	PCICA	PCIXCC	CEX2	CEX3A	CEX3C
1024 bits	yes	yes	yes	yes	Yes
2048 bits	Yes No on VSE	yes	yes	yes	yes
4096 bits	no	no	no	No on z10 and below Yes on z196	Yes on z10 and z196

- 4096-bit keys far ahead for most VSE customers
- However, some customers already wanted to move to 2048-bit keys, but then realized that they didn't have a crypto card. TCP/IP for VSE provides RSA encryption/decryption up to 1024 bits.

Supported CPACF algorithms per processor

Algorithm	z890 / z990	System z9 BC or EC	System z10 BC or EC	zEnterprise 196 (2)
MD5	yes (1)	yes (1)	yes (1)	yes (1)
SHA-1	yes	yes	yes	yes
SHA-224	no	yes	yes	yes
SHA-256	no	yes	yes	yes
SHA-384	no	no	yes	yes
SHA-512	no	no	yes	yes
DES	yes	yes	yes	yes
TDES	yes	yes	yes	yes
AES-128	no	yes	yes	yes
AES-192	no	no	yes	yes
AES-256	no	no	yes	yes

(1) **Only available as software implementation in TCP/IP for VSE/ESA, not via CPACF!**

(2) **The z196 additionally supports a number of encrypted key functions that are currently not recognized by VSE (see Principles of Operation manual)**

Overview on utilities and tools

- **Host-side functionality**
  - VSE crypto device driver
  - VSE support for TS1120/TS1130 tape drives
  - Encryption Facility for z/VSE V1.2
  - CIAL utilities provided with TCP/IP for VSE
  - SSL support in TCP/IP and various applications (FTP, Telnet, CICS Web Support, Connectors, MQ, etc.)
- **PC-side utilities**
  - Keyman/VSE (maintain keys and certificates)
  - VSE Navigator (Java-GUI to access VSE file systems and functions, support for SSL)

Crypto device driver - commands

- **Available commands can be queried via help command:**
  - msg fb,data=help
  - The commands are described in the VSE Admin book

Shows crypto status

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

New with VSE 4.3 →

Crypto device driver - show crypto configuration in z/VSE

- **Can be displayed on console via device driver STATUS=CR command:**
  - First part shows device driver status and list of crypto cards

```
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 ........... : 4
FB 0011   NO. OF POSTED CALLERS .............. : 4
FB 0011   AP-QUEUE INTERRUPTS AVAILABLE ...... : YES
FB 0011   AP-QUEUE INTERRUPTS STATUS ......... : DISABLED
FB 0011   AP CRYPTO POLLING TIME (1/300 SEC).. : 1
FB 0011   AP CRYPTO WAIT ON BUSY (1/300 SEC).. : 75
FB 0011   AP CRYPTO RETRY COUNT ............... : 5
FB 0011   AP CRYPTO TRACE LEVEL ............... : 0
FB 0011   TOTAL NO. OF WAITS ON BUSY ......... : 0
FB 0011   CURRENT REQUEST QUEUE SIZE ......... : 0
FB 0011   CURRENT PENDING QUEUE SIZE ......... : 0
FB 0011   ASSIGNED APS : PCICC / PCICA ....... : 0 / 0
FB 0011                  CEX2C / CEX2A ....... : 3 / 2
FB 0011                  CEX3C / CEX3A ....... : 2 / 2
FB 0011                  PCIXCC .............. : 0
FB 0011     AP  0 : CEX2A   - ONLINE
FB 0011     AP  1 : CEX2A   - ONLINE
FB 0011     AP  2 : CEX2C   - ONLINE
FB 0011     AP  4 : CEX2C   - ONLINE
FB 0011     AP  5 : CEX2C   - ONLINE
FB 0011     AP  8 : CEX3C   - ONLINE
FB 0011     AP  9 : CEX3A   - ONLINE
FB 0011     AP 10 : CEX3C   - ONLINE
FB 0011     AP 11 : CEX3A   - ONLINE
```

Crypto device driver - show crypto configuration in z/VSE

- **Second part shows CPACF functions**
  - Availability of particular CPACF functions depends on the processor and enablement of feature code #3863
  - This output is for example taken from a z10:

```
...
FB 0011 CPU CRYPTOGRAPHIC ASSIST FEATURE:
FB 0011   CPACF AVAILABLE ..................... : YES
FB 0011   INSTALLED CPACF FUNCTIONS:
FB 0011     DES, TDES-128, TDES-192
FB 0011     AES-128, AES-192, AES-256, PRNG
FB 0011     SHA-1, SHA-256, SHA-512
FB 0011 END OF CPACF STATUS
```

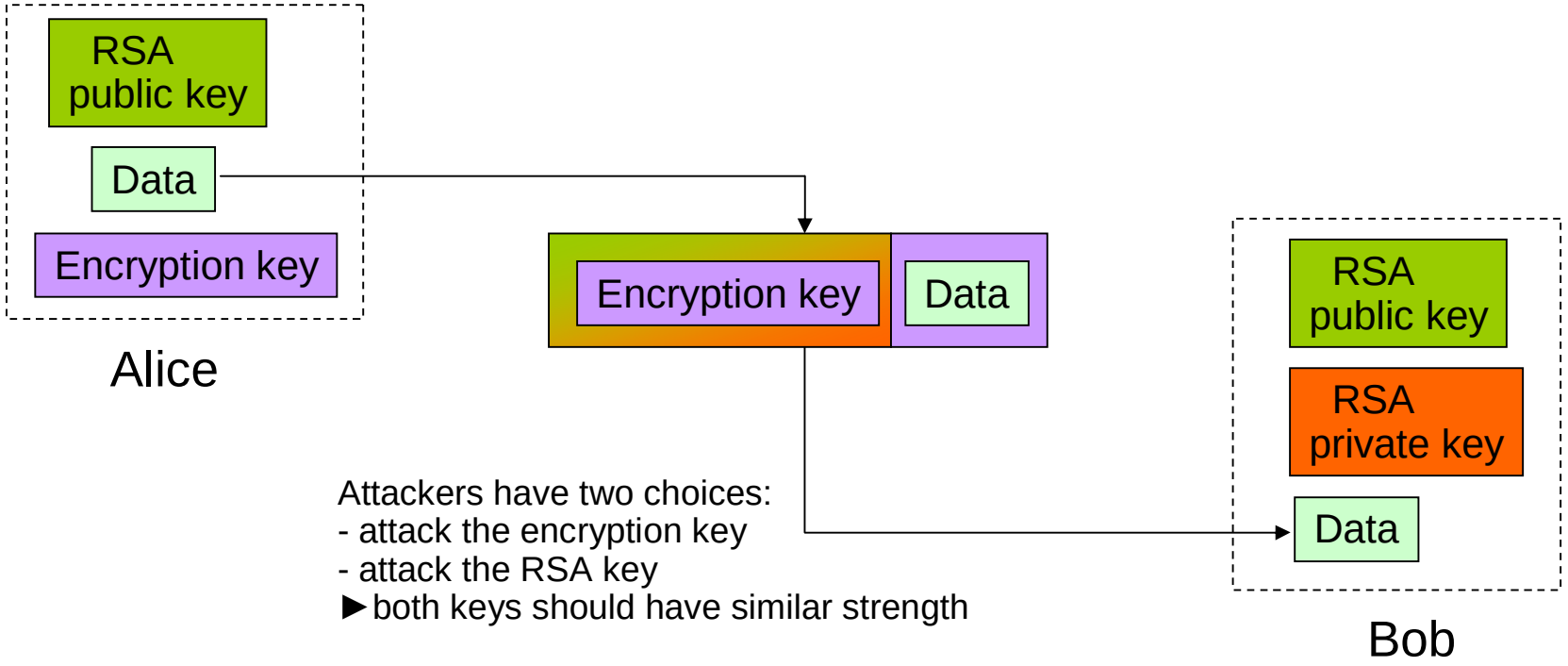
Enhancements with z/VSE 4.3

New with z/VSE 4.3: AP-interrupts

- **Support for AP-interrupts is a new function of System z10 and zEnterprise 196**
- **A hardware interrupt is issued when a response is ready for de-queueing from a card.**
  - Removes the need for the formerly used polling mechanism
  - User can switch between polling and interrupts (default: polling)
  - Using interrupts increase throughput for certain workloads without increasing CPU load
- **Not available under VM!**
- **Supported cards are**
  - Crypto Express2 and
  - Crypto Express3
- **The VSE crypto device driver provides new commands:**
  - APEAI, enable AP interrupts for all APs
  - APDAI, disable AP interrupts for all APs

New with z/VSE 4.3: Support for 4096-bit RSA keys

- **First: a look how and when RSA is used**
  - SSL: during the SSL handshake when opening an SSL connection
  - Data encryption (e.g. Encryption Facility): protect the symmetric encryption key with an RSA key



Comparison of key strength

- **Equivalent key sizes (Source: RFC4880)**

Asymmetric key size (bits)	Symmetric key size (bits)	
1024	80	
2048	112	← Triple-DES (3 keys)
3072	128	← AES-128
4096		
7680	192	← AES-192
15360	256	

- **RSA 4096 fills the gap between AES-128 and AES-192**
- **Required hardware for RSA-4096:**
  - Crypto Express3 (CEX3A or CEX3C)
- **Required software:**
  - z/VSE 4.3 with APAR **DY47171 (PTF UD53607)**
  - TCP/IP for VSE/ESA 1.5F with APAR **PM33000 (UK64983)**
  - Keyman/VSE for creating the 4k key and SSL certificates (CIALCREQ does not support 4k keys)

New with z/VSE 4.3: RSA key generation on mainframe

- **Old:**
  - RSA keys are created on a workstation either with the Keyman/VSE tool or a CSI-provided utility. Such tools are called “CIAL clients”
  - Keys are uploaded to the TCP/IP provided CIALSRVR utility and stored in a library member
- **New:**
  - RSA keys can be created directly on the mainframe using a crypto card
  - New VSE crypto device driver function, described in the “HW crypto vendor API doc”
  - Required hardware:
    - PCIXCC
    - Crypto Express2 in coprocessor mode (CEX2C)
    - Crypto Express3 in coprocessor mode (CEX3C)
  - Required software:
    - z/VSE 4.3 with APAR DY47171 / PTF UD53607
    - TCP/IP 1.5F with APAR PM33000 / PTF UK64983

RSA key generation on mainframe - example

- **CSI utility CIALSRVR is updated to support new command GENRSAPK**
- **TCP/IP Programmer's Guide is updated with errata doc from Dec 20, 2010:**
  - New API function described: `cry_rsa_genprvk( )`
  - The new function is included with zap 1.5F 419
- **Current example:**

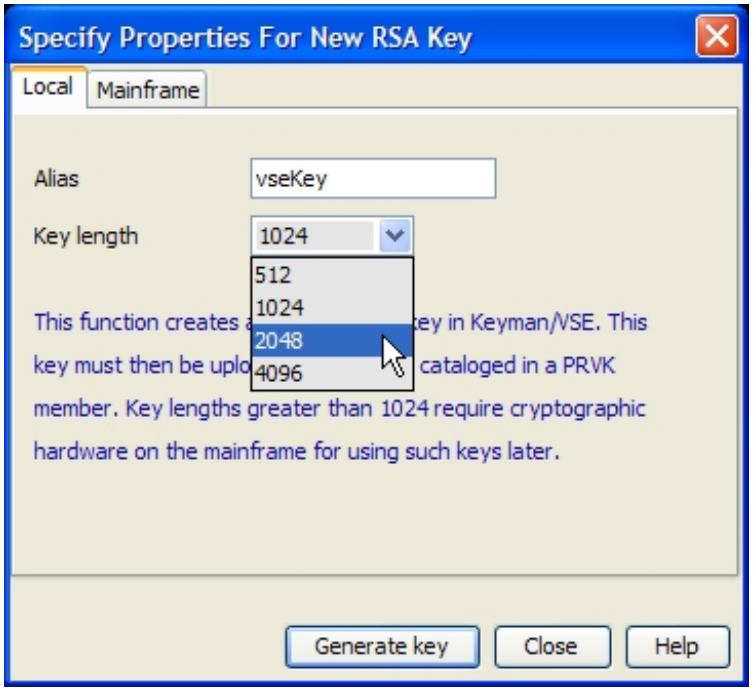
```
* $$ JOB JNM=CIALGRSA,DISP=D,CLASS=Z
// JOB CIALGRSA GENERATE RSA KEY PAIR
// OPTION SYSPARM='00'
// LIBDEF *,SEARCH=(PRD2.TCP15F,PRD2.CONFIG,PRD1.BASE)
// EXEC CIALSRVR,SIZE=CIALSRVR,PARM='CRYPTO.KEYRING.RSA4096'
GENRSAPK 4096
/*
/&
* $$ EOJ
```

New with z/VSE 4.3: Random number generation

- **New VSE crypto device driver function**
  - Requires a coprocessor card (PCIXCC, CEX2C, CEX3C)
  - Allows creating 8 up to 8192 random bytes per request
  - Random numbers are “true random numbers”
  - Works without any seed value
- **New API function is provided by CSI**
  - TCP/IP Programmer’s guide with errata doc from Dec 20, 2010 describes the new API function:
    - `cry_gen_random( )`
    - Max number of random bytes limited to 2048
  - Currently there is no CSI utility exploiting this function

New with VSE 4.3: Keyman/VSE enhancements

- **Support for 4096-bit keys**
- **Support for key generation on VSE:**

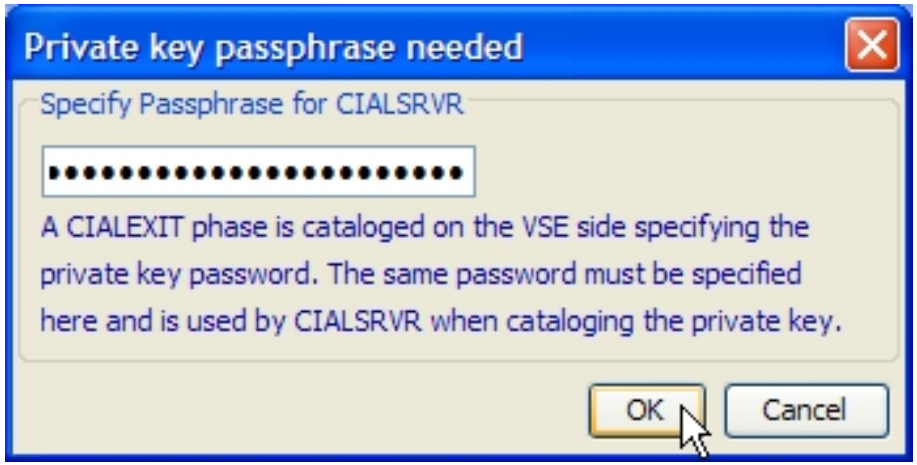


Up to now: Create key locally and upload to VSE

New: Create key on VSE using a crypto card

New with VSE 4.3: Keyman/VSE enhancements

- **Support for a CIALEXIT phase**
  - Allows specifying a custom passphrase and encryption keys for uploading RSA keys from a CIAL client.
  - A sample CIALEXIT JCL is provided in subdirectory /samples
  - When a CIALEXIT phase is cataloged on VSE, the CIAL client must specify the correct passphrase when sending a key to CIALSRVR
  - Keyman prompts for the passphrase when a CIALEXIT phase is cataloged on VSE



New with VSE 4.3: VSE Navigator enhancements

- **New dialogbox for Encryption Facility**
- **Menu choices encrypt / decrypt**
  - Automatic check if Encryption Facility available on VSE side
  - Right-click VSE library members or VSAM files
  - Check for available algorithms on host side
- **Needs VSE Connector Client**
- **Download from VSE homepage**
- **Provided “as is”**

TCP/IP Enhancements

- **CIALGPUB (ZP15F435)**
  - New utility to extract the public portion of the RSA private key
- **CIALPUBK (ZP15F436)**
  - New utility to read the output from CIALGPUB
  - Will then create a .PUBK lib.sublib member that contains just the public portion of the RSA key

New with z/VSE 4.3: ZIP support

- **Introduced as part of Encryption Facility for z/VSE V1.2 OpenPGP.**
  - EF optionally uses ZIP for compressing data before encrypting
- **Code downloaded and ported from http://zlib.net**
  - Based on code-level zlib 1.2.3
- **New phase $IJBZLIB**
  - Part of z/VSE base operating system
  - Located in IJSYSRS.SYSLIB
  - Provides an LE-C API
- **Currently only used by Encryption Facility, OpenPGP**
- **Could be used by customers and vendors also**
  - ZIP-file with a usage example downloadable from VSE homepage http://www.ibm.com/systems/z/os/zvse/downloads/samples.html
  - Docs, examples, FAQs available on http://zlib.net
- **Support:**
  - Provided via mailbox zvse@de.ibm.com

More information

z/VSE Administration

http://www.ibm.com/systems/z/os/zvse/documentation/#vse

Redbook “Security on IBM z/VSE”, SG24-7691-01

http://www.redbooks.ibm.com/abstracts/sg247691.html?Open

IBM Cryptographic Hardware Products

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

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

http://www.ibm.com/security/products/

Download Keyman/VSE, VSE Navigator, VSE Connector Client

http://www.ibm.com/systems/z/os/zvse/downloads/

TCP/IP Optional Features book

http://www.csi-international.com/products/zVSE/TCP-IP/TCP-IP-doc.htm

Questions