Session IS04

Security and Encryption
What's new in System z?

Dr. Manfred Gnirss

Technical Marketing Competence Center Europe,

R&D Support Support Centers Boeblingen

IBM Deutschland Research & Development GmbH

gnirss@de.ibm.com

Trademarks

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

IBM*	IMS	z10
IBM logo*	Resource Link	z10 BC
ibm.com	RMF	z10 EC
APPN*	System z	zSeries
CICS*	System z9*	z/VSE
DB2*	System z10	z/Architecture*
Destination z	System z10 Business Class	z/OS*
eServer	WebSphere*	z/VM*
HiperSockets	z9*	

* Registered trademarks of IBM Corporation

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.
Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.
Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.
Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.
Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.
UNIX is a registered trademark of The Open Group in the United States and other countries.
Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.
ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.
IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency, which is now part of the Office of Government Commerce.

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.

Acknowledgement

My very best thanks belong to

Alan Altmark

z/VM Development

IBM, Endicott

and

Jörg Schmidbauer

z/VSE Development & Service 1

IBM, Böblingen

for their input to this presentation

Agenda

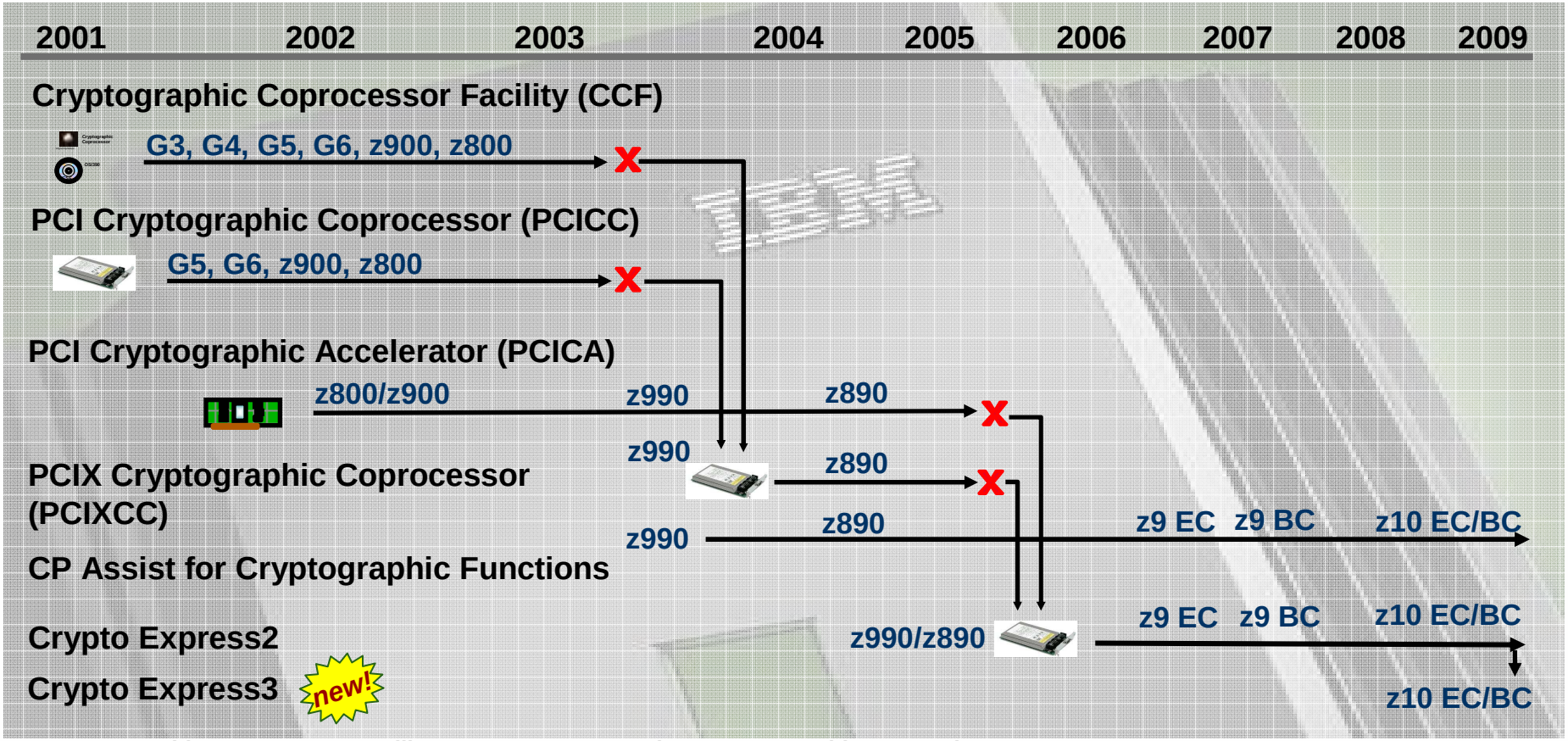
- **IBM System z10 EC GA3 and z10 BC GA Crypto Enhancements**
- **z/VM Security News**
- **Linux on System z selected topics**
- **z/VSE Security and Encryption**

System z10:Cryptographic Hardware Support

Summary:

- **Planning and installation/configuration tasks for CEX2 feature simplified by dynamic assingment of adapters/cards, domains to LPAR**
  - Dynamic changes can be temporary or permanent (activation profile)
  - Candidate AP.Domains cannot be removed if they are online
  - Candidate APs cannot be added if the changed configuration would intersect with an active LPAR definition (AP.Domain)
- **New Domain Zeroize function**
- **New CPACF functions with IBM System z10**
  - AES 256
  - SHA 512
- **System z10 EC GA3 z10 BC GA2:**
  - Crypto Express3
  - CPACF Secure/protected Key
  - TKE 6

System z Crypto History



- **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 limited "Clear key" crypto functions from any CP/IFL**
  - NOT equivalent to CCF on older machines in function or Crypto Express2 capability
- **Crypto Express2 – Combines function and performance of PCICA and PCICC**
- **Crypto Express3 – PCI-e Interface, additional processing capacity with improved RAS**

Statement of Direction – October 2009

- **Removal of Crypto Express2 feature:**
  - The IBM System z10 EC and z10 BC will be the last servers to offer Crypto Express2 (FC 0863) as a feature, either as part of a new-build order, or carried forward on an upgrade.

z10 – Protected key CPACF – a blending clear key and secure key cryptography

Clear versus Secure Keys

The security of encryption relies upon keeping the value of the key a secret. A secure key is simply a key that has been encrypted under another key, usually the master key. A clear key is a key that has not been encrypted under another key and, therefore has no additional protection within the cryptographic environment.

The CPACF enhancement is designed to:

- Help facilitate the continued privacy of key material when used by the CPACF for high performance data encryption.
- Provide additional security for cryptographic keys.
- Leverage the unique z/Architecture® and helps to ensure that key material is not visible to applications or operating systems when used for encryption operations.
- Provide significant throughput for large volumes of data and low latency for small blocks of data.
- Enhance the information management tool, IBM Encryption Tool for IMS™ and DB2® Databases, by improving performance for protected key applications.

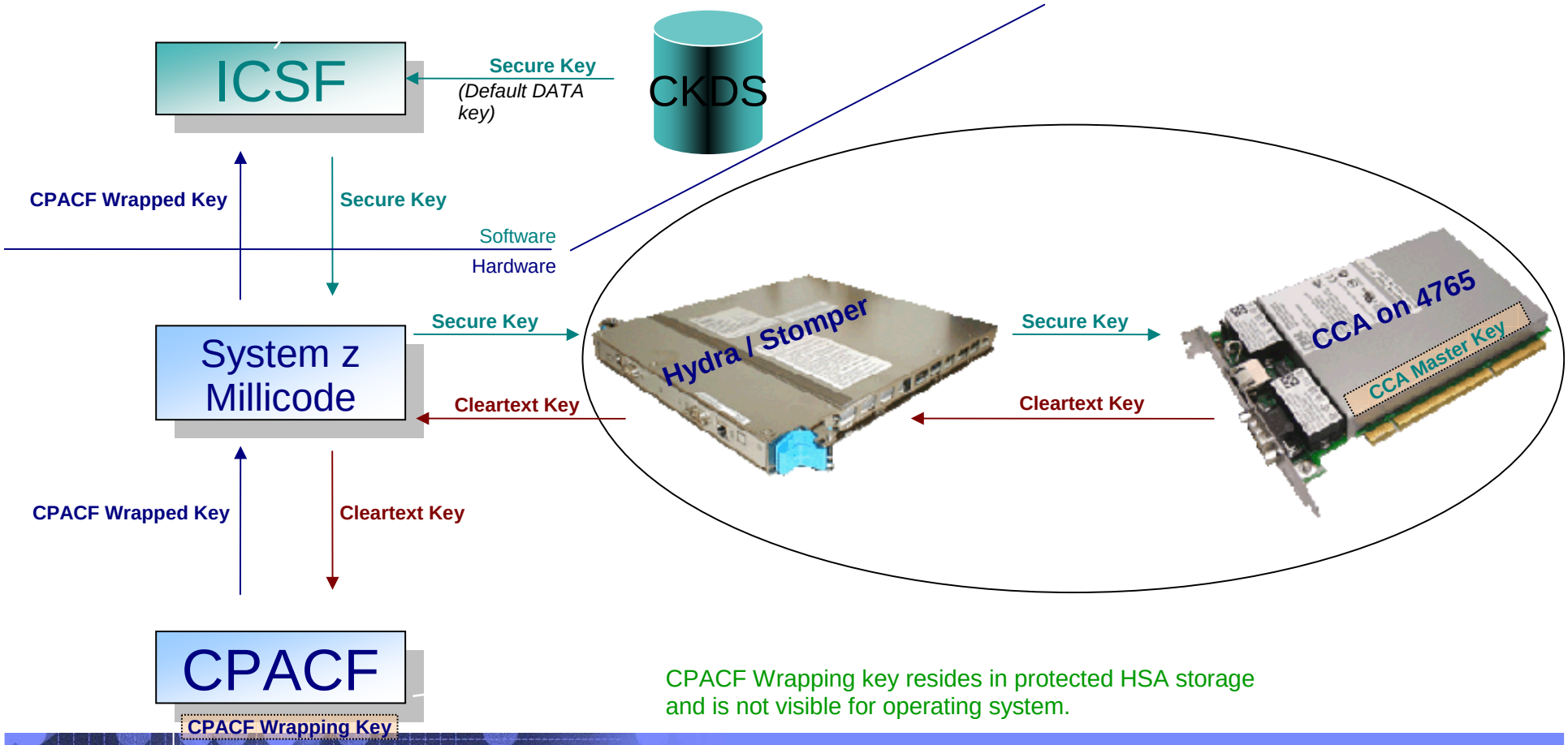
System z Symmetric Encryption – Enhanced View

	zSeries 900	System z z9 & z10		System z z10
	Secure Key	Clear Key	Secure Key	Secure Key CPACF
Key Wrapping: Host Storage	CCA Master Key – **Key material is never visible in the clear outside the tamper resistant hardware boundary**	None **– Key material is visible in the clear in system and application storage .**	CCA Master Key – **Key material is never visible in the clear outside the tamper resistant hardware boundary**	CPACF Wrapping Key **– Key material is not visible in the clear in *operating system or application storage*.**
Key Wrapping: Key Store	CCA Master Key – **Key material is never visible in the clear outside the tamper resistant hardware boundary**	None **– Key material is visible in the clear key store.**	CCA Master Key – **Key material is never visible in the clear outside the tamper resistant hardware boundary**	CCA Master Key – **Key material is never visible in the clear outside the tamper resistant hardware boundary**
Key Store	**CKDS or *application key file***	**CKDS or *application key file***	**CKDS or *application key file***	**CKDS only**
Encryption Engine	CCF	CPACF **or software**	CEX2C	CPACF
Symmetric Encryption Algorithms	**DES and TDES**	**DES, TDES and AES**	**DES, TDES and AES**	**DES, TDES and AES**
Benefits	*High Performance* *High Security*	*High Performance*	*High Security*	*High Performance* *High Security*

Secure Key CPACF - Key Wrapping

CPACF Wrapped key stored in ICSF address space in fetch protected storage.

Source key is stored in CKDS as a CCA MK wrapped key.

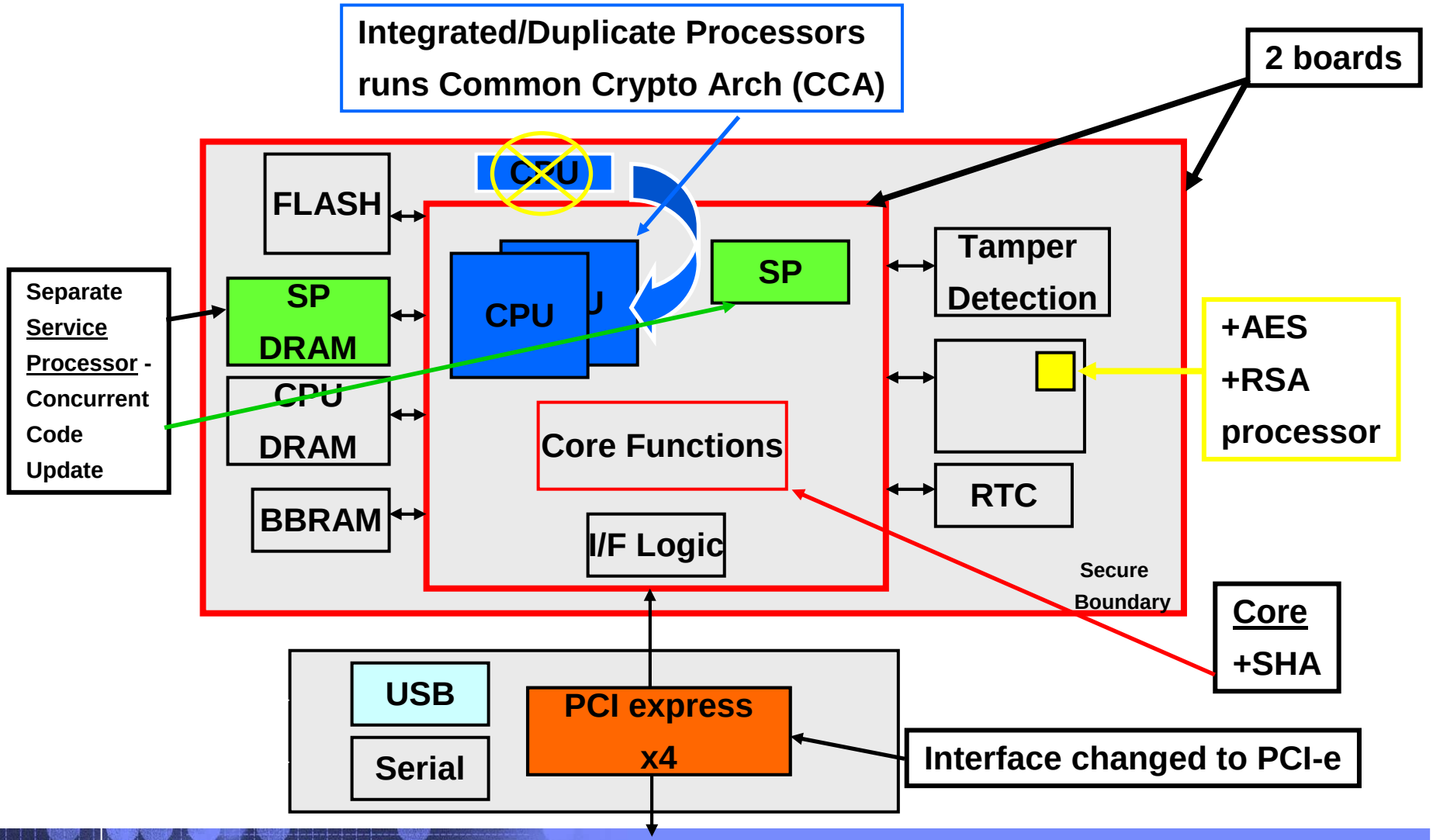


CPACF Wrapping key resides in protected HSA storage and is not visible for operating system.

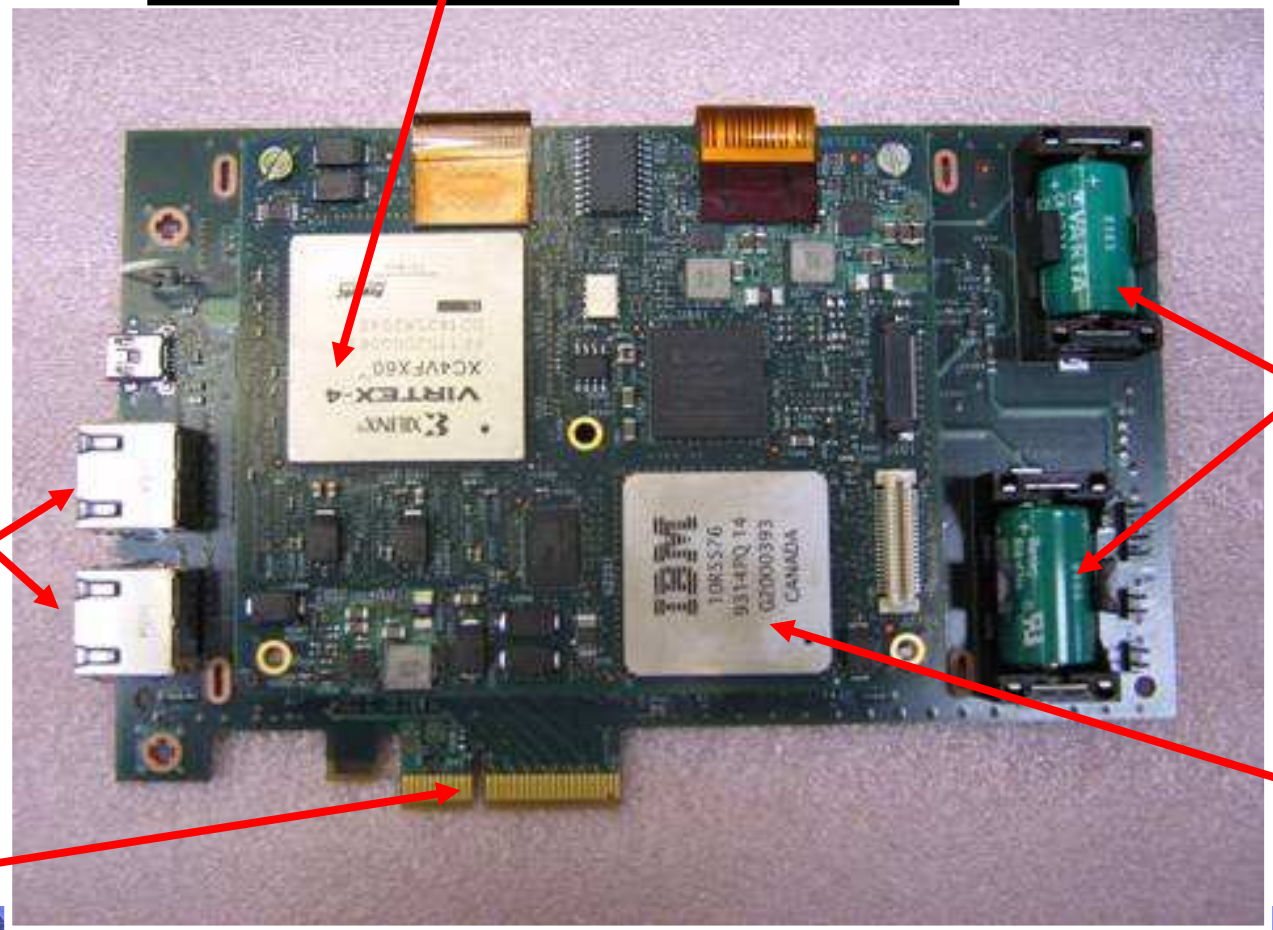
z10 Crypto Express3 – Hardware Design

- **Crypto Express3**
  - One or two Coprocessor features. One Coprocessor feature for z10 BC only
  - Each processor can be defined as a Cryptographic Coprocessor or an Accelerator
  - A minimum of two features must be ordered
- Integrated and duplicated Processors into field-programmable gate array (FPGA) to support Common Cryptographic Architecture (CCA)
- Specialized hardware to perform DES, TDES, AES, RSA, SHA1 and SHA-2 cryptographic operations
  - **SHA-2**
    SHA-2 (256-bit) hardware based on FIPS PUB 180-2 Secure Hash Standard
    SHA-256 is intended to provide 128 bits of security against collision attacks
  - **RSA**
    Two 2048-bit RSA engines are designed to provide improved performance for symmetric and asymmetric operations
- Separate Service Processor
- PCI-express (PCI-e)
- Designed to provides a state-of–the art tamper sensing and responding, programmable hardware to protect the cryptographic keys and sensitive custom applications
- The tamper-resistant hardware security module, which is contained within the Crypto Express3, is designed to meet the FIPS 140-2 Level 4 security requirements for hardware security modules

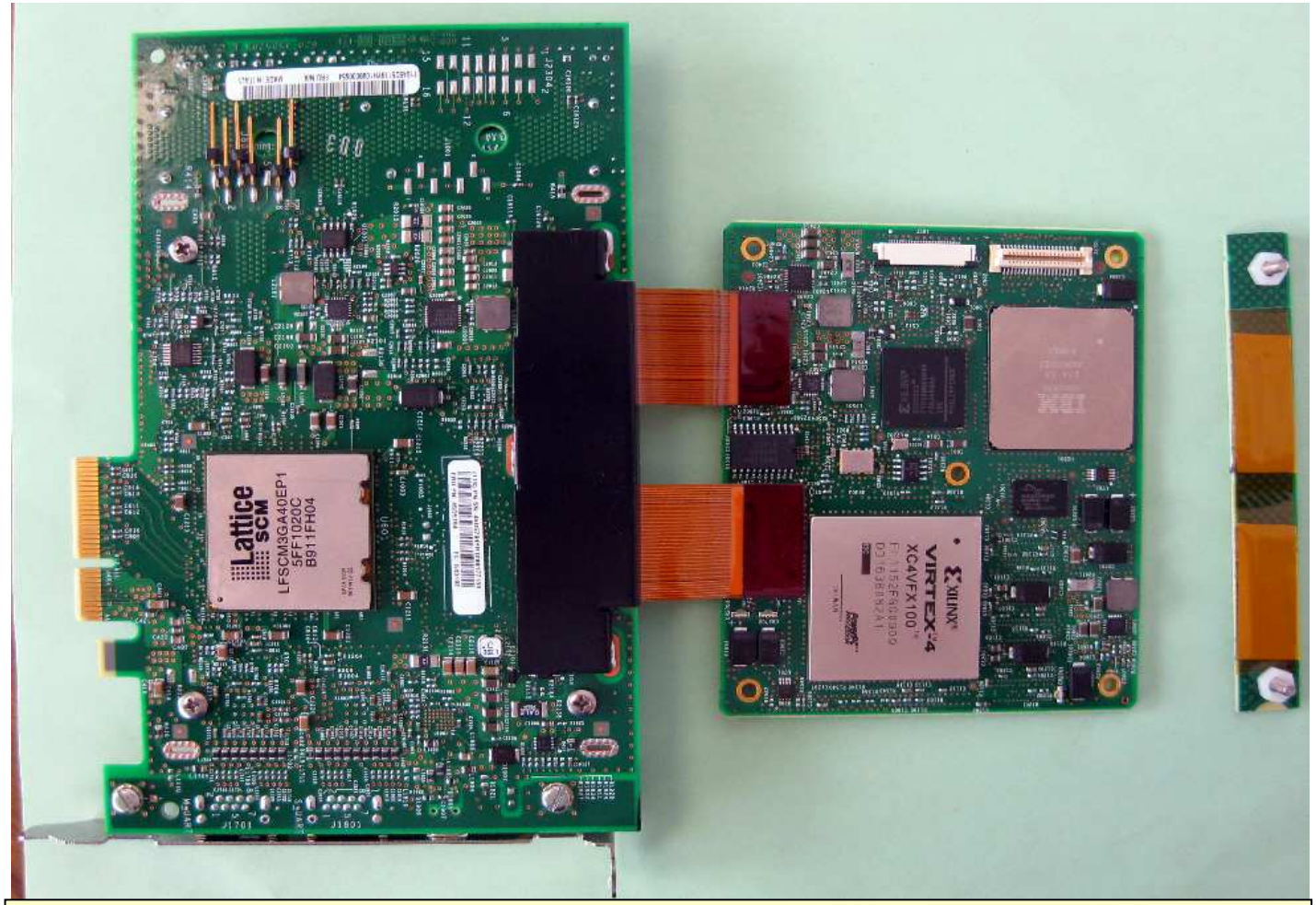
z10 Crypto Express3 (logical view)



z10 Crypto Express3 Internal View of single Coprocessor

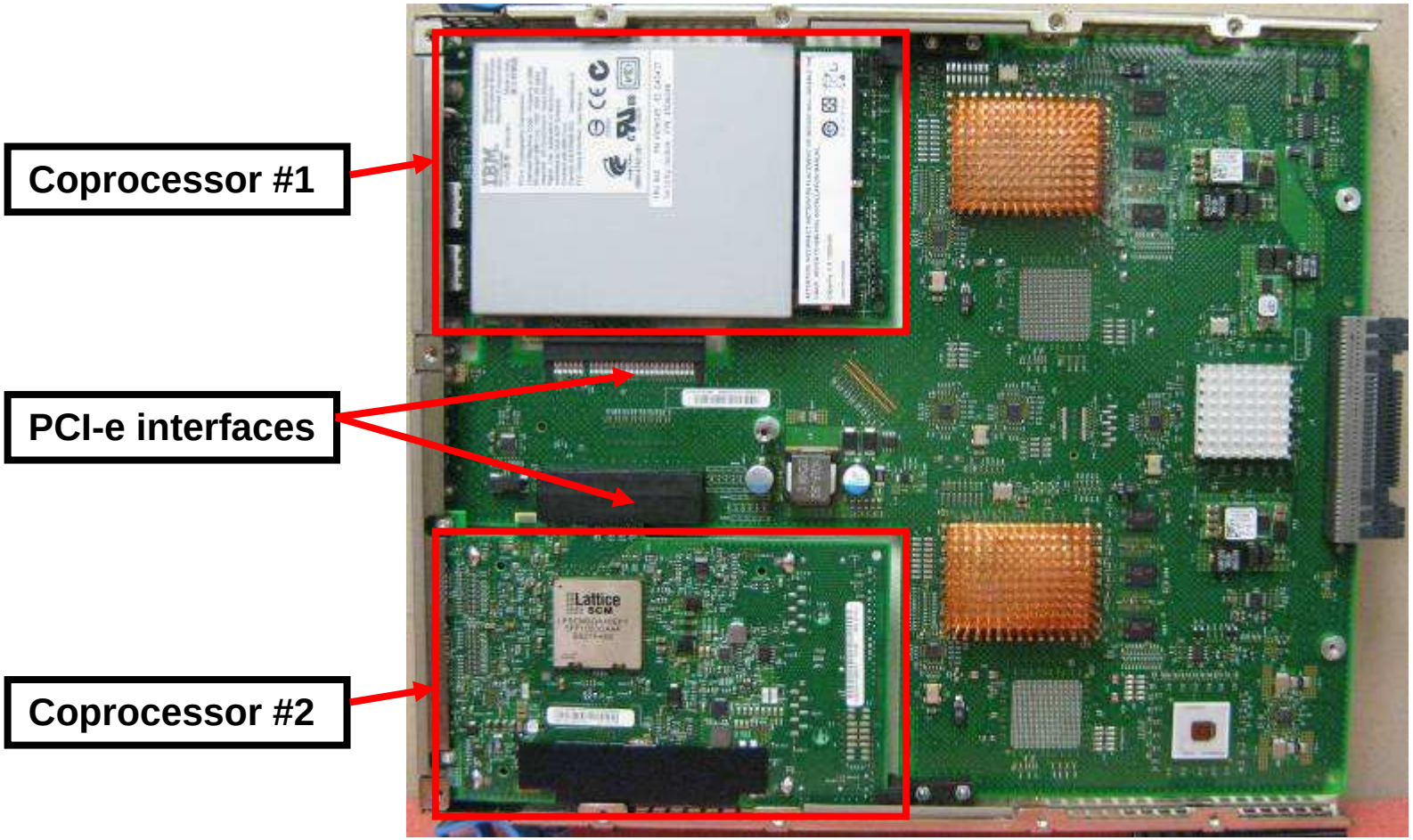


z10 Crypto Express3 Internal View of single Coprocessor



Un-encapsulated PCIe Base Card / Bottom Side to Secure Module Card – Top Side

Crypto Express3 2-P Physical View



Crypto Express3 1-P card does not have Coprocessor #2

Crypto Express3 1-P Physical View

z10 Crypto Express3 feature highlights

- Dynamic power management to maximize RSA performance while keeping within temperature limits of the tamper-responding package
- Virtualization: all logical partitions (LPARs) in all Logical Channel Subsystems (LCSSs) have access to the Crypto Express3 feature, up to 32 LPARs per feature
- Designed for improved reliability, availability and serviceability (RAS)
- Secure code loading that enables the updating of functionality while installed in application systems
- Executes its cryptographic functions asynchronously to a Central Processor (CP) operation in System z10 BC and z10 EC servers

Continued

z10 Crypto Express3 features highlights

- Lock-step-checking of dual CPUs for enhanced error detection and fault isolation of cryptographic operations performed by coprocessor when a PCI-E adapter is defined as a coprocessor
- Dynamic addition / configuration of cryptographic features to logical partitions without an outage
- Updated cryptographic algorithms used in loading the Licensed Internal Code (LIC) with the TKE workstation to keep in step with current recommendations for cryptographic strength
- Support for smart card applications using Europay, MasterCard Visa specifications
- Health Monitoring of mesh, temperature, voltage, soft tamper and low battery

z10 Crypto Express3 defined as a Cryptographic Coprocessor

- **When one or both of the two PCI-E cryptographic adapters are configured as a coprocessor can be used to:**
  - Encrypt and decrypt data by utilizing secret-key algorithms. Algorithms supported for data confidentiality are:
    - Double-length key DES
    - Triple-length key DES
    - AES algorithms that have 128, 192 and 256-bit data-encrypting keys
- **Generate, install, and distribute cryptographic keys securely using both public and secret key cryptographic methods**
- **Generate, verify, and translate personal identification numbers (PINs)**
- **Generate, verify, and translate 13- through 19- digit personal account numbers (PANs).**
- **Ensure the integrity of data by using message authentication codes (MACs), hashing**
  - Algorithms, and Rivest-Shamir-Adelman (RSA) public key algorithm (PKA) digital
  - Signatures
- **Key management using TDES, RSA or other security based algorithmic processes**
- **Highly secure encryption processing, use of secure encrypted key values, and User Defined Extensions (UDX) to CCA**
- **Secure remote key loading of encryption keys to ATMs, point of sale terminals (POS) and PIN entry devices**
- **Cryptographic key exchanges between IBM CCA and Non-CCA servers**
- **Generation of high quality random numbers for keys and other cryptographic applications**

z10 Crypto Express3 defined as an Accelerator

- **When one or both of the two PCI-E cryptographic adapters are configured as an accelerator, the Crypto Express3 feature can be used for:**
  - High performance clear-key RSA functions
  - Acceleration of modular arithmetic operations, that is, the RSA cryptographic operations used with the SSL/TLS protocol.
  - Offloading compute-intensive RSA public-key and private-key cryptographic operations employed in the SSL protocol
- **Supported functions include:**
  - PKA Decrypt (CSNDPKD), with PKCS-1.2 formatting
  - PKA Encrypt (CSNDPKE), with zero-pad formatting
  - PKA Digital Signature Verify
  - The RSA encryption and decryption functions support key lengths of 512 bits to 4,096 bits, in the Modulus Exponent (ME) and Chinese Remainder Theorem (CRT) formats.

New Trusted Key Entry Workstation with Licensed Internal Code (LIC) 6.0

- **The Trusted Key Entry (TKE) workstation is a combination of hardware and software, network-connected to the server, and designed to provide a security-rich, flexible method for master and operational key entry as well as local and remote management of the cryptographic coprocessor**
- **The TKE workstation has one Ethernet port and supports connectivity to an Ethernet Local Area Network (LAN) operating at 10 and 100 Mbps**
  - The workstation includes a system unit, mouse, keyboard, flat panel display, DVD-RAM drive to install Licensed Internal Code (LIC), and a PCI-X Cryptographic Coprocessor
  - The workstation has one Ethernet port and a USB port for attaching a Smart Card Reader.
  - TKE workstations can also be used to control the z9 BC, z9 EC, z10 BC and z10 EC servers
- **TKE FC 0840 will be available on IBM System z9® Business Class (z9 BC) and Enterprise Class (z9 EC), z10 BC and z10 EC servers, beginning January 1, 2010**
- **If Trusted Key Entry is required on z10 BC and z10 EC, then a TKE workstation must be used**

z10 Trusted Key Entry 6.0 Licensed Internal Code (LIC)

- Usability enhancements
  - Includes stronger cryptography encryption for TKE protocols inbound /outbound authentication.
  - The TKE uses cryptographic algorithms and protocols in communication with the target cryptographic adapters in the host systems it administers.
  - The following enhancements have been made in this area:
- **Authentication**
  TKE Certificate Authorities (CAs) initialized on a TKE workstation with TKE 6.0 LIC can issue certificates with 2048-bit keys. Previous versions of TKE used 1024-bit keys
  - Transport keys
    The transport key used to encrypt sensitive data sent between the TKE workstation and a Crypto Express3 coprocessor has been strengthened from a 192-bit TDES key to a 256-bit AES key
  - Signature keys
    The signature key used by the TKE workstation and the Crypto Express3 coprocessor has been strengthened from 1024-bit key to a 4096-bit key. Replies sent by a Crypto Express3 coprocessor on the host are signed with a 4096-bit key

Trusted Key Entry 6.0 Smart Card Support

- **The TKE 6.0 LIC contains support to increase the key strength for TKE Certificate Authority (CA) smart cards, TKE smart cards, and signature keys stored on smart cards from 1024-bit to 2048-bit strength**

- **Only smart cards (FC 0884) with smart card reader (FC 0885) support the creation of TKE Certificate Authority (CA) Smart Cards, TKE smart cards, or signature keys with the new 2048-bit key strength. Smart cards (FC 0888) and smart card readers (FC 0887) will continue to work with the 1024-bit key strength**

z10 Crypto Express 3 – UDX

- **UDX (User Defined eXtension)**
  - Extends the functionality of IBM's CCA (Common Cryptographic Architecture) application program
    - Customized cryptographic verb controls per customer
  - Can't mix/match UDX definitions across Crypto Express 2 & Crypto Express 3
    - HMC/SE panels ensure that UDX files are applied to appropriate Crypto card type
- **UDX toolkit for System z with Crypto Express3**
- **The following are the User Defined Extension (UDX) Requirements for migration to Crypto Express3**
  - Upgrade of crypto card code to CCA level 4.0 ... (few changes from CCA release 3.30)
  - Upgrade of z/OS Service Routine for HCR7770 (major changes)

Software requirements for z10 GA3 Crypto features

- **Crypto Express3 and Crypto Express3-1P requires at a minimum:**
  - z/OS V1.9, z/OS V1.10 or z/OS V1.11 with the Cryptographic Support for z/OS V1R9-V1R11 Web deliverable planned to be available November 20, 2009
  - z/VM® V5.3 with PTFs for guest exploitation
  - z/VSE™ V4.2 and IBM TCP/IP for VSE/ESA V1.5.0 with PTFs
  - z/TPF V1.1 (acceleration mode only)
  - Linux on System z distributions:

    Current Novell SUSE and RedHat distributions support the same functionality as Crypto Express2. Secure key is not supported

Note: z/OS V1.9, z/OS V1.10 or z/OS V1.11 with the Cryptographic Support for z/OS V1R9-V1R11 Web deliverables may be obtained at:

http://www.**ibm.com**/systems/z/os/zos/downloads/

Agenda

- **IBM System z10 EC GA3 and z10 BC GA Crypto Enhancements**
- **z/VM Security News**
- **Linux on System z selected topics**
- **z/VSE Security and Encryption**

Security vs. Integrity

- **Security is only meaningful in the presence of system integrity!**
  - Integrity prevents bypass of security controls
  - Audit trail confirms conformance
    - Consider External Security Manager (RACF) for improved auditing

RACF Security Server for z/VM FL610

- **RACF Security Server for z/VM provides**:
  - Encrypted extended-length mixed-case passwords and password life-cycle management
  - Access Control Lists (ACLs) for z/VM system resources and networks
  - Separation of system and security administration duties
  - Authentication, authorization, and audit services to other products or servers
  - Protection from customer-defined resources
  - Ability to implement multiple security zones in a single z/VM instance
  - A detailed record of administrator and virtual server activities
- **RACF authentication and audit services are available to remote hosts through the z/VM LDAP server**
  - Adapted from the IBM Tivoli Directory Server for z/OS
  - Authorization services are available to Linux by use of the Linux LDAP pluggable authentication module (PAM)
- **Licensed as an IPLA optional feature of z/VM V6.1**
  - OTC charge based on Engine-based Value Units
  - Can be licensed on standard and IFL processors
  - Operates only on z/VM V6.1
  - S&S required for traditional service and no-charge upgrades
  - Preinstalled but disabled, license required

z/VM RACF Security Server feature

- z/VM 5.3 RACF database mapping error!
  - Unpredictable results if sharing with z/OS or z/VM 5.4
  - Apply APAR VM64383 – Follow the instructions EXACTLY
    - Do NOT upgrade database templates or share the database until this APAR is applied.
- Database has been updated with new templates
  - RACFCONV will fix-up a broken 5.3 database as part of migration, but any 5.3 system that is using it better have VM64383 applied!

z/VM RACF Security Server feature . . .

- IRRUT200 (database copy) instructions updated
  - No serialization, so no sharing
  - Must be run from RACFVM user ID
- IRRUT400 (database copy/split/merge/extend) instructions and examples updated
  - Can be run on active, shared databases

z/VM RACF Security Server feature . . .

- Password change logging for LDAP
  - When password is changed by administrator or user, a PKCS #7 encrypted envelope is created and placed into the RACF database
  - An LDAP change log record is created
  - LDAP client can extract the encrypted field

z/VM RACF Security Server feature . . .

- RACF recognizes current and alternate system operators when RACF server is down
  - Commands are accepted from the current system operator
    - SYSTEM_USERIDS
    - ALTERNATE_OPERATORS
    - SET SYSOPER
- – Allows commands and LOGON, deferring to CP for authorization and password checking

LDAP Server

- Upgrade to z/OS 1.10 ITDS
- Published back-end APIs to enable usage by other ESMs
- Support for password change logging
  - z/OS uses RACF certificate services
  - z/VM uses System SSL services
- Password phrase can now be used in an ldap bind

z/VM SSL server

- **Updated SSL server does not require a Linux distribution**
  - Deploy SSL/TLS services more quickly than in prior versions of z/VM
- **z/VM SSL server includes:**
  - Network-free SSL server administration
    - The SSL server is managed without requiring a network connection between the SSL server administrator and the SSL server
  - SSL/TLS session protection includes encryption using AES and triple-DES
    - Uses CPACF encryption hardware on the System z10 server
    - No exploitation of Cryptographic Coprocessors (cards)
  - Adapted from z/OS V1.10 System SSL
    - The System SSL GSKKYMAN utility is used to manage the SSL server certificate database. Includes certificate requests, renewal, import, and export
  - APIs are not published or supported for customer use

SSL Server

- **Certificate management via gskeyman**
  - Introduced in z/VM 5.3 with the LDAP server
  - Data held in BFS
  - Create user certficiates in response to a request
  - Create intermediate CAs and trusted CAs
  - Certificate export, import, renewal
  - Menu driven (linemode, so automation is possible)

- Working on plan to provide private key migration from z/VM 5.2 and 5.3

FTP Clear Command Channel (CCC)

- CCC subcommand recognized by z/VM client and server
- Issued **after** user ID and password are sent
- Control connection switches to clear-text
- File transfer is always encrypted

FTP Clear Command Channel (CCC) . . .

- Enables firewalls to dynamically open and close data ports for file transfer
  - Just like for non-secure FTP
- Enables 3rd-party audit of file transfer
- Eliminates need for PassivePortRange in the server

FTP Clear Command Channel (CCC) . . .

- Partner must support RFC 4217
  - Early drafts of the RFC did not define the behavior of CCC, so it was inferred
- z/OS FTP includes “TLSRFCLEVEL” option in FTP.DATA to control. The default is draft.
- No option is provided in z/VM to use the draft version

IBM Tivoli zSecure Manager for RACF z/VM

- **Combines capabilities of the most-used zSecure Audit and Admin functions for the virtual machine environment to:**
  - z/VM security management tasks with simple, one-step actions that can be performed without detailed knowledge of RACF command syntax
  - Quickly identify and prevent problems in RACF before they become a threat to security and compliance
  - Help ease the burden of database consolidation
  - Create comprehensive audit trails without substantial manual effort
  - Generate and view customized audit reports with flexible schedule and events elections
  - Licensed as an IPLA product and can operate on IFL processors
- **Requires ISPF for VM (5684-043)**
  - Helps make IBM Tivoli zSecure Manager for RACF z/VM more easy to use and more user friendly
  - ISPF/PDF adds some additional capabilities like ISPF browse and edit
  - ISPF is not available for ordering as an IPLA product but is available on a special-bid basis for licensing on IFL processors

Disk and tape encryption

- **Disk encryption**
  - Helps ensure your data-at-rest stays safe and secure with z/VM support for the use of the IBM Full Disk Encryption features of the DS8000
    - No z/VM configuration change is required to use the encryption features
    - Encryption status of a volume can be easily determined using a simple z/VM command

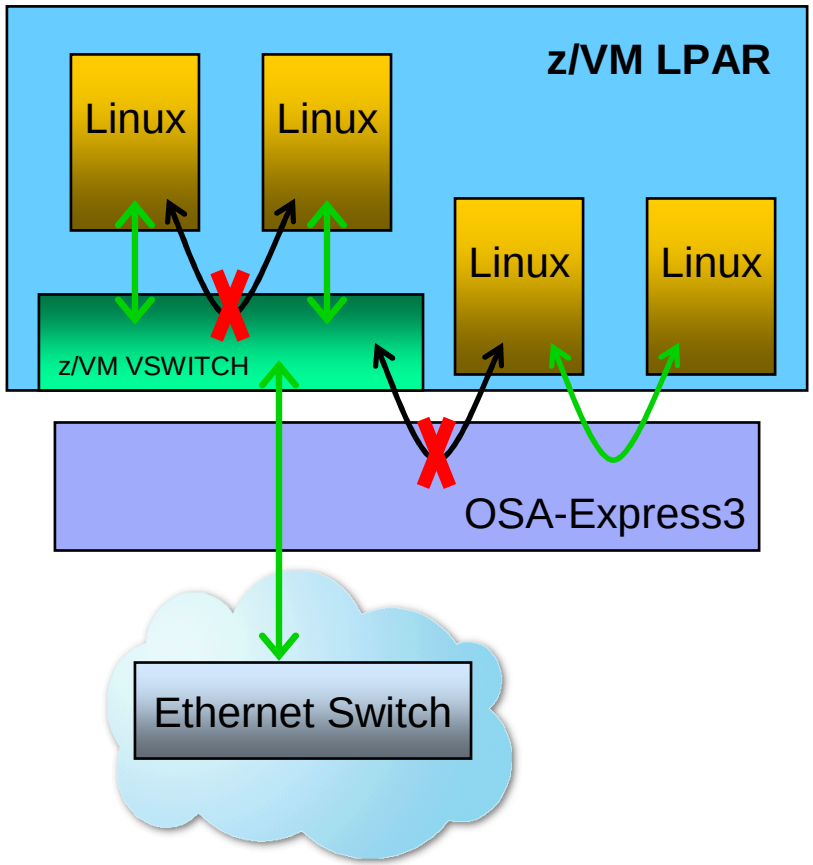
- **Tape Encryption**
  - Helps protect data on tape in a cost-effective way by providing support for drive-based data encryption
    - IBM System Storage TS1120 Tape Drive (machine type 3592, model E05)
    - IBM System Storage TS1130 Tape Drive (machine type 3592, model E06)
  - Support includes encryption for DDR, SPXTAPE, all CMS tape utilities, as well as for other guests that do not provide their own encryption enablement
  - z/VSE guests can use DFSMS/VM FL221 to locate encryption-capable 3592 tape drives in an Enterprise Automated Tape Library

Virtual Switch (VSWITCH) port and QDIO data connection isolation

- Create more secure multi-tier applications using virtual security zones
- Control which guests can use the VSWITCH
- Assign guests to specific VLANs using virtual access ports
- Control access to VLANs used by guests with virtual trunk ports
- Prevent guest-to-guest communications within the VSWITCH using VSWITCH isolation
- Guests using an isolated VSWITCH will be unable to communicate directly with other partitions sharing the OSA port
- Provided by OSA-Express2 and OSA-Express3 QDIO Data Connection Isolation function
  - Requires the following minimum MCLs with Driver 76 for the System z10 servers:
    - OSA-Express2 requires N10953.002
    - OSA-Express3 requires N10959.004 and N10967.055

z/VM Virtual Switch and OSA-Express Port Isolation

- **Allows users to restrict guest-to-guest communications within a Virtual Switch by exploiting OSA-Express QDIO data connection isolation**
- **Provides a mechanism to isolate a QDIO data connection on an OSA port**
  - Enables network isolation for operating systems sharing physical network connectivity



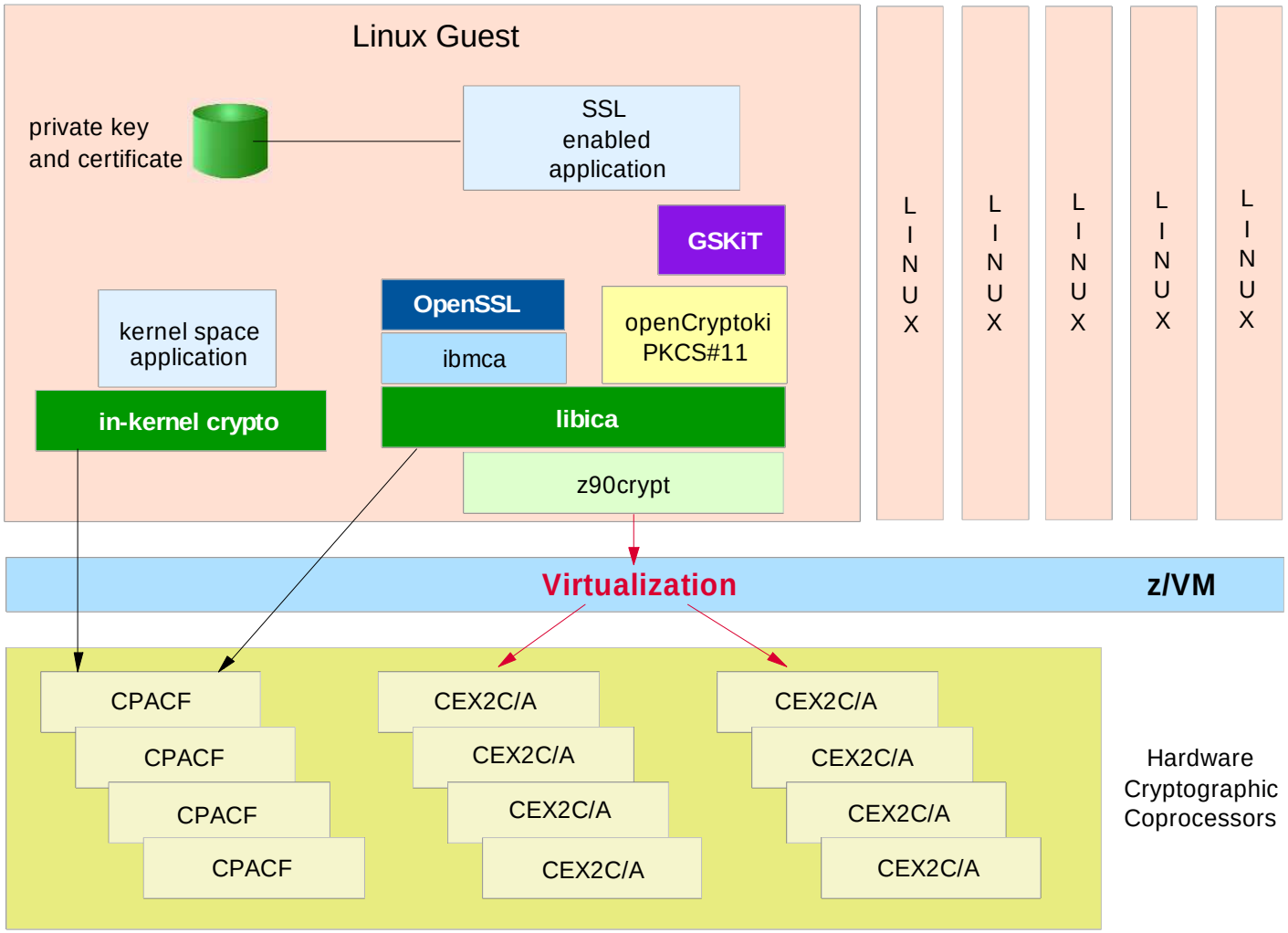
Support for Crypto Express3

- **Guest support for Crypto Express3 on the System z10 with the PTF for APAR VM64656 for z/VM V5.3 and later, planned to be available in November, 2009**

Agenda

- **IBM System z10 EC GA3 and z10 BC GA Crypto Enhancements**
- **z/VM Security News**
- **Linux on System z selected topics**
- **z/VSE Security and Encryption**

Access to Cryptographic Hardware Support with Linux for System z



z90crypt device driver

- Acess to CEX2C and CEX2A for clear key encryption
- Acess to CEX2C for secure key encryption
- Access to CEX3C and CEX3A in “near” future.
- z90crypt supports only 1 domain
- z90crypt can select domain automatically

– Not necessary to specify a domain for clear key
  Domain=-1 (this is the default) is used: Domain with highest number or AP devices (AP queues) is used. If multiple domains with identical (highest) number of AP devices, then domain with lowest number is used.
– Specify a domain for secure key

- If multiple AP devices, then improved load balancing between devices
- Poll thread to reduce latency for an application while waiting for result of CEX2C or CEX2A execution.
- Poll_thread=1 system is polling for result while waiting (attention, this is CPU intensive)
- Specify domain and poll_thread during load or in /etc/sysconfig/z90crypt
- modprob, insmod, or script rcz90crypt
- Don’t forget to configure load automatically of z90crypt for boot initialization (via chkconfig z90crypt on)

z90crypt: device driver status

```
gnirss@tmcc-123-168:~> cat /proc/driver/z90crypt
zcrypt version: 2.1.0
Cryptographic domain:  1
Total device count:  1
PCICA count: 0
PCICC count: 0
PCIXCC MCL2 count: 0
PCIXCC MCL3 count: 0
CEX2C count:  1
CEX2A count: 0
requestq count: 0
pendingq count: 0
Total open handles: 1
Online devices: 1=PCICA 2=PCICC 3=PCIXCC(MCL2) 4=PCIXCC(MCL3) 5=   CEX2C 6=CEX2A
        050000000000000 000000000000000  000000000000000 000000000000000

Waiting work element counts
        000000000000000 000000000000000 000000000000000 000000000000000

Per-device successfully completed request counts
   00000000 00000 143 00000000 00000000 00000000 00000000 00000000 00000000
. . .

gnirss@tmcc-123-168:~> cat /sys/bus/ap/devices/card01/request_count
323
```

z90crypt News

High resolution timer

Linux kernel version 2.6.27 or later a high resolution timer is used instead of the standard timer. Polling at nanosecond intervals rather than the 100 Hz intervals used by the standard timer. (RHEL 6, SLES 10 SP3, [SLES 11 SP1])

```
[root@h05lp38 linux-2.5]# cat /sys/bus/ap/poll_timeout
250000
```

Using AP adapter interrupts

Increase cryptographic performance on a IBM System z10 system by using AP interrupts mechanism instead of the polling mode.

During module initialization the zcrypt device driver checks whether AP adapter interrupts are supported by the hardware. If so, AP polling is disabled and the interrupt mechanism is automatically used. (RHEL 5.4, SLES 10 SP3, [SLES 11 SP1])

```
[root@h05lp38 linux-2.5]# cat /sys/bus/ap/ap_interrupts
1
```

Generating and accessing long random numbers

The support of long random numbers enables user-space applications to access large amounts of random number data through a character device.

(CEX2C (coprocessor) must be installed and configured, under z/VM: dedicated to guest, CCA lib.,z90crypt loaded) (RHEL 5.3, SLES 10 SP3, SLES 11 SP1)

```
/dev/hwrng
```

Query libica and CPACF support

Small program **icainfo** to list CPACF support via libica V 1.3.9 on running system

Example: z10 without CPACF enabled:

```
h05lp08:~ # icainfo
The following CP Assist for
Cryptographic Function (CPACF)
operations are supported by
libica on this system:
SHA-1:    yes
SHA-256:  yes
SHA-512:  yes
DES:      no
TDES-128: no
TDES-192: no
AES-128:  no
AES-192:  no
AES-256:  no
PRNG:     no
```

Example: z10 with CPACF enabled:

```
zlx9080a:~/wim # icainfo
The following CP Assist for
Cryptographic Function (CPACF)
operations are supported by
libica on this system:
SHA-1:    yes
SHA-256:  yes
SHA-512:  yes
DES:      yes
TDES-128: yes
TDES-192: yes
AES-128:  yes
AES-192:  yes
AES-256:  yes
PRNG:     yes
```

New: Tool icastats in libica

Tool icastats

- Number of executed operations of supported cryptographic algorithms in libica
  - in software within libica
  - with hardware support
- Not yet in libica Version 1.3.7 - i.e. not yet in current SLES und RHEL
- Starting with libica V2 (already available on SourceForge)

After reset:

```
[root@t6329002 ~]# icastats --reset
[root@t6329002 ~]# icastats
 function | # hardware | # software
----------+------------+------------
     SHA1 |          0 |          0
   SHA224 |          0 |          0
   SHA256 |          0 |          0
   SHA384 |          0 |          0
   SHA512 |          0 |          0
   RANDOM |          0 |          0
 MOD EXPO |          0 |          0
  RSA CRT |          0 |          0
  DES ENC |          0 |          0
  DES DEC |          0 |          0
 3DES ENC |          0 |          0
 3DES DEC |          0 |          0
  AES ENC |          0 |          0
  AES DEC |          0 |          0
```

After start of Apache with SSL enabled:

```
[root@t6329002 apache2]# icastats
 function | # hardware | # software
----------+------------+------------
     SHA1 |         27 |          0
   SHA224 |          0 |          0
   SHA256 |          0 |          0
   SHA384 |          0 |          0
   SHA512 |          0 |          0
   RANDOM |         10 |          0
 MOD EXPO |          6 |          0
  RSA CRT |          3 |          0
  DES ENC |          0 |          0
  DES DEC |          0 |          0
 3DES ENC |          1 |          0
 3DES DEC |         27 |          0
  AES ENC |          0 |          0
  AES DEC |          0 |          0
```

New command: lszcrypt

lszcrypt

display information about cryptographic adapters managed by zcrypt and zcrypt's AP bus attributes managed by zcrypt

- card type
- online status
- hardware card type
- hardware queue depth
- request count

The following AP bus attributes can be displayed:

- AP domain
- configuration timer
- poll thread status

Before you start:

- sysfs file system must be mounted

```
[root@h0513002 tools]# lszcrypt -VV
card04: CEX2C       online  hwtype=7  depth=8 request_count=4
card05: CEX2C       online  hwtype=7  depth=8 request_count=2
card08: CEX3C       online  hwtype=9  depth=8 request_count=6
card0a: CEX3C       online  hwtype=9  depth=8 request_count=5
```

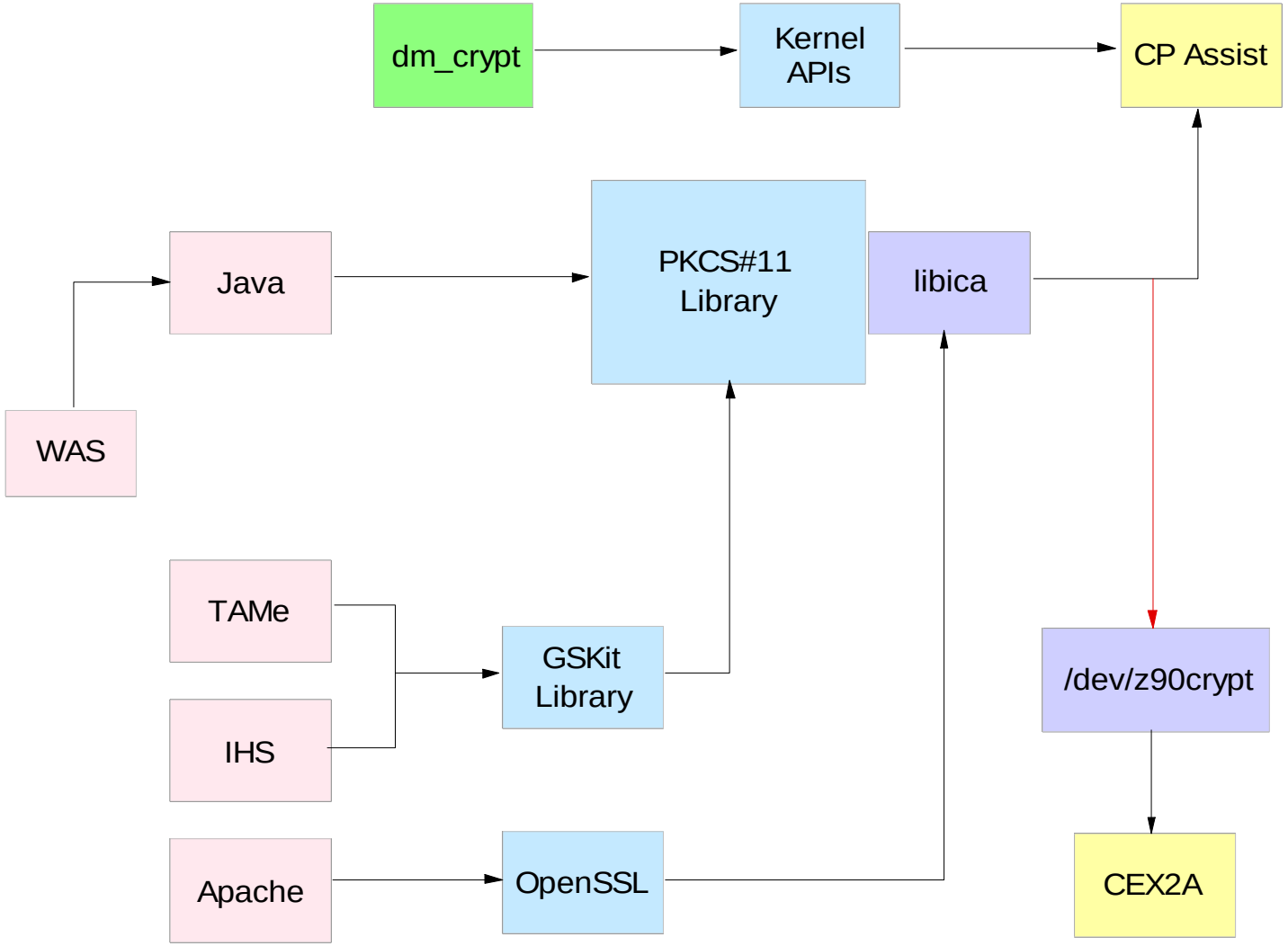
New command: chzcrypt

chzcrypt
configure cryptographic adapters managed by zcrypt and modify zcrypt's AP bus attributes

Before you start:
- You need root permissions
- sysfs file system must be mounted

```
[root@h0513002 tools]# chzcrypt -h
Usage: chzcrypt [<options>] [<cryptographic adapter ids>]
Modify zcrypt configuration.
<options>
-e|--enable
        Set the given cryptographic adapter(s) online.
-d|--disable
        Set the given cryptographic adapter(s) offline.
-a|-all
        Set all available cryptographic adapter(s)
online/offline.
        Must be used in conjuction with the enable or
disable option.
-p|--poll-thread-enable
        Enable zcrypt's poll thread.
-n|--poll-thread-disable
        Disable zcrypt's poll thread.
. . .
```

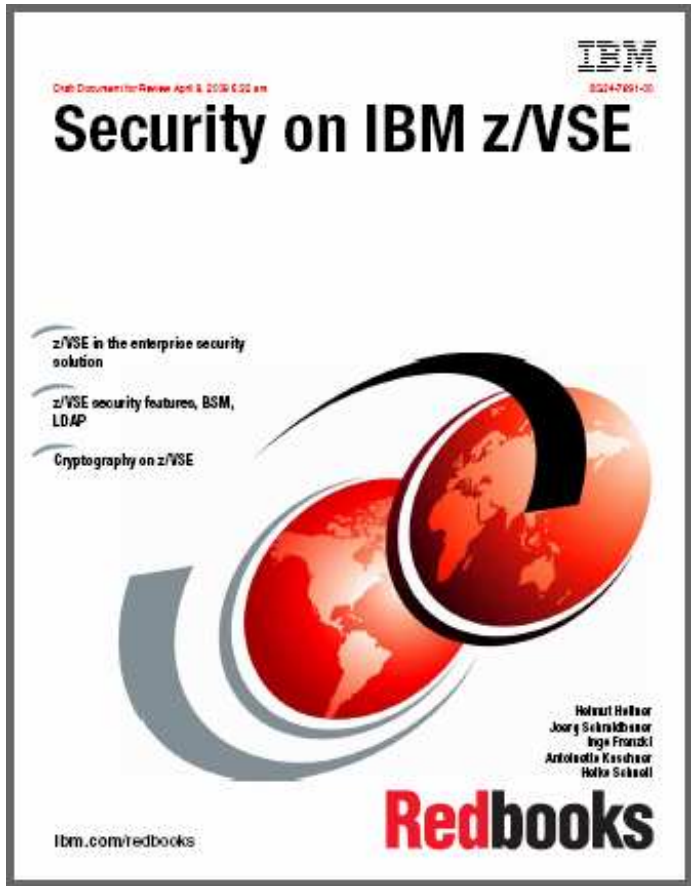
Clear key Crypto Solutions



Agenda

- **IBM System z10 EC GA3 and z10 BC GA Crypto Enhancements**
- **z/VM Security News**
- **Linux on System z selected topics**
- **z/VSE Security and Encryption**

New Redbook: "Security on IBM z/VSE"



Available on:

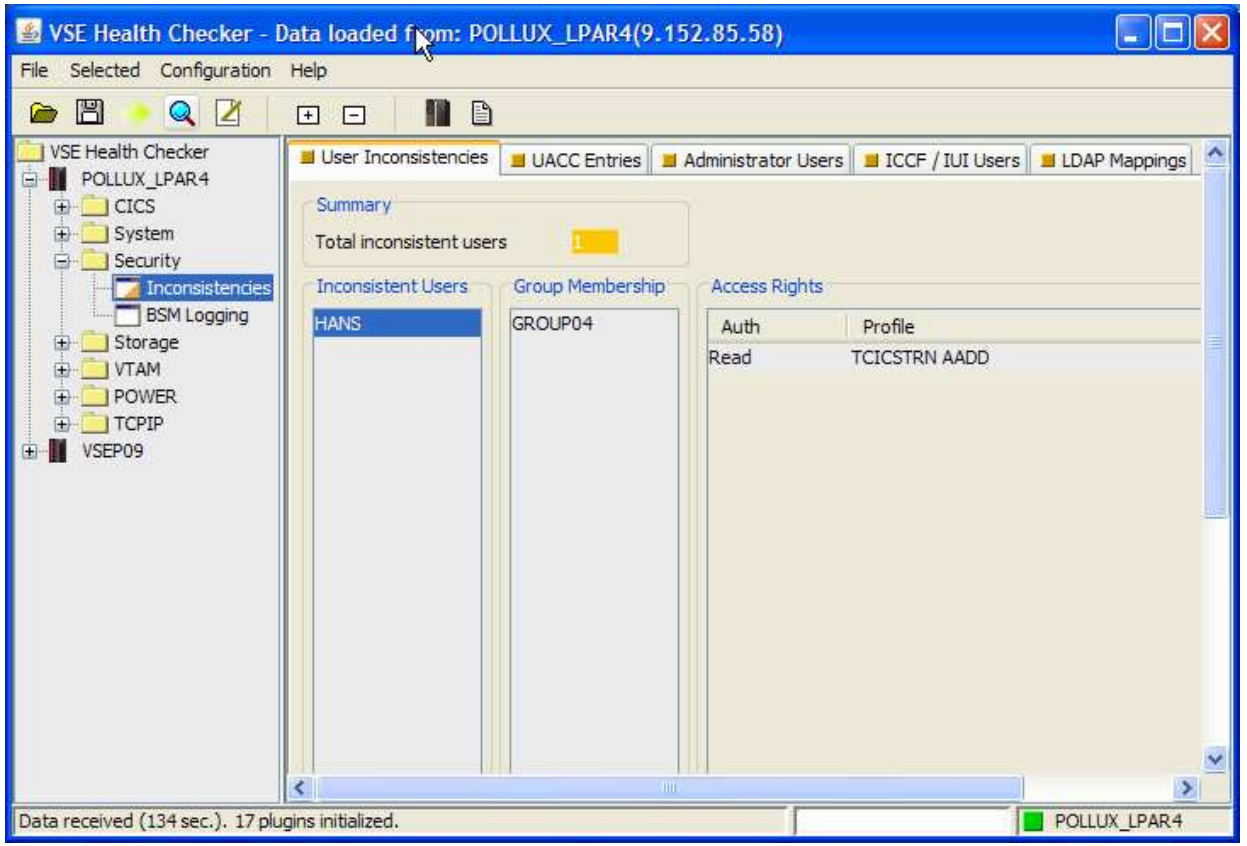
http://www.redbooks.ibm.com/redpieces/abstracts/sg247691.html?Open

Table of contents

Updated October 20, 2009

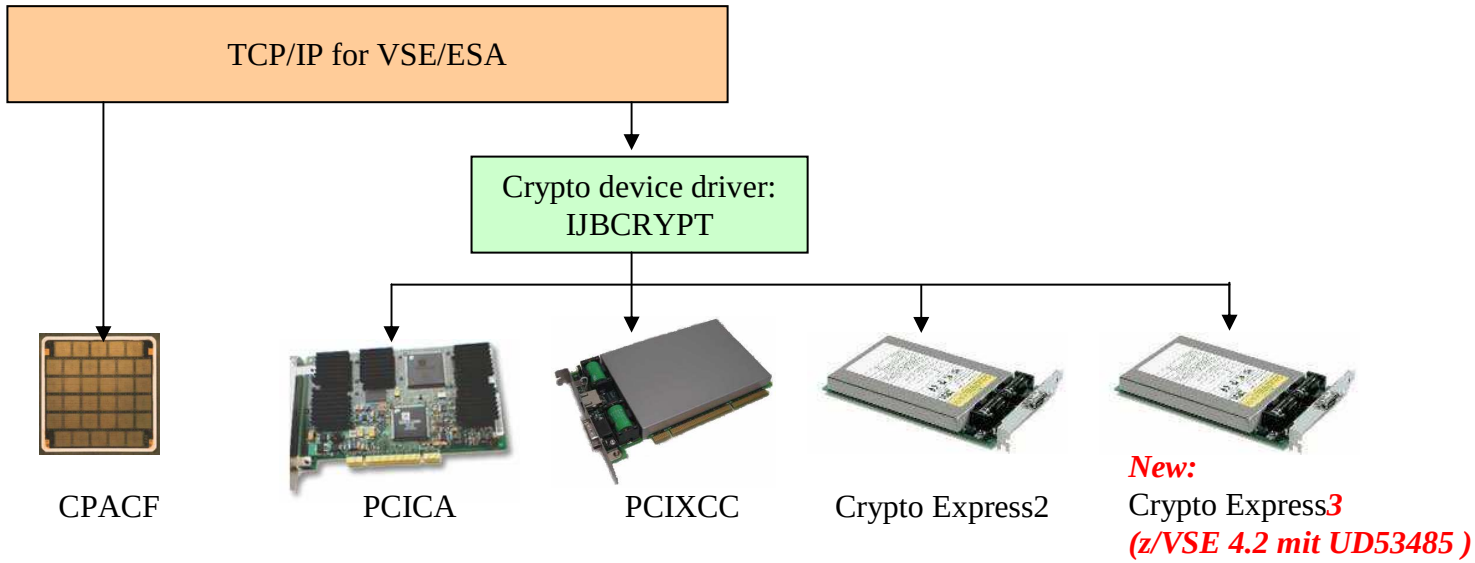
VSE Health Checker

- **New security support**
  - BSMXREF tool used in HC
  - User and UACC inconsistencies
  - LDAP mappings
  - BSM logging
- **Needs the VSE Connector Client**
  - Download from VSE homepage
  - Free tool, provided “as is”



z/VSE Crypto device driver

- **Since VSE/ESA 2.7**
- **Part of Basic Security Manager (BSM)**
- **Subtask IJBCRYPT in FB (Job SECSERV)**
- **Support of crypto cards**
- **Operator commands (MSG FB,DATA=?)**
- **Used transparently by TCP/IP for VSE/ESA**

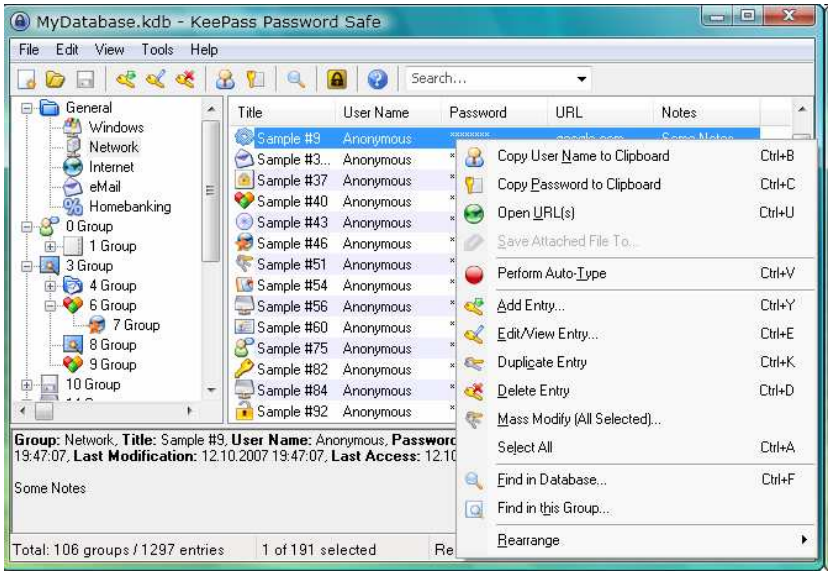


Encryption Facility for z/VSE

- **Host-based optional priced feature, first shipped in 2007**
- **New release 1.2 available with z/VSE 4.2.1 in July 2009 with OpenPGP support in addition to currently used encrypted data format**
- **Provides encryption for single SAM files, VSAM files, or VSE Library members, but also for complete backups made with any backup tool either from IBM or vendors (tapes, vtapes)**
- **Similar to the "Encryption Facility for z/OS"**
  - http://www.ibm.com/servers/eserver/zseries/zos/encryption_facility/
- No special tape hardware requirements (e.g. TS1120, TS1130)
- **IBM crypto hardware exploitation**
  - Crypto cards (PCICA, PCIXCC, CEX2) and CPACF
- **Two main functions**
  - Password-based encryption
  - Public-key encryption

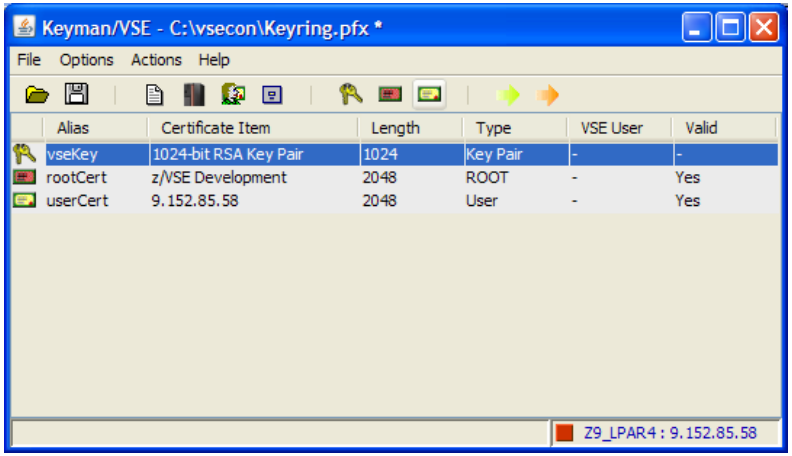
Password-based encryption (PBE)

- **Encryption key (data key) is generated from**
  - the given secret password (8 … 32 characters)
  - and some additional parameters including some random number (the “salt” value)
- **These additional values are stored in the encrypted dataset**
  - When encrypting the same data twice with the same password, the resulting encrypted data will be completely different, because of the randomly created salt value.
- **No need to deal with keys, but**
- **Need to manage/archive passwords**
  - Many free tools available, e.g.
  - KeePass : http://keepass.sourceforge.net/



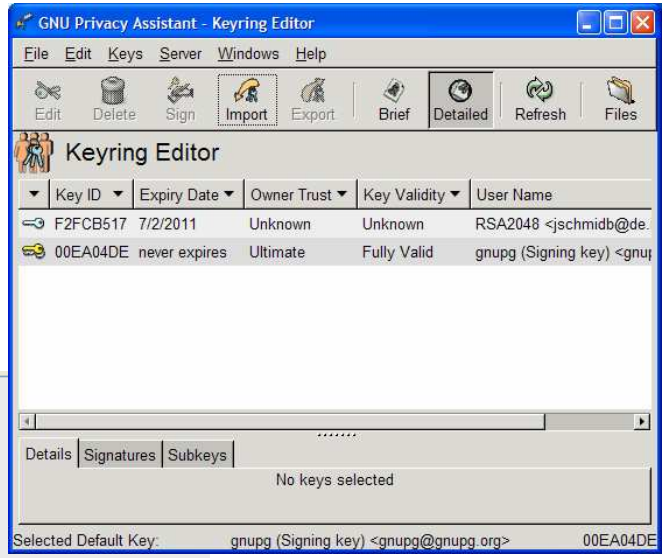
Public-key encryption (PKE)

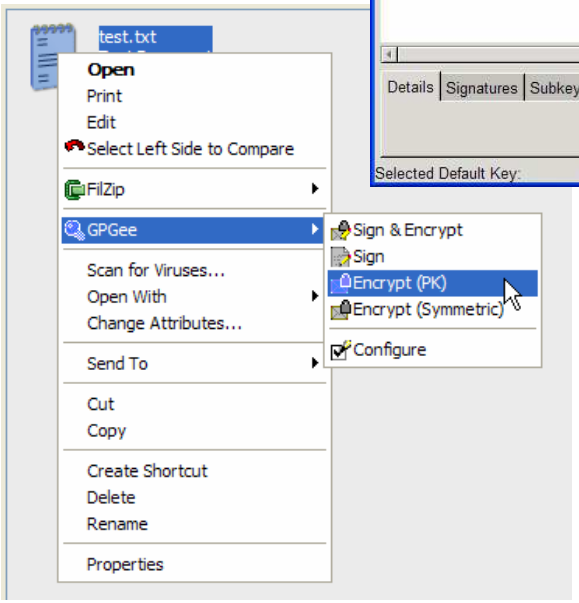
- **Encryption key (data key) is randomly generated**
- **Data key is then encrypted with one or more public keys of the recipients of the encrypted data**
  - Needs a Crypto Express2 or PCIXCC card for 2048 bit keys
  - Crypto cards are transparently used also for 1024 bit keys when available
- **Encrypted data key is put into the encrypted dataset together with the encrypted data**
- **Up to 16 recipients are able to decrypt the data key and thus, the encrypted data, using their corresponding private key**
- **No passwords, but need to manage / exchange RSA keys**
  - Can be done with the Keyman/VSE tool



What is PGP?

- **PGP: “Pretty good privacy”**
  - originally created by Philip Zimmermann in 1991
  - often used for signing and encrypting e-mails
  - OpenPGP standard (RFC 2440 / 4880) in 1998.
- **Trust model**
  - Web-of-trust model in contrast to hierarchical trust model
  - Public keys are wrapped into PGP certificates, which are different from the usual x.509 certificates
- **Implementations**
  - Free implementations, like GnuPG, GPG4Win
  - Commercial implementations from PGP Corp., McAfee Inc., IBM (Encryption Facility for z/OS, now also for z/VSE).





Refer to Wikipedia for more information about OpenPGP:
http://en.wikipedia.org/wiki/Openpgp

Relationship Encryption Facility V1.1 and V1.2

- **V1.1 ships one utility:**

IJBEFVSE
- TDES, AES-128
- System z data format
- System z based compression

- **V1.2 ships two utilities:**

IJBEFVSE (unchanged)
- TDES, AES-128
- System z data format
- System z based compression

IJBEFPGP
- DES, TDES, AES-128, 192, 256
- OpenPGP data format
- ZIP/ZLIB based compression

V1.1 no more orderable after V1.2 is available.

Compare Encryption Facility V1.1 and V1.2

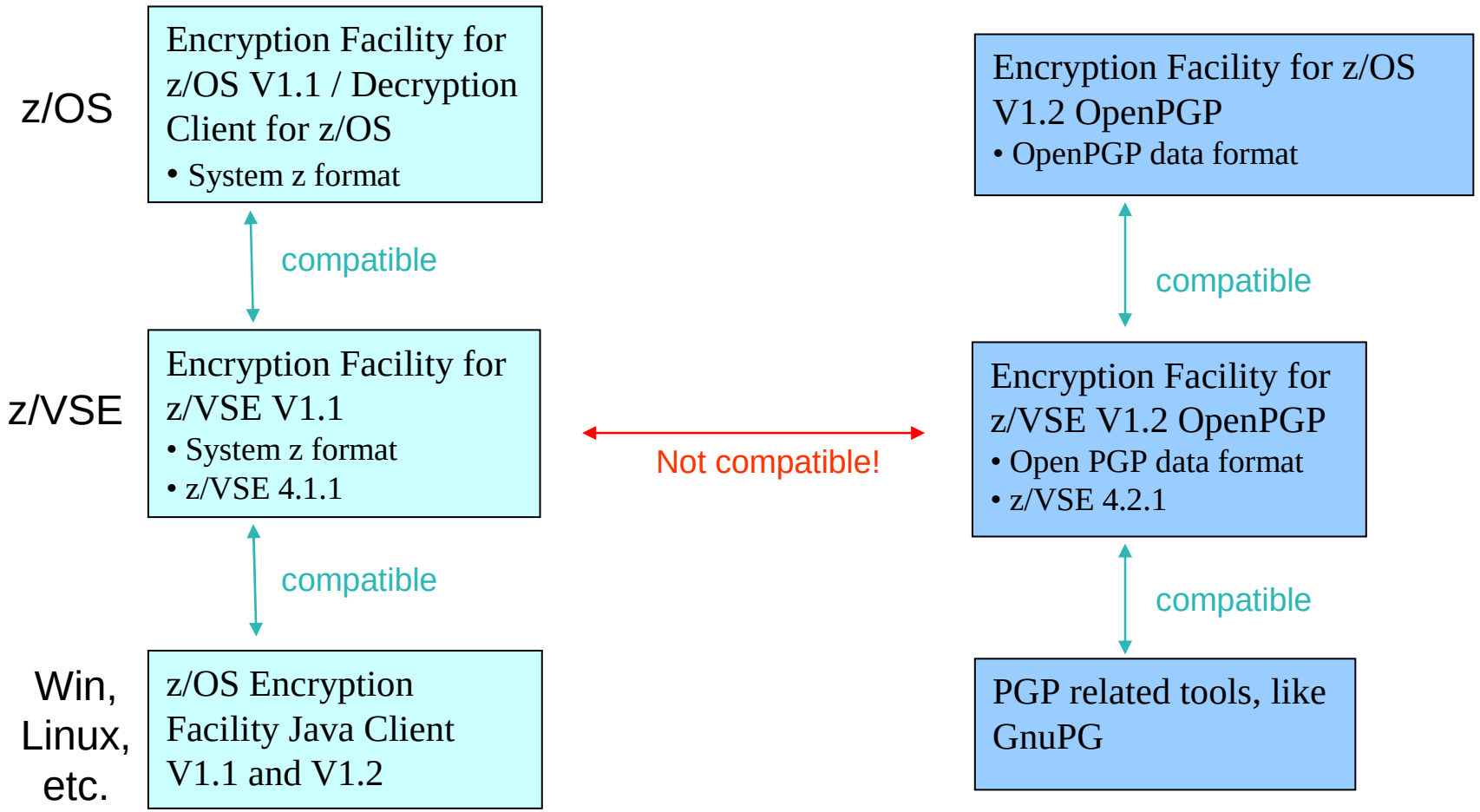
What is Common?

- **Password-based encryption**
  - Encryption key created from given password
  - But: the way how the encryption key is calculated from the password is different in IJBEFVSE and IJBEFPGP
- **Public-key encryption**
  - Encryption key generated by random
  - Encryption key encrypted by an RSA public key
  - Max. 16 recipients possible

What is different?

- **Encrypted data format**
  - IJBEFVSE provides System z data format
  - IJBEFPGP provides OpenPGP data format
- **Compatibility**
  - IJBEFVSE provides compatibility to IBM provided Java client, Decryption client for z/OS
  - IJBEFPGP provides compatibility to PGP implementations
- **Algorithms**
  - IJBEFPGP supports more algorithms
  - IJBEFPGP provides better System z hardware exploitation (e.g. AES-256, SHA-512)
- **Compression**
  - ZIP/ZLIB versus System z based compression
  - ZIP/ZLIB compression is done in software !

Support on z/OS and data format compatibility



Flexible support of record and stream data

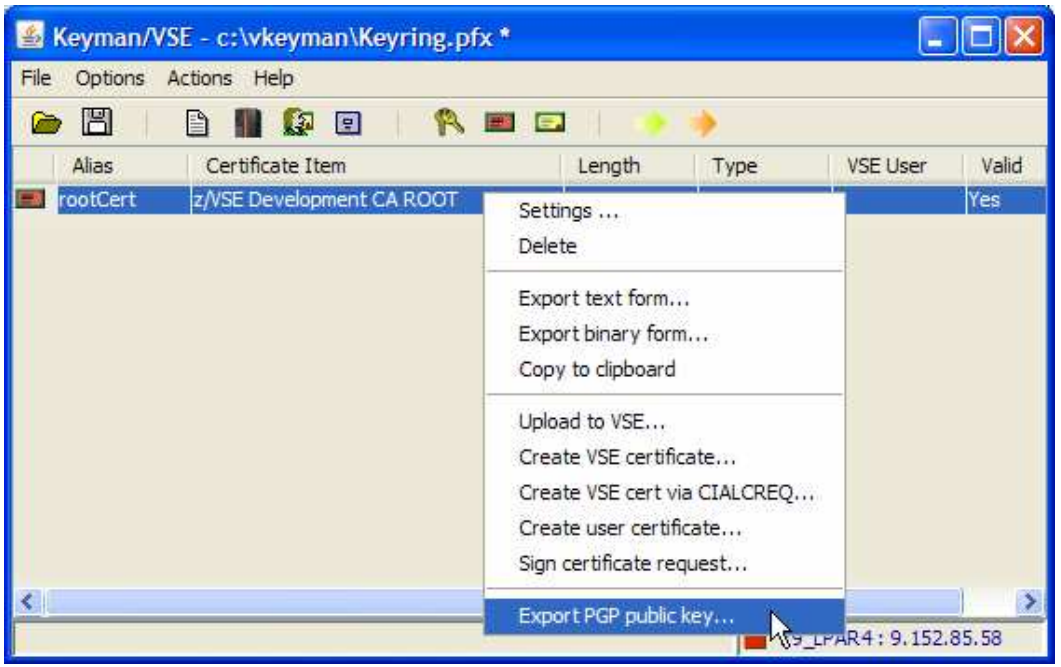
- **Integrate the PGP standard into a VSE mainframe environment**
  - PGP has been invented to support workstation files, email exchange
  - On a mainframe we typically have record-based data (e.g. VSAM), but also some kind of stream data (tapes, vtapes)

Encrypt / decrypt	z/VSE	z/OS or workstation
z/VSE	USE_RECORD INFO	-
z/OS or workstation	-	-

- **Option USE_RECORDINFO**
  - Should only be used when encrypting *AND* decrypting on VSE
  - Puts a data structure with LRECL, RECFM, and BLKSIZE of clear input dataset into encrypted dataset
  - The use of such “private/experimental” data structures is described in the OpenPGP standard
  - This data structure is ignored by other PGP implementations
  - In addition to that, each clear data record is prefixed with a 6-byte header containing its length
  - This length information is processed when decrypting the encrypted data
  - Therefore: decrypted data has exactly the same record structure as original input data.

Exchange of public keys

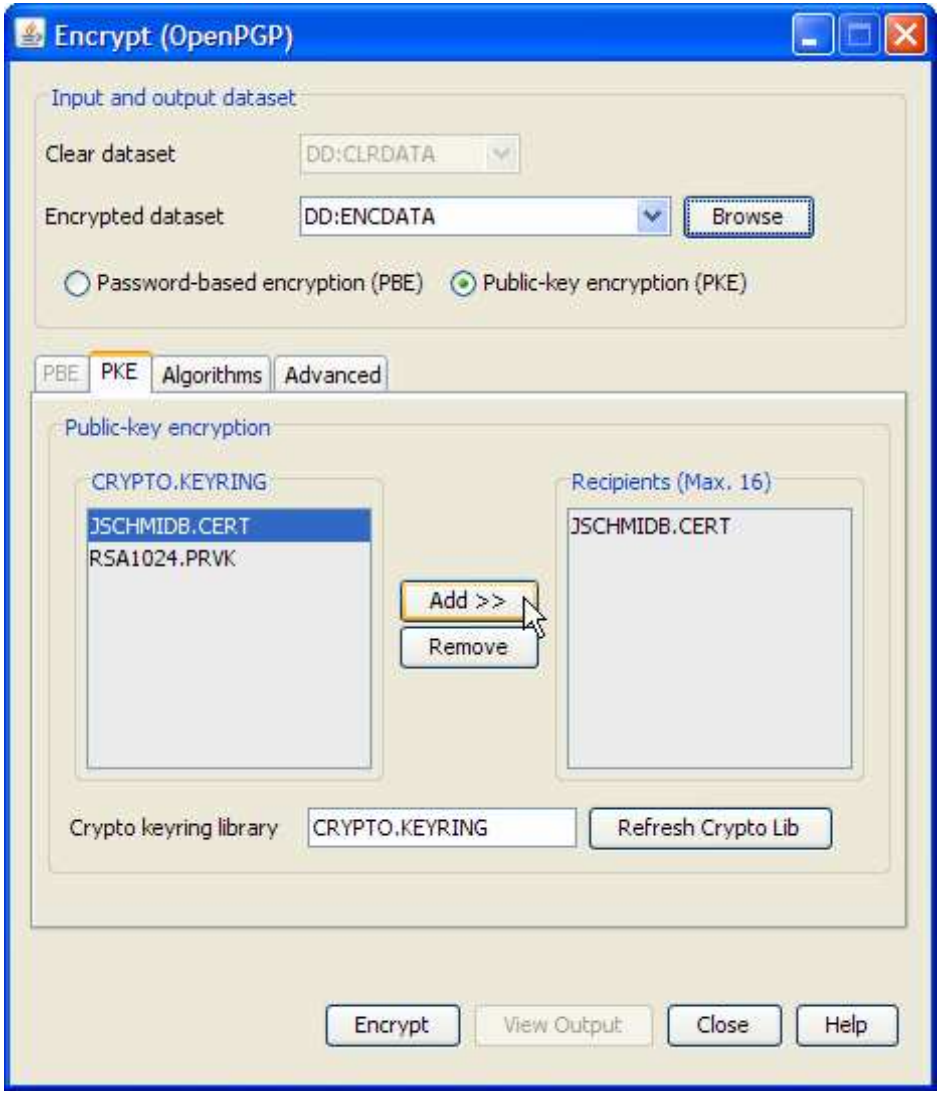
- **Done with Keyman/VSE tool:**
  - http://www.ibm.com/servers/eserver/zseries/zvse/downloads/#vkeyman
- **New version provides some additional functions for OpenPGP:**
  - Import / export of PGP public keys
  - Conversion between PGP format and x.509 format
  - Send converted x.509 certificates to VSE and vice versa
  - available for download since July 2009



Note: PGP certificates are different to x.509 certificates

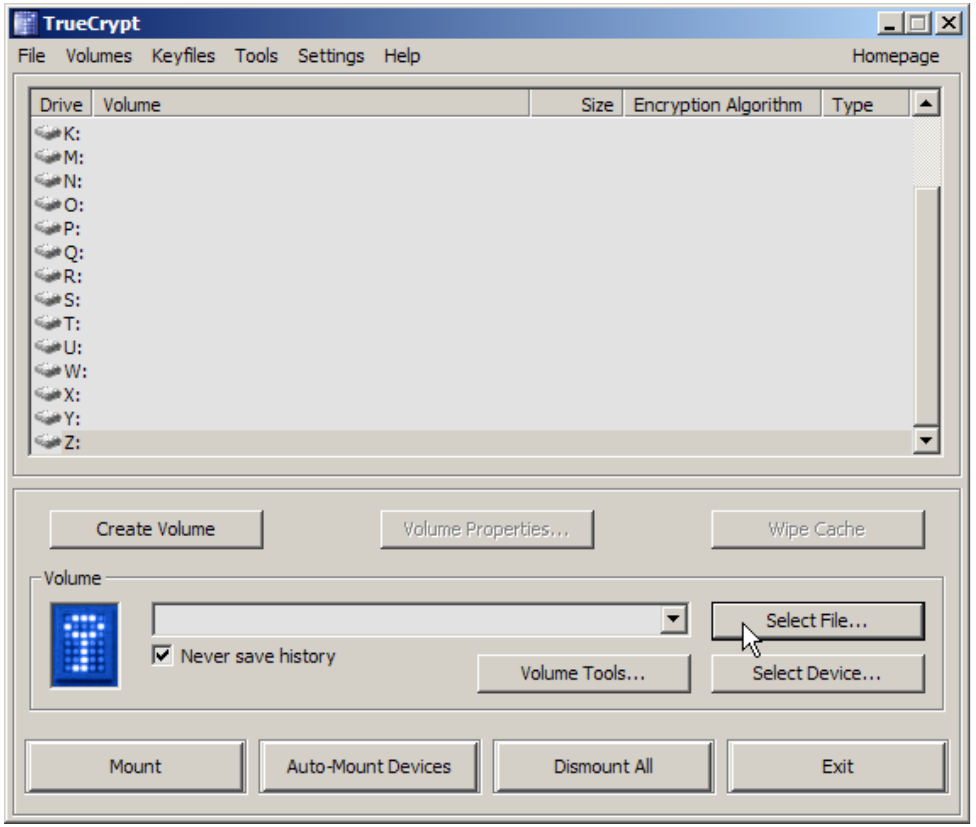
VSE Navigator

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



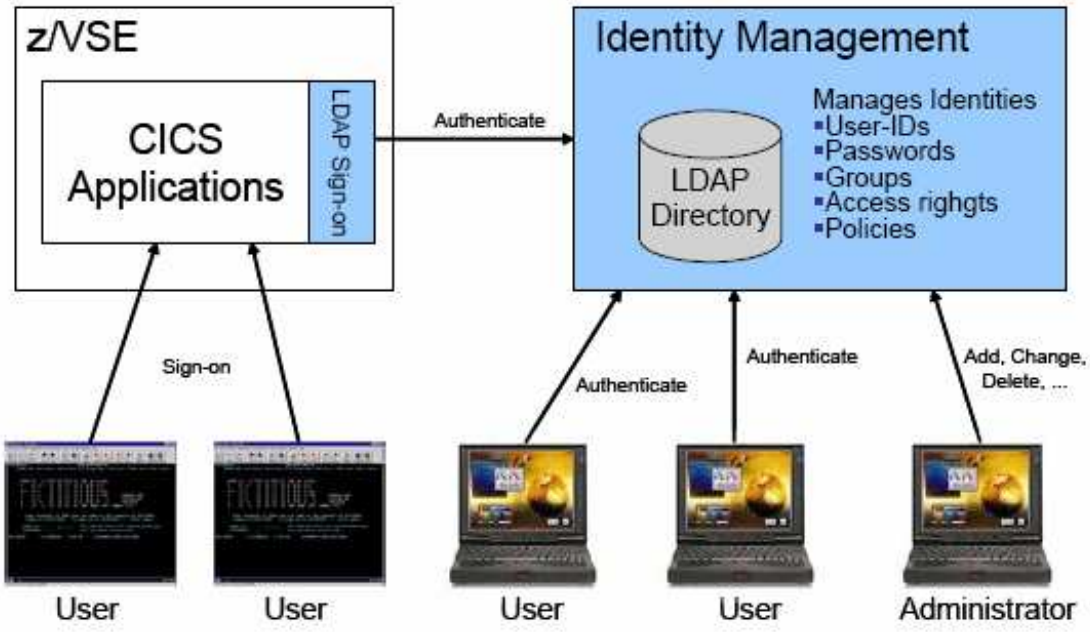
Usage Example for Truecrypt

- **Open-Source Software**
- **Download from www.truecrypt.org**
- **Encrypted data stored in a „drive/volume“. Access to data is transaprent**
- **Potential usage with z/VSE:**
  - Backups on VTAPE and AWSTAPE Files reside in a Truecrypt Volume on a Windows or Linux server



New LDAP Client for z/VSE

- **LDAP user IDs and passwords length: up to 64 characters**
- **Enterprise wide central administration of user IDs and passwords**
- **Identical password on all systems, incl. z/VSE**
- **SSL encryption for LDAP Client and Server connection**
- **Example in new Redbook „Security on IBM z/VSE“, SG24-7691**
- **Consistency-Check for LDAP included in VSE Health Checker**



Thank You

Questions ?

Appendix

More information (1)

Overview on security

New: Redbook: Security on IBM z/VSE, SG24-7691

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

VSE Health Checker

http://www.ibm.com/servers/eserver/zseries/zvse/downloads/#healthchecker

BSM cross reference tool (BSMXREF)

http://www.ibm.com/servers/eserver/zseries/zvse/downloads/tools.html#bsmxref

Encryption Facility

z/VSE 4.2.1 announcement letter on VSE homepage

http://www.ibm.com/servers/eserver/zseries/zvse/

z/VSE Administration

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

Encryption Facility for z/OS

http://www.ibm.com/systems/z/os/zos/encryption_facility/

More information (2)

OpenPGP support

RFC 4880 OpenPGP Message Format

http://tools.ietf.org/html/rfc4880

OpenPGP on Wikipedia

http://en.wikipedia.org/wiki/Openpgp

The GNU Privacy Guard

http://www.gnupg.org/

Keyman/VSE tool

http://www.ibm.com/servers/eserver/zseries/zvse/downloads/#vkeyman

VSE Connector Client

http://www.ibm.com/servers/eserver/zseries/zvse/downloads/#vsecon

VSE Navigator

http://www.ibm.com/servers/eserver/zseries/zvse/downloads/#navi

Redbook: Encryption Facility for z/OS V1.2 OpenPGP Support, SG24-7434

http://www.redbooks.ibm.com/abstracts/sg247434.html?Open

More information (3)

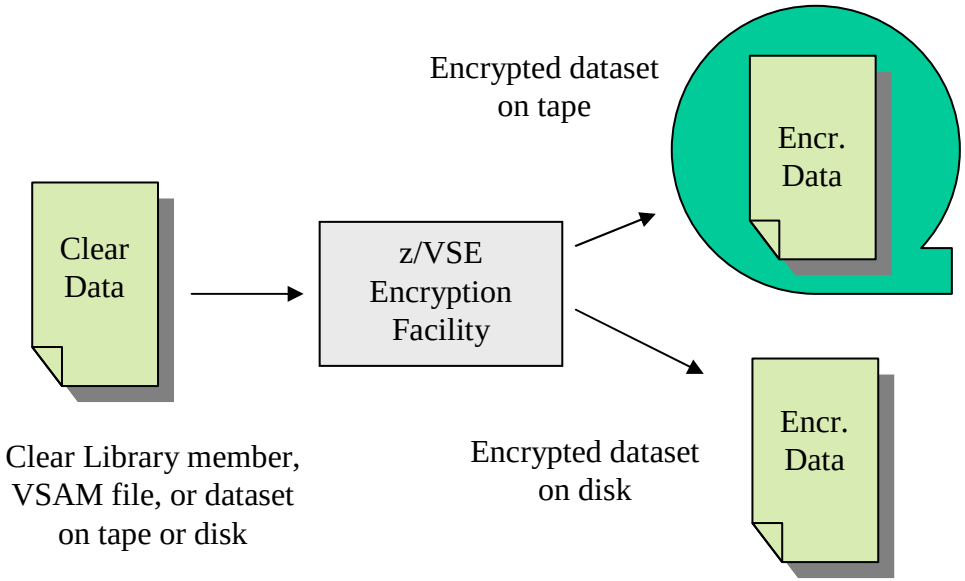
Linux on System z,Device Drivers, Features, and Commands, Development stream dddd dddd ddd d(Kernel 2.6.31), SC33-8411-03

Redbook: Security on z/VM, SG24-7471

Secure Key Solution with the Common Cryptographic Architecture Application Programmer's Guide, SC33-8294

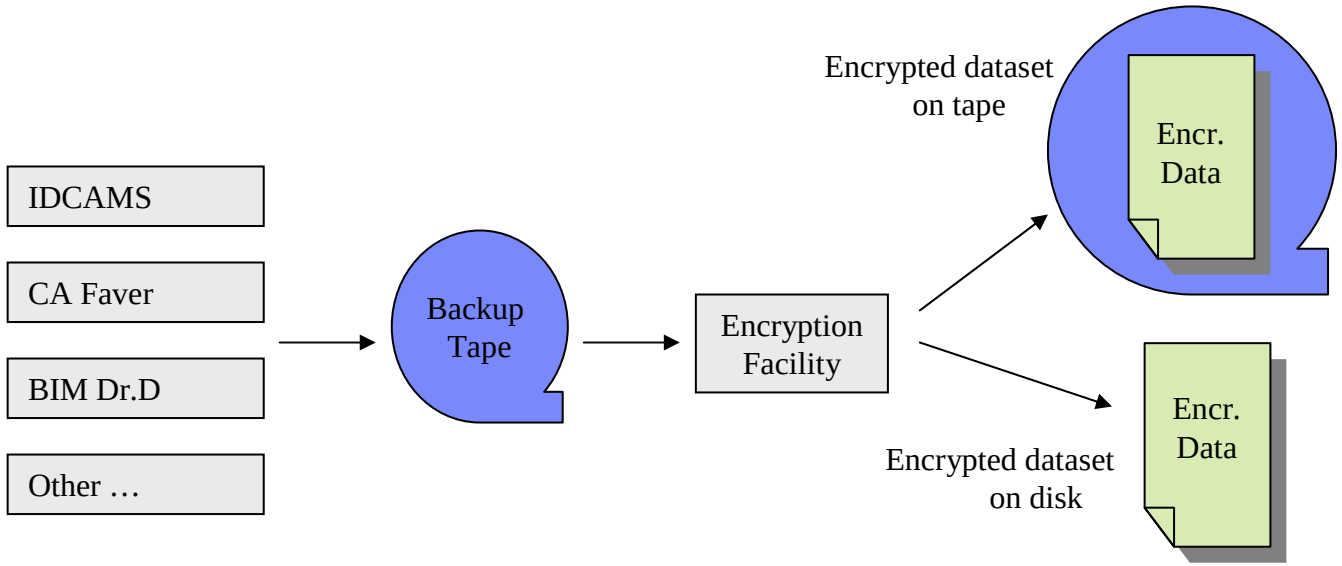
Backup Material

z/VSE Encryption Facility - Encryption of a single file



- Same behavior for both releases of Encryption Facility.

z/VSE Encryption Facility - Encryption of a complete backup



- Any proprietary backup tape can be encrypted and written to a second tape or to disk.
- Note that the complete input tape results in just one encrypted dataset, which resides on tape or disk.

z/VSE Encryption Facility - Summary of Differences

	IJBEFVSE	IJBEFPGP
Encrypted data format	System z format	OpenPGP format
Compatibility with	EF for z/OS V.1.1, EF for z/OS Java client	Any OpenPGP implementations, like GnuPG, EF for z/OS V1.2
Symmetric Algorithms	TDES and AES-128	DES, TDES, AES-128, 192, 256
Hash algos for PBE	SHA-1	MD5, SHA-1, 224, 256, 384, 512
Compression	System z provided compression	ZIP, ZLIB based compression
RSA key lengths	512, 1024, 2048	512, 1024, 2048
Public key format	x.509 certificates	PGP certificates
Signatures	None	RSA signatures (*)

(*) provided in next refresh

z/VSE Encryption Facility - JCL example

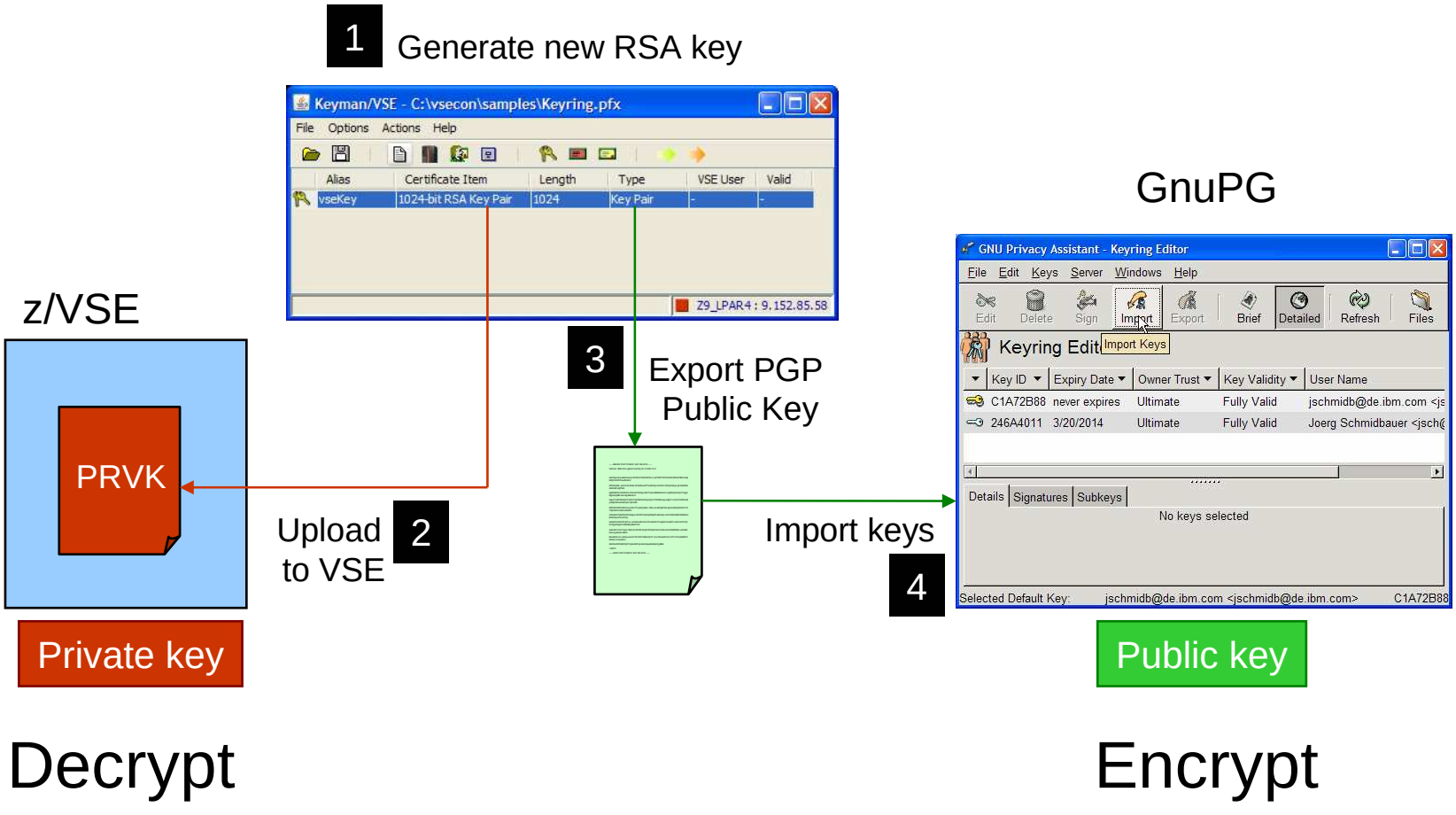
```
* $$ JOB JNM=PBE,CLASS=S,DISP=D
// JOB PBE ENCRYPT USING A PASSWORD
// LIBDEF *,SEARCH=(PRD2.SCEEBASE,PRD2.PROD,PRD2.DBASE)
// EXEC IJBEFPGP
PB_ENCRYPT     <- password-based encryption
S2K_PASSPHRASE=MYPASSWD    <- 8 to 32 char password
S2K_CIPHER_NAME=AES_256    <- encryption algorithm
COMPRESSION=1  <- use best speed for compression
COMPRESS_NAME=ZIP  <- ZIP compression
USE_RECORDINFO    <- maintain record structure of clear input file (only on z/VSE!)
DIGEST_NAME=SHA224  <- this digest algo is used when creating the data key from the password
CLRFILE=DD:CLRDATA  <- clear input VSAM file (ESDS, KSDS, RRDS)
ENCFILE=DD:ENCDATA  <- encrypted VSAM file (ESDS)
/*
/&
* $$ EOJ
```

Keywords are mainly the same as in EF for z/OS V1.2 and GnuPG.

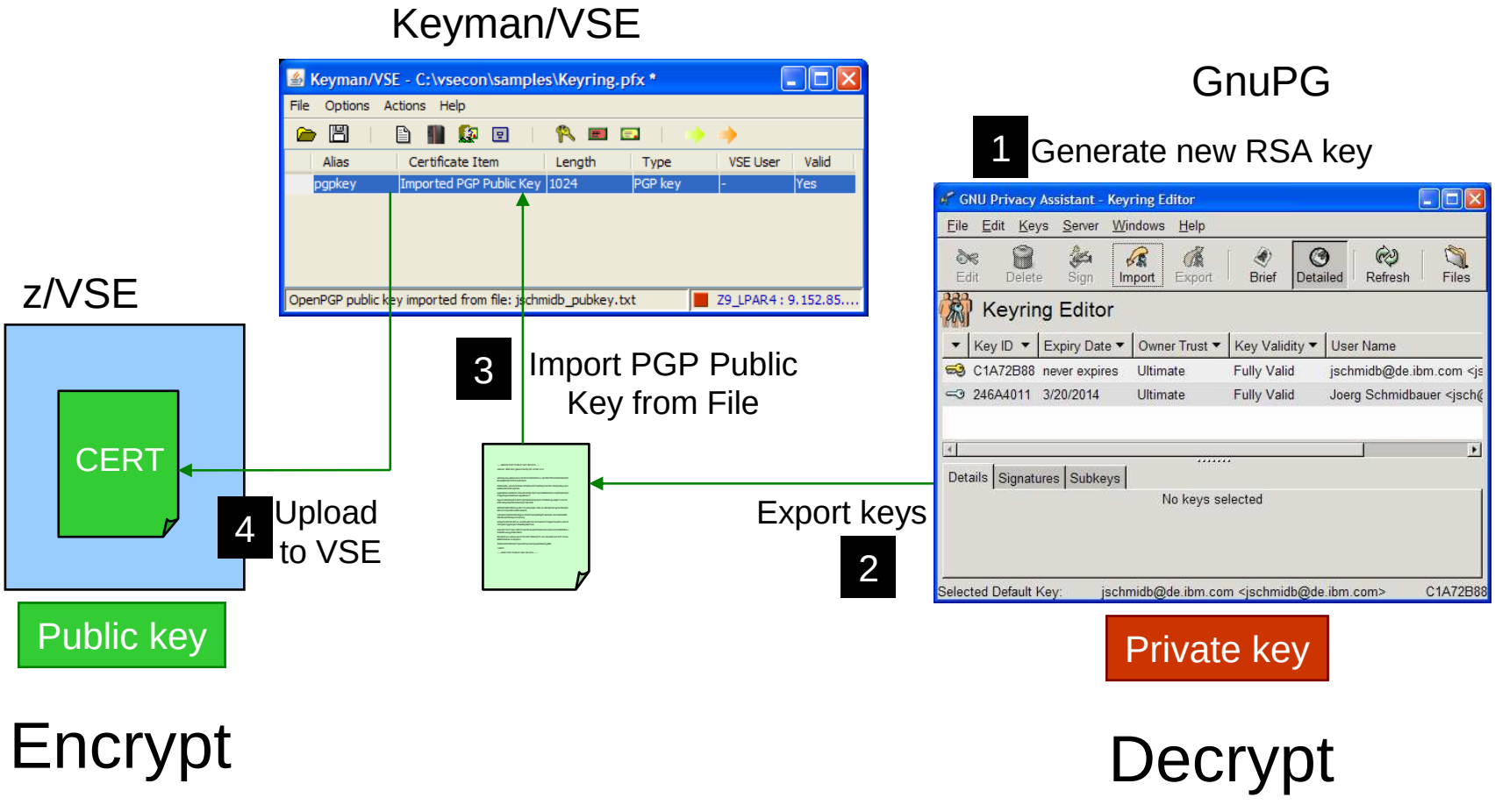
z/VSE Encryption Facility - Some thoughts on compression

- Compression is always applied before encryption.
- Amount of data
  - When using compression, less data has to be encrypted.
    - Except when clear data is binary, like .jpg, where the compression ratio is very small, sometimes zero.
    - In very rare situations compressed data can get bigger than uncompressed data using ZIP
- Security
  - Compression adds additional security by removing any recognizable patterns from original clear data before encryption.
- Speed
  - Compression is usually slower than decompression, because a compression dictionary has to be built during compression. Decompression is just a simple table lookup.
- File size
  - When encrypting/compressing small files, the process may get slower compared to not using compression, because of the compression overhead.
- Hardware support
  - ZIP/ZLIB compression is pure software, while System z compression is done in microcode.

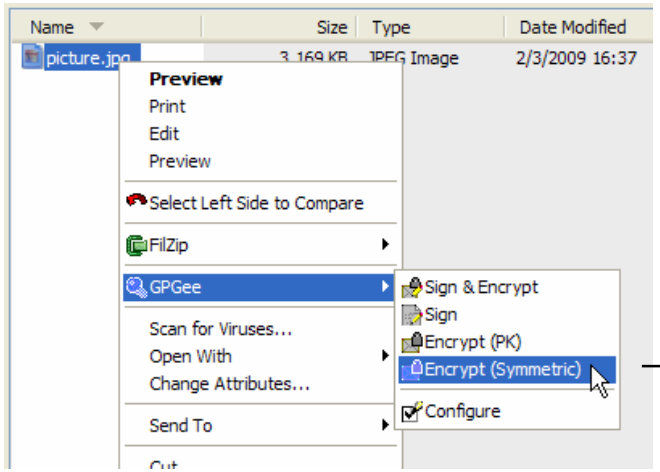
z/VSE Encryption Facility - Scenario 1: decrypt on VSE



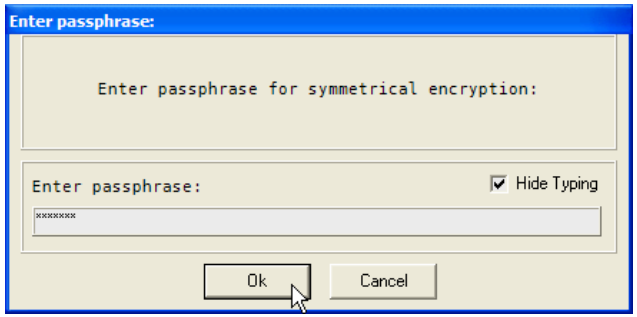
z/VSE Encryption Facility - Scenario 2: encrypt on VSE



Example scenario



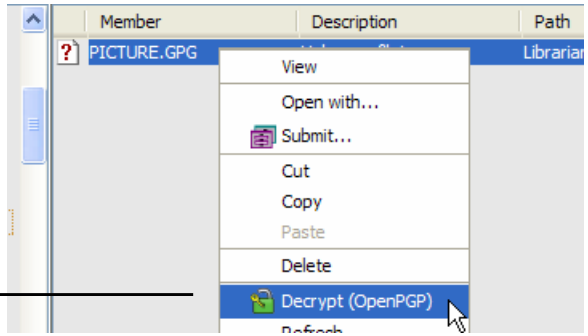
Encrypt via GnuPG / GPGee



Picture.gpg

FTP to VSE

```
* $$ JOB JNM=PBD,CLASS=S,DISP=D
// JOB PBD DECRYPT USING A PASSWORD
// LIBDEF *,SEARCH=(PRD2.SCEEBASE,PRD2.PROD,PRD2.DBASE)
// EXEC IJBEFPGP
DECRYPT
S2K_PASSPHRASE=MYPASSWD
CLRFILE=DD:PRIMARY.JSCH(PICTURE.JPG)
ENCFILE=DD:PRIMARY.JSCH(PICTURE.GPG)
/*
/&
* $$ EOJ
```



Decrypt via VSE Navigator

Supported algorithms

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

(*) algorithm available as software implementation in TCP/IP for VSE/ESA 1.5E or higher
(**) requires TCP/IP for VSE/ESA 1.5E or higher. 2048 bit keys require a PCIXCC or Crypto Express2

Algorithms not supported on VSE

- **These algorithms are listed in the OpenPGP standard, but not available on z/VSE:**
  - Symmetric
    - CAST5, Blowfish, Twofish, IDEA
  - Asymmetric
    - DSA
  - Hash
    - RIPEMD-160
  - Compression
    - BZip2

When a dataset has been encrypted or compressed on z/OS or on a workstation using one of these unsupported algorithms, decryption is not possible on VSE!

HW and SW prerequisites

- **z890 / z990 or higher**
- **“CPU Assist for cryptographic function” (CPACF) enabled (*)**
- **TCP/IP for VSE/ESA for public key encryption**
  - 1.5E with ZP15E214 or
  - 1.5F
- **Crypto Express2 or PCIXCC for 2048-bit public keys**
- **z/VSE 4.1 or later**
  - Encryption Facility V1.1 still available for z/VSE 4.1 (unchanged)
  - OpenPGP support requires z/VSE 4.2.1, because of dependencies to the z/VSE base

(*) CPACF is a no-charge feature, available only on z890, z990, z9 and z10 servers

Availability of EF V1.2

- **July 17, 2009, together with z/VSE 4.2.1**
- **Optional priced feature**
- **Program number: 5686-CF8**
- **Documentation in z/VSE 4.1.2 Administration book, Chapter 45**
  - Available in July on CD-ROM, or
  - Download as PDF from:

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

Corrective service

EF V1.1	EF V1.2
DY46717 (PTF UD53196) DY47051 (PTF UD53499)	DY46973 (z/VSE 4.2.1 refresh)