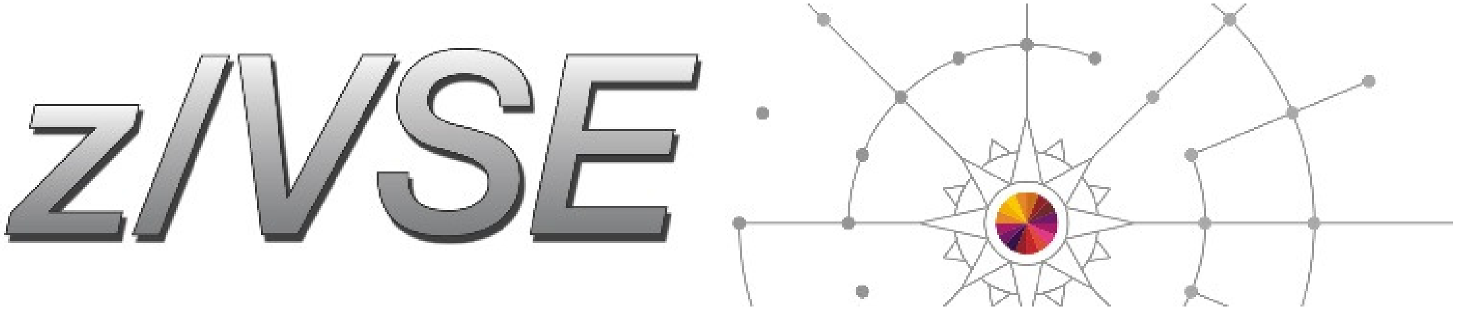
News on z/VSE Security, Crypto Support and OpenSSL for z/VSE



Ingo Franzki
Joerg Schmidbauer

http://www.ibm.com/zVSE

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

Not all common law marks used by IBM are listed on this page. Failure of a mark to appear does not mean that IBM does not use the mark nor does it mean that the product is not actively marketed or is not significant within its relevant market.

Those trademarks followed by ® are registered trademarks of IBM in the United States; all others are trademarks or common law marks of IBM in the United States.

For a complete list of IBM Trademarks, see www.ibm.com/legal/copytrade.shtml :

*, AS/400®, e business(logo)®, DBE, 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®, System i, System i5, System p, System p5, System x, System z, System z9®, BladeCenter®

The following are trademarks or registered trademarks of other companies.

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.

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

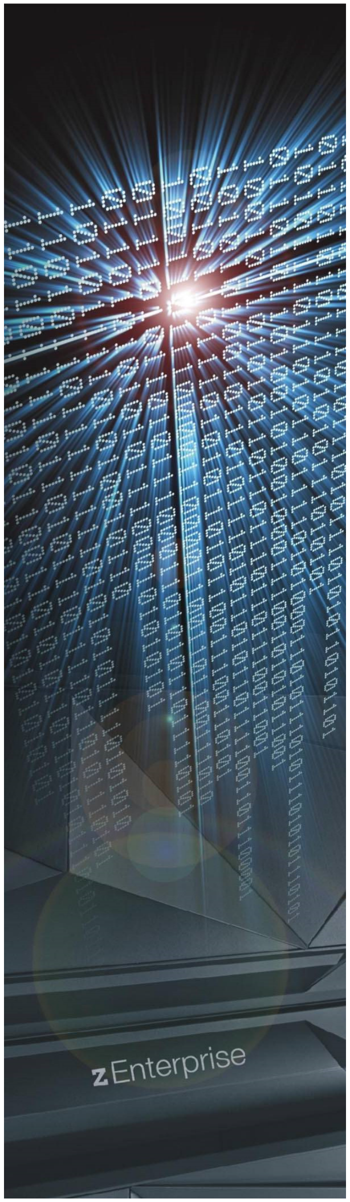
Notes:
Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's 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.

Agenda

- **Introduction**

- **Cryptography basics**
  - Encryption algorithms
  - Encryption keys
  - Diffie-Hellman versus RSA
  - Elliptic Curve Cryptography
  - Recommendations

- **Using cryptography with z/VSE**
  - Full tape encryption
  - Encryption Facility for z/VSE
  - SSL/TLS
  - SecureFTP
  - Hardware cryptography support on z Systems
  - OpenSSL
  - What’s new with z/VSE V6.2

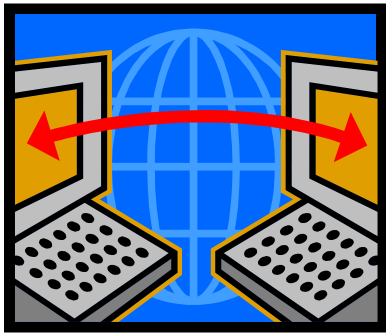


Why secure VSE ?

- **Prevent unauthorized access to VSE and data**
  - Keep secret data secret
  - Data modification by unauthorized users

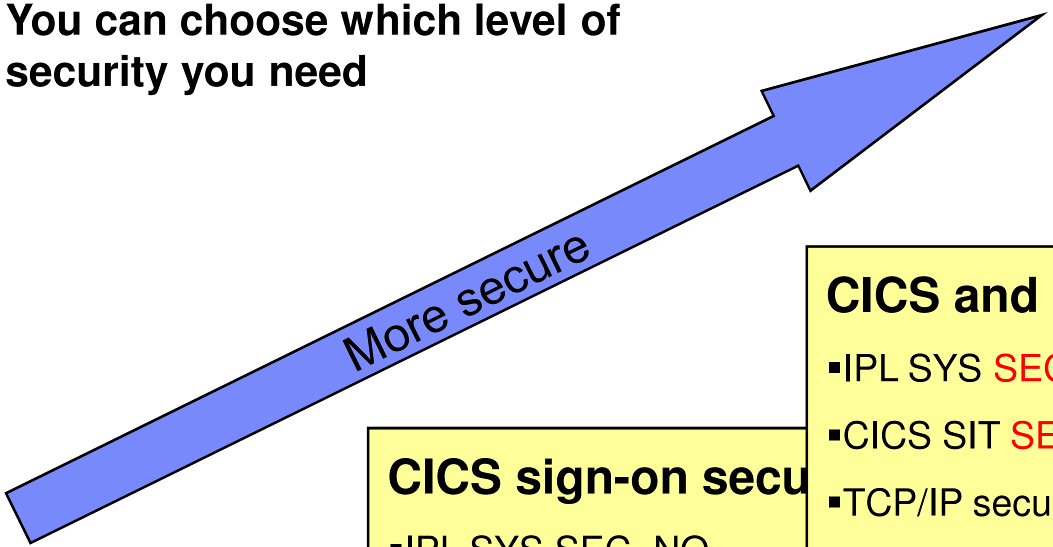
- **Prevent users from damaging the VSE system (maybe by accident)**
  - Deletion of members or entries
  - Submission of jobs

- **Prevent unauthorized remote access to VSE**
  - Today most computers are part of a network
  - Theoretically every system in the network could connect to your VSE system
  - FTP allows to access production data
    - VSAM
    - POWER entries (listings)



Securing you system – Protection levels

You can choose which level of security you need



No security or homegrown se

- IPL SEC=NO
- CICS SIT SEC=NO
- No TCP/IP security

→ No real protection from inside nor outside !

CICS sign-on secu

- IPL SYS SEC=NO
- CICS SIT SEC=YES
- No TCP/IP security

→ Only protected if signing in through CICS. No protection for batch or remote

CICS and batch s

- IPL SYS SEC=YES
- CICS SIT SEC=YES
- TCP/IP security active

→ Protected against ac Inside (e.g. batch) and outside (CICS and TCP/IP)

Extended security

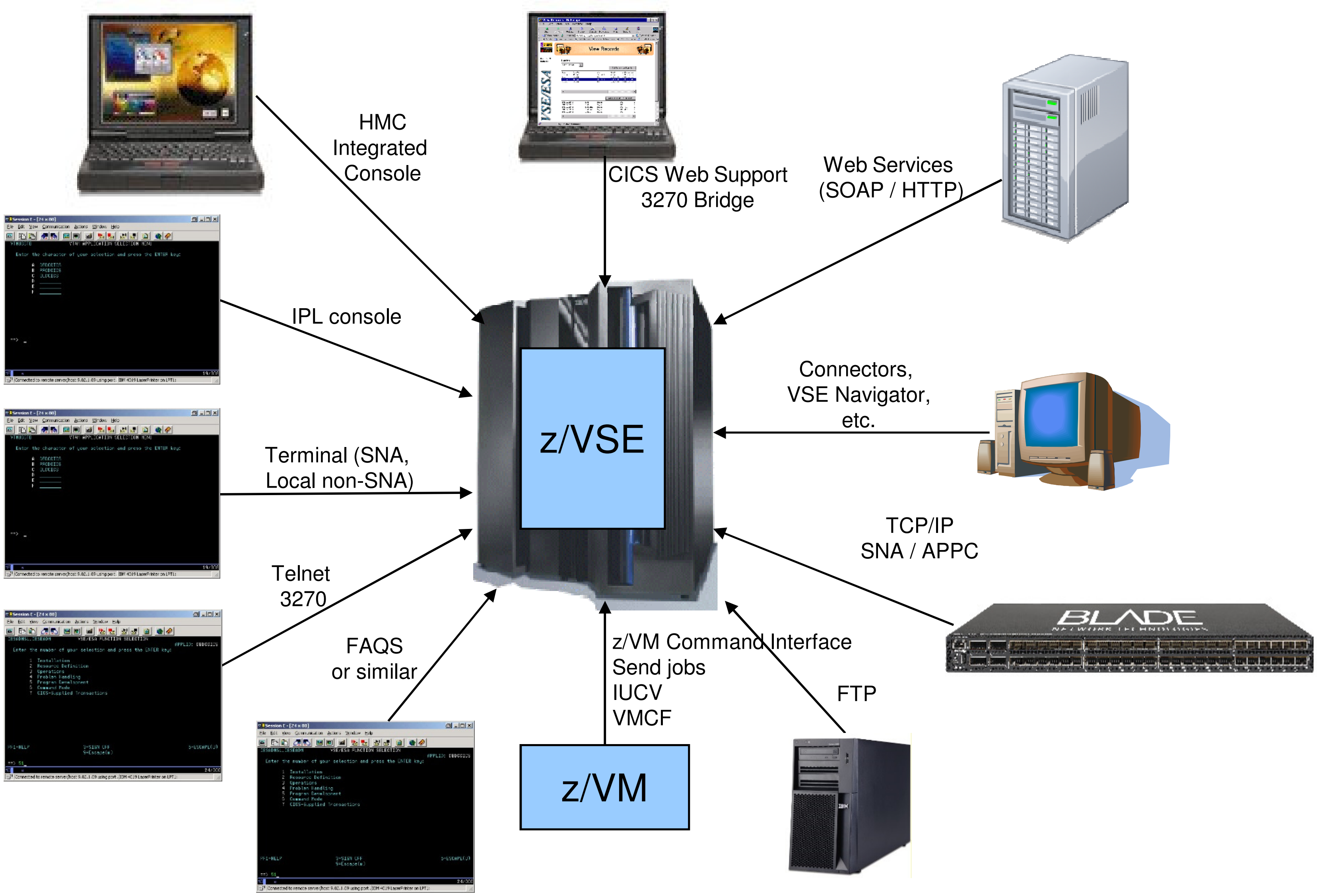
- IPL SYS SEC=YES
- CICS SIT SEC=YES
- TCP/IP security active
- Using extended security features
  - FACILITY resources
  - JCL security
  - LDAP signon
  - Data encryption & SSL
  - Auditing

Required level of protection depends on

→What resources you want to protect

→Against whom (inside, outside)

Ways into your z/VSE system – Are you securing them all?



HMC Integrated Console

CICS Web Support
3270 Bridge

Web Services
(SOAP / HTTP)

IPL console

Connectors,
VSE Navigator,
etc.

Terminal (SNA,
Local non-SNA)

z/VSE

TCP/IP
SNA / APPC

Telnet
3270

FAQS
or similar

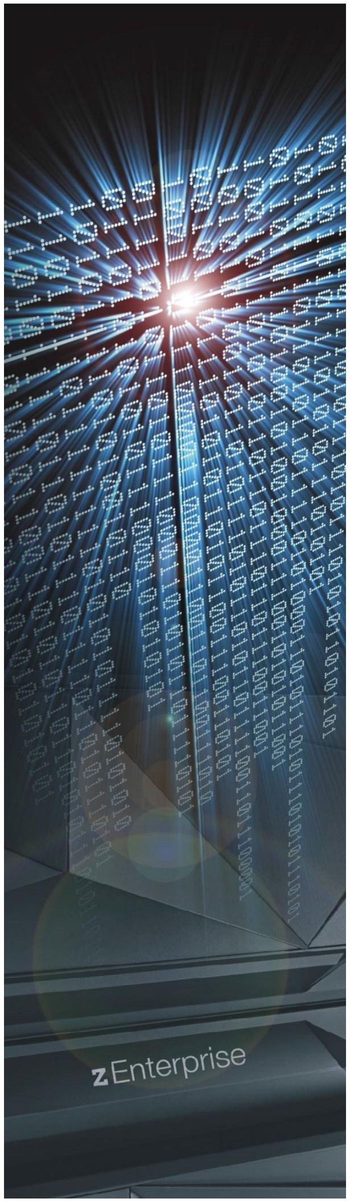
z/VM Command Interface
Send jobs
IUCV
VMCF

FTP

z/VM

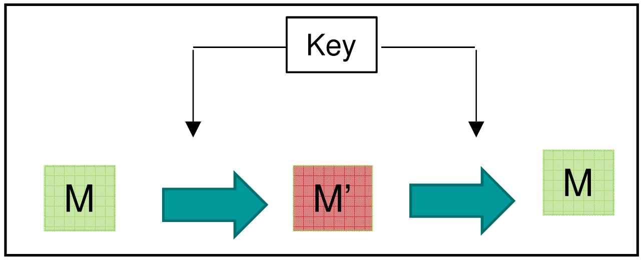
Agenda

- **Introduction**
- **Cryptography basics**
  - – Encryption algorithms
  - – Encryption keys
  - – Diffie-Hellman versus RSA
  - – Elliptic Curve Cryptography
  - – Recommendations
- **Using cryptography with z/VSE**
  - – Full tape encryption
  - – Encryption Facility for z/VSE
  - – SSL/TLS
  - – SecureFTP
  - – Hardware cryptography support on z Systems
  - – OpenSSL
  - – What’s new with z/VSE V6.2

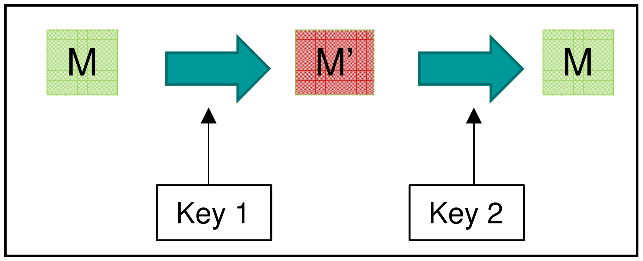


Encryption basics

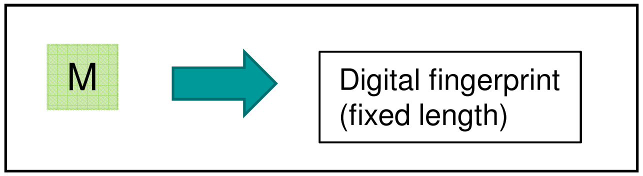
- **Symmetric encryption**
  - The same key is used to encrypt and decrypt
  - Example: RC4, DES, 3DES, AES



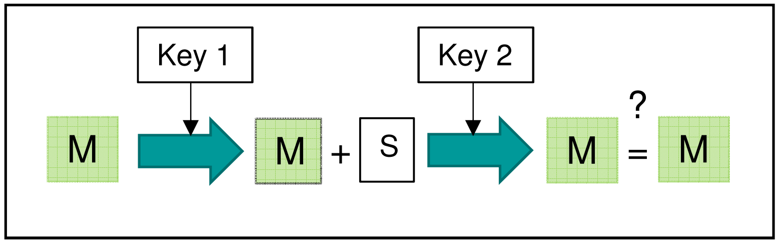
- **Asymmetric encryption**
  - One key is used for encryption, another key is used for decryption (public and private keys)
  - Example: RSA, Elliptic Curve Cryptography



- **Hash Algorithms**
  - A digital fingerprint of a text
  - Example: MD5, SHA



- **Signatures**
  - To create a digital signature asymmetric algorithms are used, mainly RSA



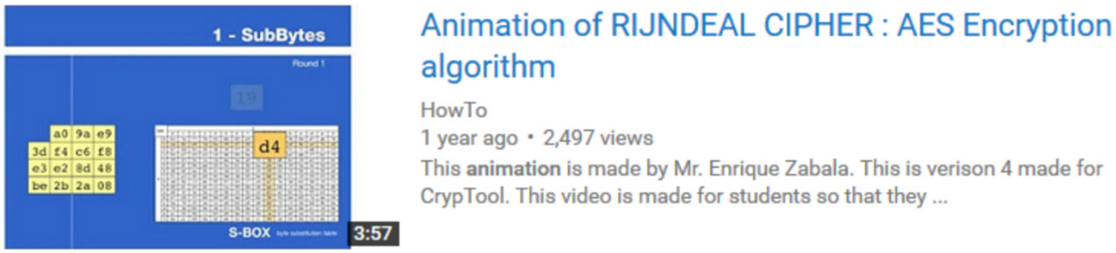
Different kinds of encryption keys

- **Keys that consist of numbers which are based on mathematical algorithms (asymmetric algorithms)**
  - RSA, Example: public key = (23,143), private key = (47,143)
    - Encryption of the number 7: 7^{23} mod(143) = 2
    - Decryption: 2^{47} mod(143) = 7

In this example, one could easily 'guess' the private key of 47 (i.e. brut force).

In reality this is done using much longer numbers, e.g. numbers of 4096 bits length

- **Keys that consist of random bit patterns (symmetric algorithms)**
  - The key consist of a bit pattern of fixed length, e.g.
    - 16 Bytes = 128 bit results in 2^{128} = 3,4*10^{38} possibilities
    - 32 Bytes = 256 bit results 2^{256} = 1,1*10^{77} possibilities
  - Example: Youtube: https://www.youtube.com/watch?v=evjFwDRTmV0



Animation of RIJNDEAL CIPHER : AES Encryption algorithm

HowTo

1 year ago • 2,497 views

This **animation** is made by Mr. Enrique Zabala. This is verison 4 made for CrypTool. This video is made for students so that they ...

Encryption key sizes

… and their security level

RSA	ECDH	Symmetric	Hash	Security (bits)
		RC4		<?
		DES	MD5	<?
			SHA-1	<80
1024	160			80
2048	224	TDES	SHA-224	112
3072	256	AES-128	SHA-256	128
4096				
7680	384	AES-192	SHA-384	192
15360	512	AES-256	SHA-512	256

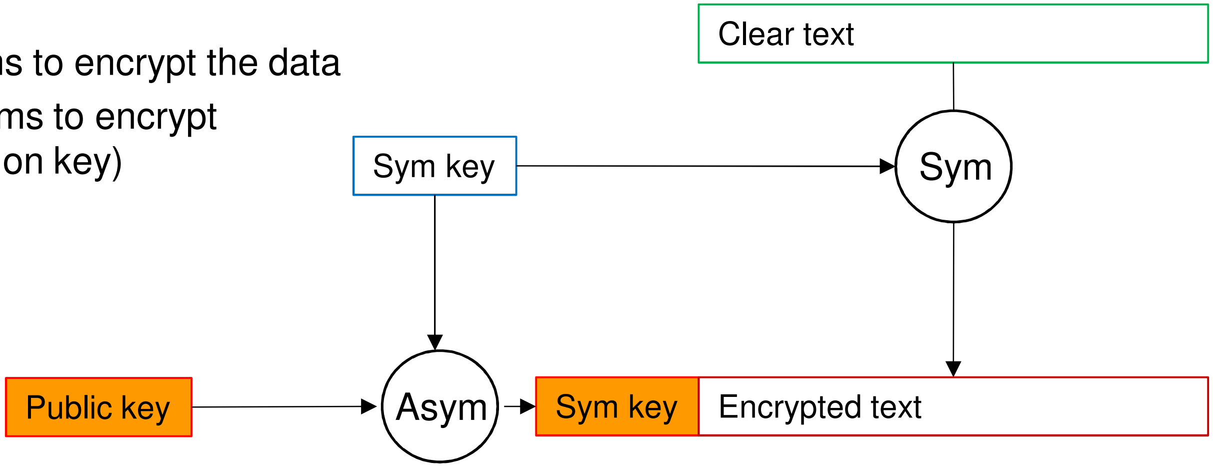
This is what we normally want

Why all these different encryption algorithms?

- **Asymmetric algorithms**
  - Are slower by factors than symmetric algorithms
  - Used to uniquely identify a communication partner
  - Can only encrypt a certain number of bytes

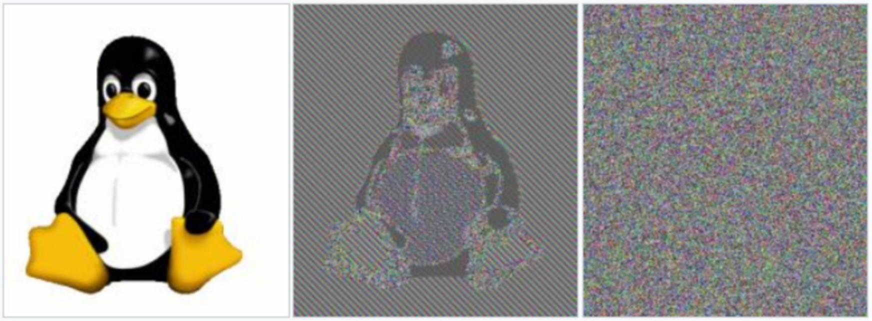
- **Symmetric algorithms**
  - Based on bit-shifting and logical computations (XOR, etc.)
  - Very fast
  - Can encrypt any numbers of bytes (usually in blocks of 8 or 16 bytes)

- **Idea:**
  - Use symmetric algorithms to encrypt the data
  - Use asymmetric algorithms to encrypt the symmetric key (session key)



Encryption modes (chaining)

- **ECB (Electronic Codebook)**
  - Each data block is encrypted separately



Original image

Encrypted using ECB mode

Modes other than ECB result in pseudo-randomness

Source: Wikipedia

- **CBC (Cipher Block Chaining)**
  - The result of the encryption of one data block is fed into the encryption of the next data block

- **GCM (Galois Counter Mode)**
  - Encryption and generation of a hash (digital fingerprint) in one step
  - Most current and securest mode

AES-GCM supported in hardware on z14!

- **Others**
  - CFB - Cipher Feedback
  - OFB - Output Feedback
  - XTS - XEX-based tweaked-codebook mode with ciphertext stealing
  - ...

SSL/TLS Connection establishment and key exchange

- **RSA-based:**
  - Commonly used
  - Long-term attacks are possible, because the session key is sent (encrypted) over the line
- **Diffie-Hellman based:**
  - Usage increases
  - Needs up to 30% more CPU
  - Long-term, attacks are NOT possible (forward secrecy), because the session key is not sent over the line
  - Usually used in combination with Elliptic Curve Cryptography (ECC) for better performance
  - https://www.youtube.com/watch?v=3QnD2c4Xovk

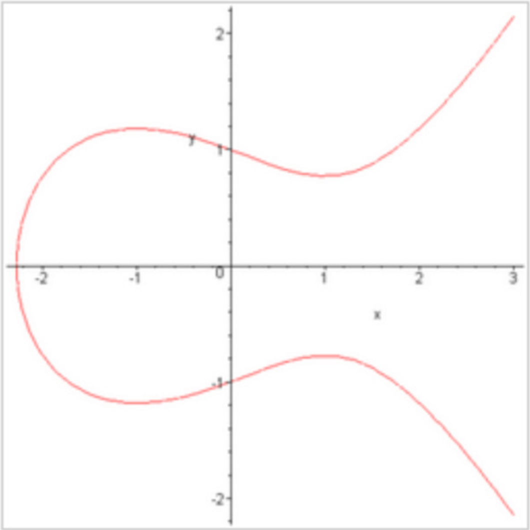
Public Key Cryptography: Diffie-Hellman Key Exchange (short version)

Art of the Problem

4 years ago • 366,437 views

Diffie-Hellman key exchange was one of the earliest practical implementations of key exchange within the field of cryptography.

Some more info on Elliptic Curve Cryptography (ECC) …



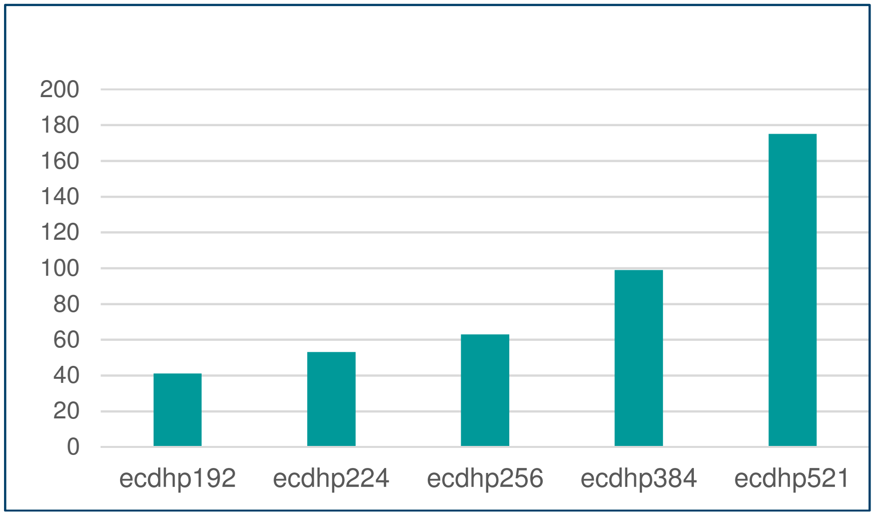
- **Elliptic Curves**
  - Described through $y^2 = x^3 + ax + b$
  - Mathematical calculation based on points on the curve

- **Two types of curves:**
  - Prime Curves (NIST)
  - Brainpool curves
    - Are being researched and provided by an working group of German governmental institutions and companies, including the German BSI (equivalent to U.S. NIST)
    - Are supported with OpenSSL 1.0.2 (and Java)
    - Also supported by Keyman/VSE
    - Refer to
      - http://www.ecc-brainpool.org/ (German website)
      - https://en.wikipedia.org/wiki/Elliptic_curve_cryptography#Implementation

- **ECC acceleration supported on CEX4C and later**
  - z/VSE 6.2: Added hardware acceleration for ECC in z/VSE and OpenSSL

Hardware support for ECC on z/VSE 6.2

- **Performance**



(x-axis: elliptic curves, y-axis: performance increase by factor)

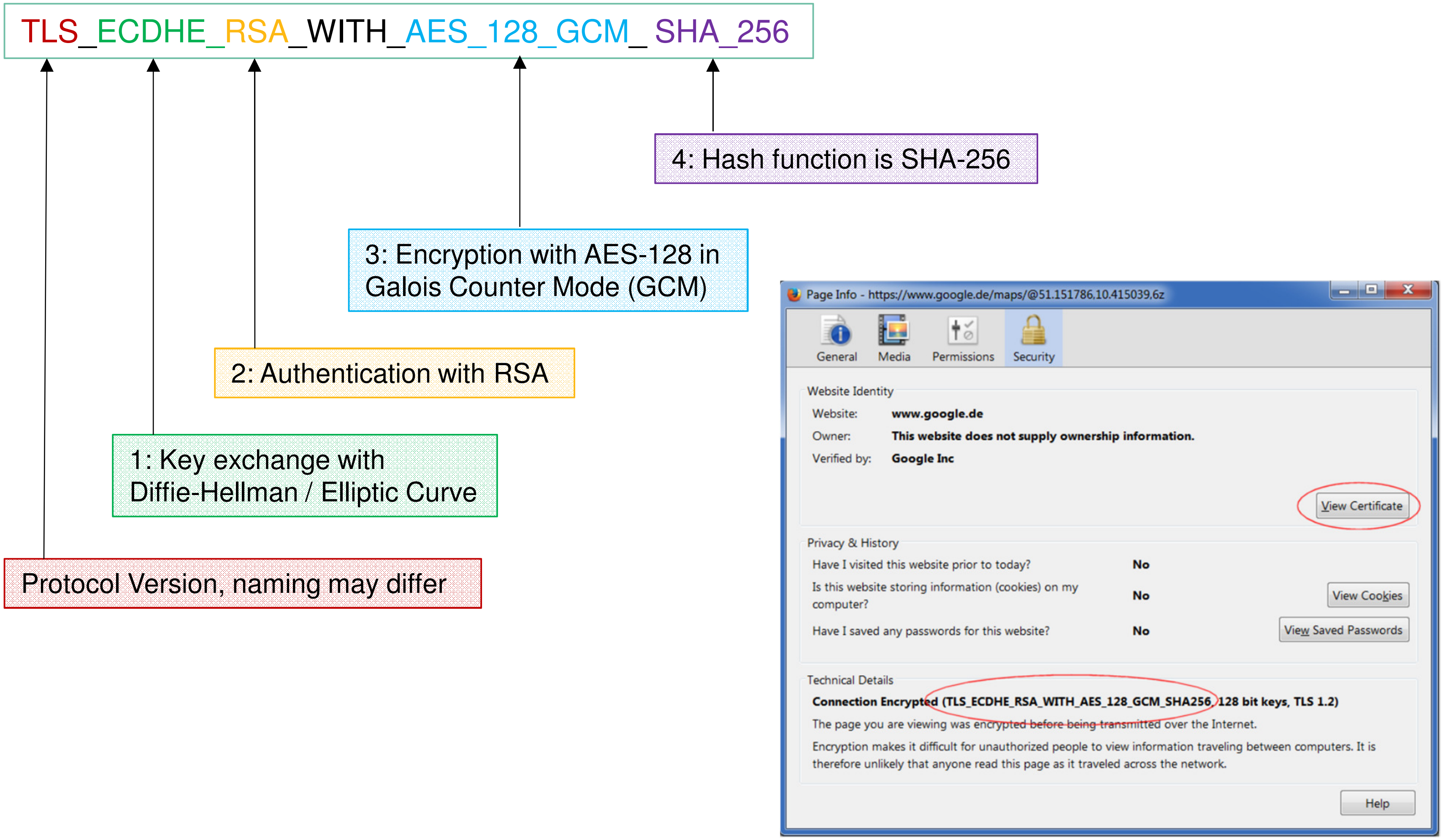
Requires CEX4S CCA coprocessor or later with internal CCA level of 4.2 or higher.

Check card’s CCA level with new z/VSE 6.2 crypto command on console:

```
msg fb,data=apstat ap=2 statcca
FB 0115 Adapter Status of AP 2 (Coprocessor)
...
FB 0115   CCA application version ................ : 4.4.59z
FB 0115   CCA application build date ............. : 20160511
FB 0115   Host application user authority ........ : DEFALT15
```

All together builds an SSL/TLS cipher suite

Example: maps.google.de



TLS_ECDHE_RSA_WITH_AES_128_GCM_ SHA_256

4: Hash function is SHA-256

3: Encryption with AES-128 in Galois Counter Mode (GCM)

2: Authentication with RSA

1: Key exchange with Diffie-Hellman / Elliptic Curve

Protocol Version, naming may differ

Page Info - https://www.google.de/maps/@51.151786,10.415039,6z

Website Identity

Website: **www.google.de**

Owner: **This website does not supply ownership information.**

Verified by: **Google Inc**

Privacy & History

Have I visited this website prior to today? **No**

Is this website storing information (cookies) on my computer? **No**

Have I saved any passwords for this website? **No**

Technical Details

Connection Encrypted (TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, 128 bit keys, TLS 1.2)

The page you are viewing was encrypted before being transmitted over the Internet.

Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.

Recommendations

- **Symmetric encryption:**
  - RC4 (Ron‘s Code 4), from the 80‘s, Stream cipher → Insecure
  - DES, 3DES (Data Encryption Standard), 1977, Block cipher → also treated as insecure nowadays
  - AES (Advanced Encryption Standard), 2000, Block cipher → Recommended (AES-128/256)
- **Asymmetric encryption:**
  - RSA (Rivest, Shamir, Adleman), 1977, → Use key sizes >= 2048 bits
  - ECC (Elliptic Curve Cryptography) (from the 80’s) → Use in combination with RSA, 256-bit curve
- **Hash Algorithms („digital fingerprint“)**
  - MD5 (Message Digest 5) → Insecure
  - SHA-1 (Secure Hash Algorithm, 2001) → no longer considered secure
  - SHA-2 (224, 256, 384, 512), 2002 → Recommended hash algorithm
  - SHA-3, standardized 2015 -> Successor of SHA-2, may not be available in applications
- **SSL/TLS protocol versions**
  - SSL 3.0 → Do not use this anymore
  - TLS 1.0 / 1.1 → May be used if TLS 1.2 is not available
  - TLS 1.2 → Recommended

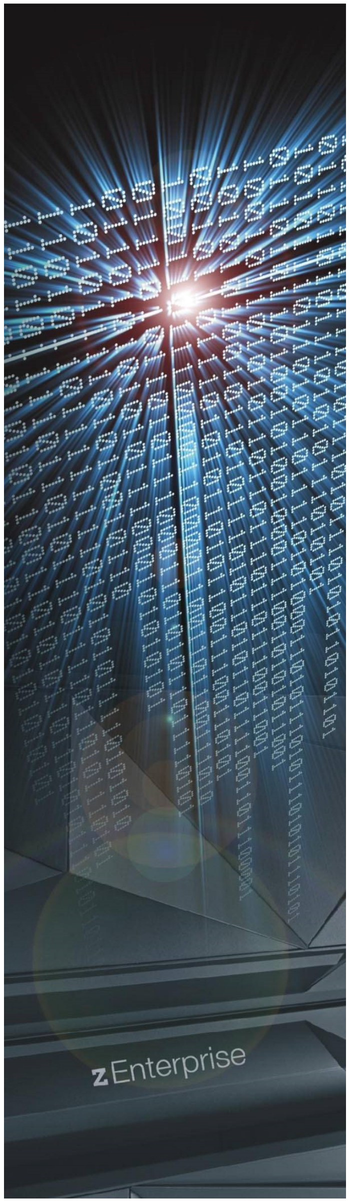
SHA3 supported in hardware on z14!

What’s coming next?

- **TLS 1.3**
  - First draft from 2016
  - Removes all deprecated and insecure algorithms
  - Key exchange only using Diffie-Hellmann, preferable with Elliptic-Curve
  - Data encryption with AES-GCM only
  - Already available in:
    - Google Chrome 56 (needs manual activation)
    - Firefox 52 (TLS 1.3 is activated per default)
    - OpenSSL TLS 1.3 support available with OpenSSL V1.1.1

Agenda

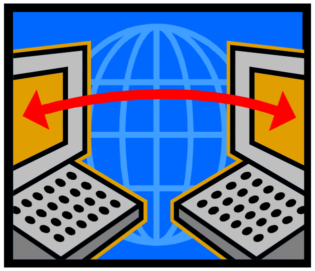
- **Introduction**
- **Cryptography basics**
  - Encryption algorithms
  - Encryption keys
  - Diffie-Hellman versus RSA
  - Elliptic Curve Cryptography
  - Recommendations
- **Using cryptography with z/VSE**
  - Full tape encryption
  - Encryption Facility for z/VSE
  - SSL/TLS
  - SecureFTP
  - Hardware cryptography support on z Systems
  - OpenSSL
  - What's new with z/VSE V6.2



Using cryptography with z/VSE

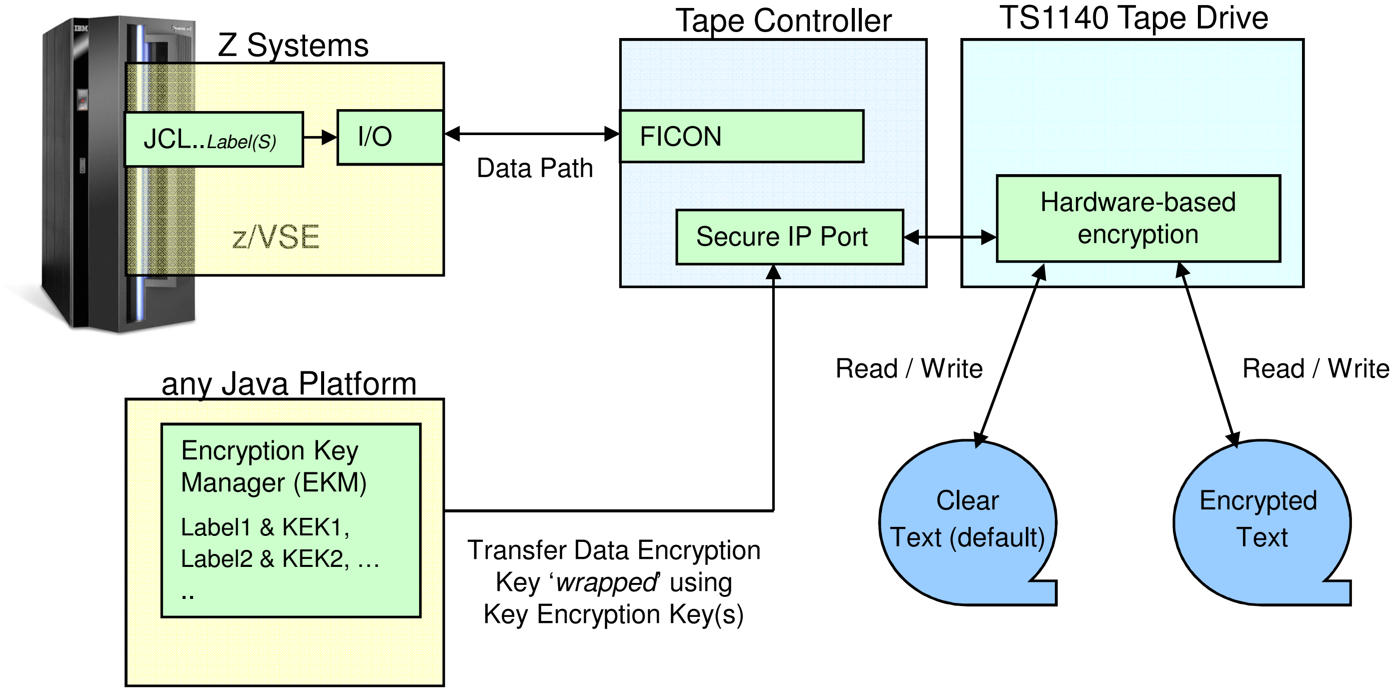
Main areas of cryptography:

- **Encryption of data transmitted over network connections**
  - SSL/TLS, HTTPS
  - SecureFTP
  - Secure Telnet / TN3270



- **Encryption of data stored on disk or tape**
  - Encryption of backups or archives
  - Exchange of encrypted and/or signed data with customers or business partners
  - TS1140 Encrypting Tape Drive
  - Encryption Facility for z/VSE

IBM Tape Encryption – TS1140



encryption mode (03=write)

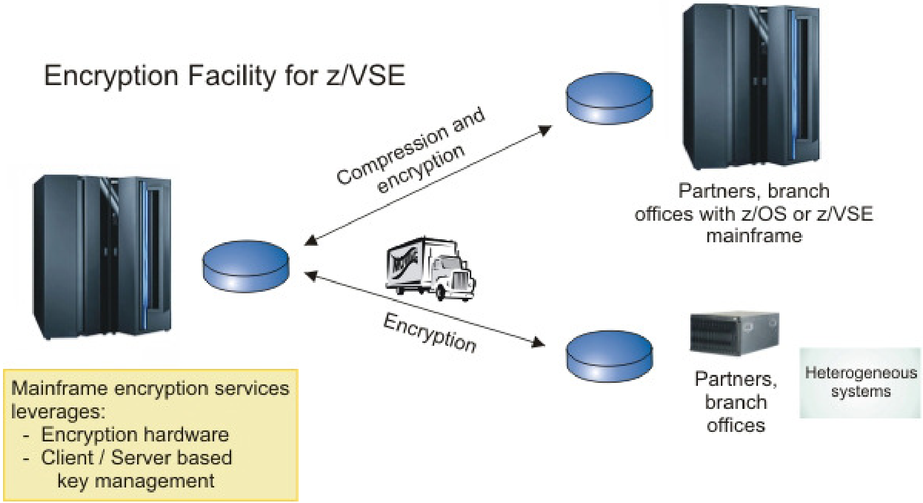
```
// JOB ENCRYPT
// ASSGN SYS005,480,03
// KEKL UNIT=480,KEKL1='MYKEKL1',KEM1=L,KEKL2='MYKEKL2',KEM2=L
// EXEC LIBR
  BACKUP LIB=PRD2 TAPE=SYS005
/*
/&
```

encoding mechanism (L=Label, H=Hash)

key label1 (name of the 1. KEK-key in EKM)

Encryption Facility for z/VSE

- Secure business and customer data
- Address regulatory requirements
- Protect data from loss and inadvertent or deliberate compromise
- Enable sharing of sensitive information across platforms with partners, vendors, and customers
- Enable decrypting and encrypting of data to be exchanged between z/VSE and non-z/VSE platforms


Encryption Facility for z/VSE
Compression and encryption
Partners, branch offices with z/OS or z/VSE mainframe
Encryption
Partners, branch offices
Heterogeneous systems
Mainframe encryption services leverages:
- Encryption hardware
- Client / Server based key management

- The Encryption Facility for z/VSE is packaged as an optional, priced feature of VSE Central Functions V8.1 (5686-CF8-40).

- The Encryption Facility for z/VSE V1.1 uses z Systems data format

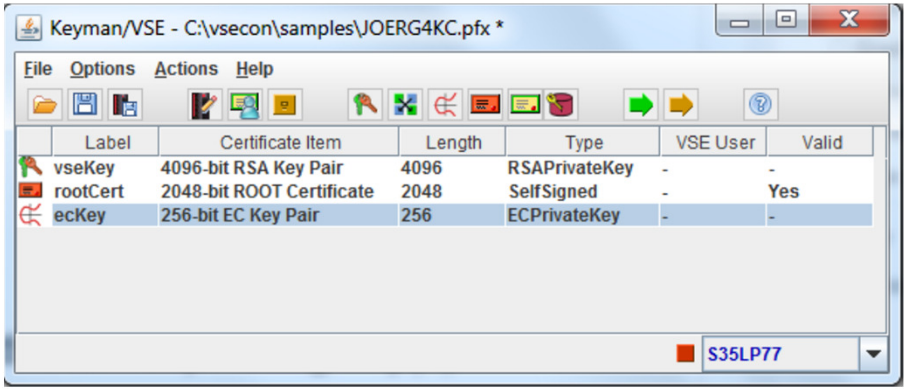
- The Encryption Facility for z/VSE V1.2 uses the standard OpenPGP data format
  - PGP stands for „Pretty Good Privacy“, invented by Phil Zimmermann in 1991
  - Open Standard, described in RFCs 2440 and 4880
  - Compatible with Encryption Facility for z/OS V1.2 and many other OpenPGP implementations

Key & Certificate Management

Cryptography uses Keys and Certificates

- **Key Management is not trivial**
  - Key must often be kept secure for a very long time
  - You must be able to associate the encrypted data with the corresponding key(s)
  - Encrypted data and the corresponding key(s) must be strictly separated

- **Keyman/VSE**
  - Creation of RSA keys and digital certificates
  - Upload of keys and certificates to VSE
  - Creation of PKCS#12 keyring files (use with Java-based connector or import into a Web browser)
  - Support for PEM files for OpenSSL
  - Download from VSE Homepage http://www.ibm.com/systems/z/os/zvse/downloads/#vkeyman

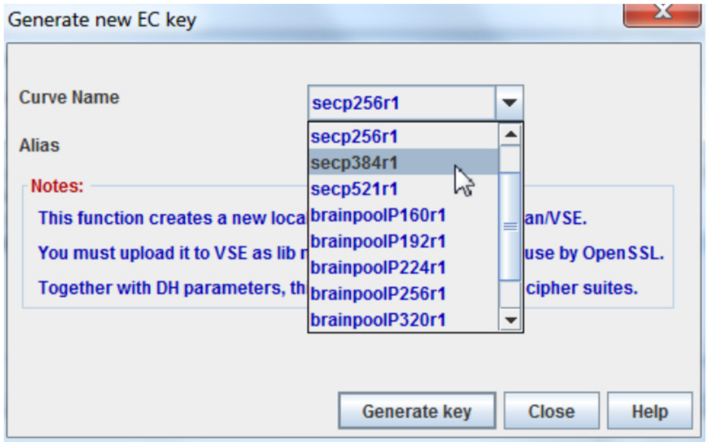


Keyman/VSE - C:\vsecon\samples\JOERG4KC.pfx *

Label	Certificate Item	Length	Type	VSE User	Valid
vseKey	4096-bit RSA Key Pair	4096	RSAPrivateKey	-	-
rootCert	2048-bit ROOT Certificate	2048	SelfSigned	-	Yes
ecKey	256-bit EC Key Pair	256	ECPrivateKey	-	-

Keyman/VSE updates

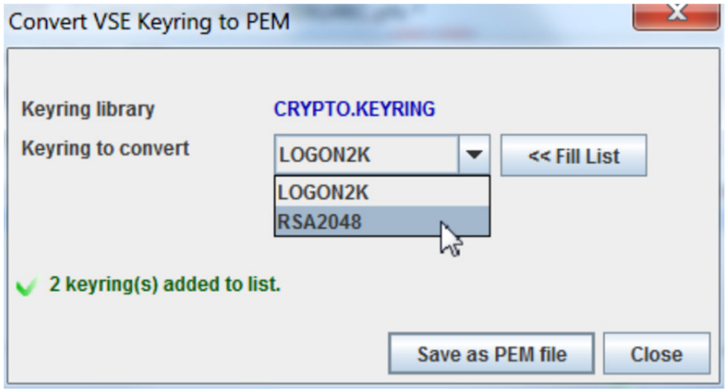
- **ECC support**
  - Create and upload Elliptic-Curve (EC) key pairs.
- **SHA-256 support**
  - Support SHA-256 signatures in certificates.
  - This may require additional 1.5F zaps on TCP/IP for VSE.
- **Convert CSI keyrings to PEM**
  - Use existing PRVK, CERT, and ROOT members on VSE and build an equivalent PEM file for OpenSSL


Generate new EC key

Curve Name: secp256r1

Alias

Notes:
This function creates a new loca[...]an/VSE.
You must upload it to VSE as lib r[...]use by OpenSSL.
Together with DH parameters, th[...]cipher suites.

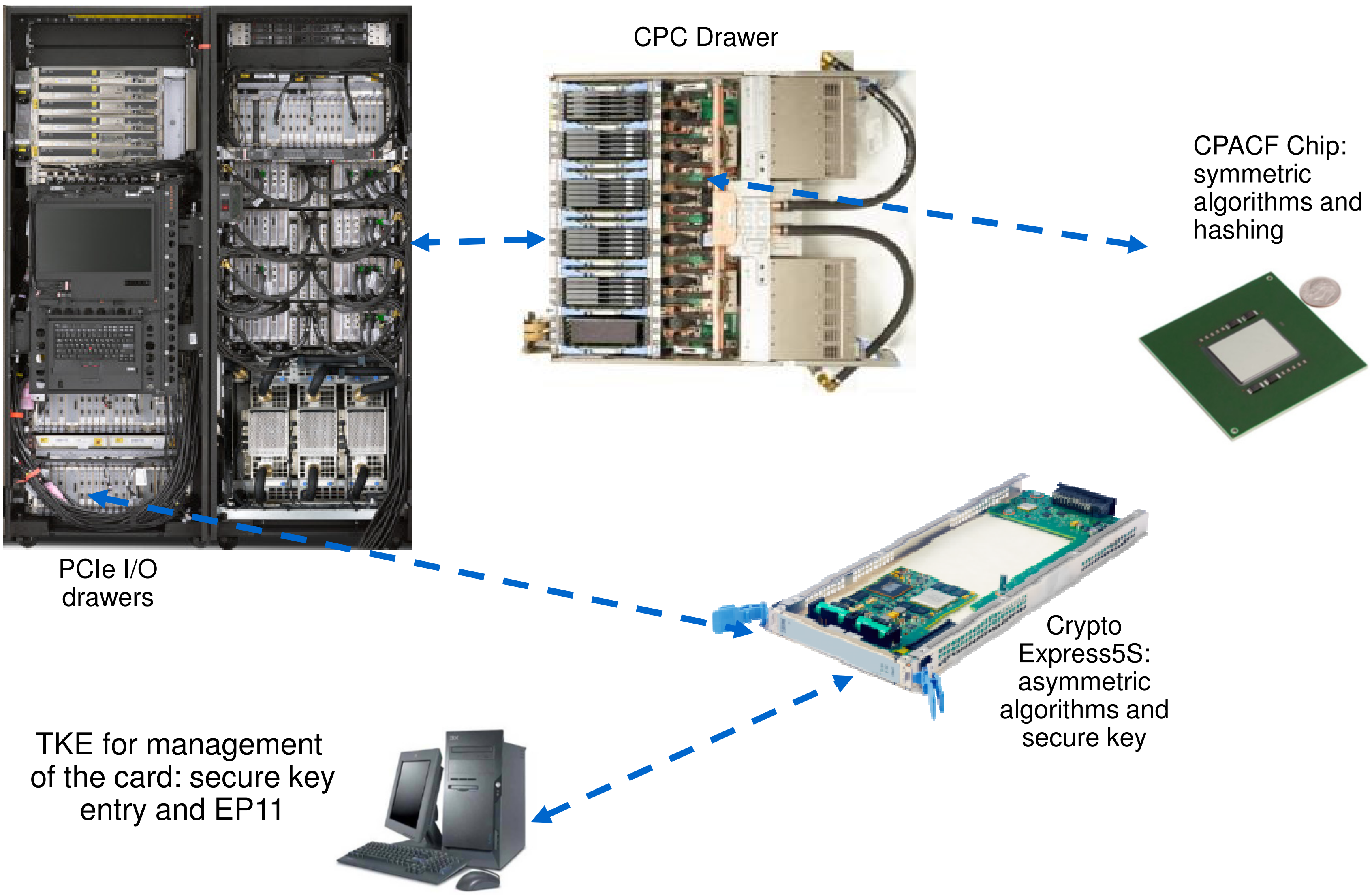

Convert VSE Keyring to PEM

Keyring library: CRYPTO.KEYRING

Keyring to convert: LOGON2K

✓ 2 keyring(s) added to list.

Hardware Crypto Support on z Systems



CPC Drawer

CPACF Chip: symmetric algorithms and hashing

PCIe I/O drawers

Crypto Express5S: asymmetric algorithms and secure key

TKE for management of the card: secure key entry and EP11

Crypto Express6S

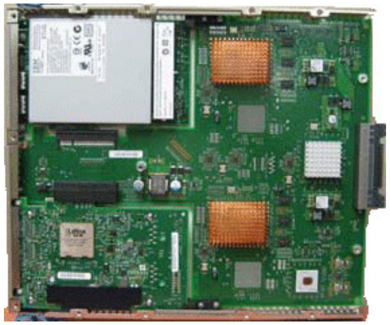
- Exclusive to IBM z14
- One-port card, i.e. one AP (adjunct processor) per physical card
  - 2 cards min, 16 cards max per machine
- Seneca I/O cage (the ‘S’ in the name)
- Can be configured in one of three ways:
  - CEX6A: Accelerator
  - CEX6C: IBM Common Cryptographic Architecture (CCA) coprocessor
  - CEX6P: IBM Enterprise Public Key Cryptography Standards (PKCS) #11 (EP11) coprocessor
- Form factor comparison CEX3 / CEX6S:

Support for Crypto Express6S

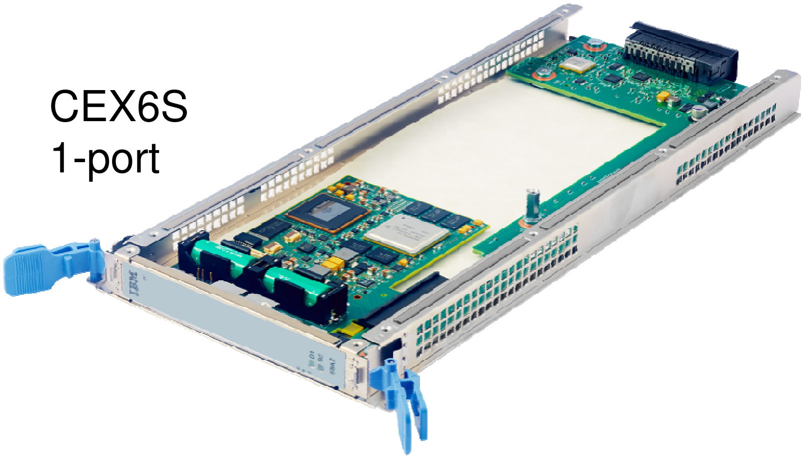
- Included in z/VSE 6.2 GA version
- APAR DY47715 for z/VSE 5.2
- APAR DY47716 for z/VSE 6.1

NEW!

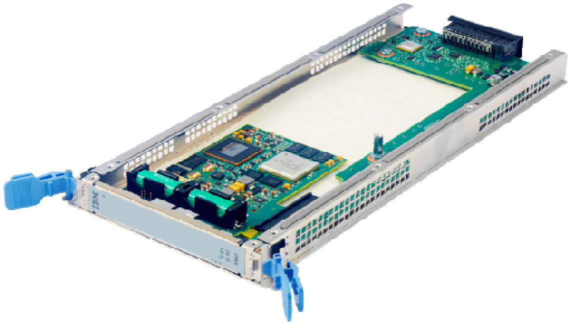
CEX3
2-port



CEX6S
1-port



z/VSE Hardware Configuration



- **z/VSE hardware configuration not necessary for crypto hardware**
  - No IOCDS definition in VSE
  - No device type
  - No ADD statement
  - You may have to define the devices in the HMC (LPAR) or z/VM directory

- **Use of crypto hardware is transparent to end users and applications**
  - But use of crypto hardware can be disabled via option

- **How to setup cryptographic hardware for VSE:**
  - http://www.ibm.com/systems/z/os/zvse/documentation/security.html#howto

```
FB 0095 1J054I FOUND A CRYPTO EXPRESS5S CARD AT AP 0
FB 0095 1J054I FOUND A CRYPTO EXPRESS5S CARD AT AP 3
FB 0095 1J005I HARDWARE CRYPTO DEVICE DRIVER INITIALIZED SUCCESSFULLY.
FB 0095 1J006I USING AP QUEUE 79
```

Using crypto cards under z/VM

- **There are two ways for assigning cards to a z/VM guest**
  - CRYPTO APVIRT
    - z/VM assigns a virtual crypto domain (AP Queue) to the z/VM guest and shows only one AP to the guest
    - z/VM hides CCA coprocessors in favor of accelerators
    - Virtualized cards don’t have all features of dedicated cards
  - CRYPTO APDEDICATE
    - Assignment of cards like in LPAR mode
    - Requests from guest system are directly forwarded to the hardware

- **Recommendation**
  - APDEDICATE wherever possible
    - Otherwise CCA coprocessor functions may get lost (e.g. random number generation, used in Encryption Facility and OpenSSL)
    - Load Balancing done by VSE is better
  - Optimal is one accelerator and one CCA coprocessor

OpenSSL Support

- **What is OpenSSL?**
  - OpenSSL is an Open Source project providing an SSL/TLS implementation and key management utilities
  - Available for most Unix-style operating systems, MAC, Windows, and IBM System i (OS/400)
  - For details on OpenSSL refer to http://www.openssl.org/

- **Why OpenSSL on z/VSE?**
  - The TCP/IP stack from Connectivity Systems, Inc. has an own SSL/TLS implementation
  - What about the other two stacks:
    - IPv6/VSE from Barnard Systems, Inc.
    - Linux Fast Path (LFP) provided by IBM
  - All stacks could use one single SSL/TLS implementation: **OpenSSL**
  - OpenSSL is widely used in the industry
  - Latest RFC’s implemented
  - One central place for access to crypto hardware, software updates, migration to higher versions

Welcome to the OpenSSL Project

The OpenSSL Project is a collaborative effort to develop a robust, commercial-grade, fu
implementing the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security
general purpose cryptography library. The project is managed by a worldwide communit
communicate, plan, and develop the OpenSSL toolkit and its related documentation.

OpenSSL is based on the excellent SSLeay library developed by Eric A. Young and Tin
under an Apache-style licence, which basically means that you are free to get and use it f
subject to some simple license conditions.

Date	Newsflash

OpenSSL Support

- **What is available on z/VSE?**
  - OpenSSL 1.0.2h runtime library (with PTF UD54224)
  - New component: z/VSE cryptographic services, 5686-CF9-17-51S
  - Available on z/VSE 5.1 plus PTFs, or newer z/VSE releases
  - Software implementations for all algorithms with all key lengths
  - Hardware Crypto Support (Crypto Express cards and CPACF)
  - Programming APIs:
    - OS390 / z/OS compatible SSL API (gsk_initialize(), gsk_secure_soc_init(), etc.)
    - Subset of the OpenSSL API (LE/C)

- **OpenSSL Exploitation**
  - IPv6/VSE product exploits OpenSSL
    - **SSL Proxy Server** (BSTTPRXY)

      Proxies a clear text connection into
      an SSL/TLS connection and vice versa
    - **Automatic TLS Facility** (BSTTATLS)

      Automatically converts any application
      into SSL/TLS application
  - **User applications and z/VSE Connectors** (using LE/C Socket Interface)
    - Via LE/C Socket API Multiplexer

BSI BARNARD SOFTWARE, INC.

News with z/VSE 6.2

- **Hardware crypto operator interface for ESM customers**
  - The z/VSE crypto device driver runs as a subtask (IJBCRYPT) in the BSM security server partition (FB by default)
  - Customers using an ESM (CA TopSecret, BIM Alert, etc.) had to start phase IJBCRYPT in a partition to start the device driver
  - IJBCRYPT does not provide an operator interface.
    - No influence on behavior of device driver possible
    - No status information of device driver visible
  - New with z/VSE 6.2: Phase IJBHCOPR
    - Start in any partition, full control via operator interface

```
S1 0045 // JOB IJBHCOPR - OPERATOR INTERFACE FOR CRYPTO
        DATE 09/07/2017, CLOCK 10/50/39
S1 0115 1J022I CPU CRYPTOGRAPHIC ASSIST FEATURE AVAILABLE.
S1 0045 Crypto device driver running (MSG nn,DATA=? for help)
S1 0115 1J054I FOUND A CRYPTO EXPRESS4S CARD AT AP 0
S1 0115 1J054I FOUND A CRYPTO EXPRESS4S CARD AT AP 1
S1 0115 1J054I FOUND A CRYPTO EXPRESS4S CARD AT AP 2
S1 0115 1J005I HARDWARE CRYPTO DEVICE DRIVER INITIALIZED SUCCESSFULLY.
S1 0115 1J006I USING AP QUEUE 15
```

News with z/VSE 6.2

- **OpenSSL component of z/VSE enhancements:**
  - The OpenSSL component of z/VSE (z/VSE Cryptographic Services) will be upgraded to benefit from newer SSL/TLS functions
  - The OpenSSL component will transparently use hardware acceleration for Elliptic Curve Cryptography (ECC), if available

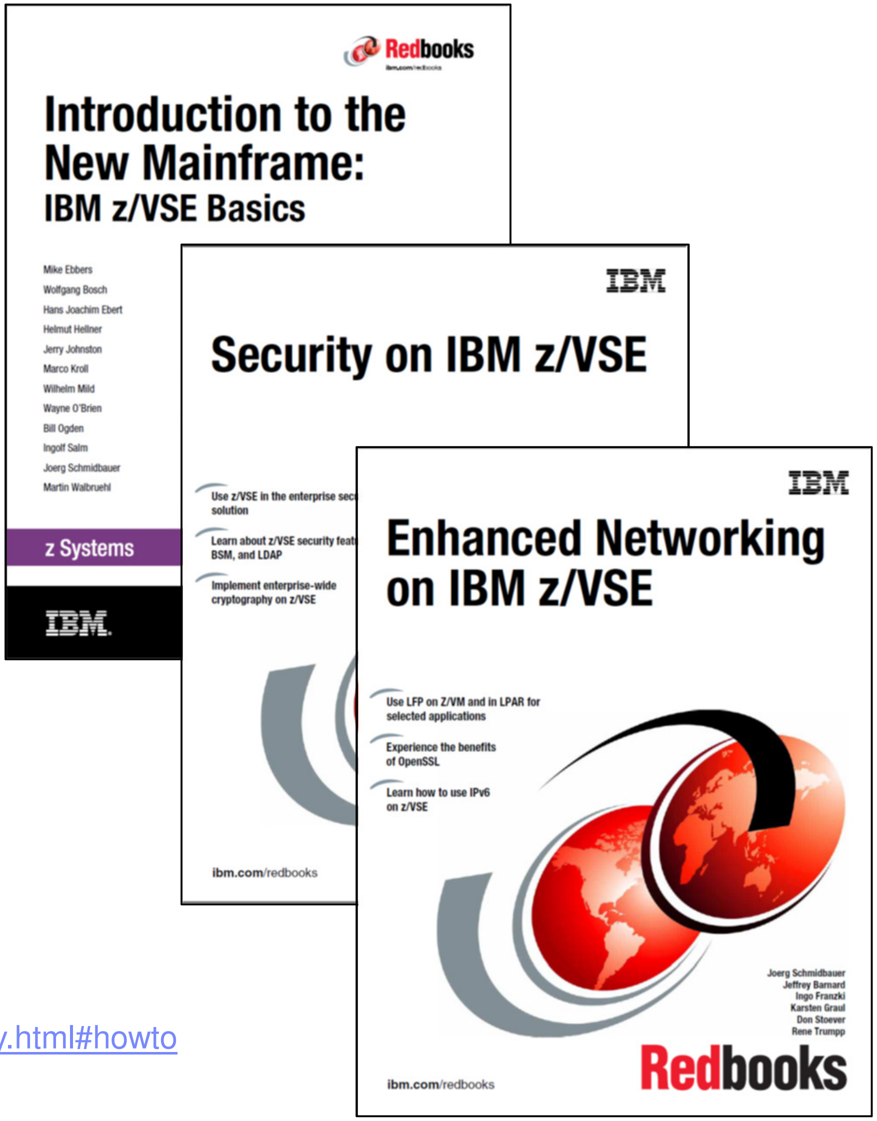
- **CICS TS V2.2 security enhancements:**
  - OpenSSL support for CICS Web Support will give clients more flexibility and allow them to take advantage of the OpenSSL security

- **EZA API enhancements:**
  - The EZA 'Multiplexer' and the EZA OpenSSL support will simplify the use of the EZA interface with any TCP/IP stack and allow to transparently use OpenSSL with EZA SSL-applications

- **VTAPE enhancements:**
  - Clients can use SSL/TLS connections for remote VTAPEs (virtual tapes) to protect sensitive data during network transfer

Important books

- **z/VSE Administration, SC34-2692**
  - Everything on encryption and SSL/TLS
  - Encryption Facility for z/VSE
  - TS1140 tape encryption
- **z/VSE TCP/IP Support, SC34-2706**
  - Overview on TCP/IP stacks
  - OpenSSL
- **Redbook: Enhanced Networking on IBM z/VSE, SG24-8091**
  - Focus on IPv6/VSE and OpenSSL
- **Redbook: Security on IBM z/VSE, SG24-7691**
  - Focus on CSI TCP/IP for VSE
- **Redbook: IBM z/VSE Basics, SG24-7436**
  - VSE in general
  - New chapter 18 on encryption
- **z/VSE e-business Connectors, User's Guide**
- **CICS Enhancements Guide, GC34-5763**
- **Technical articles on the z/VSE web page:** http://www.ibm.com/systems/z/os/zvse/documentation/security.html#howto



Thank You

Please forward your questions or remarks to
zvse@de.ibm.com

More Information

… on VSE home page: http://ibm.com/vse

- Ingolf's z/VSE blog: https://www.ibm.com/developerworks/mydeveloperworks/blogs/vse
- Requirements: https://www-03.ibm.com/systems/z/os/zvse/contact/requirement.html
- z/VSE service & support: http://www-03.ibm.com/systems/z/os/zvse/support/

z/VSE Live Virtual Classes

z/VSE	@ http://www.ibm.com/zvse/education/
LINUX + z/VM + z/VSE	@ http://www.vm.ibm.com/education/lvc/

Join the LVC distribution list by sending a short mail to zvse@de.ibm.com