z/VSE Live Virtual Class Series

Security and Cryptography on z/VSE

Joerg Schmidbauer

jschmidb@de.ibm.com

May 27, 2009

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.

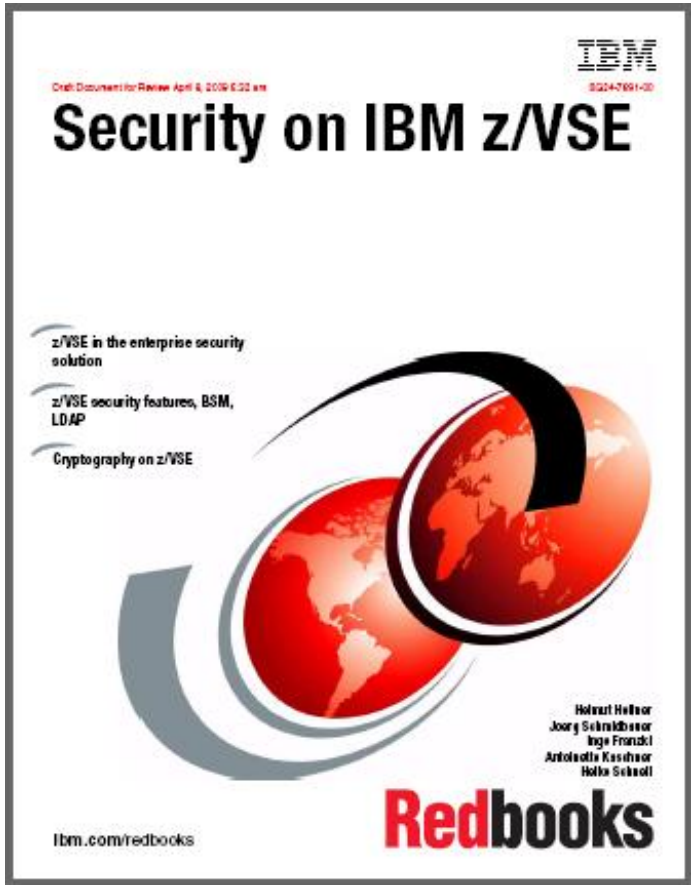
The information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this 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 on security**
  - New VSE redbook
  - VSE Health Checker updates
- **Encryption Facility for z/VSE**
  - Password-based encryption
  - Public key encryption
- **OpenPGP support**
  - Encryption Facility V1.2
  - Keyman/VSE
  - Open Source GnuPG
  - Support on z/OS

New Redbook: "Security on IBM z/VSE"



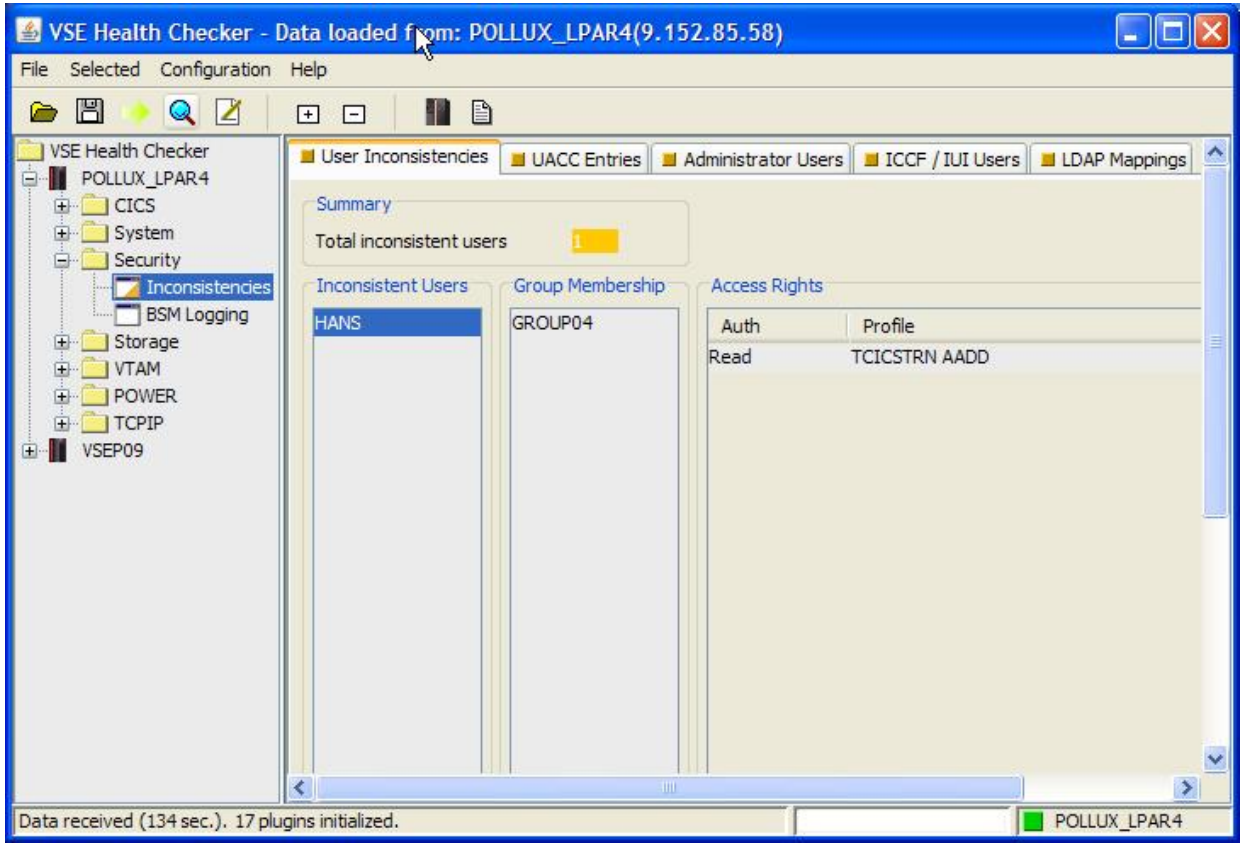
Available on:

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

Table of contents

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"**

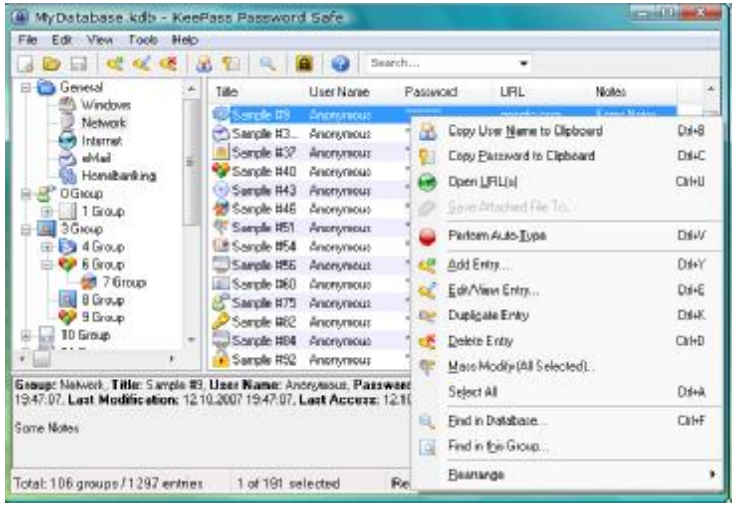


Encryption Facility for z/VSE

- **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/
- **IBM crypto hardware exploitation**
  - Crypto cards (PCICA, PCIXCC, CEX2) and CPACF
- **Eligible for MWLC pricing**
- **Two main functions**
  - Password-based encryption
  - Public-key encryption

Password-based encryption (PBE)

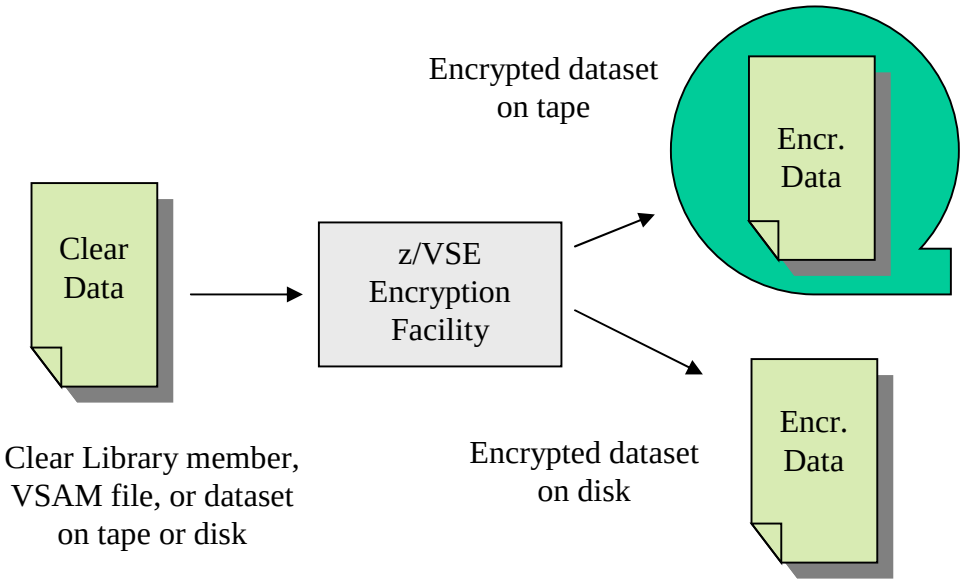
- **Encryption key (data key) is generated from**
  - the given secret password (8 … 32 characters)
  - and some additional parameters including some random number (the “salt” value)
- **These additional values are stored in the encrypted dataset**
  - When encrypting the same data twice with the same 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)

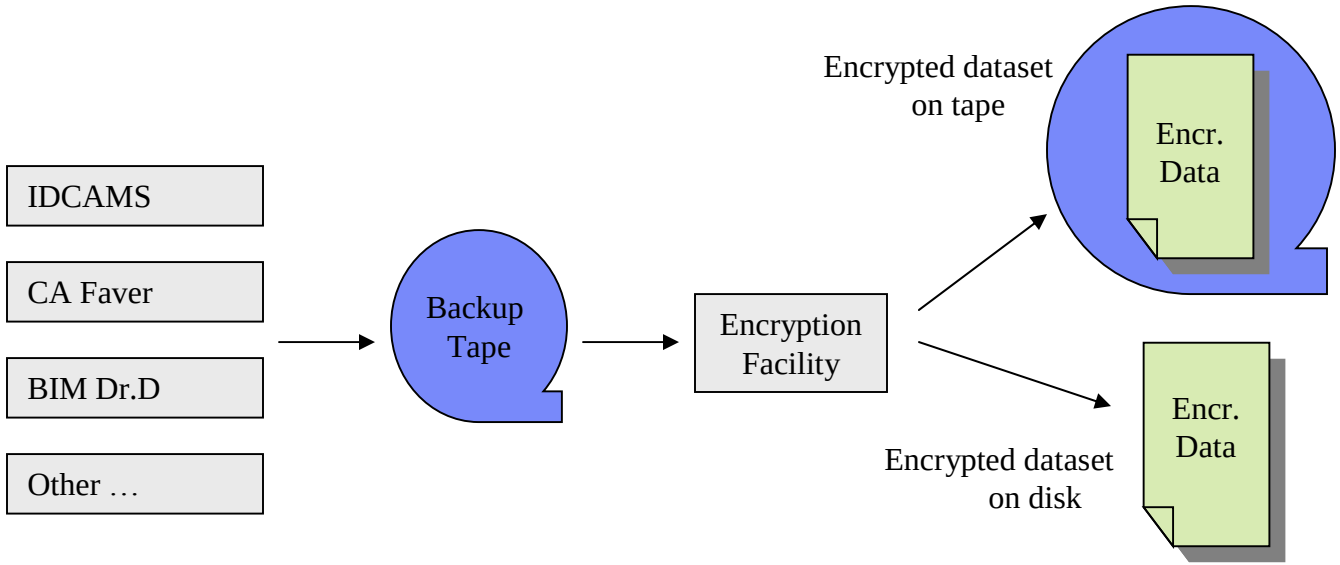
- **Encryption key (data key) is randomly generated**
- **Data key is then encrypted with one or more public keys of the recipients of the encrypted data**
  - Needs a Crypto Express2 or PCIXCC card for 2048 bit keys
  - Crypto cards are transparently used also for 1024 bit keys when available
- **Encrypted 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

Encryption of a single file



§ Same behavior for both releases of 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.

Customer value

- No special tape hardware requirements (e.g. TS1120, TS1130)
  - But exploits IBM crypto hardware (crypto cards and CPACF)
- Host-based utility, no additional client/server workstations
- Easy to use
  - No special setup necessary for password-based encryption
- Supports all VSE data formats: single files and complete tape backups (LIBR, IDCAMS, POWER, etc.)
- Supports even proprietary vendor backup formats
  - By just encrypting any given tape
- Encrypted datasets and tapes can easily be exchanged between business partners even on non z platforms
  - Password-based
  - Public-key based
  - System z data format
  - *New:* OpenPGP data format

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 to 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 when V1.2 available.

What's the same for both utilities?

- **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's different?

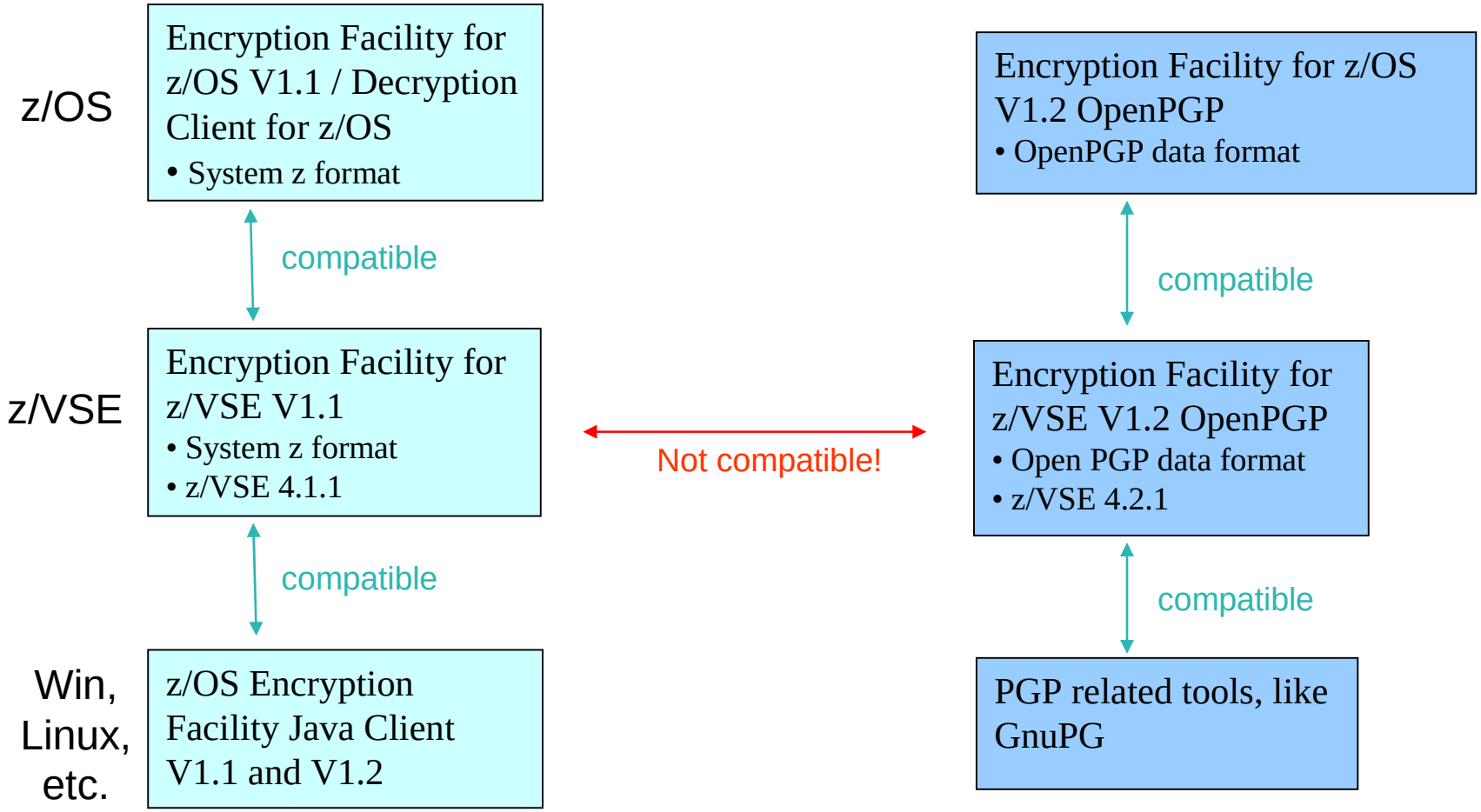
- **Encrypted data format**
  - IJBEFVSE provides System z data format
  - IJBEFPGP provides OpenPGP data format
- **Compatibility**
  - IJBEFVSE provides compatibility to IBM provided Java client, Decryption client for z/OS
  - IJBEFPGP provides compatibility to PGP implementations
- **Algorithms**
  - 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 !

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

Support on z/OS and data format compatibility



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)

How to handle record-based 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)
- **Exchange of public keys with a PGP environment**
  - PGP certificates are different to x.509 certificates

Flexible support of record and stream data

- **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.

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

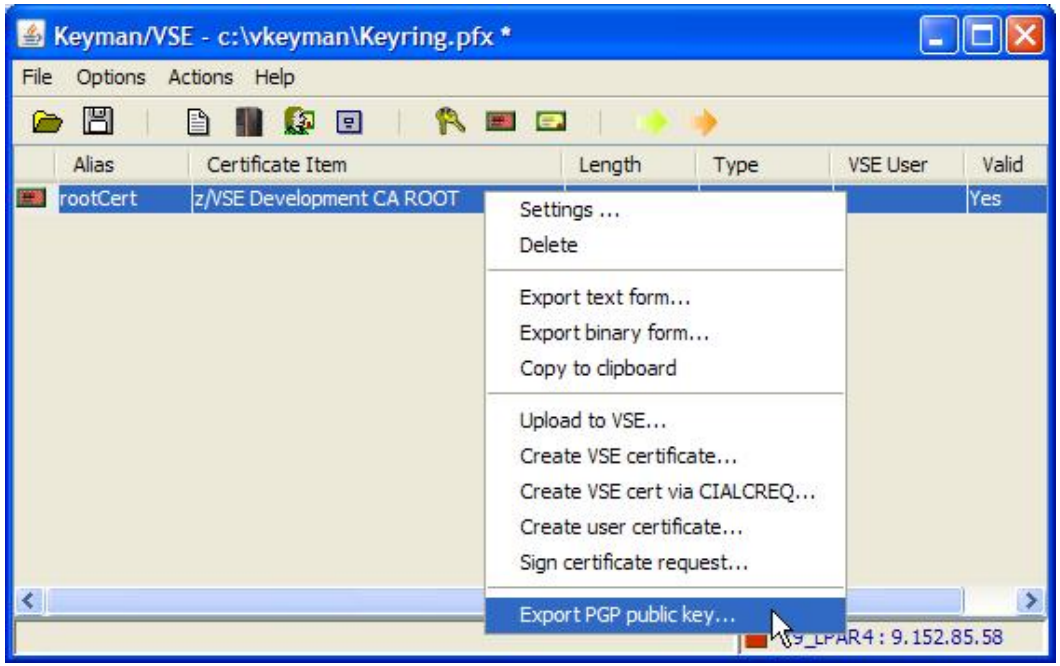
JCL example

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

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

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
  - Will be available for download in July 2009

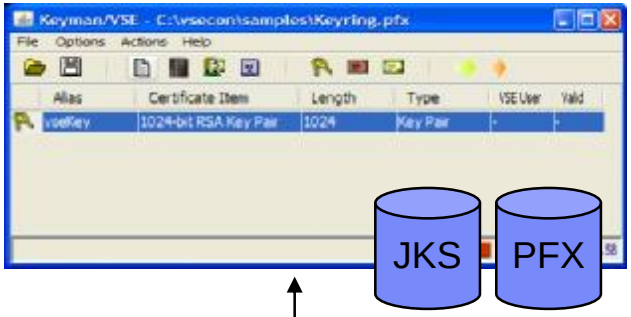


Exchange of public keys

EF for z/OS
- PGP public keys
- x.509 certificates
- Java keystores

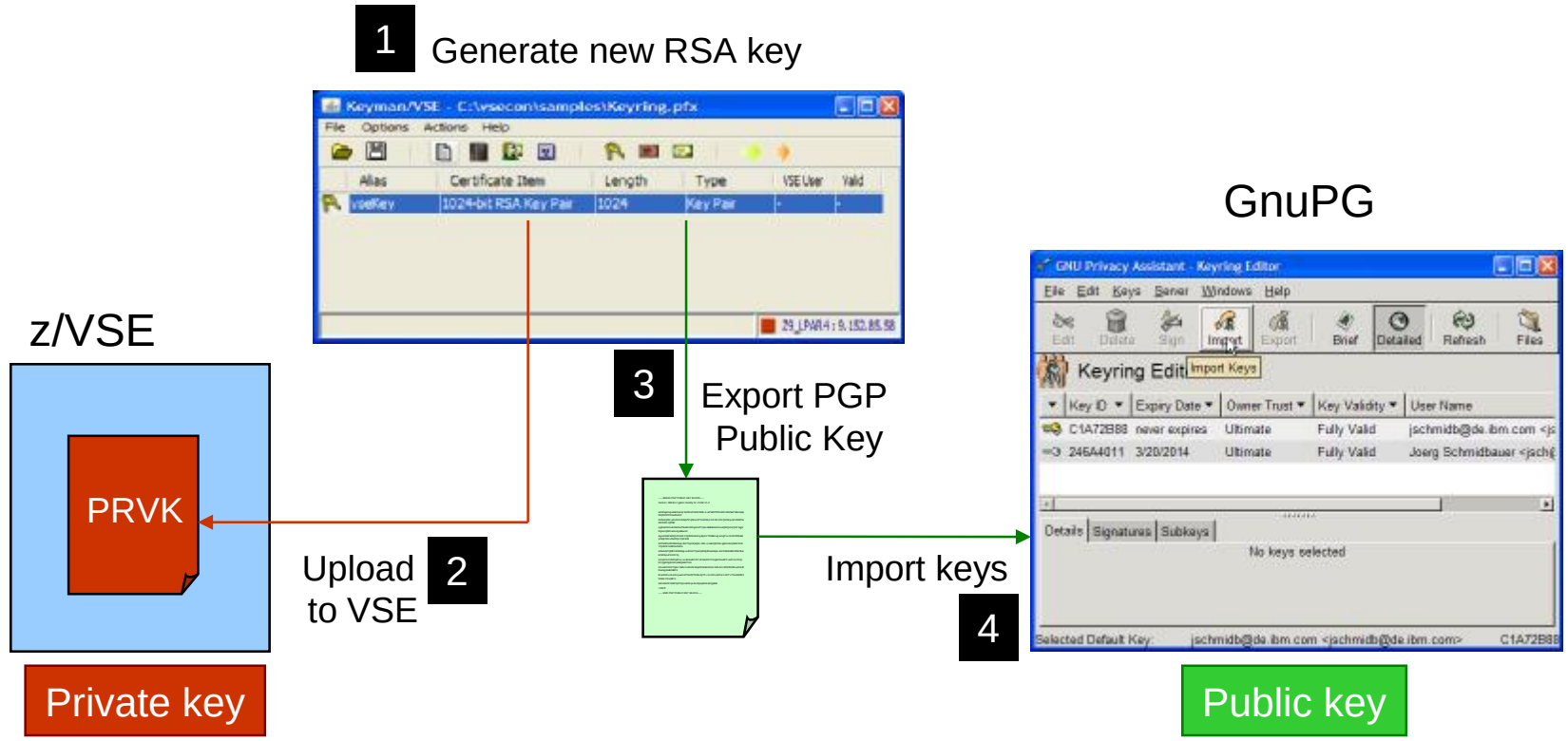
GnuPG
- PGP public keys

Keyman/VSE

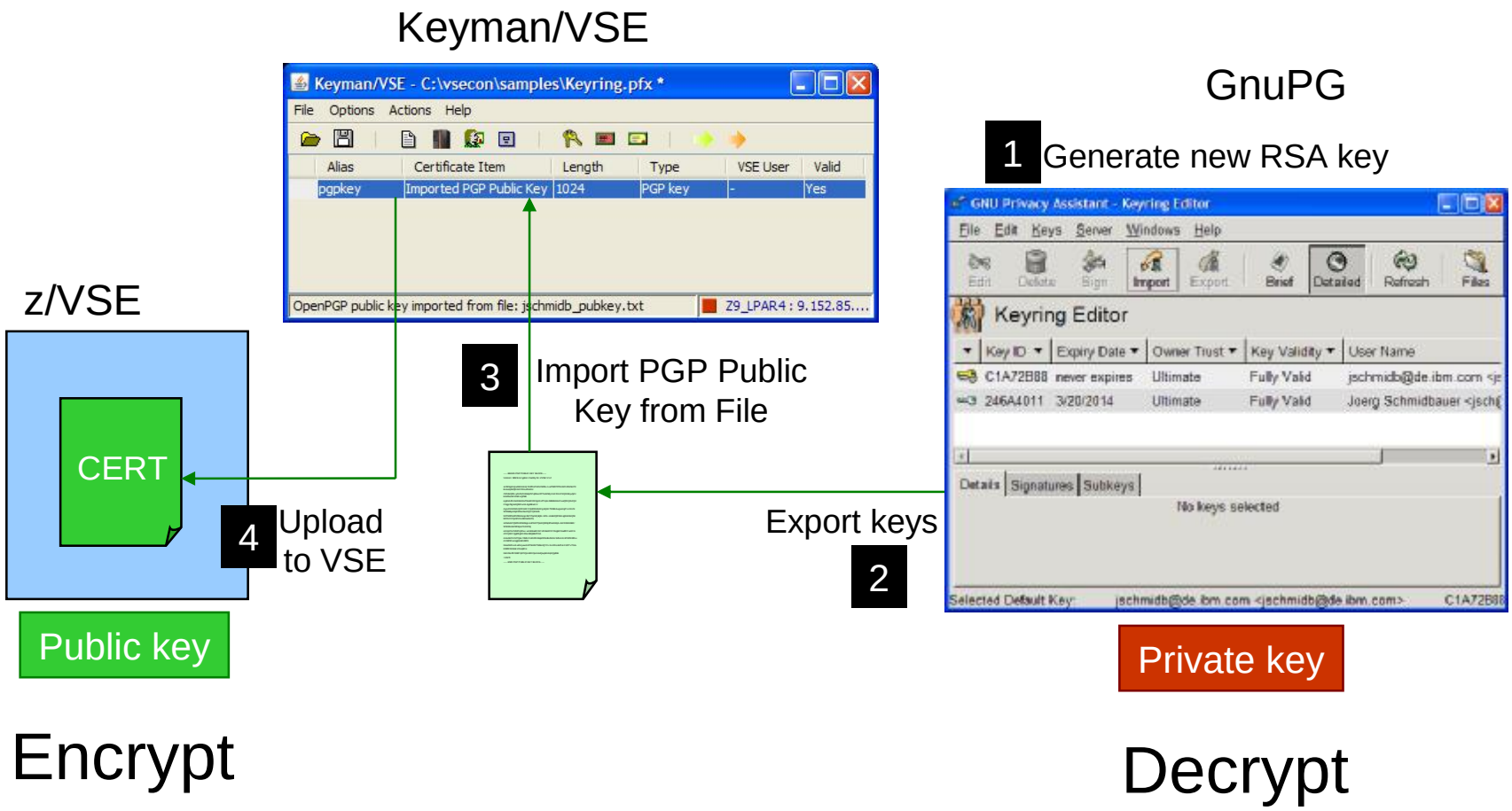


EF for z/VSE
- x.509 certificates
- PRVK members

Scenario 1: decrypt on VSE



Scenario 2: encrypt on VSE

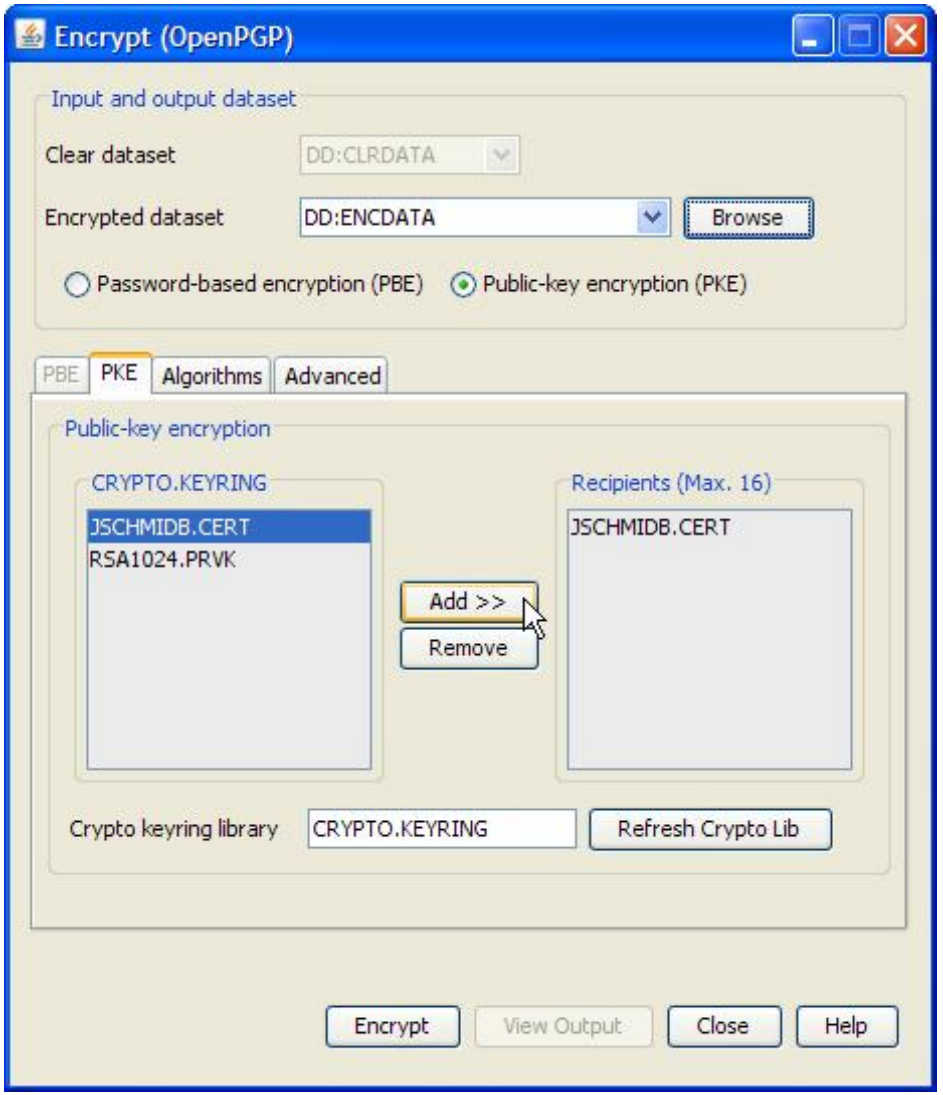


Some thoughts on compression

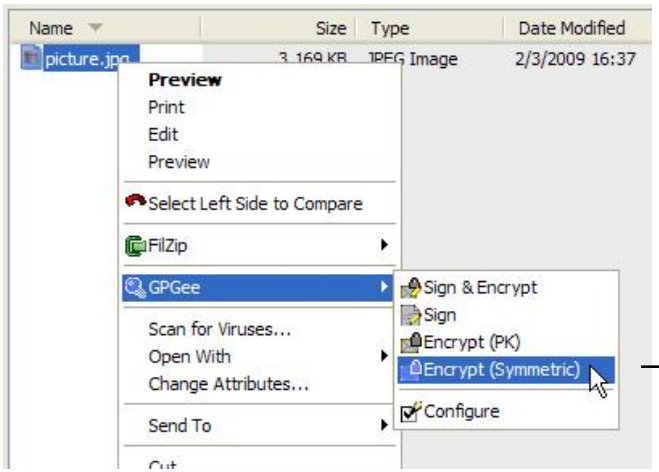
- Compression is always applied before encryption.
- Amount of data
  - When using compression, less data has to be encrypted.
    - Except when clear data is binary, like .jpg, where the compression ratio is very small, sometimes zero.
    - In very rare situations compressed data can get bigger than 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.

VSE Navigator

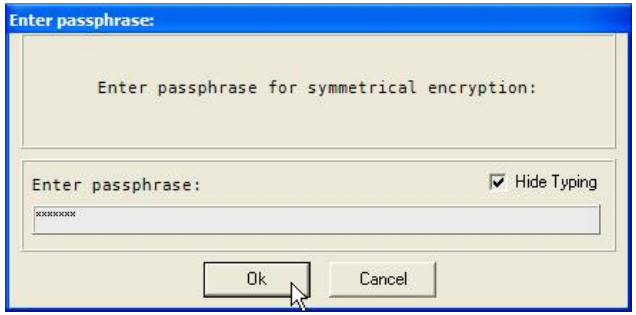
- **GUI for PGP encryption**
  - Right-click VSE library members or VSAM files
  - Menu choices encrypt / decrypt
  - Automatic check if IJBEFPGP phase available on VSE side
  - Check for available algorithms on host side
- **Needs VSE Connector Client**
- **Download from VSE homepage**
- **Provided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



Example scenario



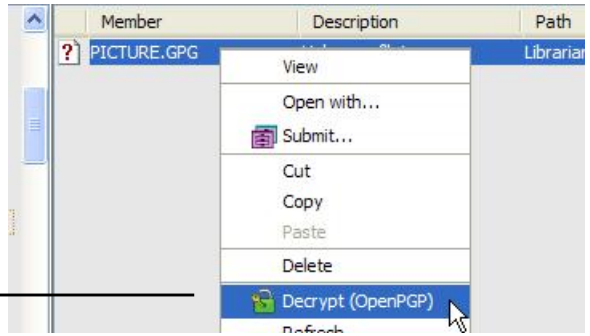
Encrypt via GnuPG / GPGee



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

Positioning of EF to TS1120 / TS1130

	TS1120 / TS1130	Encryption Facility
High volume backup/archiving	**x**	**-**
Data encryption for rest on VSE disks	**-**	**x**
Data encryption for subsequent file transfer (e.g. FTP)	**-**	**x**
Local archiving	**x**	**x**
Data exchange with remote sites having TS11xx	**x**	**-**
Use existing TS11xx environment with EKM	**x**	**-**
Data exchange with Encryption Facility for z/OS	**-**	**x**
Data exchange with workstations	**-**	**x**
Password-based encryption	**-**	**x**
Public key based encryption	**x**	**x**
Offload CPU cycles	**x**	**-**

Summary

- **Encryption Facility for z/VSE now ships two utilities**
  - IJBEFVSE (System z data format)
  - IJBEFPGP (OpenPGP)
- **IBM hardware crypto exploitation**
  - CPACF
  - Crypto cards
- **Many free tools available**
  - IBM z/OS Java client for EF V1.1
  - Open Source tools for PGP support (GnuPG, GPGee, GPG4Win)
  - Keyman/VSE for key management and exchange
  - KeePass for managing passwords
  - VSE Navigator with graphical interface for PGP encryption
- **Password-based encryption for quick data exchange**
- **Public key encryption for higher level of security**
- **OpenPGP support available in July 2009**

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

Questions