z/VSE Live Virtual Class Series

Encryption Facility for z/VSE V1.1

Program number: 5686-CF8-40

Joerg Schmidbauer

jschmidb@de.ibm.com

Nov 29, 2007

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.

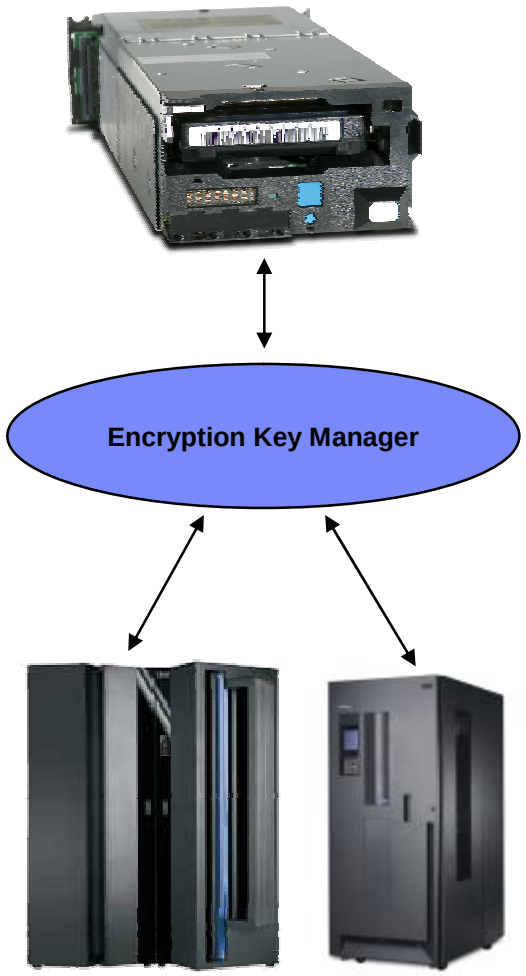
Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

Agenda

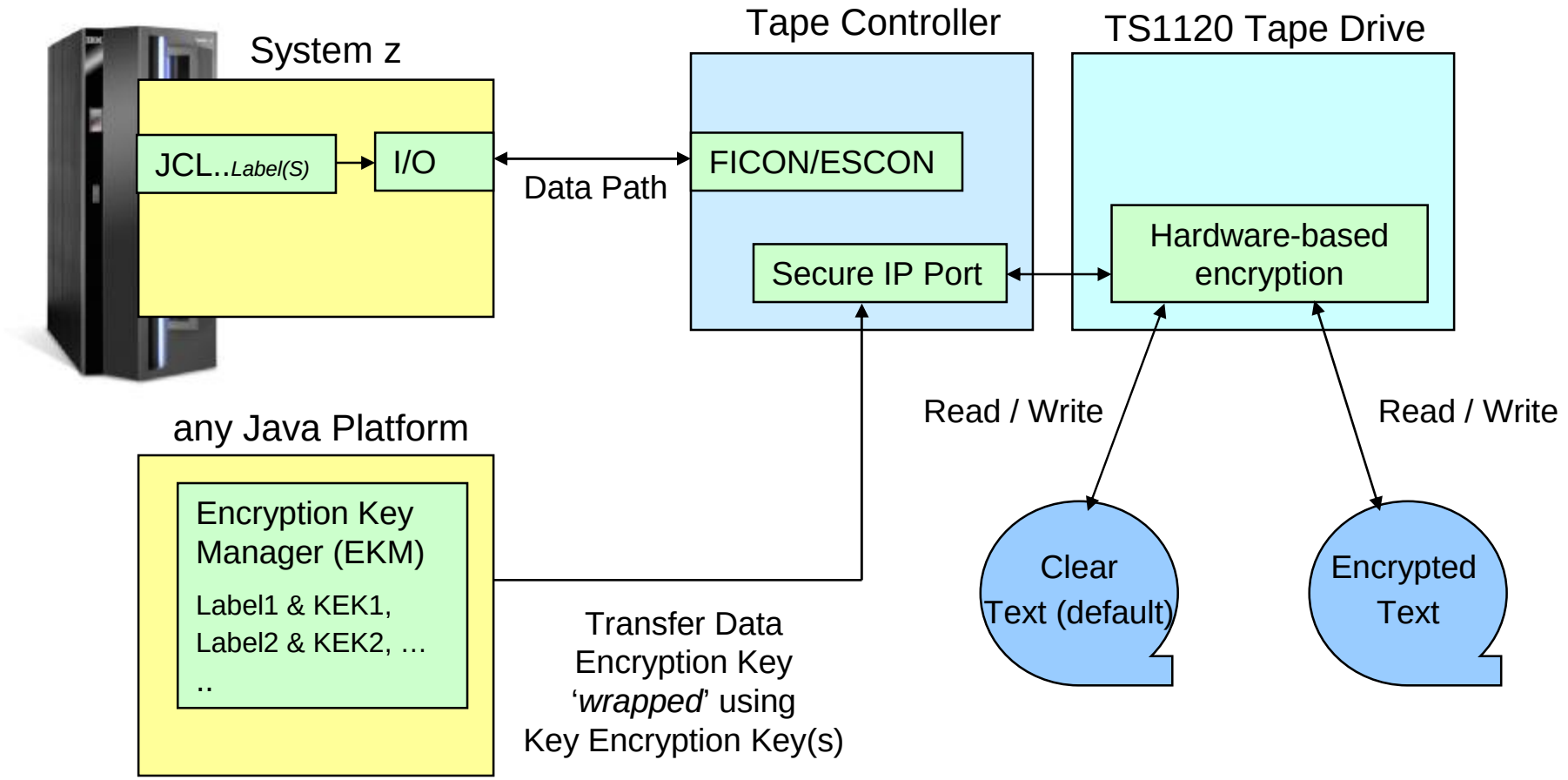
- **News: Loss of sensitive data in UK**
- **Overview: TS1120 tape drive**
- **Encryption Facility for z/VSE**
  - Password-based encryption
  - Public key encryption
- **Relationship to**
  - z/OS Encryption Facility
  - TS1120

IBM TS1120 Tape Drive Encryption

- **Standard feature on new TS1120 tape drives**
- **Supports “traditional” and “encrypted” modes of operation**
- **encryption “disabled” unless otherwise specified**
- **Implements data encryption using AES-256 encryption**
- **Data is automatically compressed then encrypted – no change in media utilization**
- **Supported by z/VSE V4.1 & V3.1**
- **IBM Encryption Key Manager (EKM) for Java platform™**
  - EKM stores and manages labels and key encrypting keys
  - runs on z/OS, AIX, Linux (incl System z), i5/OS, HP, Sun, & Windows
  - Secure TCP/IP connection between EKM and TS1120
  - Operates with IBM tape systems, libraries
- **Enhancements to Tivoli Storage Manager™ to exploit TS1120 encryption**



IBM Tape Encryption – TS1120



TS1120 Summary

- **Hardware-based encryption**
  - No host cycles used
- **Designed for high volume backup**
- **Encryption Key Manager (EKM) on a Java platform**
  - for centralized key management
  - with SSL connection between tape controller and EKM
- **Encryption option specified in VSE via JCL commands**
  - // ASSGN …
  - // KEKL …

What is Encryption Facility for z/VSE?

- **Host-based tool**
- **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**
- **Similar to the "Encryption Facility for z/OS"**
  - http://www.ibm.com/servers/eserver/zseries/zos/encryption_facility/
  - Compatible to Encryption Facility for z/OS V1.1 and V1.2 using System z data format
- **Support of TDES and AES-128 for data encryption**
- **IBM crypto hardware exploitation**
  - crypto cards and CPACF
- **Eligible for MWLC pricing**
- **Two main functions**
  - Password-based encryption
  - Public-key based encryption

Relationship to z/OS Encryption Facility

IBM Encryption Facility for z/VSE, 1.1
Program number: 5686-CF8-40
Runs on: System z9 EC, z9 BC
zSeries 890 or 990

Requires: z/VSE 4.1 (with DY46717) or higher;

Optional Priced Feature

- Supports encrypting and decrypting of data at rest (tapes, disk)
- Supports either Public Key/Private keys or passwords to create highly-secure exchange between partners
- Use z/OS Java Client or Decryption Client for z/OS for data exchange with client systems or decryption on z/OS.
- Use zvse@de.ibm.com mailbox for questions about z/OS Java Client and Decryption Client for z/OS when used in relation with VSE.

IBM Encryption Facility for z/OS, 1.1
Program number: 5655-P97
Runs on: System z9 EC, z9 BC
zSeries 900 or 990
zSeries 800 or 890
Requires: z/OS 1.4 or higher; z/OS.e 1.4 or higher

Java Client
Web Downloadable

Java technology-based code that allows client systems (z/OS and non-z/OS) to decrypt and encrypt data for exchange with z/OS and z/VSE systems.

Decryption Client for z/OS
Web Downloadable

Decryption only code designed to run on z/OS systems. Can process data encrypted and compressed or just encrypted by the Encryption Facility for z/OS or Encryption Facility for z/VSE.

Feature:
Encryption Services

Optional Priced Feature

- Supports encrypting and decrypting of data at rest (tapes, disk)
- Supports either Public Key/Private keys or passwords to create highly-secure exchange between partners

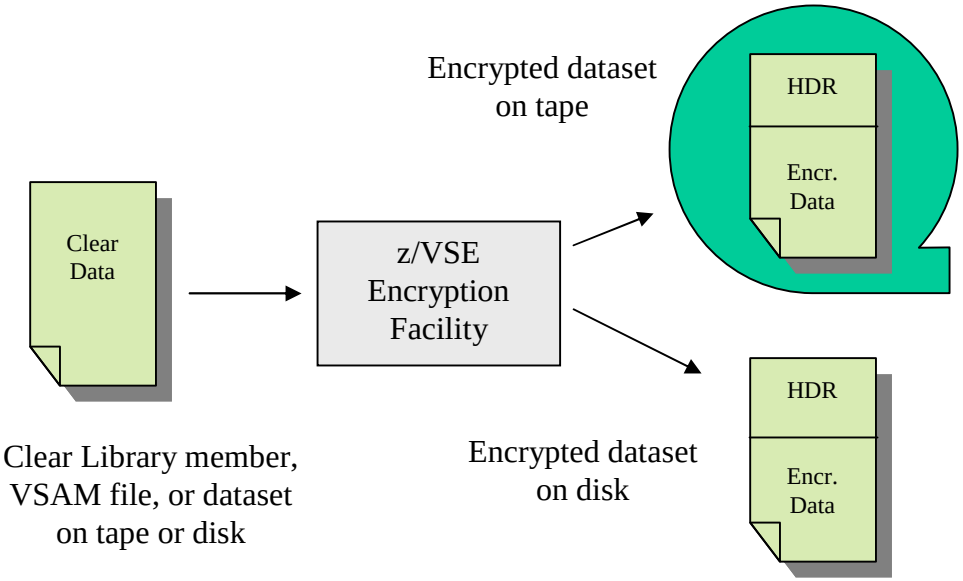
Feature:
DFSMSdss Encryption

Optional Priced Feature

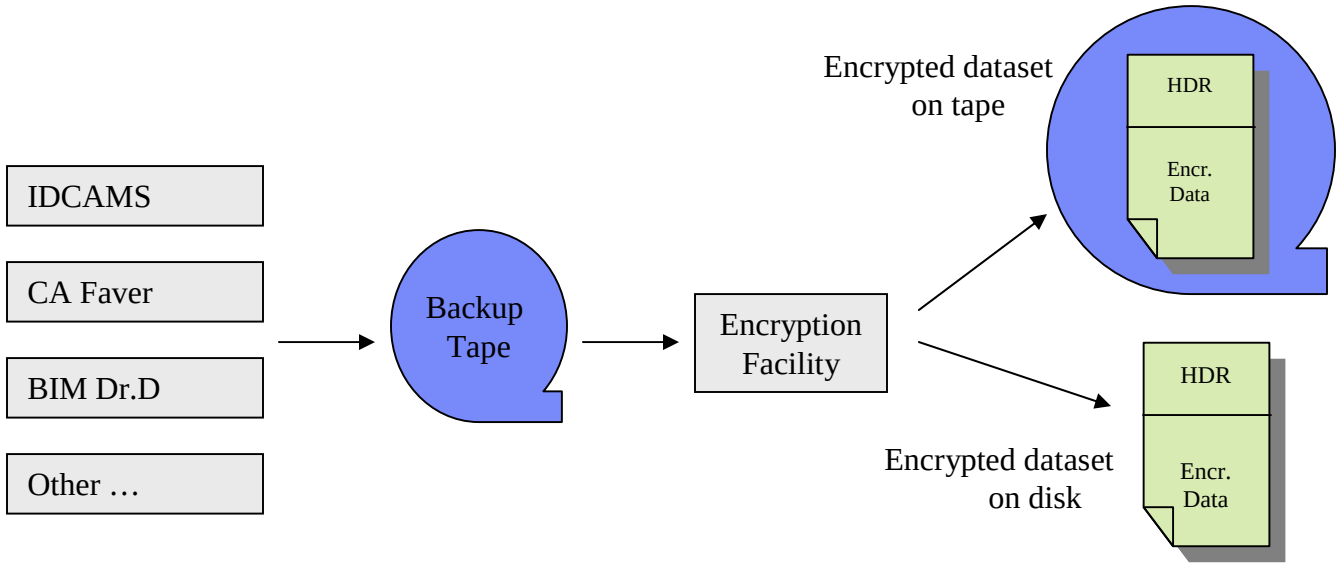
Functionality

- **Encryption/decryption of datasets**
  - A dataset can reside on disk or on tape
  - Clear dataset: LIBR member, VSAM cluster (ESDS, RRDS, or KSDS), SAM dataset on tape or disk
  - Encrypted dataset: LIBR member, a VSAM ESDS cluster or a SAM dataset on tape or disk.
  - Option to compress data prior to encryption
- **Algorithms: TDES and AES-128**
  - AES-128 requires a z9 BC or EC
  - with password-based encryption
  - with public-key encryption
- **Also available: Encryption Facility for z/OS Java Client**
  - Freely downloadable Java-tool
  - Can encrypt/decrypt datasets on any Java-capable platform, including Windows, Linux, AIX, and even z/OS
  - Source code available for customers for reference and customization
  - Can be also used by VSE customers

Encryption of a single file



Encryption of a complete backup



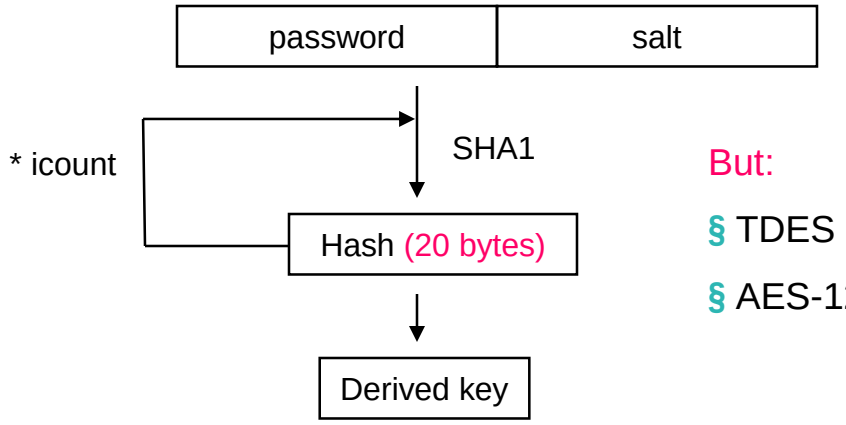
- Any proprietary backup tape can be encrypted and written to a second tape or to disk.
- Note that the complete input tape results in just one encrypted dataset, which resides on tape or disk.

Password-based encryption (PBE)

- **Encryption key (data key) is generated from**
  - the given secret password (8 … 32 characters)
  - iteration count, and
  - a 8-byte random number (the “salt”), which is different for each encryption process.
- **The iteration count and salt value are stored in the encrypted dataset header.**
  - icount and salt are not secret
  - When encrypting the same data twice with the same password and iteration count, 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/

PBE: Example for generating a key

- **Example of a "Password-based key derivation function"**
- **PBKDF1(password, salt, iteration_count, dkLen)**
- **Disadvantage:**
  - Derived key length (dkLen) limited to output of underlying hash function (MD5 = 16 bytes, SHA-1 = 20 bytes)
  - Used today only for compatibility with older applications
- **Described in RFC 2898**
- **Process:**



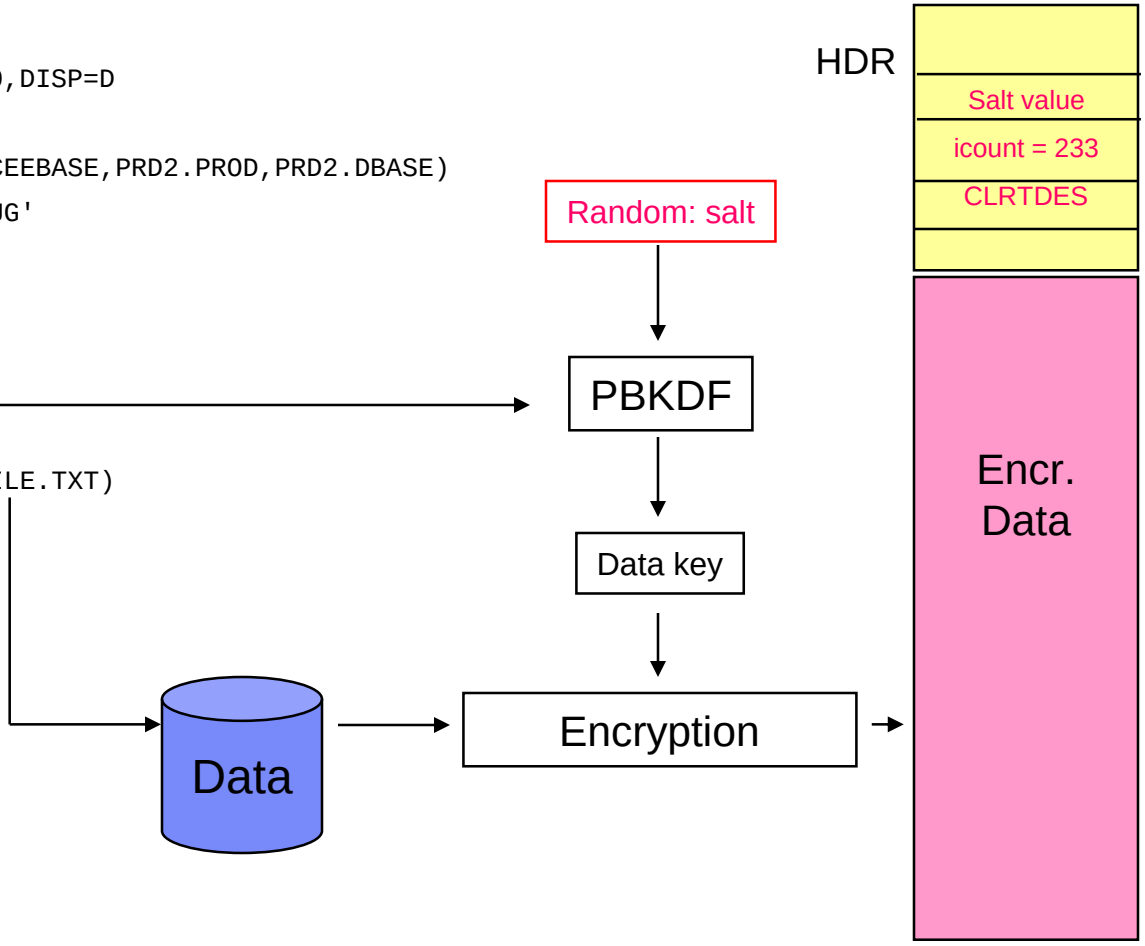
Note: this is not exactly the process used in Encryption Facility for z/VSE. It's only an example.

But:

- TDES key = 3 * 8 bytes = 24 + 8 bytes ICV = 32
- AES-128 key = 16 bytes + 16 bytes ICV = 32

PBE: Job example for encryption

```
* $$ JOB JNM=ENCMEM,CLASS=0,DISP=D
// JOB ENCMEM
// LIBDEF *,SEARCH=(PRD2.SCEEBASE,PRD2.PROD,PRD2.DBASE)
// EXEC IJBEFVSE,PARM='DEBUG'
ENCRYPT
DESC='ENCRYPTION TEST'
CLRTDES
PASSWORD=BLAHBLAH
ICOUNT=233
CLRFILE=DD:PRD2.CONFIG(MYFILE.TXT)
ENCFILE=DD:ENCDATA
/*
/&
* $$ EOJ
```

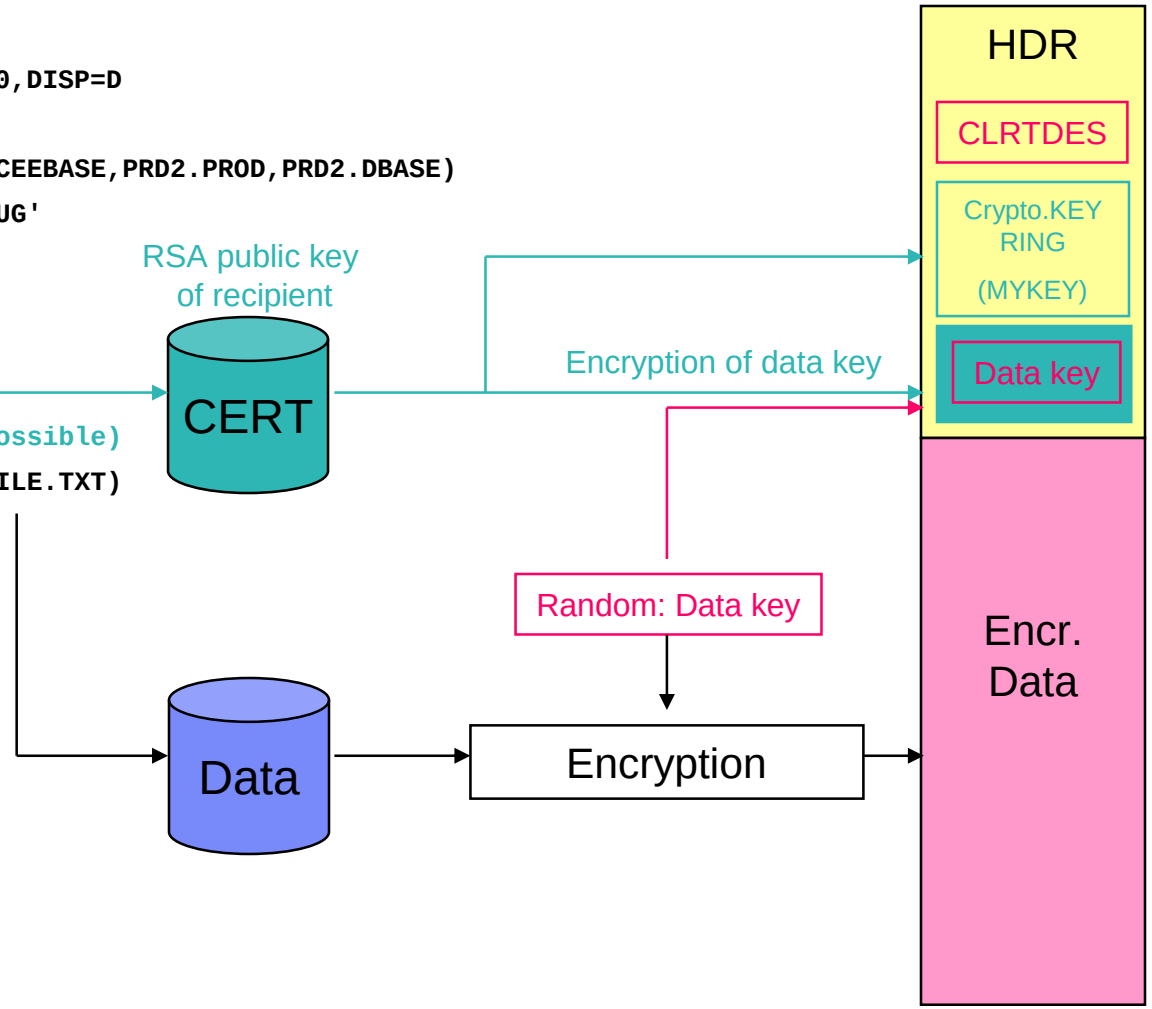


Public-key encryption (PKE)

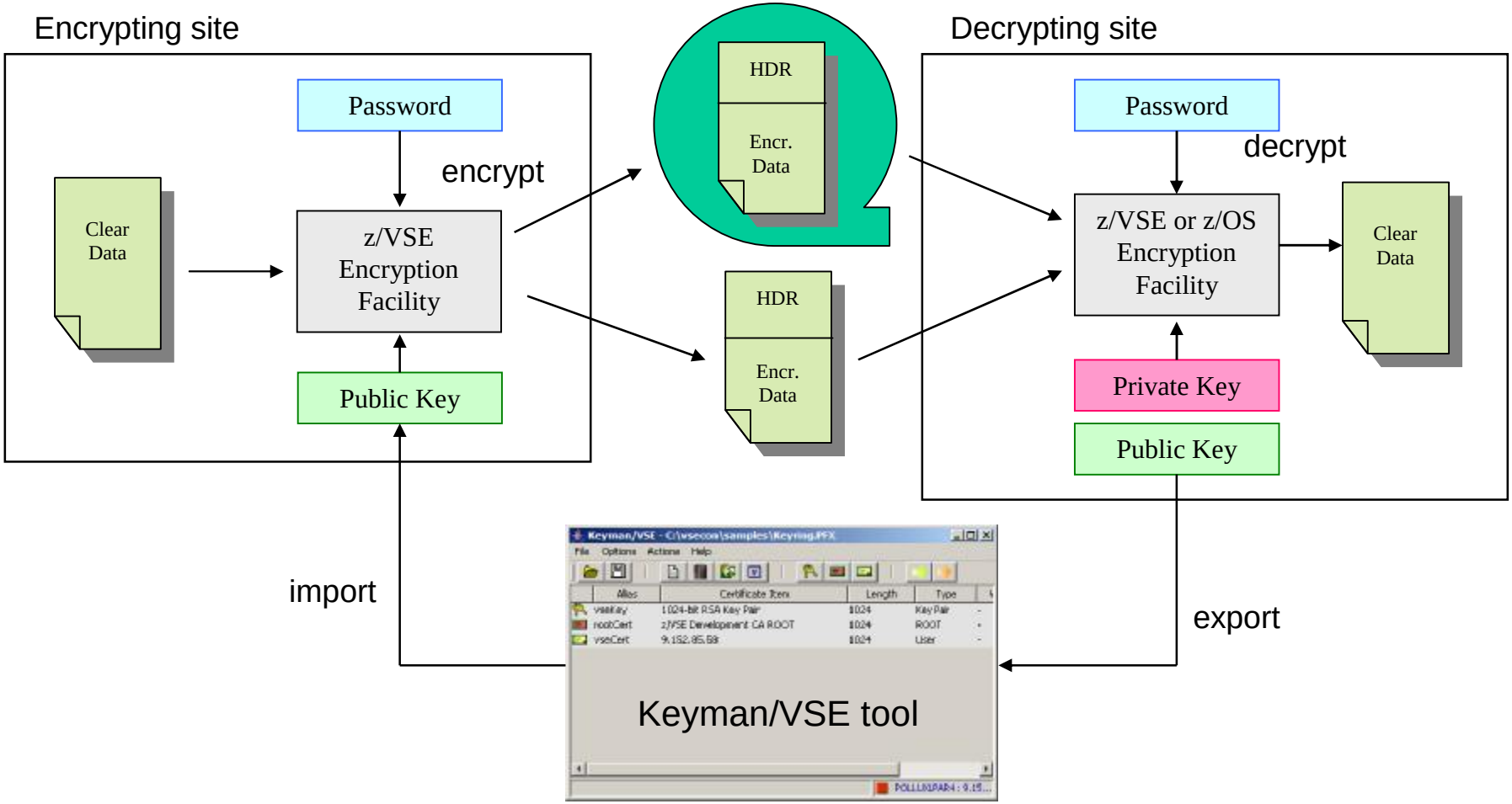
- **Encryption key (data key) is randomly generated**
- **Data key is then encrypted with the public key of the recipient of the encrypted data**
  - Needs a Crypto Express2 or PCIXCC card for 2048 bit keys
  - Crypto cards are transparently used also for 1024 bit keys when available
- **Data key is put into the encrypted dataset together with the encrypted data**
- **Only one recipient is able to decrypt the data key and thus, the encrypted data, using the corresponding private key**
- **Need to manage / exchange public RSA keys**
  - Can be done with the Keyman/VSE tool

PKE: Job example for encryption

```
* $$ JOB JNM=ENCMEM,CLASS=0,DISP=D
// JOB ENCMEM
// LIBDEF *,SEARCH=(PRD2.SCEEBASE,PRD2.PROD,PRD2.DBASE)
// EXEC IJBEFVSE,PARM='DEBUG'
ENCRYPT
DESC='ENCRYPTION TEST'
CLRTDES
RSA=CRYPTO.KEYRING(MYKEY)
(up to 16 RSA statements possible)
CLRFILE=DD:PRD2.CONFIG(MYFILE.TXT)
ENCFILE=DD:ENCDATA
/*
/&
* $$ EOJ
```



PBE and PKE scenario



Keyman/VSE

- **New Keyman/VSE version available for download:**
  - http://www.ibm.com/servers/eserver/zseries/zvse/downloads/#vkeyman
- **New version provides some additional functions for Encryption Facility, including:**
  - Support for Java keystores (JKS): allows to import certificates directly from a z/OS JKS
  - Upload self-signed certificates as CERT member on VSE

Prerequisites

- **z890/z990**
  - "CPU Assist for cryptographic function" CPACF (*) for TDES
  - TCP/IP for VSE/ESA 1.5E with ZP15E214 for public key encryption
  - CryptoExpress2 or PCIXCC for 2048-bit public key
- **z9 EC/z9 BC**
  - CPACF for TDES and AES-128
  - TCP/IP for VSE/ESA 1.5E with ZP15E214 for public key encryption
  - CryptoExpress2 or PCIXCC for 2048-bit public key

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

Availability

- **Nov 30, 2007**
- **Requires APAR DY46717 (PTF UD53196)**
- **Optional priced feature**
- **Program number: 5686-CF8-40**
- **Documentation in z/VSE 4.1.1 Administration book, Chapter 43**
  - Available on CD-ROM, or
  - Download as PDF from:

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

Customer value

- No special tape hardware requirements (e.g. TS1120)
  - 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
- Encrypted datasets and tapes can easily be exchanged between business partners even on non z platforms
  - Password-based
  - Public-key based

Positioning to TS1120

	TS1120	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 TS1120	**x**	**-**
Use existing TS1120 environment with EKM	**x**	**-**
Data exchange with Encryption Facility for z/OS V1.1	**-**	**x**
Data exchange with non z platforms (EF Java client)	**-**	**x**
Password-based encryption	**-**	**x**
Public key based encryption	**x**	**x**
Offload CPU cycles	**x**	**-**

More information

- **VSE Homepage**
  http://www.ibm.com/servers/eserver/zseries/zvse/
- **Keyman/VSE tool and VSE Connector Client**
  http://www.ibm.com/servers/eserver/zseries/zvse/downloads/
- **Encryption Facility for z/OS**
  http://www.ibm.com/servers/eserver/zseries/zos/encryption_facility/
- **IBM Encryption Facility for z/OS Java Client**
  http://www.ibm.com/servers/eserver/zseries/zos/downloads/#efclient
- **IBM PCI Cryptographic Accelerator (PCICA)**
  http://www.ibm.com/security/cryptocards/pcica.shtml
- **IBM Crypto Express2 (CEX2)**
  http://www.ibm.com/systems/z/security/cryptography.html
- **CP Assist for Cryptographic Function (CPACF)**
  http://www.ibm.com/systems/z/security/cryptography.html
- **IBM Security Products – Overview**
  http://www.ibm.com/security/products/
- **KeePass Password Safe – a free Open Source Password Manager for many operating systems**
  http://keepass.sourceforge.net/

New technical articles on VSE homepage

- http://www.ibm.com/servers/eserver/zseries/zvse/documentation/documents.html

Technical articles

How to setup Secure Telnet with VSE (PDF, 1.7MB)
Joerg Schmidbauer, IBM
How to setup Secure FTP with VSE (PDF, 1.2MB)
Joerg Schmidbauer, IBM
How to setup cryptographic hardware for VSE (PDF, 1.1MB)
Joerg Schmidbauer, IBM

Questions