



S11 – Encryption Facility for z/VSE, Verschlüsselung im und rund ums z/VSE

Jörg Schmidbauer
jschmidb@de.ibm.com



z/VSE und z/VM mit Linux on System z
GSE Frühjahrstagung
07.- 09. April 2008 in Bonn

Themen

- Thema Verschlüsselung in der Presse
- Lösungen für VSE
- Weitere Verschlüsselungstechnologien

Thema Verschlüsselung in der Presse

BBC NEWS | UK | UK Politics | Q&A: Child benefit records lost - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://news.bbc.co.uk/2/hi/uk_news/politics/7103828.stm

Google

BBC Home News Sport Radio TV Weather Languages

UK version International version | About the versions

Low graphics | Accessibility help

BBC NEWS **WATCH** One-Minute World News

News services
Your news when you want it

News Front Page

Africa
Americas
Asia-Pacific
Europe
Middle East
South Asia
UK
England
Northern Ireland
Scotland
Wales
UK Politics
Education
Magazine
Business
Health
Science/Nature
Technology

Last Updated: Thursday, 22 November 2007, 16:30 GMT

E-mail this to a friend Printable version

Q&A: Child benefit records lost

How worried should people be by the loss of discs containing child benefit recipients' personal details?

What has happened?

HM Revenue and Customs has lost computer discs containing the entire child benefit records, including the personal details of 25 million people - covering 7.25 million families overall. The two discs contain the names, addresses, dates of birth and bank account details of people who received child benefit. They also include National Insurance numbers.

How were the discs lost?

They were sent via internal mail from HMRC in Washington, in the North East of England, to the National Audit Office in London on 18 October, by a junior official, and never arrived. That broke data protection laws and is the reason Revenue and Customs chairman Paul Gray resigned.

BENEFIT RECORDS LOST

Queries answered
BBC personal finance reporter Jennifer Clarke answers your questions on the crisis

KEY STORIES

- ▶ Six more data discs 'are missing'
- ▶ Disc search moves to courier firm
- ▶ Private data 'also given to firm'
- ▶ E-mails reveal data warning
- ▶ Government challenges claims
- ▶ Cameron calls for ID cards halt
- ▶ Threat of fraud 'looms for years'
- ▶ Brown orders data spot checks
- ▶ Brown apologises for records loss
- ▶ UK's families put on fraud alert
- ▶ Government letter: full text

SKETCH

Done

BBC NEWS | UK | UK Politics | Q&A: Child benefit records lost - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://news.bbc.co.uk/2/hi/uk_news/politics/7103828.stm

Google

Technology
Entertainment
Also in the news
 Video and Audio
 Have Your Say
 In Pictures
 Country Profiles
 Special Reports

RELATED BBC SITES
 SPORT
 WEATHER
 ON THIS DAY
 EDITORS' BLOG

What is the government saying?

Prime Minister Gordon Brown told MPs: "I profoundly regret and apologise for the inconvenience and worries that have been caused to millions of families who receive child benefits. When mistakes happen in enforcing procedures, we have a duty to do everything we can to protect the public." He denied the data was lost because of "systemic" failures at the HMRC saying it had been due to procedures not being followed. He ordered security checks on all government departments to ensure data is properly protected.

What is being done to find the discs?

The Metropolitan Police, National Audit Office, Revenue and Customs staff and courier firm TNT have all been searching for the discs.

How worried should people be?

The details on the lost discs would be sought after by fraudsters. Mr Darling says the information was password protected, but that was not good enough. He said there was no suggestion that anything untoward had happened as a result of the discs' loss to date. Experts say such data should normally be sent in encrypted form.

▶ **Analysis: How worried should we be?**

SKETCH



'Profound regret'
 How Brown dealt with data crisis in weekly Commons grilling

FEATURES AND BACKGROUND

- ▶ Q&A: Child benefit records lost
- ▶ Taking cover from ID theft
- ▶ Point-by-point: Darling statement
- ▶ The dealers in data
- ▶ Life inside the beleaguered HMRC
- ▶ Timeline: Benefits records loss
- ▶ Revenue's previous data failings

HAVE YOUR SAY

- ▶ Your reaction to lost records
- ▶ 'Our data was put at risk'

WATCH/LISTEN

- ▶ **WATCH** Brown's apology
- ▶ **WATCH** Alistair Darling

RELATED INTERNET LINKS

- ▶ HMRC
- ▶ Treasury committee

The BBC is not responsible for the content of external internet sites

TOP UK POLITICS STORIES

Done

z/Journal - The Resource for Users of IBM Mainframe Systems - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.zjournal.com/index.cfm?section=issue&iid=47

Google

Z/JOURNAL

about us | editorial calendar | adve

ISSUES **ARTICLES**

z/RESOURCES

- Mainframe Buyer's Guide
- Mainframe Community
- Mainframe Jobs
- Industry News
- White Papers
- Subscribe

Search

SPONSORS

CISCO

CSI INTERNATIONAL

CDB Software, Inc.

Novell

z/JOURNAL June/July 2007 ::

OTHER ISSUES

- February/March 2008
- December/January 2008
- October/November 2007
- August/September 2007
- June/July 2007

Show All

Cover Story

Enterprise Mainframe Tape Encryption: What Are Your Options?

by Dave de la Plante , James Yu

This article examines methods to ensure that when encryption is part of a storage security solution keys can be properly managed, maintained, and recovered.

Here's a list of all the articles appearing in the current issue. As a courtesy to our subscribers, we

Done

z/Journal - The Resource for Users of IBM Mainframe Systems - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.zjournal.com/ Google

Z JOURNAL

about us | editorial calendar | adve

ISSUES **ARTICLES**

z/RESOURCES

- Mainframe Buyer's Guide
- Mainframe Community
- Mainframe Jobs
- Industry News
- White Papers
- Subscribe

Search

SPONSORS

- CISCO
- CSI INTERNATIONAL
- CDB Software, Inc.
- WILLIAM

CURRENT ISSUE

February/March 2008

Go to this issue >

FEATURED ARTICLES

Deciding What to Encrypt
 ::: by John Hill :: Stefan Kochishan
 This article highlights the importance of data encryption in a mainframe environment and offers tips you can follow to ensure your encryption is appropriate.

SOA & Response Time: A Generational Issue?
 ::: by Don Fowler
 Learn how response time affects the utility of an asset, depending on the age of the users.

z/Bottom Line: Nothing to Emulate
 ::: by Eric L. Vaughan
 It's been said that "Imitation is the sincerest form of flattery." But IBM must not be feeling the adulation.

TECH STATS

- 32% of internet users use online classifieds
- \$21.1 bln spent on Internet

INDUSTRY NEWS

Mar 05, 2008 :: OpenTech Systems Announces DR/Xpert for DB2 [FULL STORY](#)

Mar 05, 2008 :: OpenTech Systems Adds Graphical Interface to Popular DR Solution [FULL STORY](#)

Mar 05, 2008 :: Symark Selects SSH Tectia Server for its Password Management Security Appliance [FULL STORY](#)

Feb 28, 2008 ::

Done

Lösungen im VSE für die Verschlüsselung von Daten

Lösungen für VSE

▪ Sichere Übertragung von Daten

- SSL
- Secure FTP
- Secure Telnet
- Connectors mit SSL
- CICS Web Support mit SSL
- POWER PNET mit SSL

Siehe hierzu PDFs auf der
VSE Homepage:

[http://www.ibm.com/servers/eserver/
zseries/zvse/documentation/security.html](http://www.ibm.com/servers/eserver/zseries/zvse/documentation/security.html)

▪ Sicheres Speichern von Daten

- TS1120 seit z/VSE 3.1
- Neu: Encryption Facility for z/VSE V1.1 mit z/VSE 4.1.1
- Vendor Lösungen: z.B. Dr Crypto von CSI, Appliances wie z.B. mainstorconcept hier am Vendorenstand

▪ Crypto APIs

- SSL und Crypto APIs von Connectivity Systems, Inc.
- CryptLib von XPS Software GmbH mit zusätzlichen Algorithmen



Encryption Facility for z/VSE

- **Host-basiertes Batch-Tool**
- **Verschlüsselung von SAM files, VSAM files, und VSE Library members, aber auch von kompletten backups, unabhängig vom jeweiligen backup Prozess (IDCAMS, POFFLOAD, Vendor, ...)**
- **Sehr ähnlich zum “Encryption Facility for z/OS”**
 - http://www.ibm.com/servers/eserver/zseries/zos/encryption_facility/
 - Kompatibel zum Encryption Facility for z/OS V1.1 und V1.2 (“System z Datenformat”)
- **Algorithmen: TDES und AES-128 (z9 und höher)**
- **Ausnutzung der System z Crypto Hardware**
 - Crypto Karten und CPACF
- **MWLC fähig**
- **Zwei Hauptfunktionen**
 - Password-basierte Verschlüsselung
 - Public-key basierte Verschlüsselung

Beziehung zum z/OS Encryption Facility

IBM Encryption Facility for z/VSE, 1.1

Program number: 5686-CF8-40

Runs on: System z10, z9 EC, z9 BC
zSeries 890 or 990

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

Optional Priced Feature

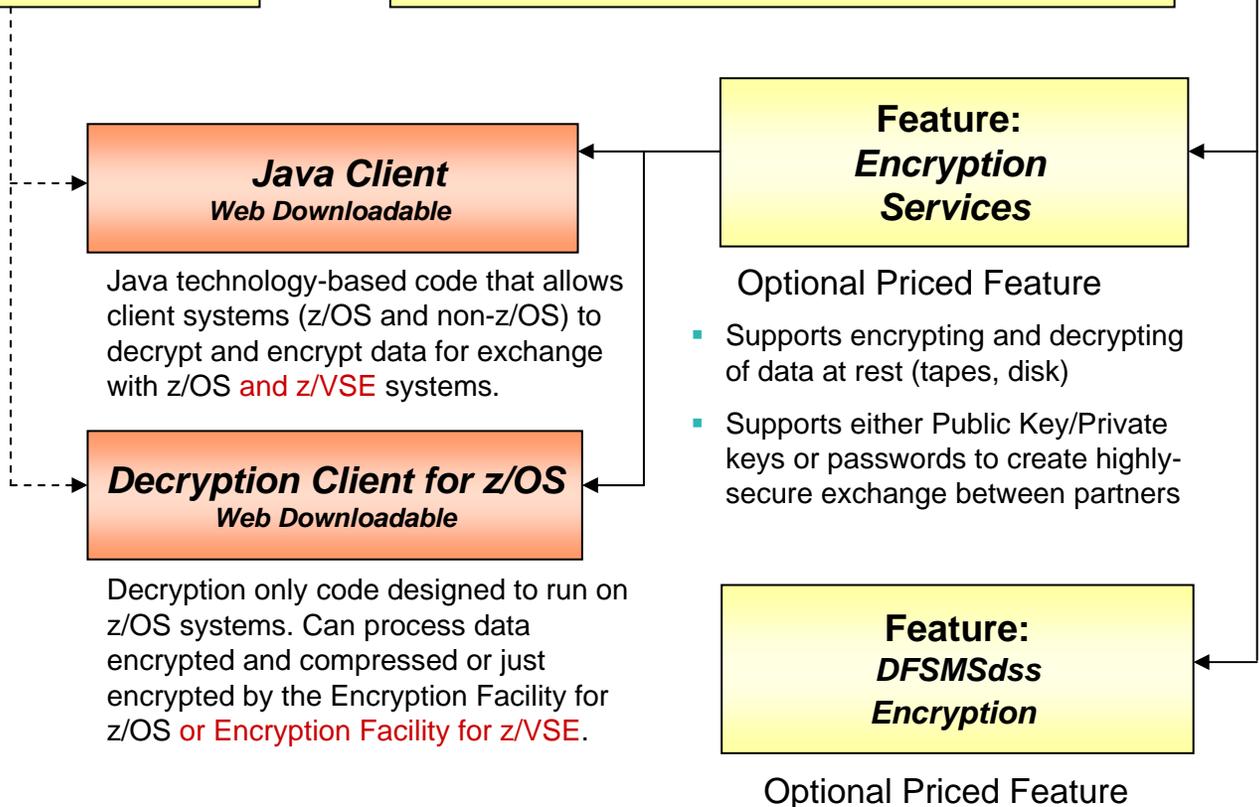
- Supports encrypting and decrypting of data at rest (tapes, disk)
- Supports either Public Key/Private keys or passwords to create highly-secure exchange between partners
- Use z/OS Java Client or Decryption Client for z/OS for data exchange with client systems or decryption on z/OS.
- Use zvse@de.ibm.com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

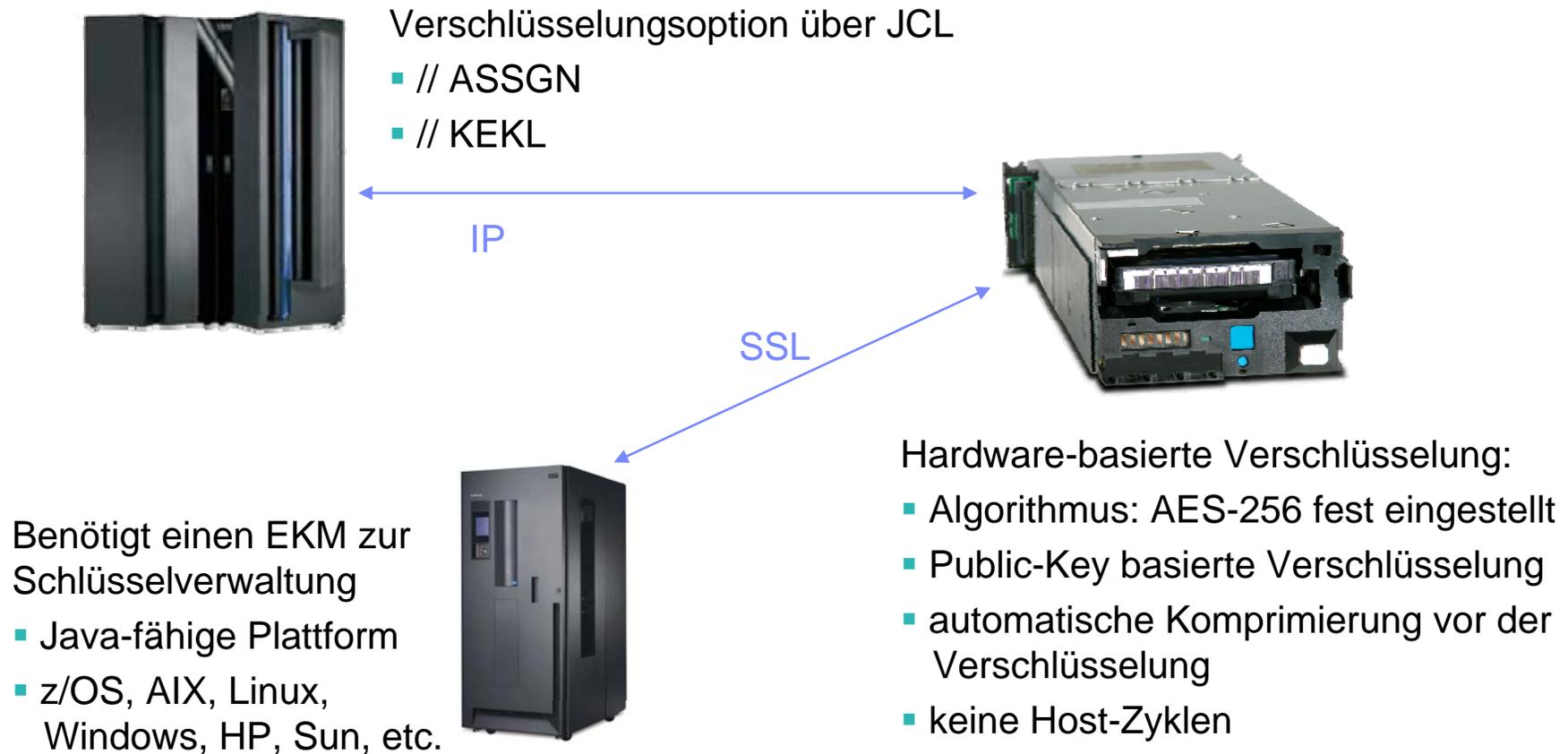
Program number: 5655-P97

Runs on: System z10, 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



TS1120 Überblick

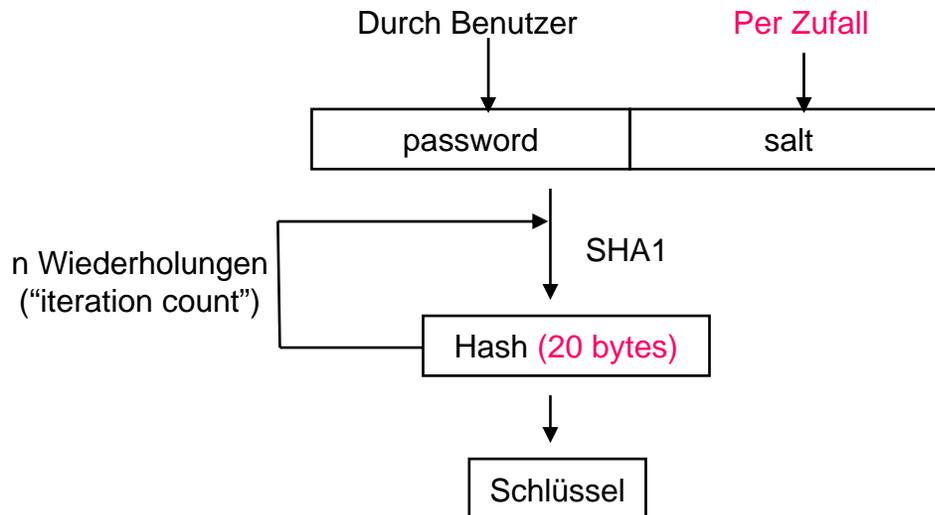


Betriebsmodi des Encryption Facility

- **Passwort-basierte Verschlüsselung**
- **Public-Key basierte Verschlüsselung**

Passwort-basierte Verschlüsselung (PBE)

- **Beispiel einer einfachen sog. “Password-based key derivation function” (PBKDF1, beschrieben in RFC2898)**
- **Nachteil dieser Funktion:**
 - Erzeugter Schlüssel kann maximal so lang sein, wie die Ausgabe der verwendeten Hash Funktion, Bsp. MD5 = 16 bytes, SHA-1 = 20 bytes
- **Prozess:**



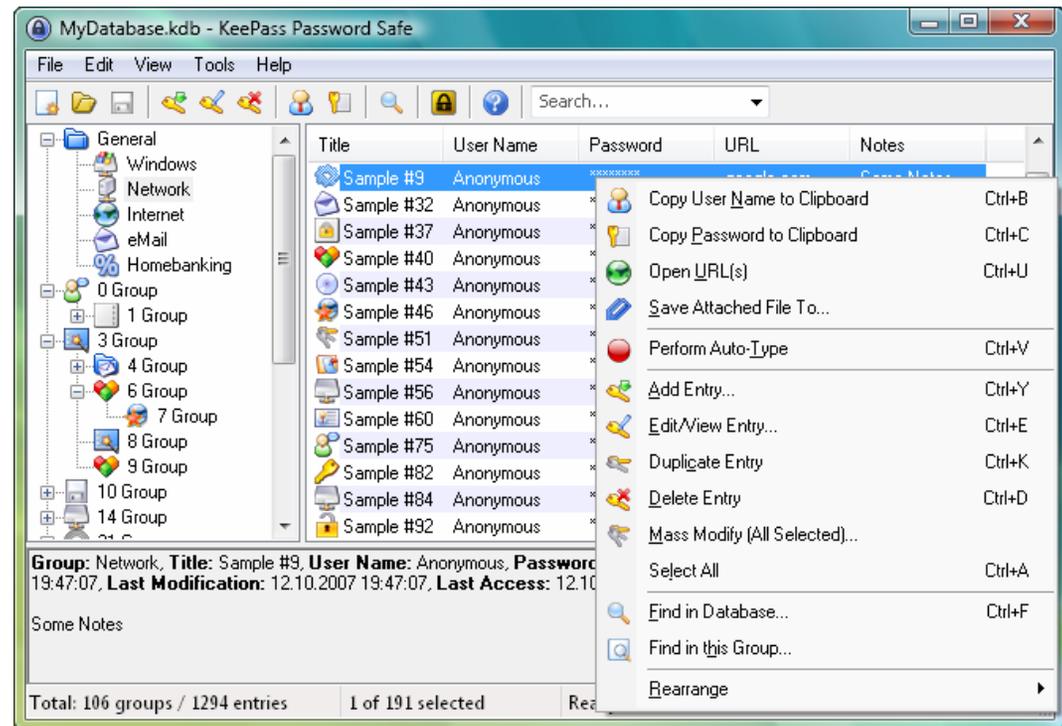
Ein damit verwandtes Verfahren, welches Schlüssel unbegrenzter Länge produzieren kann, wird im Encryption Facility verwendet.

Passwort-basierte Verschlüsselung (PBE)

- **Der encryption key (data key) wird generiert aus**
 - Dem geheimen Passwort
 - Einem “iteration count”, und
 - Einer 8-byte Zufallszahl (das sog. “salt”), welche für jeden Verschlüsselungsprozess verschieden ist.
- **Der “iteration count” und das “salt” werden im verschlüsselten Dataset abgelegt.**
 - D.h. diese zwei Werte sind nicht geheim, aber:
 - Wenn dieselben Daten ein zweites mal mit demselben Passwort und iteration count verschlüsselt werden, ergeben sich völlig unterschiedliche verschlüsselte Daten, weil das salt jedesmal anders ist.
- **Keine Notwendigkeit Schlüssel zu verwalten, aber**
- **Man muß seine Passwörter verwalten**
 - Hierzu gibt es verschiedene kommerzielle und auch freie Programme
 - Ein freies Programm: KeePass : <http://keepass.sourceforge.net/>

Keepass

- **Sicheres Aufbewahren von Passörtern**
- **Verschlüsselte Passwort-Datei**
- **Ein Master-Passwort erlaubt den Zugriff auf alle weiteren Passwörter**
- **Mögliche Verwendung mit VSE:**
 - Verwalten von Passwörtern für Encryption Facility
 - Ablegen der Keepass DB auf VSE, Doppelklick per Navigator

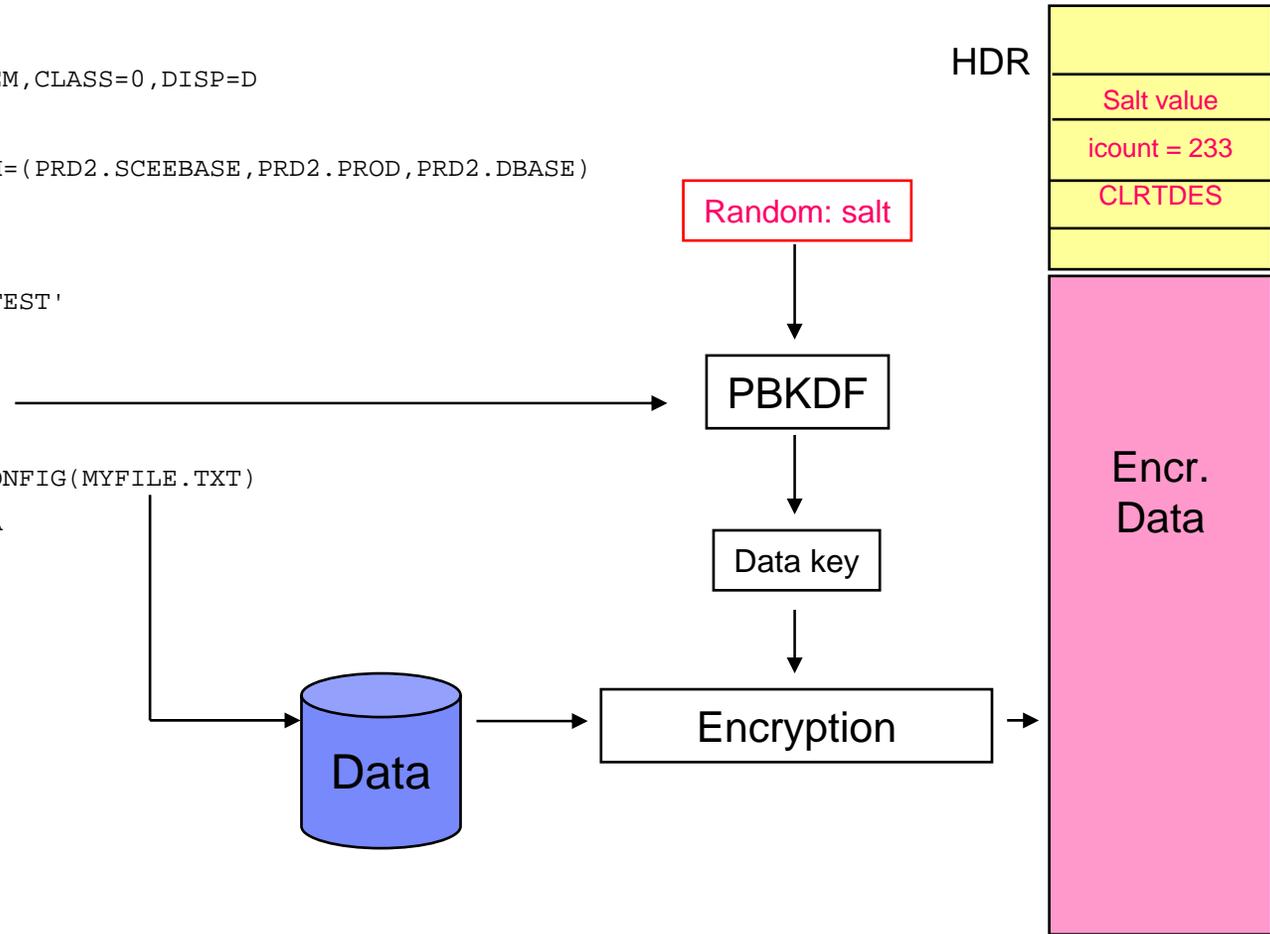


Job Beispiel für PBE Verschlüsselung

```

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

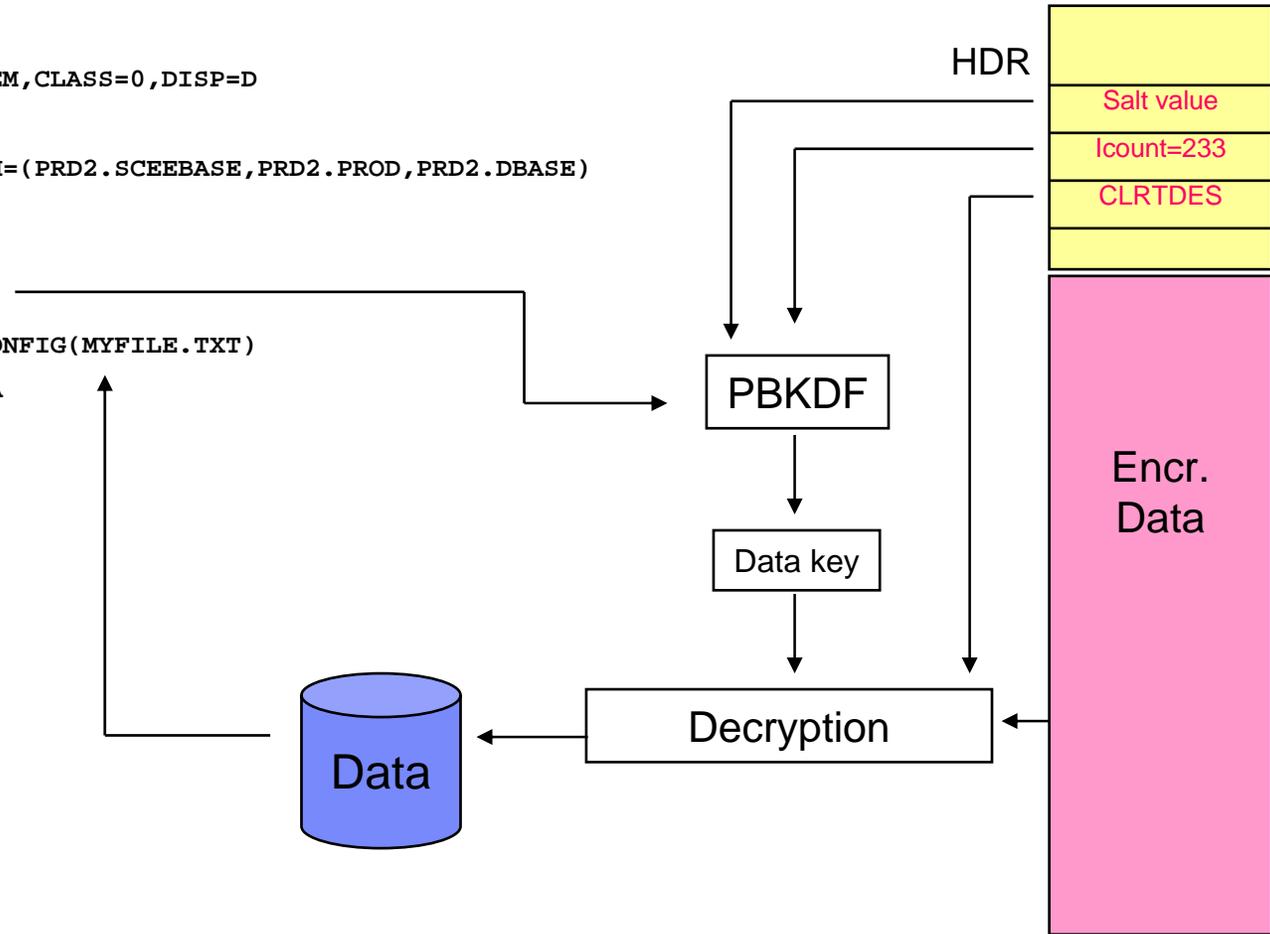
```



Job Beispiel für PBE Entschlüsselung

```

* $$ JOB JNM=DECMEM,CLASS=0,DISP=D
// JOB DECMEM
// LIBDEF *,SEARCH=(PRD2.SCEEBASE,PRD2.PROD,PRD2.DBASE)
// EXEC IJBEPVSE
DECRYPT
PASSWORD=BLAHBLAH
CLRFILE=DD:PRD2.CONFIG(MYFILE.TXT)
ENCFILE=DD:ENCDATA
/*
/&
* $$ EOJ
    
```



Public-Key basierte Verschlüsselung (PKE)

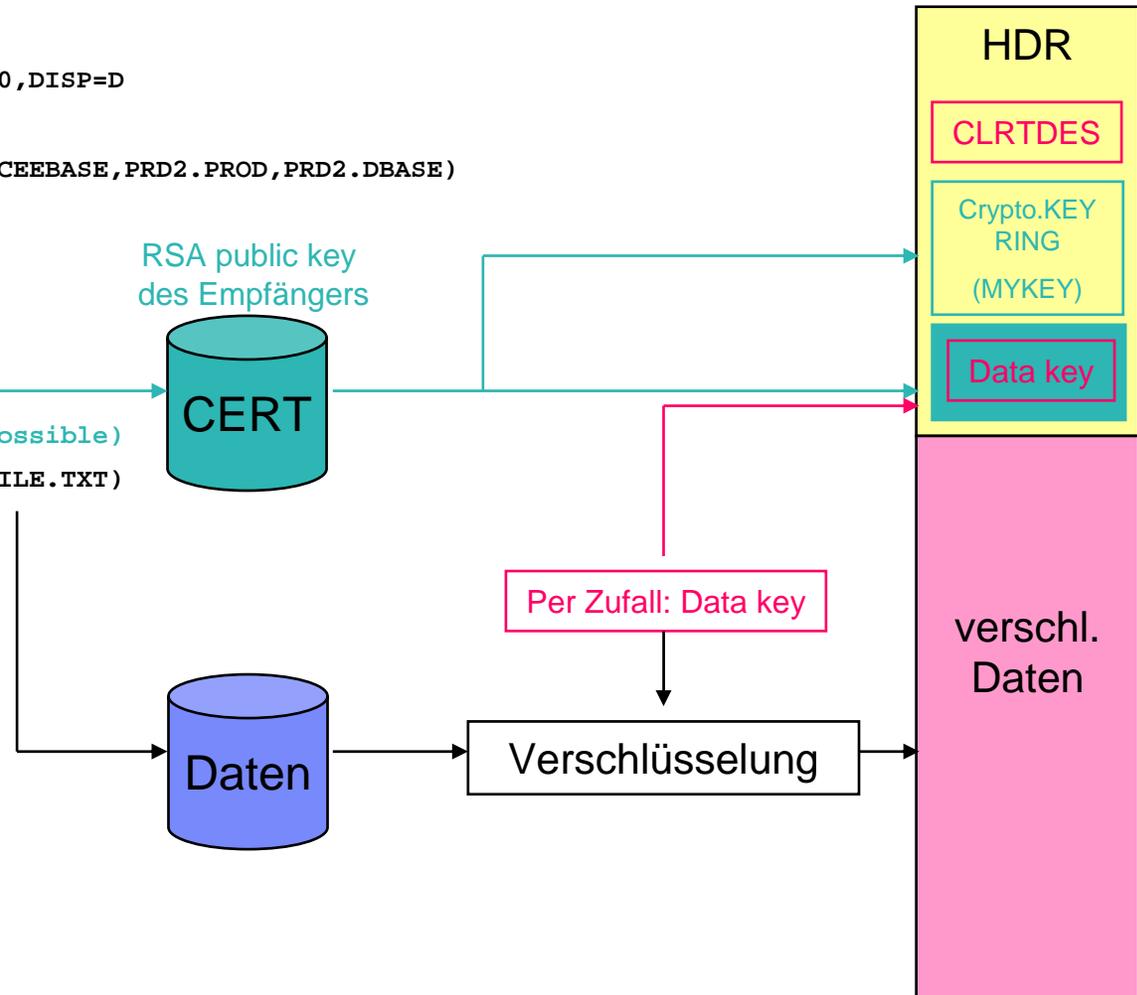
- Encryption key (data key) wird per Zufall generiert
- Data key wird dann mit dem public key des Empfängers der Daten verschlüsselt
- Data key wird zusammen mit den verschlüsselten Daten in das verschlüsselte dataset geschrieben
- Damit ist nur der Besitzer des zugehörigen privaten Schlüssels in der Lage den Data key zu entschlüsseln und damit wiederum die Daten zu entschlüsseln
- Es resultiert die Notwendigkeit, RSA Schlüsselpaare zu verwalten und auszutauschen
- Das kann z.B. mit dem Keyman/VSE Tool gemacht werden

Job Beispiel for public-key Verschlüsselung

```

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

```



Verfügbarkeit des Encryption Facility

- **Verfügbar seit 30.11.2007**
- **Voraussetzungen:**
 - CPU Assist Feature (**CPACF**), d.h. z890 / z990, z9, z10
 - **z/VSE 4.1.1** refresh (APAR DY46717, PTF UD53196)
 - TCP/IP fix **ZP15E214** für Public-key basierte Verschlüsselung
 - Crypto Express2 oder PCIXCC Karte für RSA Schlüssel der Länge **2048**
- **Ist ein „Optional priced feature“**
- **Program number: 5686-CF8-40**
- **Dokumentation im z/VSE 4.1.1 Administration Buch, Kapitel 43**
 - Buch verfügbar auf CD-ROM, oder
 - Download als PDF von der VSE Homepage:
<http://www.ibm.com/servers/eserver/zseries/zvse/documentation/#vse>

Positionierung zur TS1120

	TS1120	Encryption Facility
High volume backup/archiving	x	-
Verschlüsselung von Daten auf VSE Platten	-	x
Verschlüsselung von Daten zum anschließenden file transfer (z.B. FTP)	-	x
Lokales Archivieren von Daten	x	x
Austausch von Bändern mit Lokationen mit TS1120	x	-
Existierende Infrastruktur eines TS1120 mit EKM nutzen	x	-
Austausch von Daten mit Encryption Facility for z/OS V1.1	-	x
Austausch von Daten mit Non-Mainframe Plattformen (EF Java client)	-	x
Passwort-basierte Verschlüsselung	-	x
Public key basierte Verschlüsselung	x	x
Offload von CPU cycles	x	-

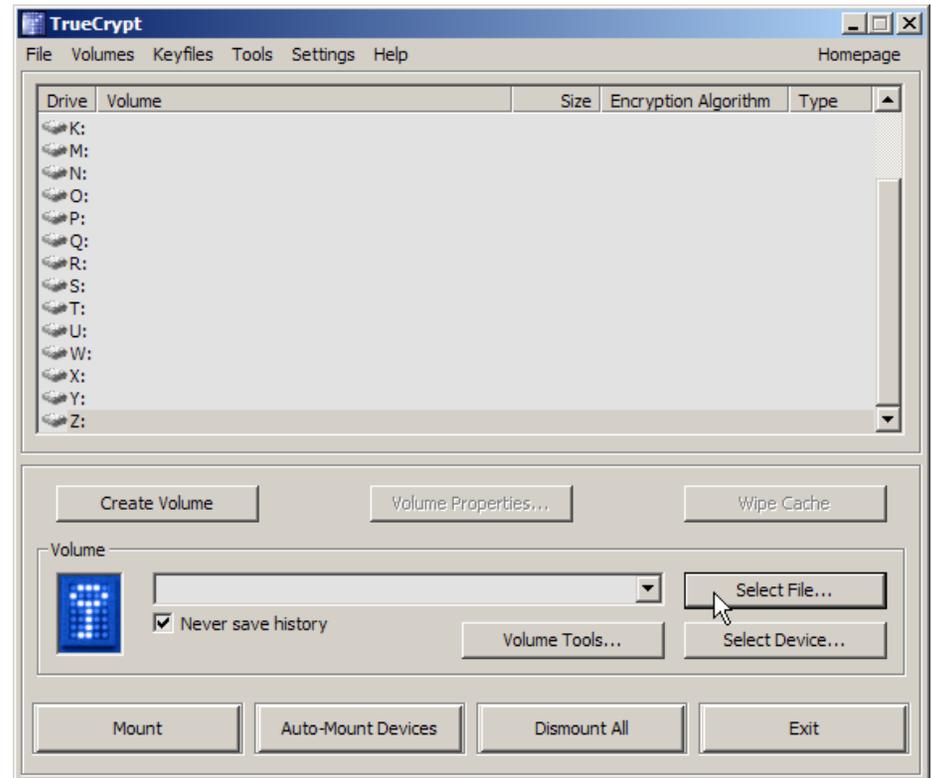
Migration von Bändern

- **Heutige Bänder haben ein Vielfaches der Kapazität von älteren Bändern.**
- **Deshalb bietet sich eine Migration von vielen kleinen Bändern auf wenige große an. Bei verschlüsselten Bändern ist zu beachten:**
- **TS1120:**
 - Die TS1120 erlaubt nur einen Schlüssel pro Band.
 - Dieser ist physikalisch auf der Bandkassette gespeichert.
 - „Umkopieren“ bedeutet damit immer auch eine Neuverschlüsselung
- **Encryption Facility**
 - Jedes Dataset ist mit eigenem Password bzw. Public-Key verschlüsselt, nicht an HW gebunden.
 - Mehrere verschlüsselte Datasets können auf ein Band kopiert werden und von dort per TLBL wieder separat gelesen und entschlüsselt werden (allerdings nicht VSAM Datasets wegen interner Tape marks)

Weitere Verschlüsselungstechnologien über das VSE hinaus

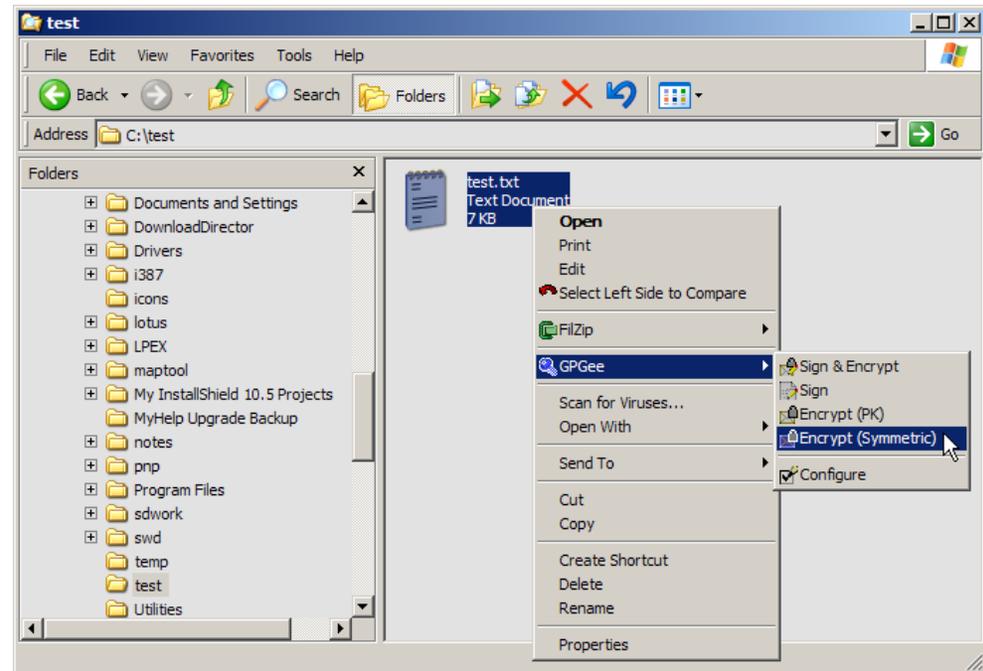
Truecrypt

- Freie Open-Source Software
- Verschlüsselte Dateien werden in der Art eines Laufwerks vorformatiert und auch als Laufwerk zugegriffen
- Mögliche Verwendung mit VSE:
 - Backups auf VTAPE und die AWSTAPE Dateien liegen in einem Truecrypt Volume in einem Windows oder Linux



Pretty-good privacy (PGP)

- Entwickelt 1991 von Phil Zimmermann
- Definiert in RFCs 2440 / 4880
- Basiert auf dem „web-of-trust“ Modell, im Gegensatz zum herkömmlichen hierarchischen Trust-Modell
- Mögliche Verwendung mit VSE:
 - Nachträgliche Verschlüsselung von aus dem VSE transferierten Daten
- Downloads:
 - <http://www.gnupg.org>
 - <http://www.gpg4win.org>



Webseiten

- **PDFs auf VSE Homepage: How to setup SecureFTP, SecureTelnet, CICS Web Support, etc.**
<http://www.ibm.com/servers/eserver/zseries/zvse/documentation/security.html>
- **Keyman/VSE tool und 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/
- **Encryption Facility for z/VSE, Dokumentation im VSE Administration Buch**
<http://www.ibm.com/servers/eserver/zseries/zvse/documentation/#vse>
- **IBM Encryption Facility for z/OS Java Client**
<http://www.ibm.com/servers/eserver/zseries/zos/downloads/#efclient>
- **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>
- **Truecrypt**
<http://www.truecrypt.org/>
- **KeePass Password Safe – a free Open Source Password Manager for many operating systems**
<http://keepass.sourceforge.net/>
- **PGP**
<http://www.gpg.org/>
<http://www.gpg4win.org>

Fragen

