IBM eServer zSeries

Sicherheit und Verschlüsselung von Daten in z/VSE 4.1 und darüberhinaus

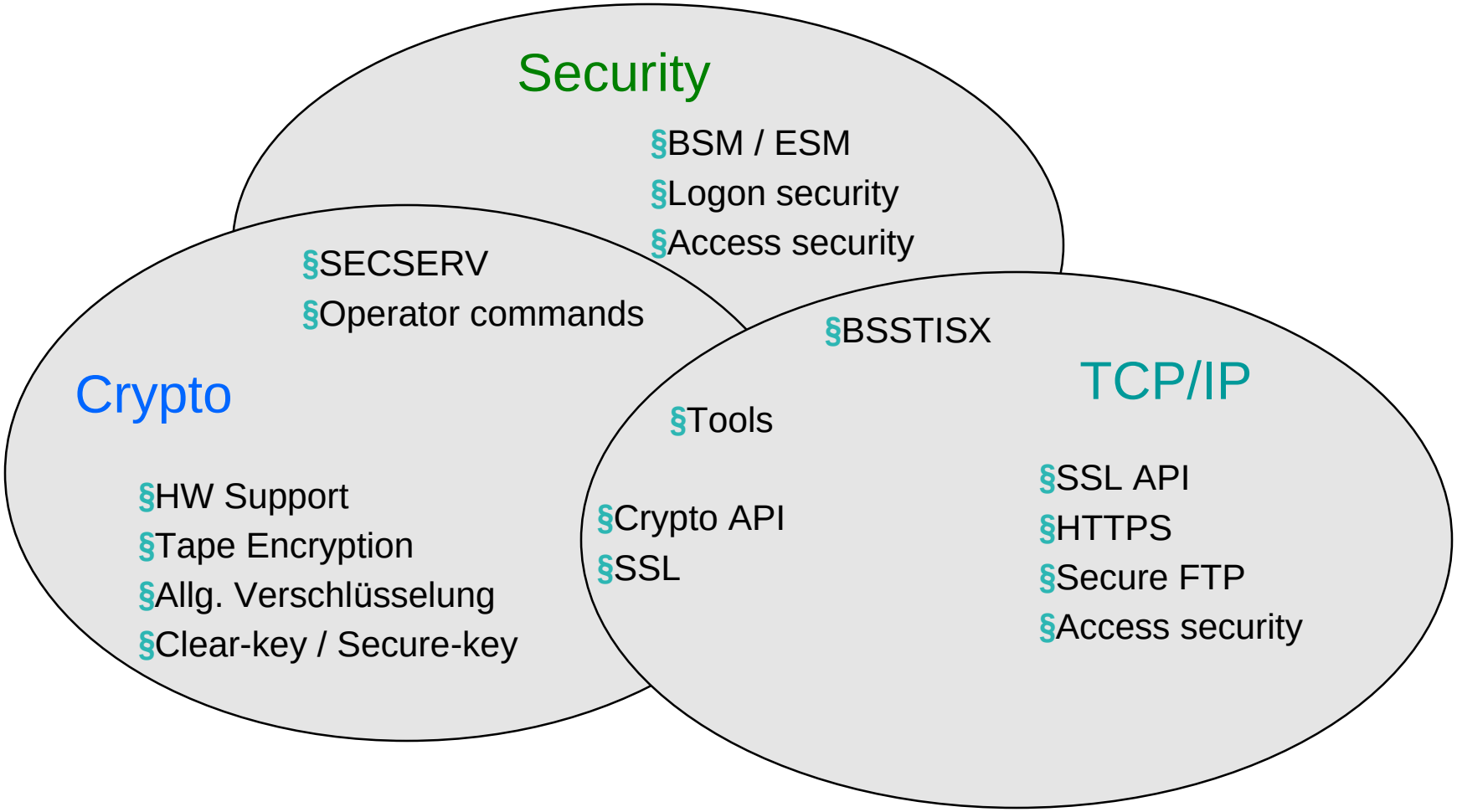
Jörg Schmidbauer
jschmidb@de.ibm.com

GSE Frühjahrstagung 2007
Berlin 26. – 28.03.2007

Agenda

- **Security**
- **TCP/IP**
- **Crypto**
  - Unterstützung von Crypto Hardware im VSE
  - Neue Funktionen zur Verschlüsselung von Backups / Archiven

Security, Crypto und TCP/IP im VSE



Security

- **BSM Erweiterungen mit z/VSE 3.1.1**
  - Benutzergruppen, Vergabe von Berechtigungen auf der Basis von Gruppenzugehörigkeit
  - Neue Admin Funktion BSTADMIN
  - Neue Resource Klassen
- **BSM Erweiterungen mit z/VSE 4.1**
  - Audit Logging und Reporting: Protokollierung von Zugriffen auf geschützte Resourcen
  - Auswertung mit Hilfe eines Report-Tools (BSTRPWTR)
  - Benutzt das CICS DMF Tool zum Sammeln der Daten in VSAM

Mehr über Security in: S11 – Neues im z/VSE V4 (Dagmar Kruse)

TCP/IP

- **Neue Security-relevante Funktionen im 1.5E**
  - Secure FTP
  - Neue Commands
    - SECURITY
    - QUERY SECURITY
  - Logging von Änderungen bzgl. Security Parameter
  - Unterstützung von Crypto Karten und CPACF
  - Unterstützung von 2048-bit RSA Schlüsseln auf der Basis von Crypto Karten

Mehr über TCP/IP in: S14 – TCP/IP V1.5 für z/VSE (John Rankin, CSI)

Crypto Unterstützung im VSE

Crypto

- **Geheimhalten vertraulicher Daten**
  - Kommunikation mit Partnern darf nicht abhörbar sein
  - Vertrauliche (interne) Daten dürfen nicht an Dritte gelangen
- **Prüfung der Identität von Benutzern**
  - Zugriff auf IT-Systeme nur durch autorisierte Personen
  - Nur ein eingeschränkter Personenkreis darf Zugriff haben auf Unternehmenskritische Daten
  - Ursprung von Informationen verifizieren (Spam, Phishing)
- **Sicherstellen der Unveränderbarkeit von Informationen**
  - Audit-sicheres Speichern oder Archivieren von Daten
  - Unveränderbarkeit der Daten sicherstellen bei elektronischer Kommunikation (z.B. e-Mail)

Crypto

- **Zwei Hauptbereiche**
  - Sicherheit von IP Verbindungen
    - SSL, HTTPS
    - SecureFTP
  - Sicherheit von abgelegten Daten
    - Verschlüsselung von Backups bzw. Archiven
    - Signieren von Daten
    - Austausch von verschlüsselten oder signierten Daten mit Kunden bzw. Geschäftspartnern

Hardware Crypto im VSE

Nach Release

	z/VSE 4.1	z/VSE 3.1	VSE/ESA 2.7	VSE/ESA 2.6
PCICA	Ja	Ja	Ja	-
CEX2C	Ja	Ja	-	-
CPACF	Ja	Ja	-	-
CEX2A	Ja	Ja	-	-
PCIXCC	Ja	-	-	-

	vor z800	z800	z900	z890	z990	z9
PCICA	-	Ja	Ja	Ja	Ja	-
PCIXCC	-	-	-	Ja	Ja	-
CEX2C	-	-	-	Ja	Ja	Ja
CPACF	-	-	-	Ja	Ja	Ja
CEX2A	-	-	-	-	-	Ja

Nach Maschine

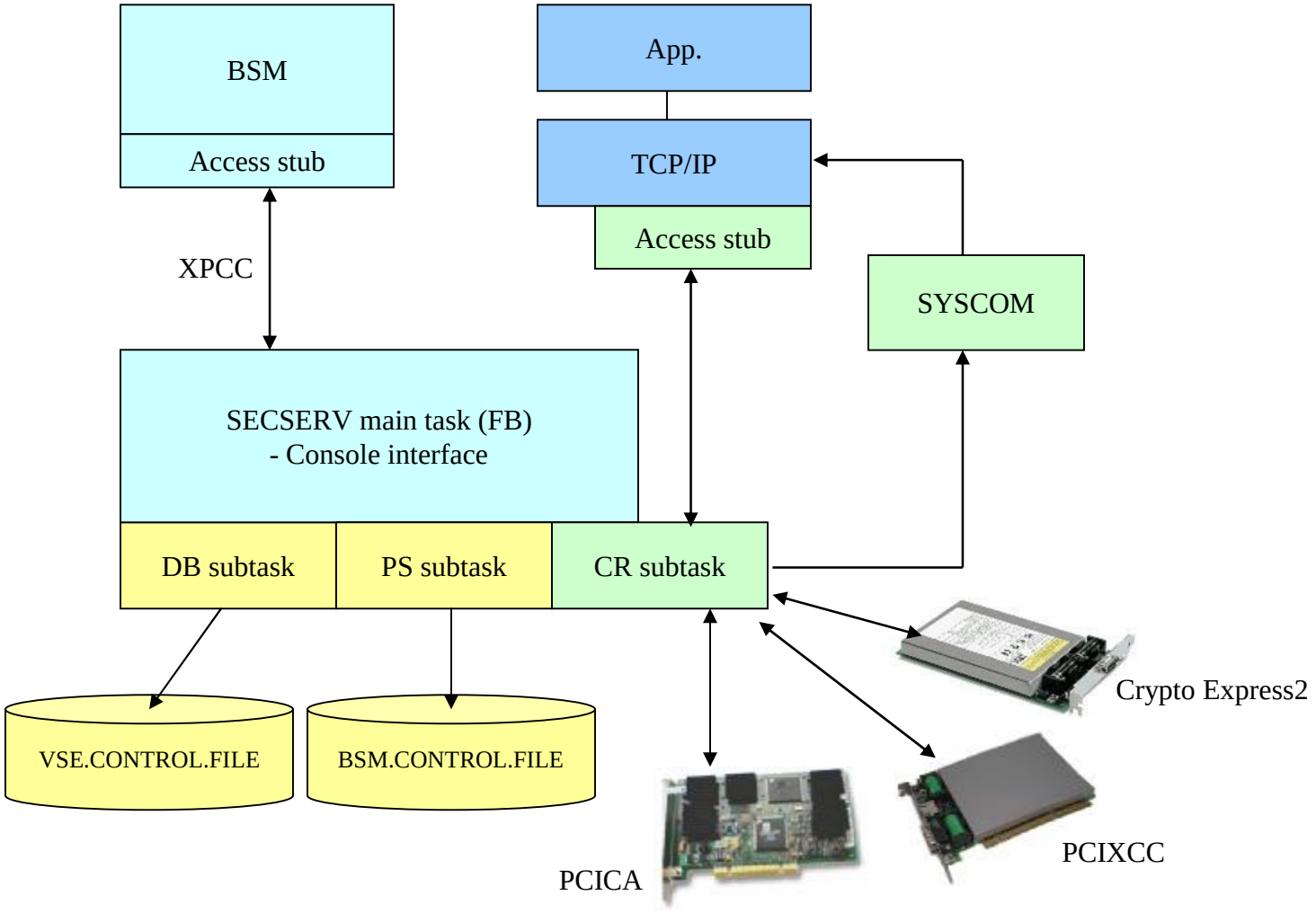
Erkennen von Crypto Devices im VSE

- **Keine spezielle Hardware Konfiguration nötig im VSE**
  - Keine IOCDS Definitionen
  - Kein spezieller Device Type
  - Kein ADD Statement in der IPL Procedure
  - Allerdings Definitionen im LPAR oder z/VM

- **Crypto Devices werden beim IPL automatisch erkannt**
  - HW Crypto wird automatisch verwendet wenn vorhanden
    - z.B. SSL oder CryptoVSE API
  - Keine Änderungen in Crypto-Anwendungen nötig

```
FB 0095 1J023I FOUND A CRYPTO EXPRESS2 CARD AT DEVICE INDEX 0
FB 0095 1J023I FOUND A CRYPTO EXPRESS2 CARD AT DEVICE INDEX 1
FB 0095 1J014I FOUND A PCICA CARD AT DEVICE INDEX 6
FB 0095 1J014I FOUND A PCICA CARD AT DEVICE INDEX 7
FB 0095 1J005I HARDWARE CRYPTO ENVIRONMENT INITIALIZED SUCCESSFULLY.
FB 0095 1J006I USING CRYPTO DOMAIN 0
FB 0095 1J022I CPU CRYPTOGRAPHIC ASSIST FEATURE AVAILABLE.
```

Überblick HW Crypto im z/VSE



Anzeige des Crypto Status

```
msg fb,data=status=cr
AR 0015 1I40I  READY
FB 0011 BST223I CURRENT STATUS OF THE SECURITY TRANSACTION SERVER:
FB 0011 ADJUNCT PROCESSOR CRYPTO SUBTASK STATUS:
FB 0011   AP CRYPTO SUBTASK STARTED .......... : YES
FB 0011   MAX REQUEST QUEUE SIZE ............. : 1
FB 0011   MAX PENDING QUEUE SIZE ............. : 1
FB 0011   TOTAL NO. OF AP REQUESTS ........... : 1234
FB 0011   NO. OF POSTED CALLERS .............. : 1234
FB 0011   AP CRYPTO POLLING TIME (1/300 SEC).. : 1
FB 0011   AP CRYPTO TRACE LEVEL .............. : 3
FB 0011   ASSIGNED APS : PCICC / PCICA ....... : 0 / 0
FB 0011                 CEX2C / CEX2A ....... : 1 / 2
FB 0011                 PCIXCC .............. : 0
FB 0011     AP  0 : CEX2C   - ONLINE
FB 0011     AP  4 : CEX2A   - ONLINE
FB 0011     AP  9 : CEX2A   - ONLINE
FB 0011   ASSIGNED AP QUEUE (CRYPTO DOMAIN)... : 6
FB 0011 CPU CRYPTOGRAPHIC ASSIST FEATURE:
FB 0011   CPACF AVAILABLE .................... : YES
FB 0011   INSTALLED CPACF FUNCTIONS:
FB 0011     DES, TDES-128, TDES-192, SHA-1
FB 0011     AES-128
FB 0011     PRNG, SHA-256
FB 0011 END OF CPACF STATUS
```

Nur bei Verwendung des BSM!

ESM Kunden: siehe VSE Administration Buch

Was wird mit der Crypto HW gemacht?

- **Crypto Karten werden momentan nur zur RSA Beschleunigung verwendet**
  - RSA decrypt beim SSL Verbindungsaufbau
  - RSA encrypt beim Signieren von Zertifikaten (CIALCREQ)
- **CPACF**
  - Symmetrische Algorithmen: DES, TDES, AES-128 (nur z9), SHA-1
  - Verwendung bei
    - SSL Datenübertragung
    - CIAL Funktionen im TCP/IP
- **Benutzung absolut transparent für TCP/IP Anwendungen**
  - Wenn Crypto HW verfügbar, werden sie benutzt, wenn nicht, werden die SW Implementierungen vom TCP/IP benutzt
  - Möglichkeit des Forcierens, aber auch explizites Ausschalten der Benutzung von Crypto HW über eine $SOCKOPT Phase

Welche Funktionen werden momentan nicht ausgenutzt?

- **Spezielle Funktionen des Coprocessor-Modus**
  - **RSA Key-Generation**
    - Hätte den Vorteil, daß RSA Schlüssel auf VSE selber generiert werden könnten
  - **Secure Key Funktionen**
    - PIN Funktionen
    - Symmetric Key Import / Export (Key Transport)
  - **Spezielle Funktionen für Banken-Software**
    - ANSI X9.17 Standard: Key generate, export, import

Secure Key vs. Clear Key

- **Unterschiedliche Arten der Verwaltung bzw. Benutzung von Schlüsseln**
  - Keys liegen unverschlüsselt im File System (“Clear Key”)
  - Keys liegen über einen festen (TDES) Key verschlüsselt im File System
    - è VSE Zustand
  - Keys liegen über einen „Secure Master Key“ verschlüsselt im File System.
    - Der Master Key ist in Hardware gespeichert
    - Sichere Key Eingabe über eine TKE oder Dialoge
    - Operationen erfolgen im Hauptspeicher, d.h. Data Keys liegen kurz unverschlüsselt im Hauptspeicher
    - Operationen erfolgen auf einer Coprocessor Karte, d.h. Data Keys tauchen nie unverschlüsselt auf.
      - è Notwendig für Banking Anwendungen, wie z.B. PIN Verifikation
      - è Unterstützt vom z/OS ICSF

Verschlüsselung von Daten

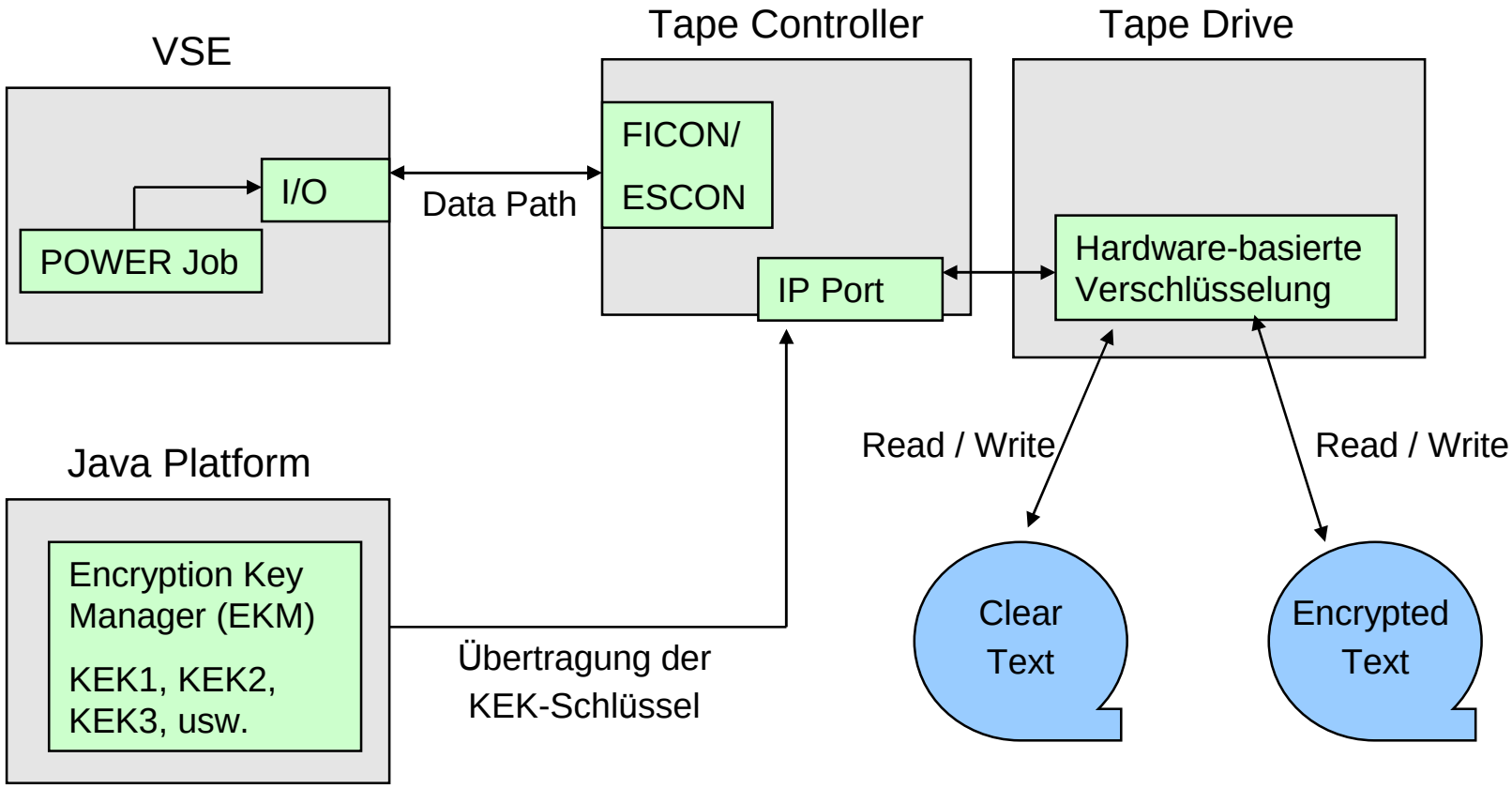
Möglichkeiten der Verschlüsselung von Daten

- **IBM System Storage TS1120 Tape Drive**
- **Mit VSE Virtual Tape (VTAPE)**
  - Backup per VTAPE auf Remote-System
  - Das Tape Image kann auf einem verschlüsselten Medium gespeichert werden
    - Verschlüsselte Datei Systeme oder Verzeichnisse (z.B. Encrypted FS unter Linux)
    - Verschlüsselungs-Tools (z.B. TrueCrypt)
    - Tivoli Storage Manager (z.B. auf Linux)
- **Verschlüsseln der Daten in den Anwendungen**
  - CryptoVSE API bietet alle benötigten Crypto-Funktionen
    - Verwendet Hardware Crypto Support wenn verfügbar
- **Lösungen von Vendoren**
  - CSI, BSI, Illustro, mainstorconcept, und andere
- **Open Source / Freeware / Shareware**
  - TrueCrypt
  - KeePass

IBM Tape Encryption – TS1120

- **Das IBM System Storage TS1120 Tape Drive unterstützt das Verschlüsseln der Daten im Tape Drive selbst**
  - Separater IBM Encryption Key Manager
    - Läuft auf einer Java Plattform (z.B. Linux, Unix, Windows)
    - Verwaltet und erstellt die Schlüssel
    - Kommuniziert mit dem Tape Drive
- **Im z/VSE 4.1 Anouncement:**
  - *“z/VSE V4.1 is designed to exploit Systems Managed Encryption with the IBMSystem Storage TS1120“*
  - *“This function will not be available at z/VSE V4.1 general availability. The function is planned to be delivered later via PTF. If you plan to use this function, check the z/VSE Web site after GA for the latest status.”*
  - Die Unterstützung wird per PTF nachgeliefert (auch für z/VSE 3.1)

TS1120 Funktionsweise



TS1120

- **Einschränkungen**
  - Ein Band kann entweder verschlüsselte oder unverschlüsselte Daten enthalten.
  - Wenn die erste Datei auf dem Band verschlüsselt wird, werden alle nachfolgenden Dateien ebenfalls mit demselben Schlüssel verschlüsselt
  - Beim Austausch von verschlüsselten Bändern ist auf jeder Seite ein TS1120 erforderlich

TS1120 Job Beispiel

```
// JOB ENCRYPT
// ASSGN SYS005,480,03
// KEKL UNIT=480,KEKL1='HUSKEKL1',KEM1=L,KEKL2='HUSKEKL2',KEM2=L
// EXEC LIBR
  BACKUP LIB=PRD2 TAPE=SYS005
/*
/&
```

Encryption Mode
(03=write)

Encoding Mechanismus
(L=Label, H=Hash)

Key Label1
(ID des 1. KEK-Schlüssels im EKM)

§ Der Data-Key kann mit zwei verschiedenen public keys (KEKs = Key Encrypting Keys) verschlüsselt werden, um das Band an zwei verschiedene Empfänger schicken zu können.

§ Mehr Info im *z/VSE 4.1 Administration* Buch (VSE Homepage!)

Vendor Lösungen

- **“Dr. Crypto” von CSI (www.e-vse.com)**
  - Unterstützt TDES, AES
  - Erfordert Dr.D 6.8 oder höher, BIM-EPIC 7.1 oder höher, SSL for VSE 1.5E
- **Firma mainstorconcept GmbH in Karlsruhe (www.mainstorconcept.de)**
  - Tape-Virtualisierung mit beliebigem Backend-Plattenspeicher
  - Verschlüsselungsmöglichkeit (AES256)
  - Vertreten hier im Vendorenforum auf der GSE!
- **“z/Encrypt” von Illustro, Inc. (www.illustro.com)**
  - Arbeitet mit existierenden Backup Lösungen
  - Basiert auf Tape Emulation
  - Verschlüsselung findet auf einem PC bzw. Workstation statt
- **“Data-Crypt” for VSE von Barnard / Thigpen (www.bsiopti.com)**
  - Leider keine detailierte Information auf BSI Webseite

Hilfreiche Open Source / Freeware-Tools

- **KeePass**
  - Gut gemachtes Tool zur Verwaltung von Passwörtern
  - Passwort Datei wird mit AES-256 verschlüsselt
- **TrueCrypt**
  - Sehr gutes Tool zum Erstellen von verschlüsselten Drive-Images
  - Erzeugt verschlüsselte Datei, welche als Laufwerk angesprochen wird
  - Schlüsselgenerierung über ein Passwort oder „Passwort-Datei“
  - Verschlüsselte Datei kann z.B. auch auf CD gebrannt oder per email verschickt werden
- **OpenPGP**
  - GnuPG Keyring Editor
  - Signieren von emails
  - Verschlüsseln von PC-Dateien
- **Aber: Vorsicht mit verschlüsselten Ordnern im Windows**
  - Ordner erkennbar an grüner Farbe
  - Verschlüsselung hängt vom Windows Passwort ab !!
  - Ordner nach Windows Passwort Änderung nicht mehr lesbar !!

Encryption Facility for z/OS

- **Host-basiertes Tool im z/OS**
  - Verschlüsselung von einzelnen Dateien
  - Verschlüsselung von ganzen Backups
  - Verwendung der System z Crypto Hardware
  - TDES und AES-128 unterstützt
  - Zwei Möglichkeiten der Schlüsselgenerierung:
    - Über ein Passwort
    - Intern per Zufallsgenerator und Schützen per Public Key
- **Java-Client zum freien Download**
  - Lesen von im z/OS verschlüsselten Daten auf Nicht-z/OS Plattformen
  - Verfügbar mit Java Quellcode als Referenz
- **Gut geeignet zum Austausch von verschlüsselten Daten / Bändern zwischen verschiedenen Systemen und Plattformen**
  - Sehr einfach, ein Passwort zu übermitteln
  - Keine speziellen Tape-Drives erforderlich

Vergleich z/VSE und z/OS

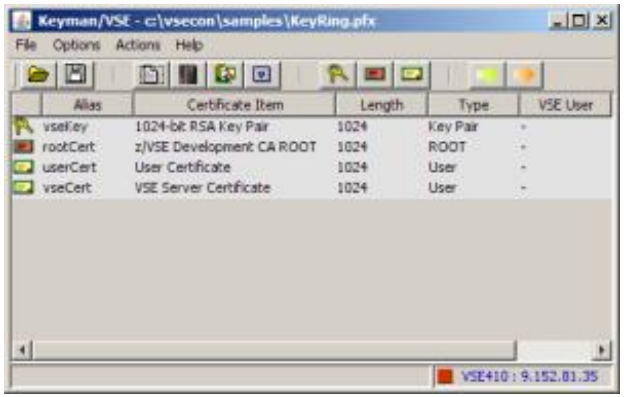
	z/VSE	z/OS
CPACF	ja	ja
Crypto Karten	ja	ja
Crypto APIs **- SSL** **- Crypto** **- CCA (**)**	 ja (*) ja (*) nein	 ja ja ja
Clear Key Crypto	ja	ja
Secure Key Crypto / TKE	nein	ja
TS1120 Tape Encryption	ja	ja
Encryption Facility	nein	ja

(*) erfordert TCP/IP for VSE/ESA
(**) Common Cryptographic Architecture

Downloads

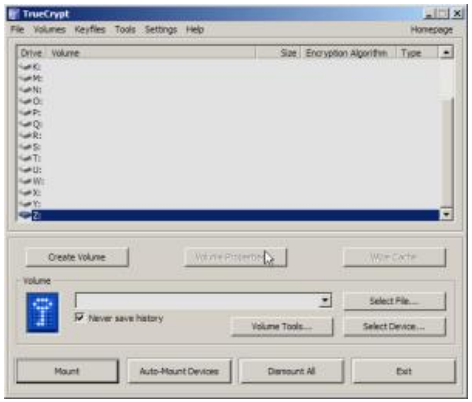
- Download Seite auf der VSE Homepage
  - http://www.ibm.com/servers/eserver/zseries/zvse/downloads/
- Encryption Key Manager (EKM)
  - http://www.ibm.com/support/us/
- Encryption Facility for z/OS
  - http://www.ibm.com/servers/eserver/zseries/zos/encryption_facility/
- KeePass Password Manager
  - http://keepass.info/
- TrueCrypt
  - http://www.truecrypt.org/

Demos am IBM-Stand



Keyman/VSE

- Aufsetzen einer SSL Verbindung



TrueCrypt

- Verschlüsseln von Dateien

KeePass

- Sicheres Aufbewahren von Passwörtern

Fragen