IBM System z Technical University

October 4–8, 2010 — Boston, MA

z/VSE Security Exploitation with Crypto Hardware

zDS02

Ingo Franzki, IBM

Authorized IBM Training

Trademarks

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.

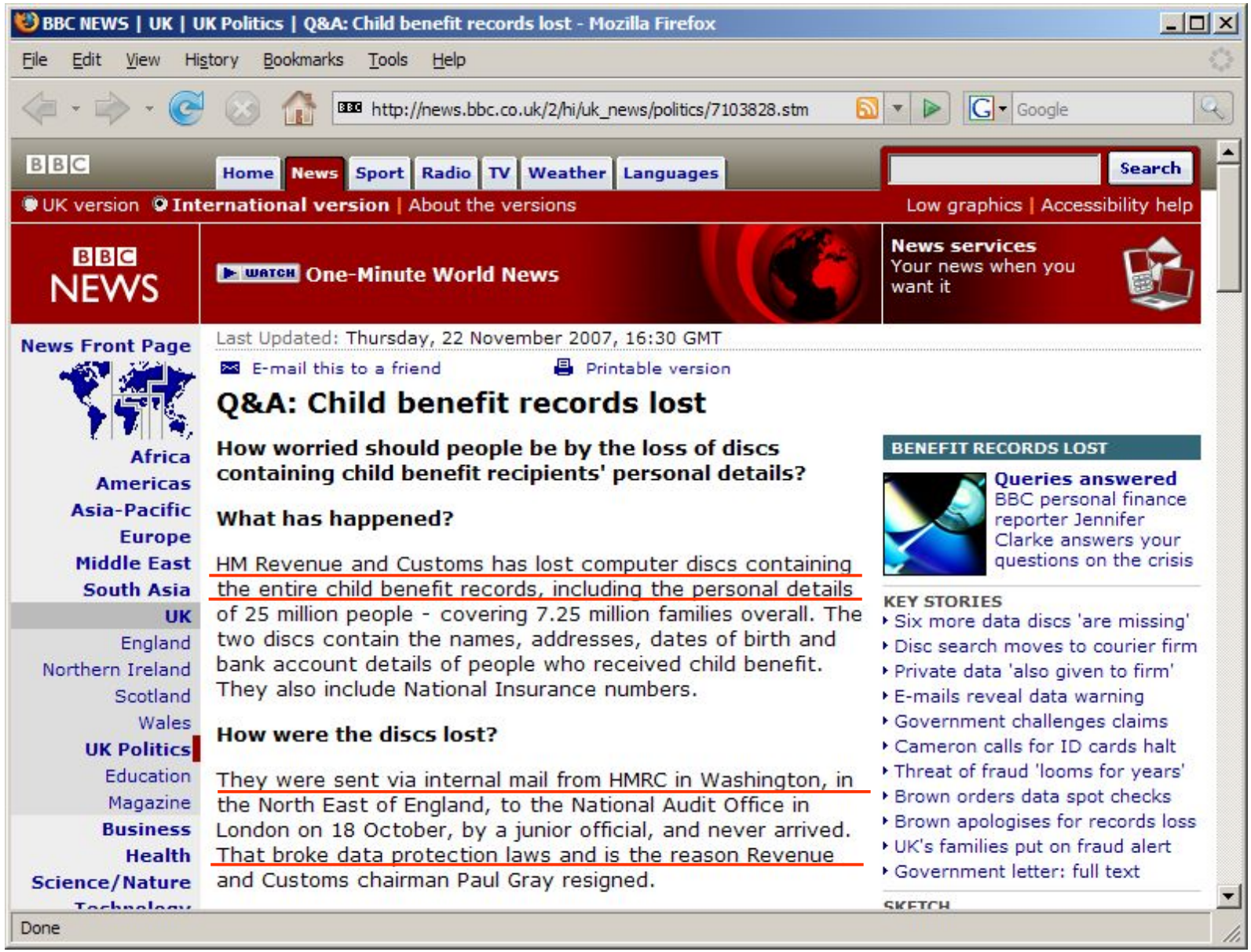
Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.
Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both 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.

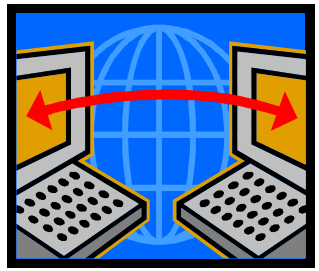
Security requirements

- **Security requirements are increasing in today's world**
  - Data security
  - Data integrity
  - Keep long-term data audit-save
- **The number of attacks increase daily**
  - Industrial spying
  - Security exploits, Denial-of-Service attacks
  - Spam, Phishing, …
- **Not paying attention to security requirements can be very expensive**
  - Your data is the heart of your company
  - Loosing your customer data is a disaster
  - You can loose customers
- **IT Security gets more and more important**
  - You need to consider the whole IT Environment not only single systems



Cryptography and data encryption

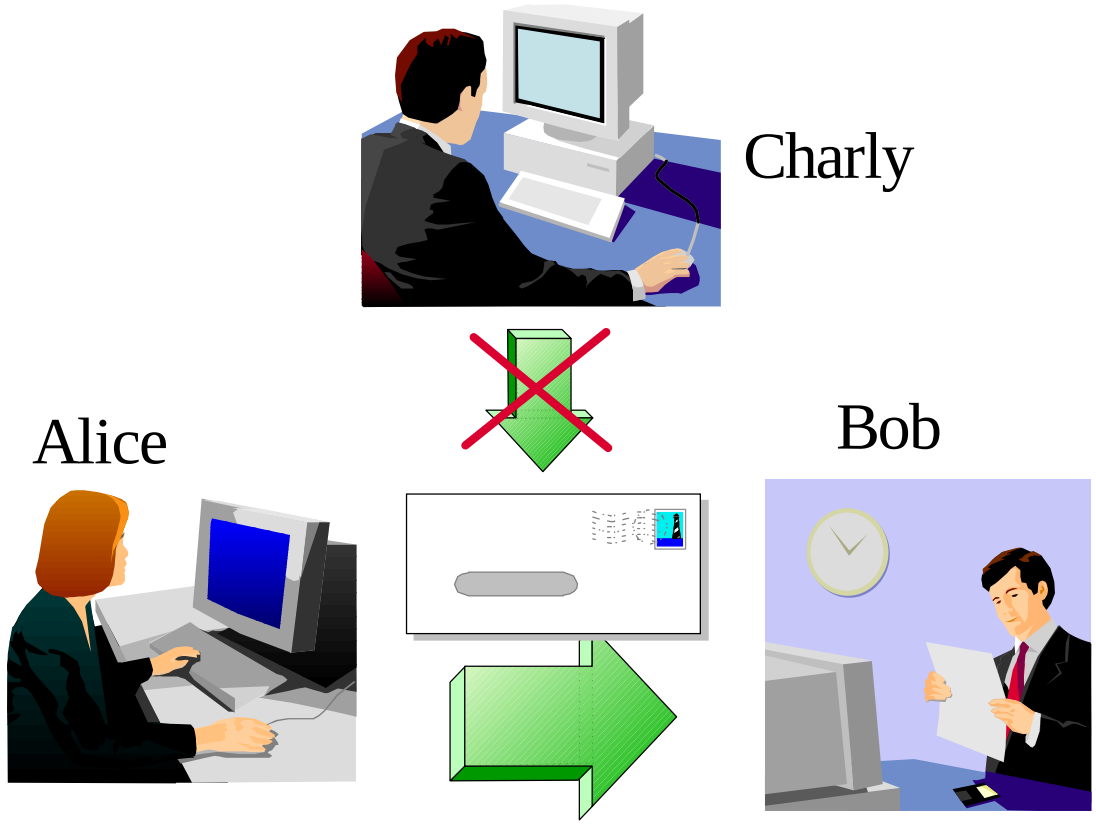
Main areas of cryptography:



- **Encryption of data transmitted over network connections**
  - SSL, HTTPS
  - SecureFTP

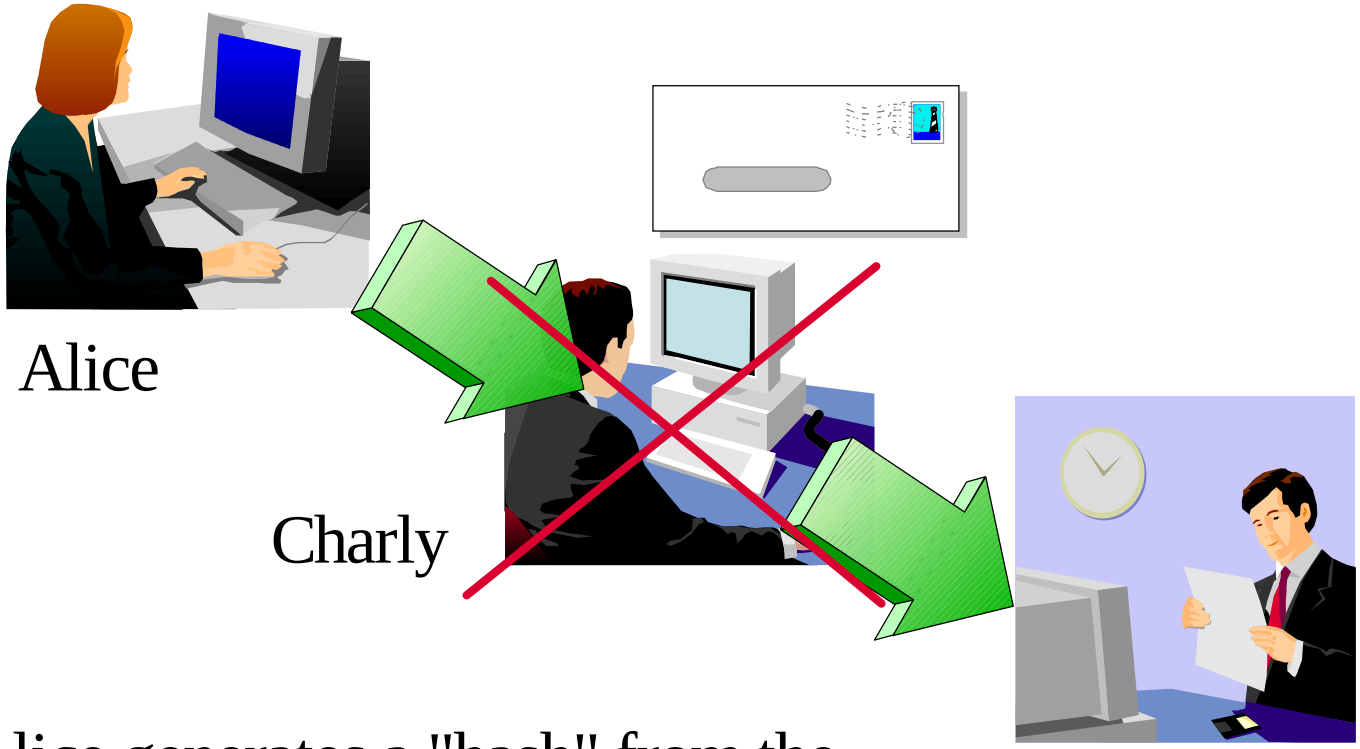
- **Encryption of data stored on disk or tape**
  - Encryption of backups or archives
  - Exchange of encrypted and/or signed data with customers or business partners
  - TS1120 Encrypting Tape Drive
  - Encryption Facility for z/VSE

Keeping Secrets



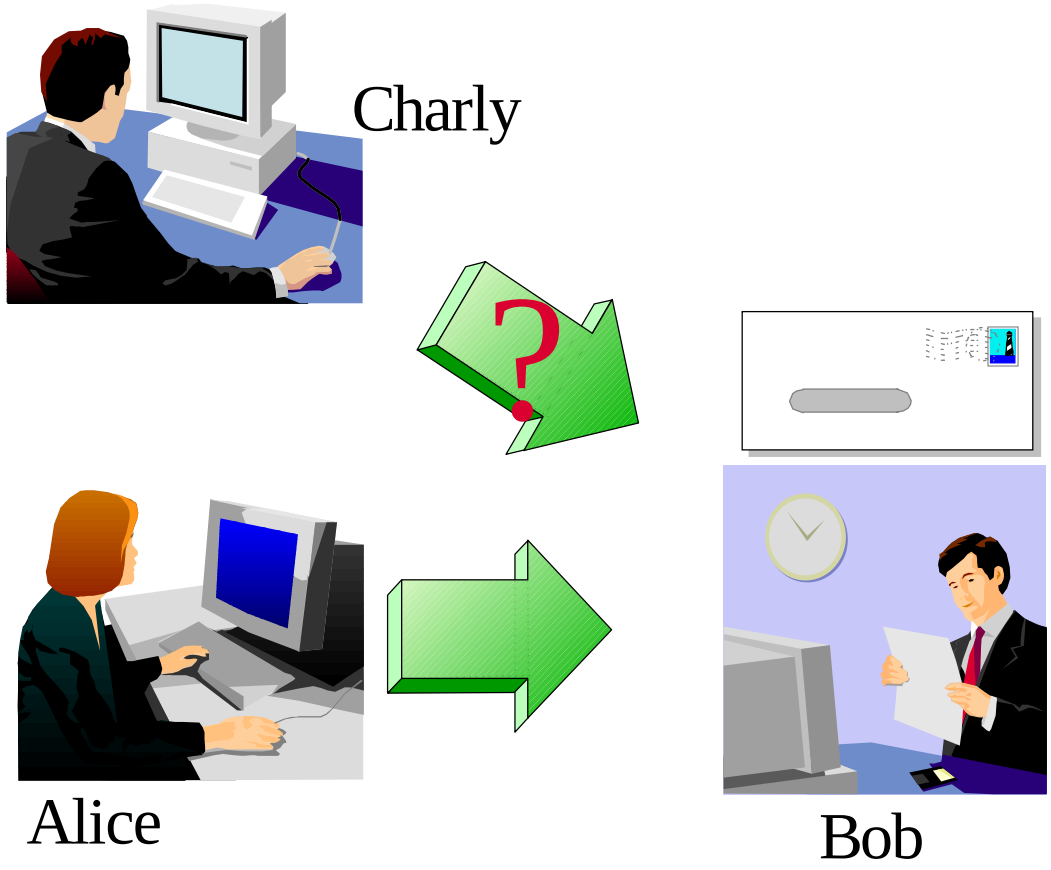
Alice encrypts the message with a secret code that only she and Bob knows

Verifying Information



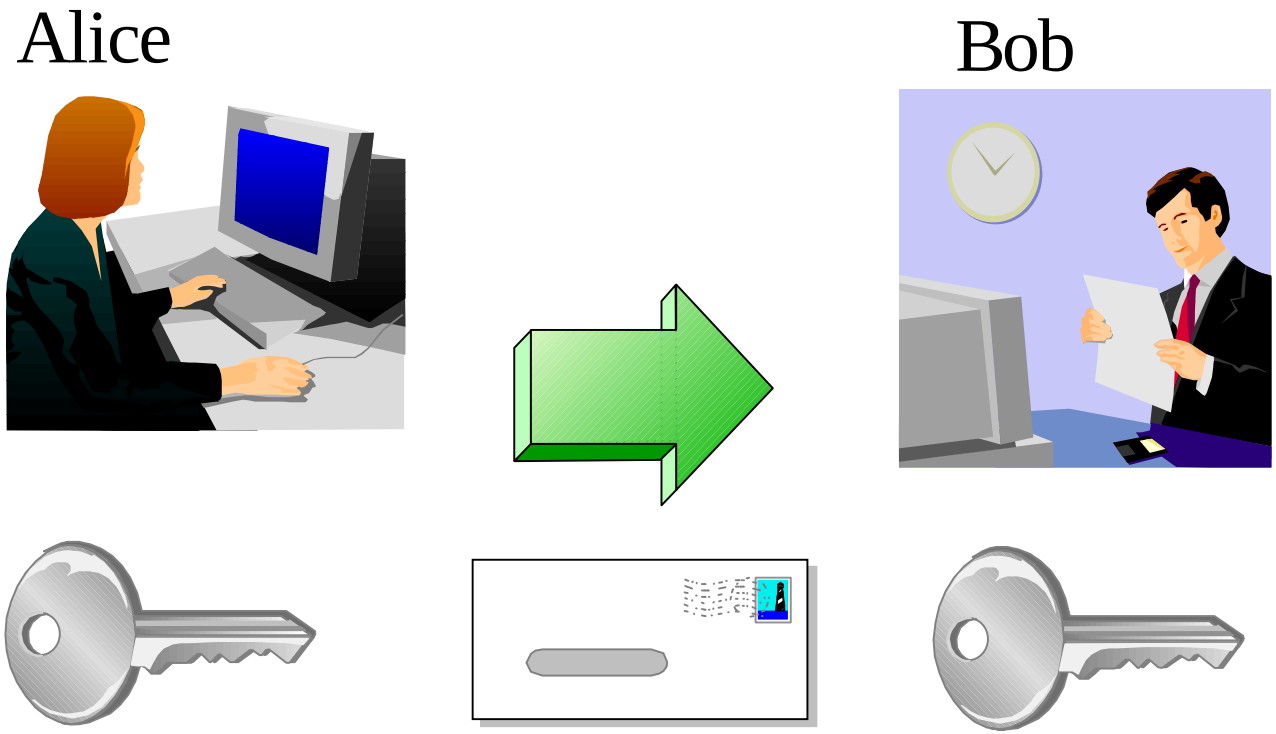
Alice generates a "hash" from the message using a secret code and attaches it to the message. Bob also generates the hash from the received message and compares it.

Proving Identity



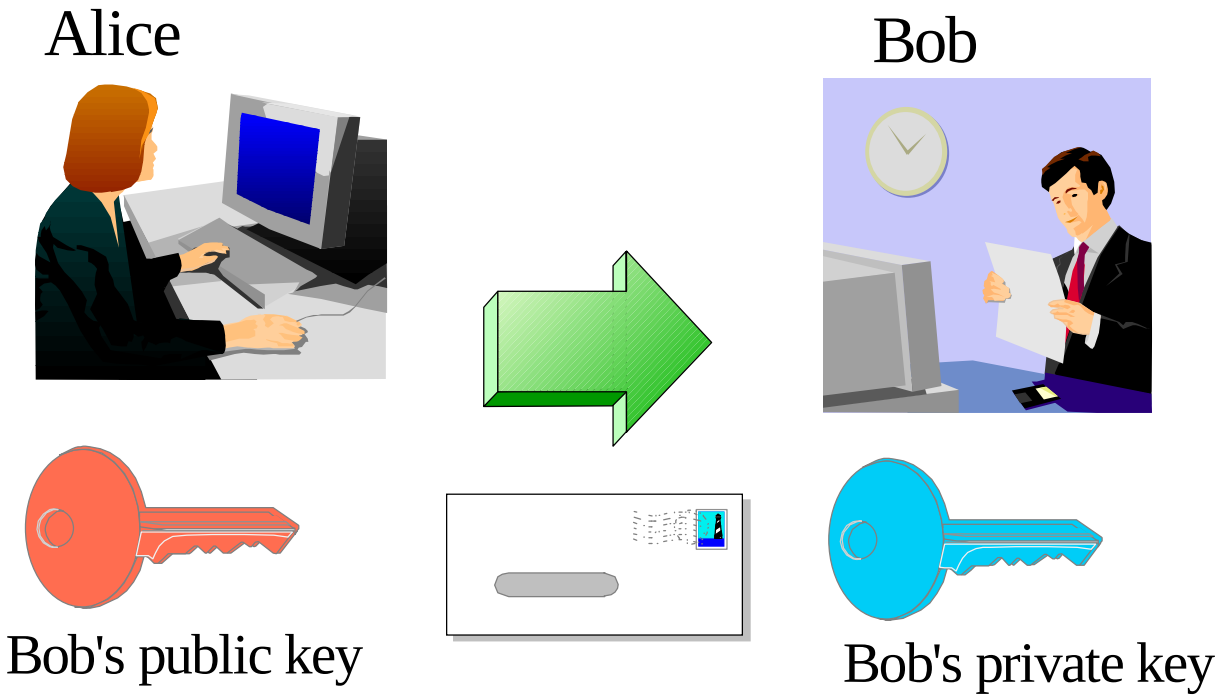
Alice "signs" the message by attaching a secret phrase that only she and Bob knows

Secret Key Cryptography - continued



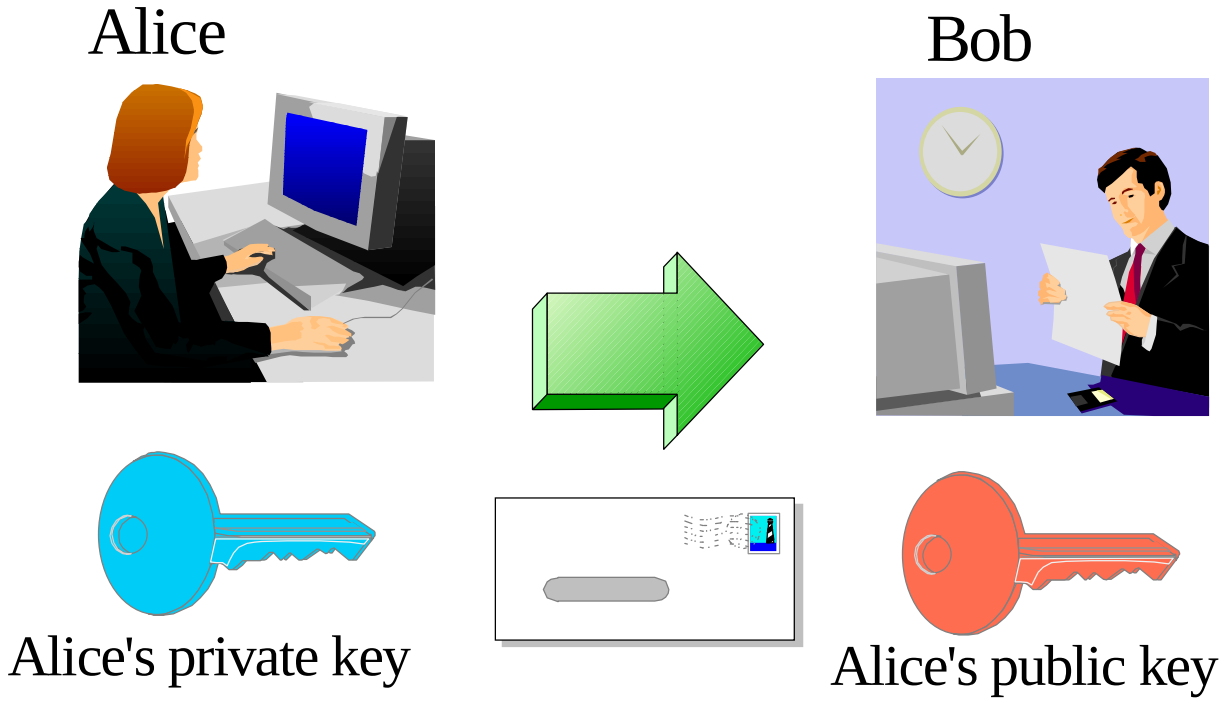
Alice encrypts the message with the secret key and sends it to Bob. Bob decrypts the message with the secret key.

Public Key Cryptography - Encrypting



Alice encrypts the message using Bobs public key and sends it to Bob. Bob decrypts it using his private key.
Since only Bob knows his private key, only he can read the message.

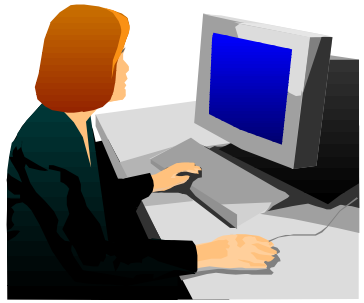
Public Key Cryptography - Signing



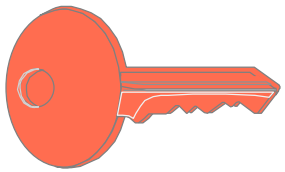
Alice encrypts the message using her private key and sends it to Bob. Bob decrypts it using Alice's public key.
The message is "signed" by Alice since it can only be decrypted using **her** public key.

Combined Symmetric and Asymmetric Cryptography

Alice

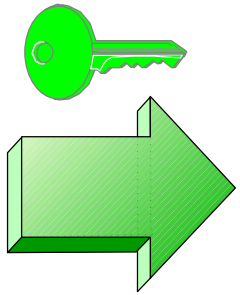


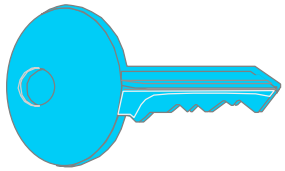
Bob



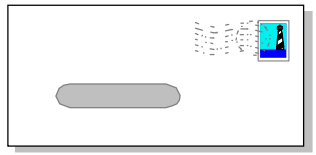
Bob's public key

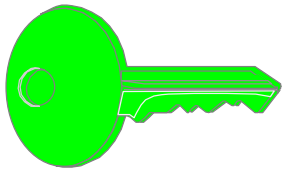
secret key



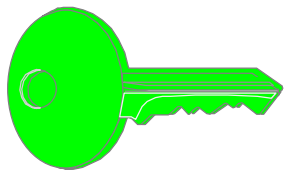


Bob's private key





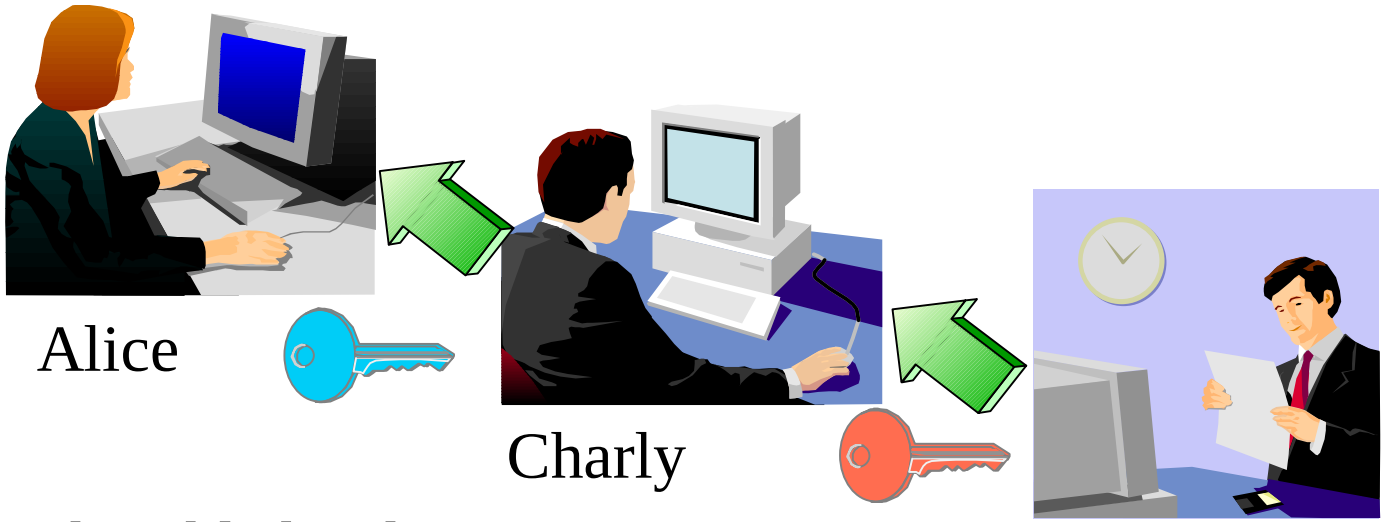
secret key



secret key

Key Management

- Key exchange is not trivial:
  - Is the public key really from the right person?

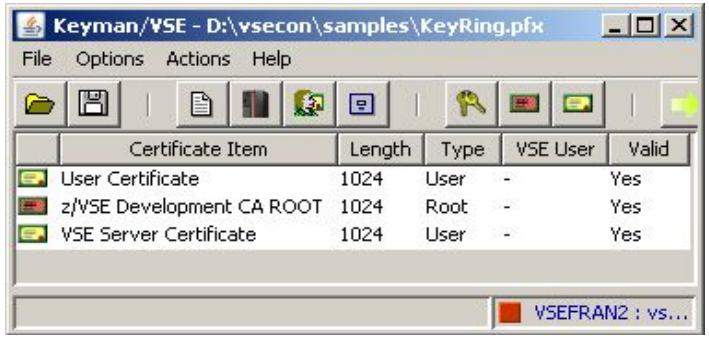


Bob publishes his public key, but Charly intercepts this and instead sends his public key to Alice.

Key & Certificate Management

Cryprography 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

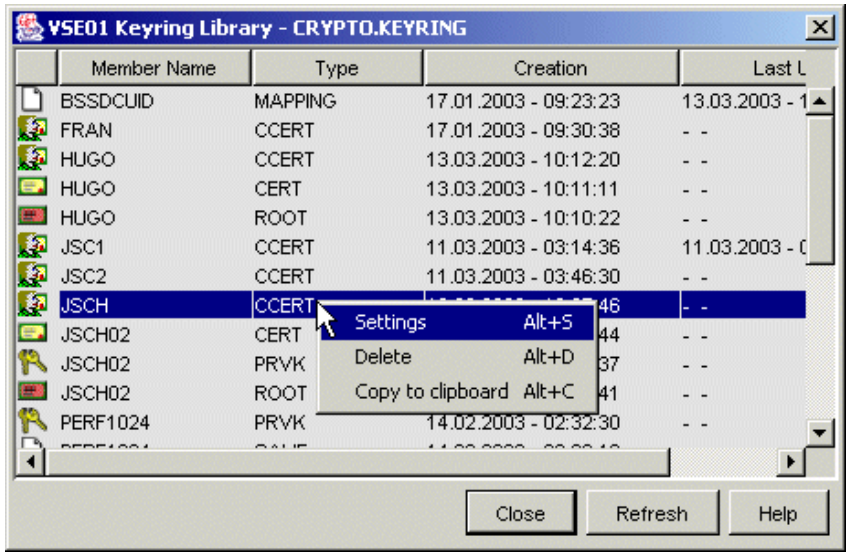


- **Keyman/VSE**
  - Creation of RSA keys and digital certificates
  - Upload of keys and certificates to VSE
  - Creation of PKCS#12 keyring files (use with Java-based connector or import into a Web browser)
  - Download from VSE Homepage http://www.ibm.com/systems/z/os/zvse/downloads/#vkeyman

Where are keys and certificates stored on VSE ?

§ Keys and certificates are stored on a VSE Library

- Usually in CRYPTO.KEYRING
- This library should be secured using the VSE security mechanisms (access protection)



§ Member types:

- .PRVK – Public/Private Key
- .ROOT – Root Certificate
- .CERT – Server Certificate
- .CCERT – Client Certificate
- BSSDCUID.MAPPING – Contains the User to Certificate mapping information

Certificates

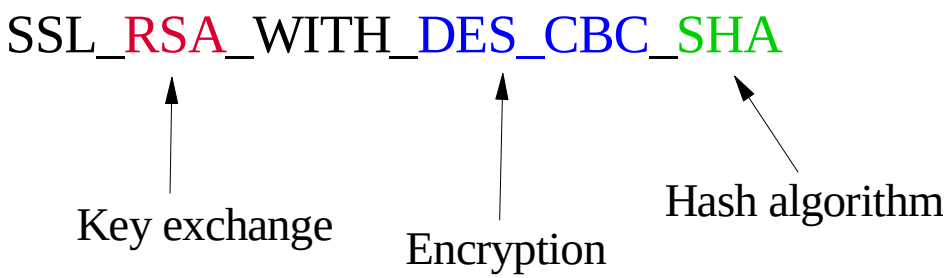
- **A certificate contains the following items**
  - The subject (name of the person)
  - The subject's public key
  - Period of validity
  - The issuer
  - Issuers signature

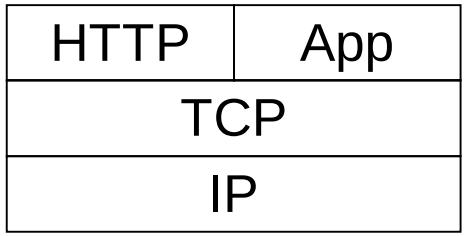
- **The issuer "signs" the certificate by encrypting a hash of the certificate content with his private key**
- **Everyone can check the sign by decrypting it with the issuers public key**

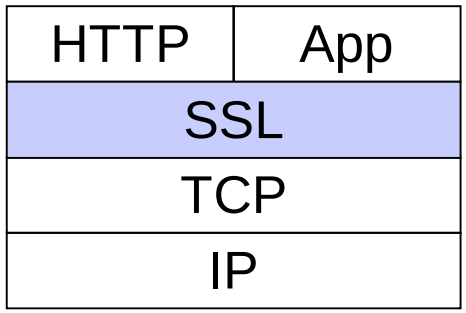
- **For production purposes, certificates are usually issued by a well known and trusted Certificate Authorities (CA)**
  - For example Thawte, VeriSign, etc.
- **For in-house use (Intranet), you can have your own Company-wide Certificate Authority**
  - Certificates are trusted inside your company, but not outside
- **For test purposes you can use self-signed Certificates (you are your own Certificate Authority)**
  - Nobody trusts these Certificates (except you)

Secure Socket Layer – Encrypted data transfer over a network

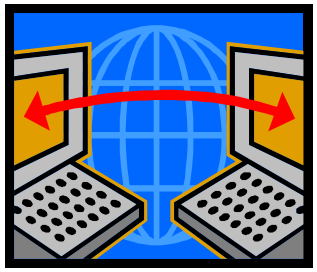
- **SSL provides a communication channel with message integrity, authentication, and confidentiality**
- **SSL is a widely used protocol**
  - Secure HTTP (HTTPS) is used very often in the Internet
- **SSL uses a TCP connection to transfer encrypted messages**
  - Uses asymmetric cryptography for session initiating
  - Uses symmetric cryptography for data encryption
- **As the name implies, SSL is a layer on top of TCP**
- **Cipher suites defines the algorithms used:**
  - For key exchange
  - For encryption
  - For hash algorithm







SecureFTP



- **The FTP protocol provides a easy and straight forward protocol for transferring files between systems on different platforms**
  - Many installations rely on it to efficiently transmit critical files that can contain vital information such as customer names, credit card account numbers, social security numbers, corporate secrets and other sensitive information
  - FTP protocol transmits data without any authentication, privacy or integrity
- **SecureFTP provides user authentication, privacy and integrity by using RSA digitally signed certificates, DES encryption and SHA-1 secure hash functions**
  - SecureFTP is integrated into TCP/IP for VSE with z/VSE V4.1 or later (at no additional charge) or offered as separately priced product by CSI
- **How to setup Secure FTP with VSE:**
  ftp://ftp.software.ibm.com/eserver/zseries/zos/vse/pdf3/How_to_setup_SecureFTP_with_VSE.pdf

Hardware Crypto Support on System z and VSE

by release

	z/VSE 4.2	z/VSE 4.1	z/VSE 3.1	VSE/ESA 2.7	VSE/ESA 2.6
PCICA	Yes	Yes	Yes	Yes	-
CEX2C	Yes	Yes	Yes	-	-
CPACF	Yes	Yes	Yes	-	-
CEX2A	Yes	Yes	Yes	-	-
PCIXCC	Yes	Yes	-	-	-

by server

	prior z800	z800	z900	z890	z990	z9	z10	z196
PCICA	-	Yes	Yes	Yes	Yes	-	-	-
PCIXCC	-	-	-	Yes	Yes	-	-	-
CEX2C	-	-	-	Yes	Yes	Yes	Yes	Yes
CPACF	-	-	-	Yes	Yes	Yes	Yes	Yes
CEX2A	-	-	-	-	-	Yes	Yes	Yes

CEX2C = Crypto Express2/3 in coprocessor mode
CEX2A = Crypto Express2/3 in accelerator mode
See: http://www.ibm.com/systems/z/security/cryptography.html

VSE Hardware Configuration

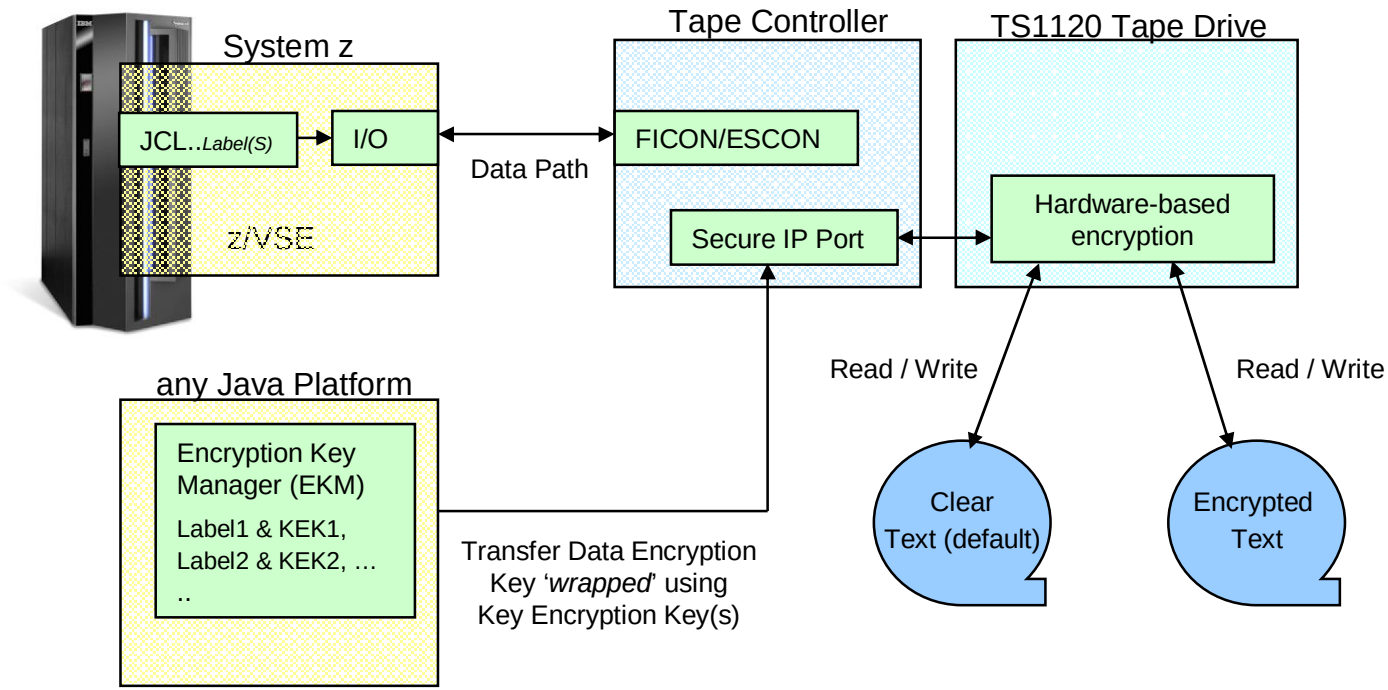
- **VSE hardware configuration not necessary for crypto hardware**
  - No IOCDS definition in VSE
  - No device type
  - No ADD statement
  - You may have to define the devices in the HMC (LPAR) or z/VM directory
- **Use of crypto hardware is transparent to end users and TCP/IP applications**
  - But use of crypto hardware can be disabled via TCP/IP SOCKOPT phase
- **How to setup cryptographic hardware for VSE:**
  - http://www.ibm.com/systems/z/os/zvse/documentation/security.html#howto

```
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.
```

IBM Tape Encryption – TS1120 & TS1130

- The IBM System Storage TS1120/TS1130 Tape Drive has been enhanced to provide drive based data encryption
- A key management component supports the generation and communication of encryption keys for the tape drives across the enterprise.
- Support is available for z/VSE:
  - *z/VSE V4.2:* *GA*
  - *z/VSE V4.1:* *DY46682 (UD53141 and UD53142)*
  - *z/VM:* *VM64062 (UM32012)*
  - *DITTO:* *PK44172 - With this APAR, DITTO/ESA for VSE supports tape encryption interactively and via standard VSE JCL in BATCH mode*
- Considerations when encrypting tapes:
  - A tape can either contain encrypted data or unencrypted data
  - If you encrypt the first file on the tape, all subsequent files will also be encrypted using the same key
    - Important for multi file tapes
  - If you send an encrypted tape to a business partner, the other side will also require a TS1120 or TS1130 to be able to read the tape

IBM Tape Encryption – TS1120 & TS1130



encryption mode
(03=write)

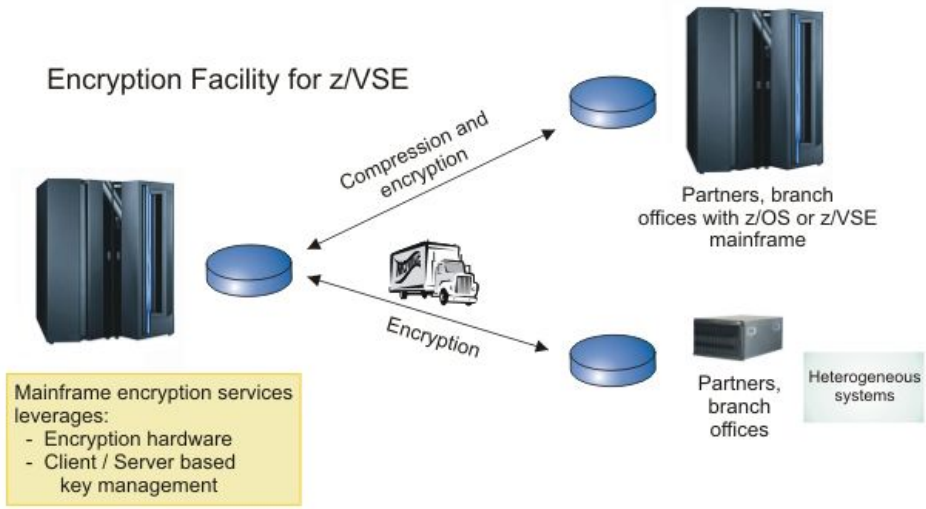
```
// JOB ENCRYPT
// ASSGN SYS005,480,03
// KEKL UNIT=480,KEKL1='MYKEKL1',KEM1=L,KEKL2='MYKEKL2',KEM2=L
// EXEC LIBR
  BACKUP LIB=PRD2 TAPE=SYS005
/*
/&
```

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



- 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 System z 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, decribed in RFCs 2440 and 4880
  - Compatible with Encryption Facility for z/OS V1.2 and many other OpenPGP implementations

Encryption Facility for z/VSE

Differences between Encryption Facility V1.1 and V1.2 OpenPGP:

	EF for z/VSE V1.1	EF for z/VSE V1.2 OpenPGP
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 OpenPGP
Symmetric Algorithms	TDES and AES-128	DES, TDES, AES-128, 192, 256
Hash algorithms	SHA1	MD5, SHA1, 224, 256, 384, 512
Compression	System z provided compression (hardware accelerated)	ZIP, ZLIB based compression (software)
RSA key lengths	512, 1024, 2048	1024, 2048
Data integrity	None	MDC
Public key format	x.509 certificates	PGP certificates
Signatures	None	RSA signatures

Encryption Facility for z/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

Other ways to encrypt your backups or tapes

Encrypt your backup data using VTAPE

- Create a backup on a remote virtual tape
- Store the tape image on an encrypted medium
  - Encrypted file system or directory (e.g. EcryptFS on Linux)
  - Use encryption tools (e.g. TrueCrypt)
  - Use Tivoli Storage Manager to store the backup data

Encrypt data in applications

- Use CryptoVSE API to encrypt the data
  - Uses Hardware Crypto Support if available

New technical articles on VSE homepage

http://www.ibm.com/systems/z/os/zvse/documentation/security.html#howto

How to setup hardware crypto with VSE

How to setup SSL with the VSE Script Connector (PDF, 900KB)
Updated: January 2010
Joerg Schmidbauer, IBM

How to setup WebSphere MQ for z/VSE V3.0 and WebSphere MQ for Windows V7.0 with secured connections using SSL (PDF, 3.0MB)
Updated: March 2009
Joerg Schmidbauer, IBM

How to use Encryption Facility for z/VSE (PDF, 380KB)
Updated: June 2010
Joerg Schmidbauer, IBM

How to setup SSL with CICS Web Support (PDF, 1.5MB)
Updated: May 2009
Joerg Schmidbauer, IBM

How to setup Secure Telnet with VSE (PDF, 1.7MB)
Updated: January 2010
Joerg Schmidbauer, IBM

How to setup Secure FTP with VSE (PDF, 1.2MB)
Updated: August 2009
Joerg Schmidbauer, IBM

How to setup SSL with VSE (PDF, 810KB)
New: August 2009
Joerg Schmidbauer, IBM

How to setup cryptographic hardware for VSE (PDF, 1.4MB)
Updated: December 2008
Joerg Schmidbauer, IBM

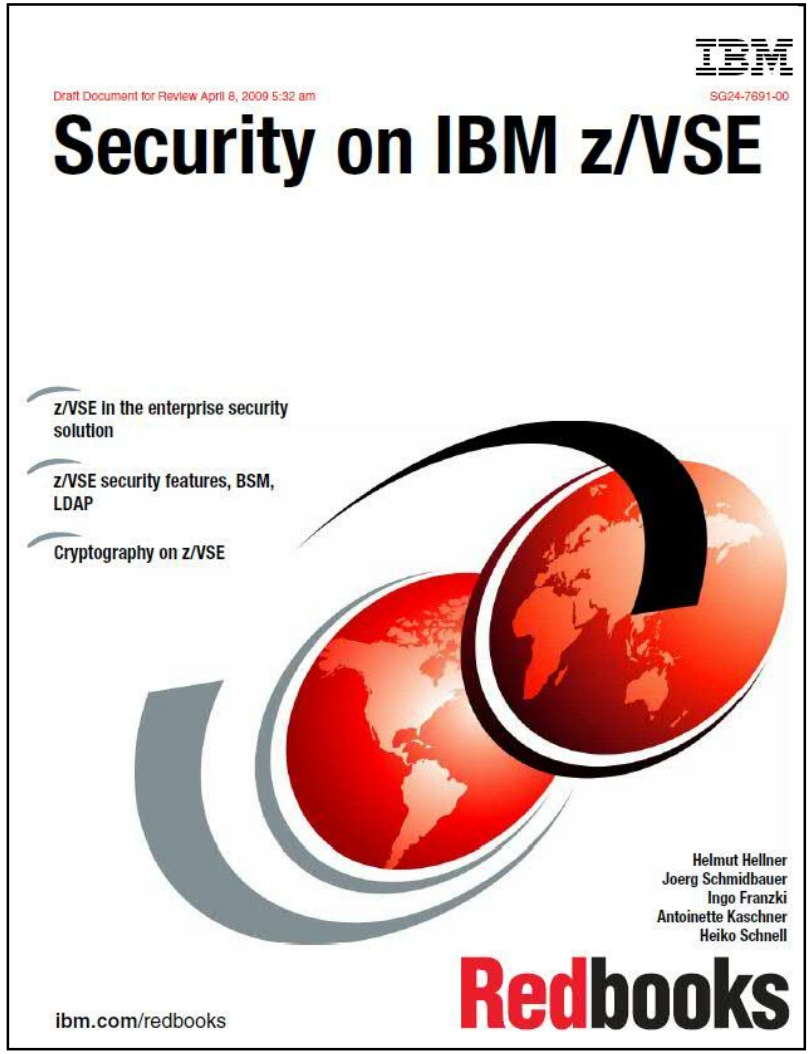
New Redbook: Security on IBM z/VSE - SG24-7691

Available since October 20, 2009
http://www.redbooks.ibm.com/redpieces/abstracts/sg247691.html

Explains security concepts as well as step by step setup

It covers:

- Basic Security Manager
- LDAP Authentication
- Cryptography & SSL
- TCP/IP Security
- SecureFTP & Secure telnet
- CICS Web Support Security
- Connector Security
- Security APIs



Related Documentation

- **New RedBook: Security on IBM z/VSE - SG24-7691**
  - http://www.redbooks.ibm.com/redpieces/abstracts/sg247691.html
- **IBM System z cryptography for highly secure transactions**
  - http://www.ibm.com/systems/z/security/cryptography.html
- **z/VSE Security Homepage**
  - http://www.ibm.com/systems/z/os/zvse/documentation/security.html
- **IBM Manuals**
  - z/VSE Planning
  - z/VSE Administration
  - OS/390 Security Server External Security Interface (RACROUTE) Macro Reference (GC28-1922)
  - OS/390 Security Server (RACF) Data Areas (SY27-2640)
  - z/VSE e-business Connectors, User's Guide
  - CICS Enhancements Guide, GC34-5763

Questions ?