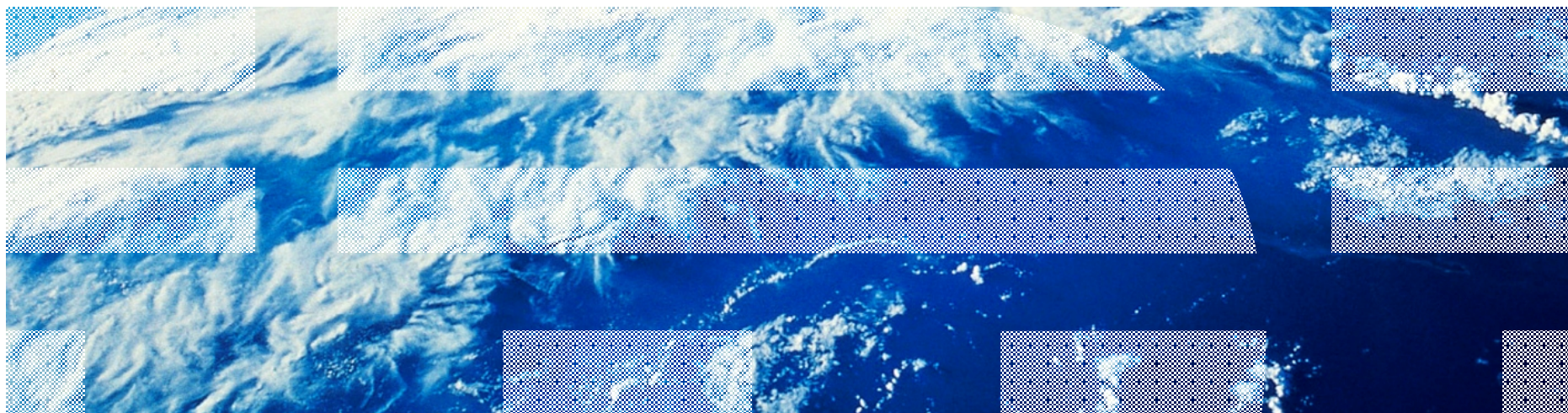# z/VSE Security Overview

Ingo Franzki, IBM

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

Why secure VSE ?

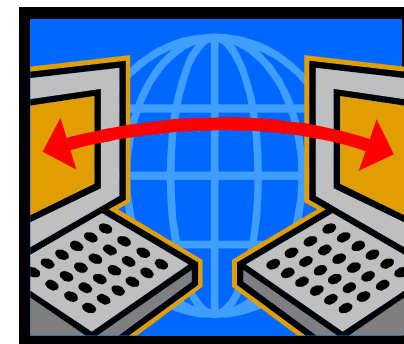§ **Prevent unauthorized access to VSE and data**
  – Keep secret data secret
  – Data modification by unauthorized users

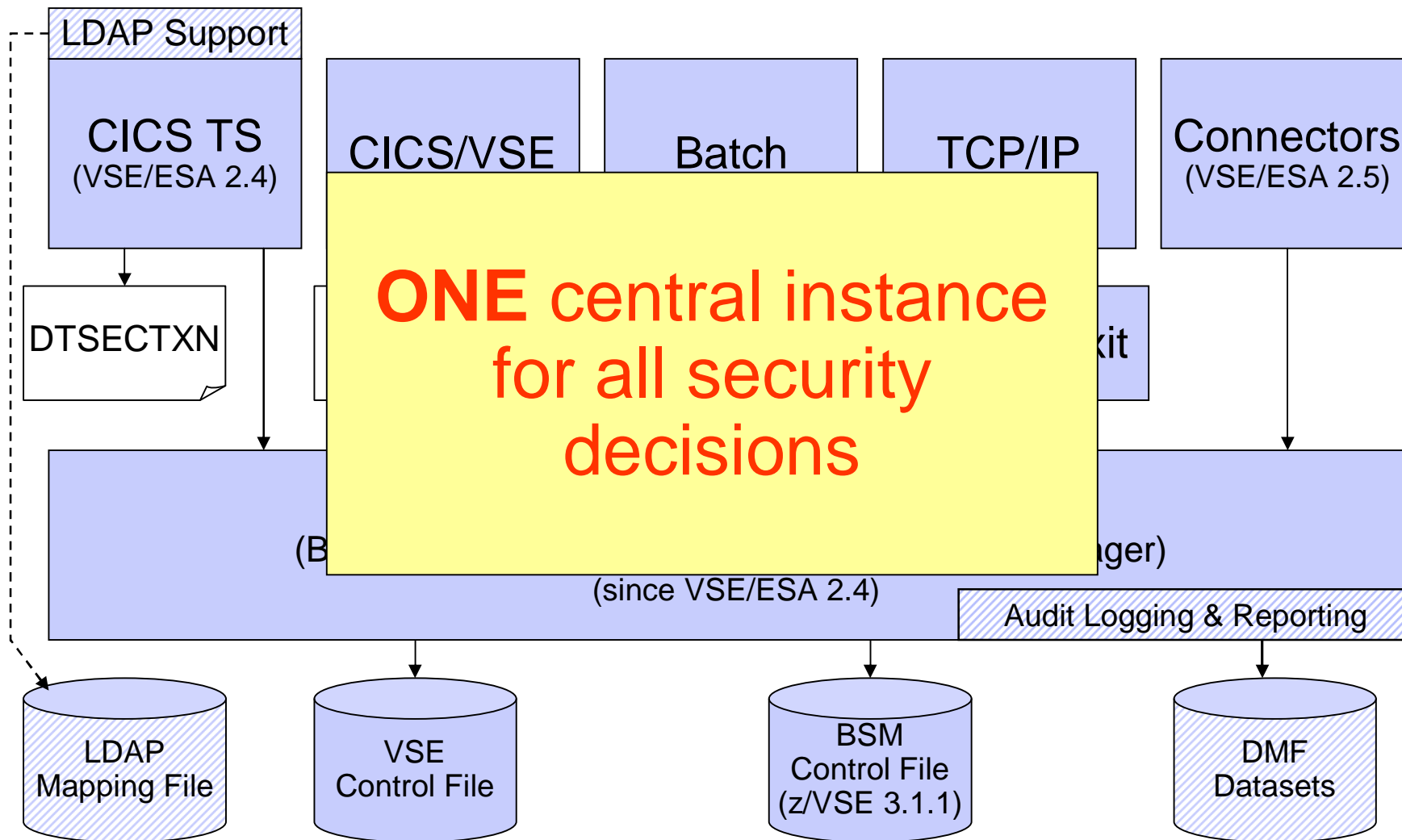§ **Prevent users from damaging the VSE system (maybe by accident)**
  – Deletion of members or entries
  – Submission of jobs

§ **Prevent unauthorized remote access to VSE**
  – Today most computers are part of a network
  – Theoretically every system in the network could connect to your VSE system
  – FTP allows to access production data
    • VSAM
    • POWER entries (listings)

VSE Security Components

LDAP Support

CICS TS
(VSE/ESA 2.4)

CICS/VSE

Batch

TCP/IP

Connectors
(VSE/ESA 2.5)

DTSECTXN

...kit

ONE central instance for all security decisions

(B...ger)

(since VSE/ESA 2.4)

Audit Logging & Reporting

LDAP
Mapping File

VSE
Control File

BSM
Control File
(z/VSE 3.1.1)

DMF
Datasets

Audit-Logging and Reporting

§ **All access attempts to <u>protected</u> resources can be logged**
  – Allowed access as well as disallowed access

§ **Possible attacks can be detected**
  – E.g. multiple logon attempts with invalid password
  – Who did when access which resource

§ **Analysis can be done using a reporting tool**
  – Summary report
  – Detailed report of all access attempts

§ **New with z/VSE 4.2:**
  – Logging of important BSTADMIN commands

§ **New since z/VSE V4.3:**
  – Audit-Logging of DTSECTAB resources

§ **To activate logging for a specific resource, you need to specify the AUDIT option (using BSTADMIN) on the resource profile:**

  AUDIT(*audit-level, access-level*)   ß New with z/VSE 4.2

  audit-level:
  ALL: All authorized accesses and detected unauthorized access attempts should be logged.
  FAILURES: All detected unauthorized access attempts should be logged (the Default).
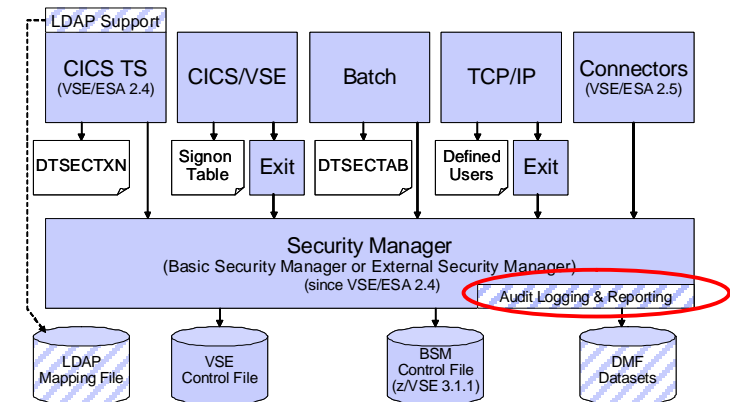 **SUCCESS:** All access attempts that were authorized should be logged.
  NONE: No logging should be done.

  access-level:
  ALTER: Logs ALTER access-level attempts only.
  READ: Logs access attempts at any level. READ is the default value if the access-level is omitted.
  UPDATE: Logs access attempts at the UPDATE and ALTER level.

Diagram labels:
LDAP Support
CICS TS (VSE/ESA 2.4) | CICS/VSE | Batch | TCP/IP | Connectors (VSE/ESA 2.5)
DTSECTXN | Signon Table | Exit | DTSECTAB | Defined Users | Exit
Security Manager (Basic Security Manager or External Security Manager) (since VSE/ESA 2.4) — Audit Logging & Reporting
LDAP Mapping File | VSE Control File | BSM Control File (z/VSE 3.1.1) | DMF Datasets

Audit-Logging and Reporting

```
05.081 09:35:32                          BSM Report - Listing of Process Records
                                      E
                                      v  Q
                                      e  u
             *Job/User                n  a
Date   Time  Name                     t  l
05.076 12:26:06  SYSA                 1  8  Job=(CICSICCF) - User verification: Sucessful termination
                 AUGUST WONG                Auth=(None),Reason=(None)
05.076 12:26:12  HUGO                 1  1  Job=(CICSICCF) - User verification: Invalid password
                 HUGO MAYER                 Auth=(None),Reason=(User ve rification failure)
05.076 12:26:17  HUGO                 1  0  Job=(CICSICCF) - User verification: Sucessful initiation / logon
                 HUGO MAYER                 Auth=(None),Reason=(None)
05.076 12:26:17  HUGO                 2  1  Job=(CICSICCF) - Resource access: Insufficient authority
                 HUGO MAYER                 Auth=(Normal),Reason=(Audit options)
                                            Resource=CESN,Intent=
05.076 12:26:18  HUGO                 1  8  Job=(CICSICCF) - User
                 HUGO MAYER                 Auth=(None),Reason=(N
05.076 12:26:29  SYSA                 1  0  Job=(PAUSEBG ) - User
                 AUGUST WONG                Auth=(None),Reason=(N
05.076 12:26:30  SYSA                 2  0  Job=(PAUSEBG ) - Reso
                 AUGUST WONG                Auth=(Administrator),
                                            Resource=MYAPPL.MYPRIN
05.076 12:26:33  SYSA                 1  8  Job=(PAUSEBG ) - User
                 AUGUST WONG                Auth=(None),Reason=(N
```

```
05.081 09:35:32                        BSM Report - Listing of User Summary
                                               --------- R e s o u r c e   S t a t i s t i c s ----------
User/       Name          ---- Job/Logon ----                    ------- I n t e n t s -------
*Job                      Success Violation    Success Violation   Alter   Update    Read    Total
HUGO      HUGO MAYER          1       1            0       1         0       0         1       1
SYSA      AUGUST WONG         1       0            1       0         0       0         1       1

05.081 09:35:32                        BSM Report - Listing of Resource Summary
                                                                 ------- I n t e n t s -------
Resource Name                         Success Violation   Alter   Update    Read    Total
Class = FACILITY
  MYAPPL.MYPRINT                          1       0         0       0         1       1
Class = TCICSTRN
  CESN                                    0       1         0       0         1       1

05.081 09:35:32                        BSM Report - General Summary

Process records:                          8

                                 --- Job / Logon  Statistics ---
Total Job/Logon/Logoff                    6
Total Job/Logon successes                 5
Total Job/Logon violations                1
Total Job/Logon attempts by undefined users   0
Total Job/Logon successful terminations   2

                                 --- Resource Statistics ---
Total resource accesses (all events)      2
Total resource access successes           1
Total resource access violations          1
```
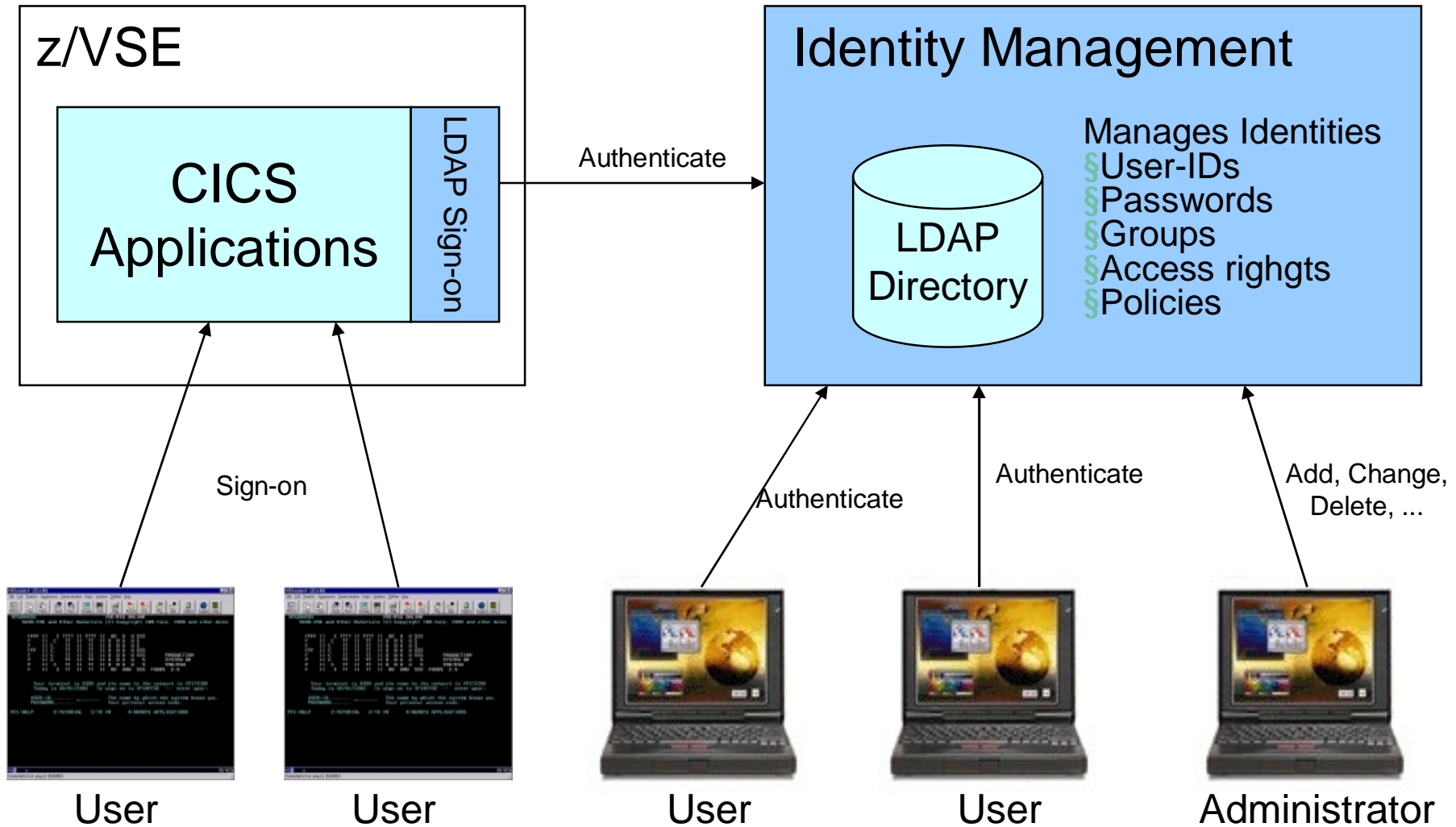
**Auditors can use reporting tools to generate**

§ Summary reports

§ Detailed reports of all access attempts

LDAP Signon Support

LDAP Signon Support

§ Enables users to sign on z/VSE using a single, comprehensive, corporate-wide 'Identity Management' systems (i.e. IBM Tivoli Identity Manager, etc.)

§ LDAP user-IDs and passwords can be up to 64 characters.

§ Helps overcome VSE internal limits:
  – 4 character VSE/ICCF user-IDs
  – 4 and 8 character CICS user-IDs
  – up to 8 character Passwords

§ LDAP sign on sits on top of existing z/VSE security manager (i.e. BSM, ESM, etc.)

§ z/VSE LDAP client can work with common LDAP servers
  – IBM Tivoli Directory server
  – z/VM LDAP server (with optional RACF repository)
  – Microsoft Active Directory, OpenLDAP, Apache Directory server, Novell eDirectory, and many others.

§ Potential benefits include improved protection, consistent access rules, ease of use for end-users
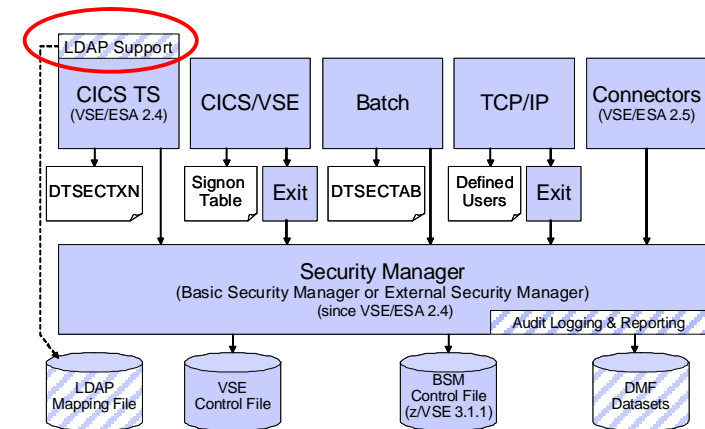
Defining a new user-ID

§ Define a new user-ID

– Interactive Interface dialog **Maintain User Profiles** (211)

§ Connect the new user-ID to groups

– Interactive Interface dialog **Maintain Security Profiles** (282)

– Show **User List** (option 6) and add the user-ID to the group

– Add the user-ID or groups to the access list of the desired resource profiles, if needed

– You can also use BSTADMIN to do this in batch.

§ Perform a BSM Security Rebuild to activate the changes

§ If you are using LDAP Authentication, you also need to add the user-ID to the LDAP mapping file via IESLDUMA

§ Since z/VSE V4.3 the User Maintanance Dialogs have been connected to each other, leading you from User Definitions, to Group Maintanance and LDAP mapping

Maintaining user-IDs

If you make changes to a user-ID, don't forget to update the groups and resources as well:

§ **When deleting a user-ID**
  – Remove it from the groups it is belonging to
  – Remove it from the access lists of any resource profiles

§ **When updating a user-ID**
  – Adapt the groups it is belonging to, if required
  – Adapt the access lists of all resource profiles, if required

§ Use the BSM Cross Reference Tool to find out where the user-ID is referenced (see separate foil)

§ Perform a BSM Security Rebuild to activate the changes

§ If you are using LDAP Authentication, you also need to update the user-ID in the LDAP mapping file via IESLDUMA

Group maintanance

§ **Per default there are GROUP01 to GROUP64**
  − coresponding to the 64 CICS transaction security keys

§ **Define a new group**
  − Interactive Interface dialog **Maintain Security Profiles** (282)
  − Use option 1 (Add) to add a new group

§ **Add user-IDs to the newly created group**
  − Show **User List** (option 6) and add the User-ID to the group

§ Do **NOT** create groups that are named the same as user-IDs

§ You can also use BSTADMIN to do this in batch.

§ Perform a BSM Security Rebuild to activate the changes

Resource profiles

§ There are 2 repositories for resource profiles:
- **DTSECTAB:** It contains the entries for z/VSE files, libraries, sublibraries, and members

- **BSM Control File:** It keeps the profiles for all the new resource classes supported by BSM

§ Access List specifies who (base on user-ID or group) has access (Read, Update, Alter) to the resource

§ If the access list contains both, a user-ID and a group that contains the user-ID
- then the access rights specified with the User-ID is effective

Migrating from older BSM versions

§ **Since z/VSE 3.1.1, BSM uses the BSM Control File instead of DTSECTXN**

– You may need to migrate transaction security definitions from DTSECTXN to BSM Control file

§ **The steps you can follow partly depends on:**

– The VSE system level from which you installed z/VSE

– Whether you performed an FSU (Fast Service Upgrade) or an initial installation.

– Whether you wish to retain the use of your previous security definitions.

§ **Please see Administration Manual Chapter 22 (page 325) for details**

– See the table that describes the steps you need to perform before and after migration of VSE

BSM Cross Reference Tool

§ The z/VSE BSM Cross Reference Tool is intended to help administrators control the profile definitions in the BSM control file.
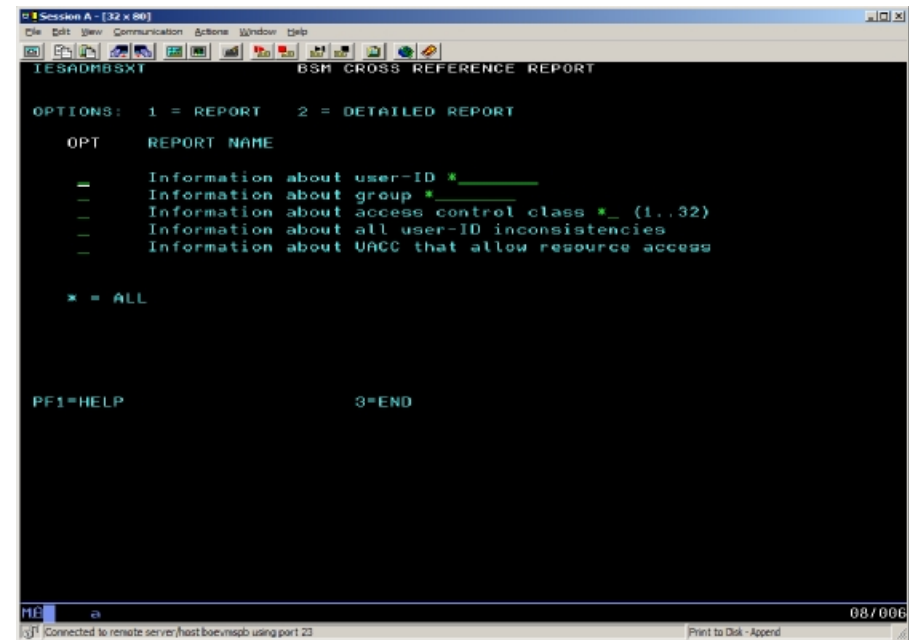
§ Example:

– When you delete a user-ID, you can use it to ensure that you have removed the user-ID from all access lists and groups.

§ The following functions are provided:

– List all groups and resource profiles which contain a specified user-ID.

– List all resource profiles where a specified group is on the access list.

– List all user-IDs found in the BSM control file but is not defined in the VSE control file.

– List all resource profiles that allow any user-ID to access a resource (UACC not NONE).

§ Runs as batch job, or via Interactive Interface Dialog (286)   à (new since z/VSE V4.3)

http://www.ibm.com/systems/z/os/zvse/downloads/tools.html#bsmxref

CICS TS Security

§ CICS sign on is performed using

– Native CICS TS sign on (CESN)

– VSE/Interactive Interface sign on (IEGM)

– Private sign on programs based on
CICS SIGNON

§ Grant access to CICS ressources

– Per individual user

– Per group

§ Resource security definitions under CICS TS

– Definition within single resource definition

- Within `CEDA DEFINE FILE: RESSEC(YES)`
- With BSTADMIN Resource Profiles for Resource Class FCICSFCT:

```
ADD FCICSFCT FILEA UACC(NONE)    (resource = FILEA)
ADD FCICSFCT FILEB UACC(NONE)    (resource = FILEB)
PERMIT FCICSFCT FILEA(GROUP1) ACCESS(UPDATE)
PERMIT FCICSFCT FILEB(GROUP1) ACCESS(READ)
```
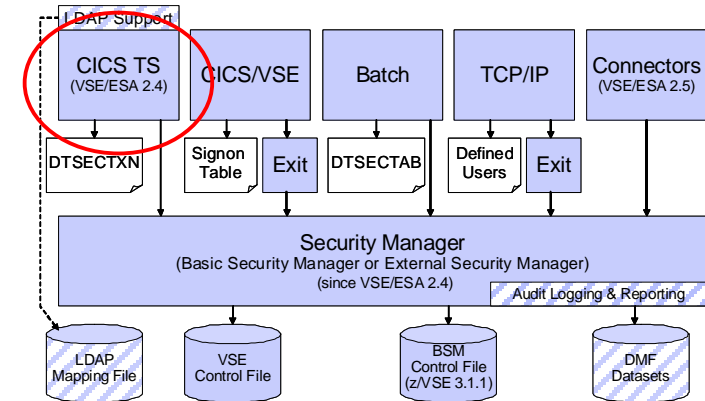
CICSUSER considerations & critical transactions

§ **Every transaction runs under the context of a user-id**
- If no user is signed on, it runs under the default user
  - DFHSIT: DFLTUSER=CICSUSER

§ **CICSUSER is predefined after base install:**
- Type 3 (ICCF is not allowed)
- Is in GROUP01, GROUP60-GROUP64
  - GROUP01 and GROUP60 is required by Interactive Interface

§ **Actions to perform after installation**
- Do not allow this user to use critical transactions
- Adjust groups this user is belonging to

§ **You need to protect critical transactions to prevent system damage by users**

Transaction	Description
USER	Display Activity Dialog, send Message to all users
CEMT	Master terminal
CEDA	Resource definition online
CEDB	Like CEDA, but no INSTALL possible
CEDC	Like CEDA, but read only
CECI	Command level interpreter
CEDF/CEDX	Execution diagnoistic facility
CETR	Trace control
CESN/CESF	Sign on/sign off
DITT	Online Ditto
others ?	

Batch Security

§ **When you have batch security active (SYS SEC=YES),
   all your jobs need to specify a user-ID and password**
  – Either using the // ID statement within the job
  – or in the * $$ JOB card

§ **ID statement or * $$ JOB specifies user id and password for a job**

       `* $$ JOB JNM=MYJOB,....,SEC=(user,password)`

or

       `// ID USER=user,PWD=password`

§ **User id and password are verified against**
  – DTSECTAB
  – Security Manager (RACROUTE)

§ **Subsystems (LIBR, VSAM, ...) uses this user id to verify access rights against DTSECTAB**

§ **When you submit jobs from the ICCF library**
  – The submitted job automatically inherits the user-ID and password from the submitting user
  – No need to specify a // ID statement or user-ID in the * $$ JOB card

§ **Inheritance only works if batch security is active at the time you do the submit**
  – Jobs that have been submitted prior to activating batch security do not have any inherited security information, you
    may have to re-submit those jobs

New since z/VSE V4.3: Protect JCL operands

§ **You can use BSM security to protect operands of specific JCL statements.**

– For example, you can protect the PERM operand of the ASSGN and LIBDEF statements.

§ **IBM provides five resource profiles of class FACILITY that are used for JCL statement checking:**

– IBMVSE.JCL.ASSGN.**PERM**

– IBMVSE.JCL.LIBDEF.**PERM**

– IBMVSE.JCL.LIBDROP.**PERM**

– IBMVSE.JCL.OPTION.**PARSTD**

– IBMVSE.JCL.OPTION.**STDLABEL**

§ **To perform JCL statement checking:**

– JCL security must be enabled (SYS SEC=YES,**JCL**)

– The minimum access right for Universal Access or user-IDs/groups must be READ

TCP/IP Security

§ In general TCP/IP uses its own user id definitions

- Readable in initialization member (IPINITxx.L)
  - `DEFINE USER,ID=user,PASSWORD=pwd`
- Duplicate user definitions
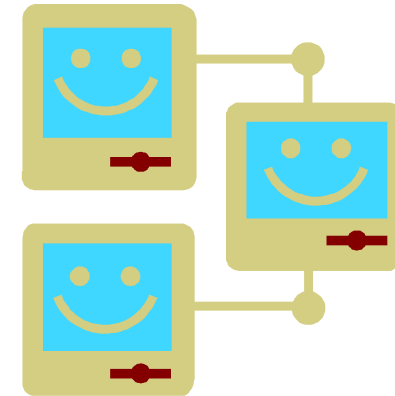
§ Security Exit available from IBM to check the user ids and resource access via Security Manager

- Issues RACROUTE calls for
  - User identification and verification
  - Resource access control
  - VSE files, libraries, members
  - POWER entries
  - SITE commands
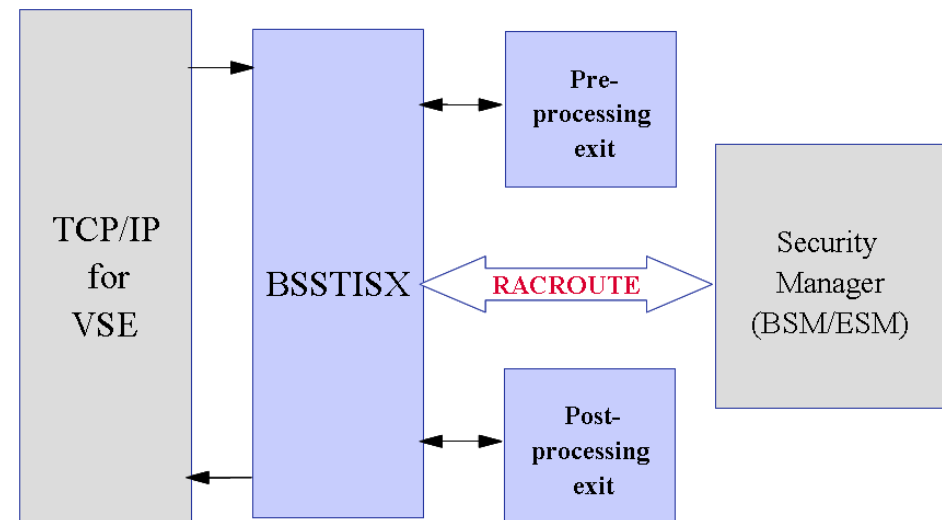
New since z/VSE V4.3: Protect WebSphere MQ resources

§ **The Basic Security Manager supports the following resource classes that are used by WebSphere MQ for z/VSE Version 3 onwards:**

- MQADMIN — Administrative type functions
- MQCMDS — Command security
- MQCONN — Connection security
- MQQUEUE — Queue resource security
- MQNLIST — Namelist resource security

§ **All resources (BSM profile names) used by WebSphere MQ are prefixed with the name of the subsystem that they are to be used by.**

- For example, if queue manager with SSID **MQV1** has a queue called **QUEUE_FOR_LOST_CARD_LIST**, the appropriate profile would be defined to the ESM or BSM in class MQQUEUE as:
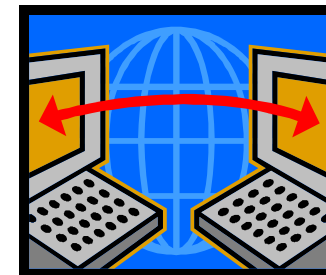 - **MQV1.QUEUE_FOR_LOST_CARD_LIST**

§ **For details, please see manual "WebSphere MQ for z/VSE System Management Guide" - GC34-6981-02 (revision 02)**

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

Key & Certificate Management
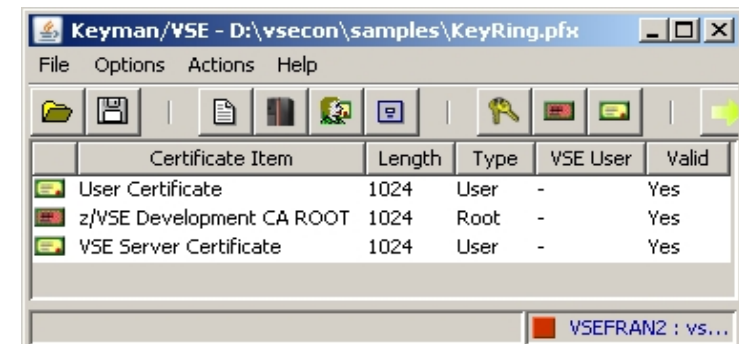
Cryprography uses Keys and Certificates

§ 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

Keyman/VSE - D:\vsecon\samples\KeyRing.pfx

File Options Actions Help

Certificate Item	Length	Type	VSE User	Valid
User Certificate	1024	User	-	Yes
z/VSE Development CA ROOT	1024	Root	-	Yes
VSE Server Certificate	1024	User	-	Yes

VSEFRAN2 : vs...

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.
  – Usually this cost money

§ **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
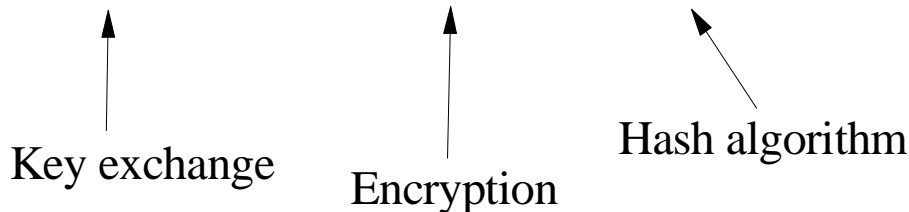– Uses symmetric cryptography for data encryption

§ **As the name implies, SSL is a layer on top of TCP**

§ **Cipher suites defines the algorithms used:**

– For key exchange
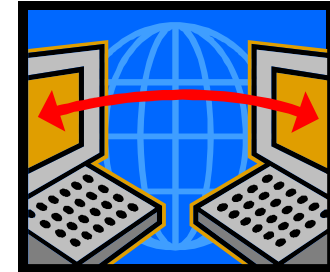– For encryption
– For hash algorithm

HTTP	App
TCP	
IP	

HTTP	App
SSL	
TCP	
IP	

SSL_RSA_WITH_DES_CBC_SHA

Key exchange

Encryption

Hash algorithm
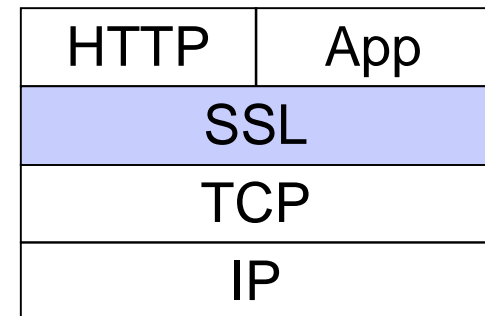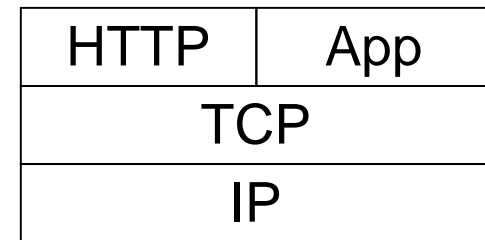
SecureFTP

- § **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 4.3	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	Yes	-
CEX2C	Yes	Yes	Yes	Yes	-	-
CPACF	Yes	Yes	Yes	Yes	-	-
CEX2A	Yes	Yes	Yes	Yes	-	-
PCIXCC	Yes	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.
```

z/VSE V4.3 – Crypto Express3 and AP queue interrupt support

§ **Support for AP-interrupts is a new function of IBM System z10 and IBM zEnterprise 196**

§ **A hardware interrupt is issued when a response is ready for de-queueing from a card.**
  – Removes the need for the formerly used polling mechanism
  – User can switch between polling and interrupts (default: polling)
  – Using interrupts increase throughput for certain workloads without increasing CPU load

§ **Not available under z/VM!**

§ **Supported cards are:**
  – Crypto Express2 and
  – Crypto Express3

§ **The VSE crypto device driver provides new commands:**
  – APEAI, enable AP interrupts for all APs
  – APDAI, disable AP interrupts for all APs

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

IBM Tape Encryption – TS1120 & TS1130
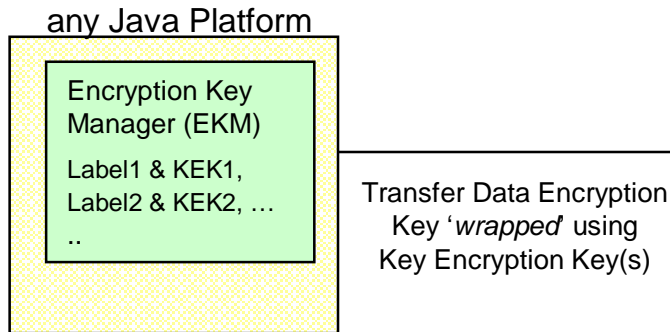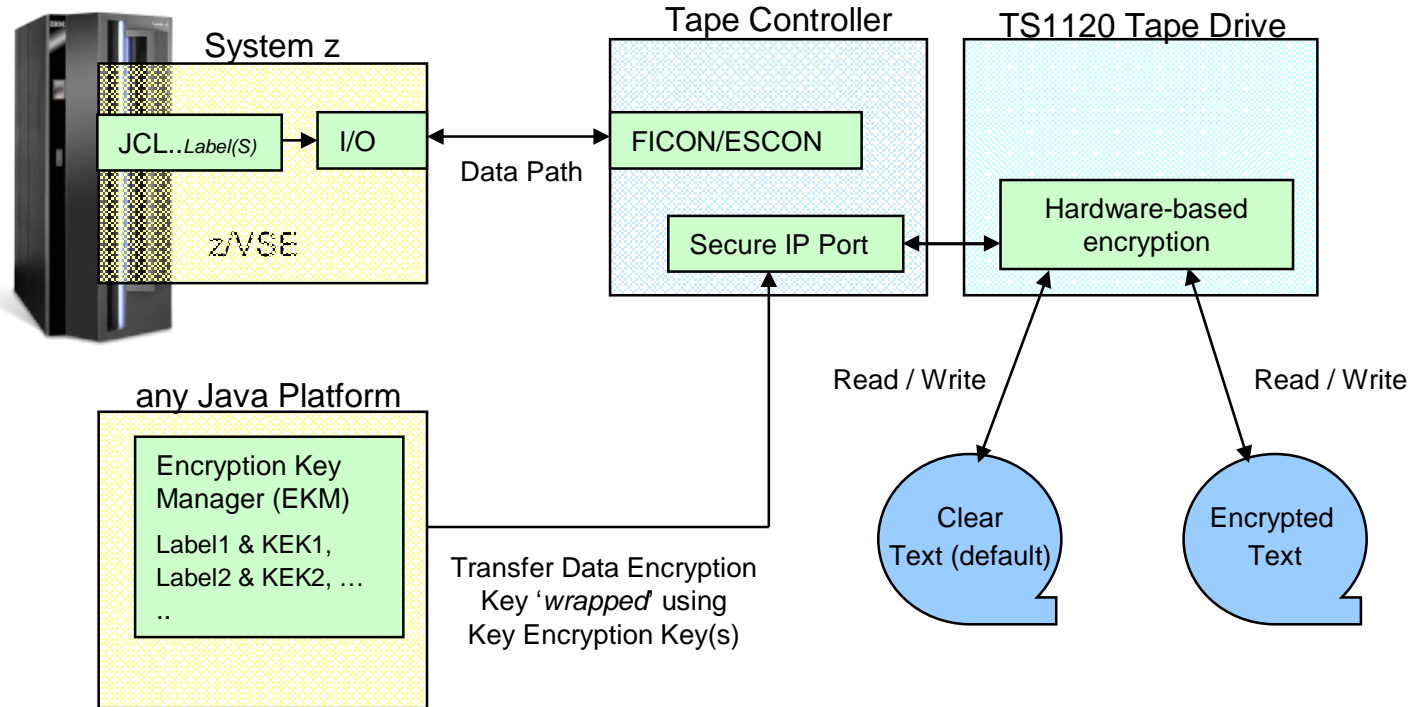

```
                                    encryption mode
// JOB ENCRYPT                        (03=write)
// ASSGN SYS005,480,03
// KEKL UNIT=480,KEKL1='MYKEKL1',KEM1=L,KEKL2='MYKEKL2',KEM2=L
// EXEC LIBR
  BACKUP LIB=PRD2 TAPE=SYS005                   encoding mechanism
/*                                               (L=Label, H=Hash)
/&
              key label1
  (name of the 1. KEK-key in EKM)
```
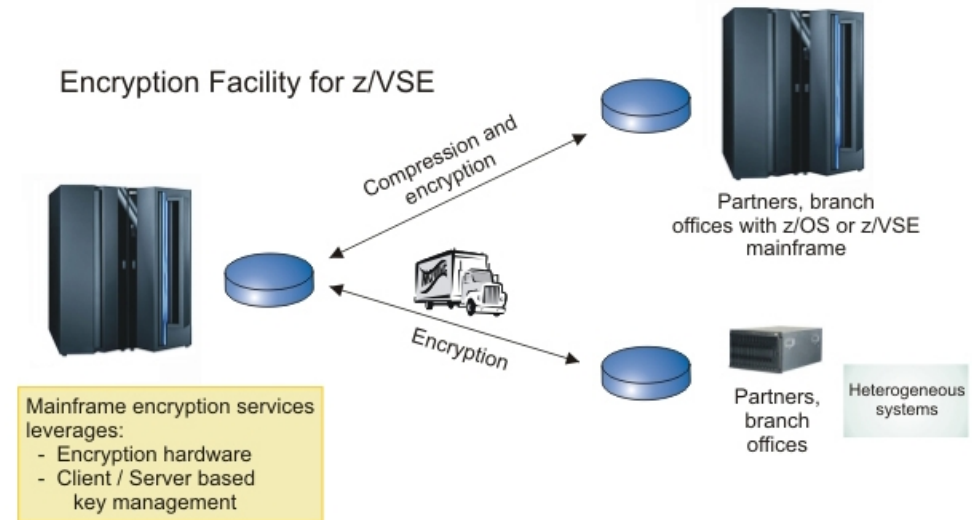
Encryption Facility for z/VSE

§ 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

Encryption Facility for z/VSE

Compression and encryption

Partners, branch offices with z/OS or z/VSE mainframe

Encryption

Partners, branch offices

Heterogeneous systems

Mainframe encryption services leverages:
- Encryption hardware
- Client / Server based key management

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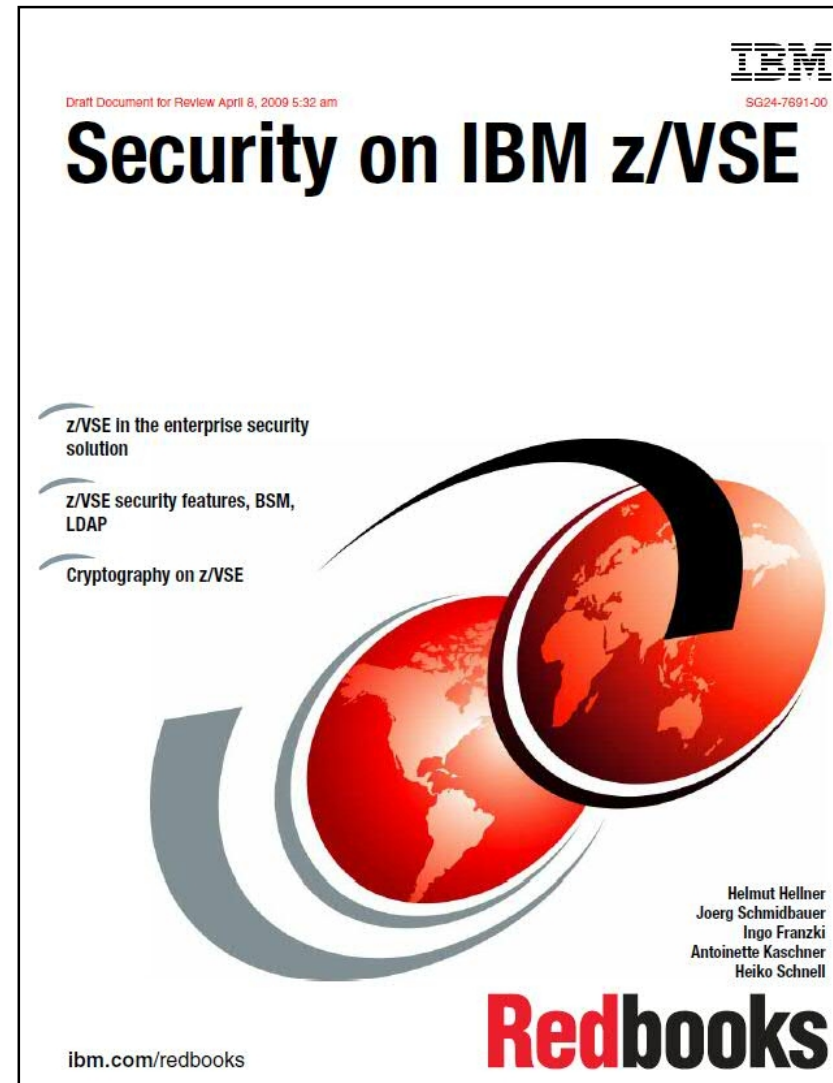
New Redbook: Security on IBM z/VSE - SG24-7691

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

§ 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 ?