How to secure your z/VSE system and data in today's interconnected world

Ingo Franzki

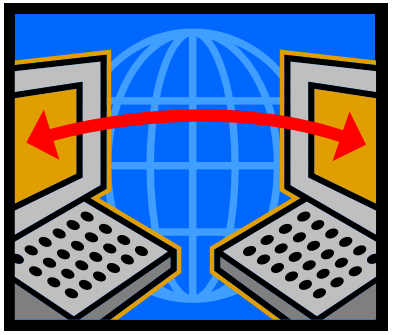
z/VSE 50
50 years of innovation

Why secure VSE ?

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

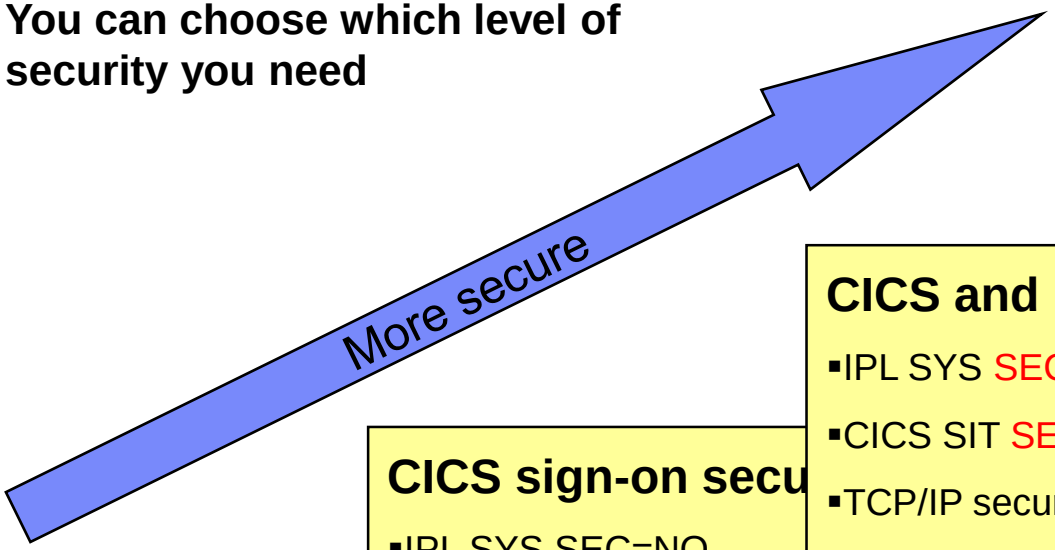
- **Prevent users from damaging the VSE system (maybe by accident)**
  - Deletion of members or entries
  - Submission of jobs

- **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)



Securing you system – Protection levels

You can choose which level of security you need



No security or homegrown se

- IPL SEC=NO
- CICS SIT SEC=NO
- No TCP/IP security

→ No real protection from inside nor outside !

CICS sign-on secu

- IPL SYS SEC=NO
- CICS SIT SEC=YES
- No TCP/IP security

→ Only protected if signing in through CICS. No protection for batch or remote

CICS and batch s

- IPL SYS SEC=YES
- CICS SIT SEC=YES
- TCP/IP security active

→ Protected against ac Inside (e.g. batch) and outside (CICS and TCP/IP)

Extended security

- IPL SYS SEC=YES
- CICS SIT SEC=YES
- TCP/IP security active
- Using extended security features
  - FACILITY resources
  - JCL security
  - LDAP signon
  - Data encryption & SSL
  - Auditing

Required level of protection depends on

→ What resources you want to protect

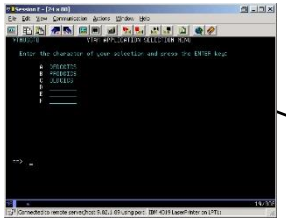
→ Against whom (inside, outside)

Ways into your z/VSE system – Are you securing them all?

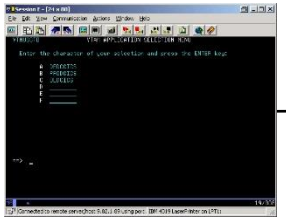
HMC
Integrated
Console

CICS Web Support
3270 Bridge

Web Services
(SOAP / HTTP)



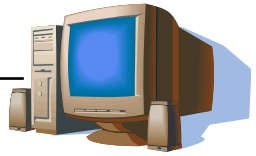
IPL console



Terminal (SNA,
Local non-SNA)

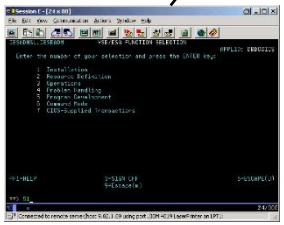
z/VSE

Connectors,
VSE Navigator,
etc.



Telnet
3270

FAQS
or similar



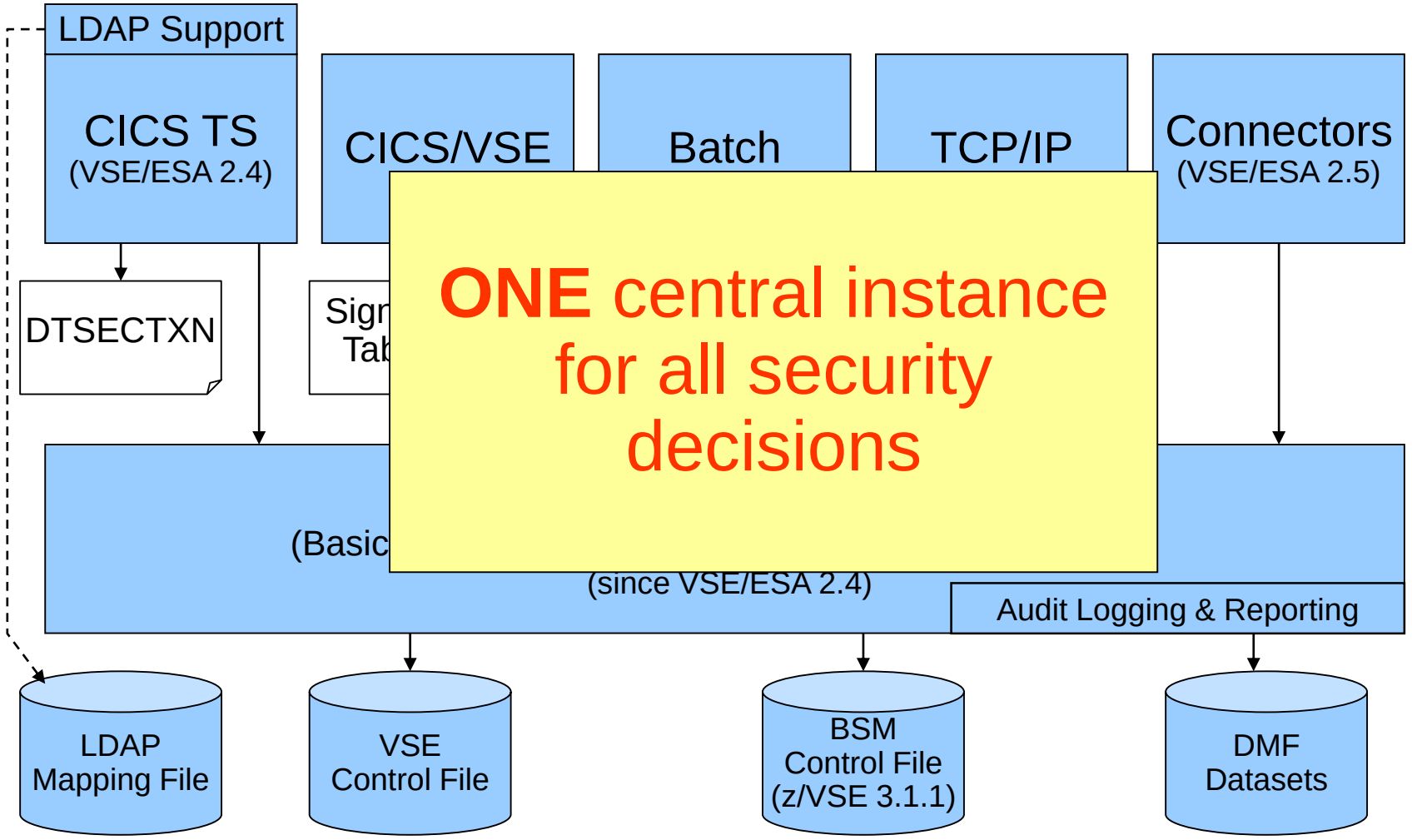
TCP/IP
SNA / APPC

z/VM Command Interface
Send jobs
IUCV
VMCF

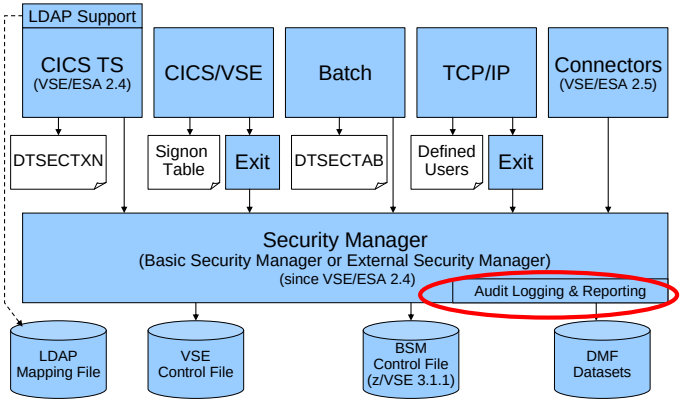
FTP

z/VM

z/VSE Security Components



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
- **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*)

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.

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 ) - Resou
                      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

z/VSE 5.2: Support for AUDITOR ID

- **The Basic Security Manger (BSM) has been enhanced to optionally separates the auditor function from the administrator function**
  - The BSM introduces a new user ID of type AUDITOR and allows you to assign the administration of the system-wide audit options to the AUDITOR only
  - The administrator keeps the responsibility to process logging information, but has no auditor rights any longer
  - The Interactive User Interface of z/VSE is extended to define the AUDITOR ID

- **If batch security is active, the auditor user ID must be authorized to**
  - execute the DMF dump services, for instance by *SETDMF FLUSH / SWITCH* and run finally *DFHDFOU*
  - to execute the BSM Report Writer (*BSTRPWTR*)
  - to access to the SMF/DMF data sets
  - to run *BSTADMIN*
  - to change the contents of BSTCNTL.

z/VSE 5.2: Support for AUDITOR ID

- **The Auditor authorization is required for use of the BSTADMIN command variations of**

```
PERFORM|PF
         [AUDIT ADMINACC|NOADMINACC] |
         [CLASS(<class-name>) CMDAUDIT|NOCMDAUDIT]
```

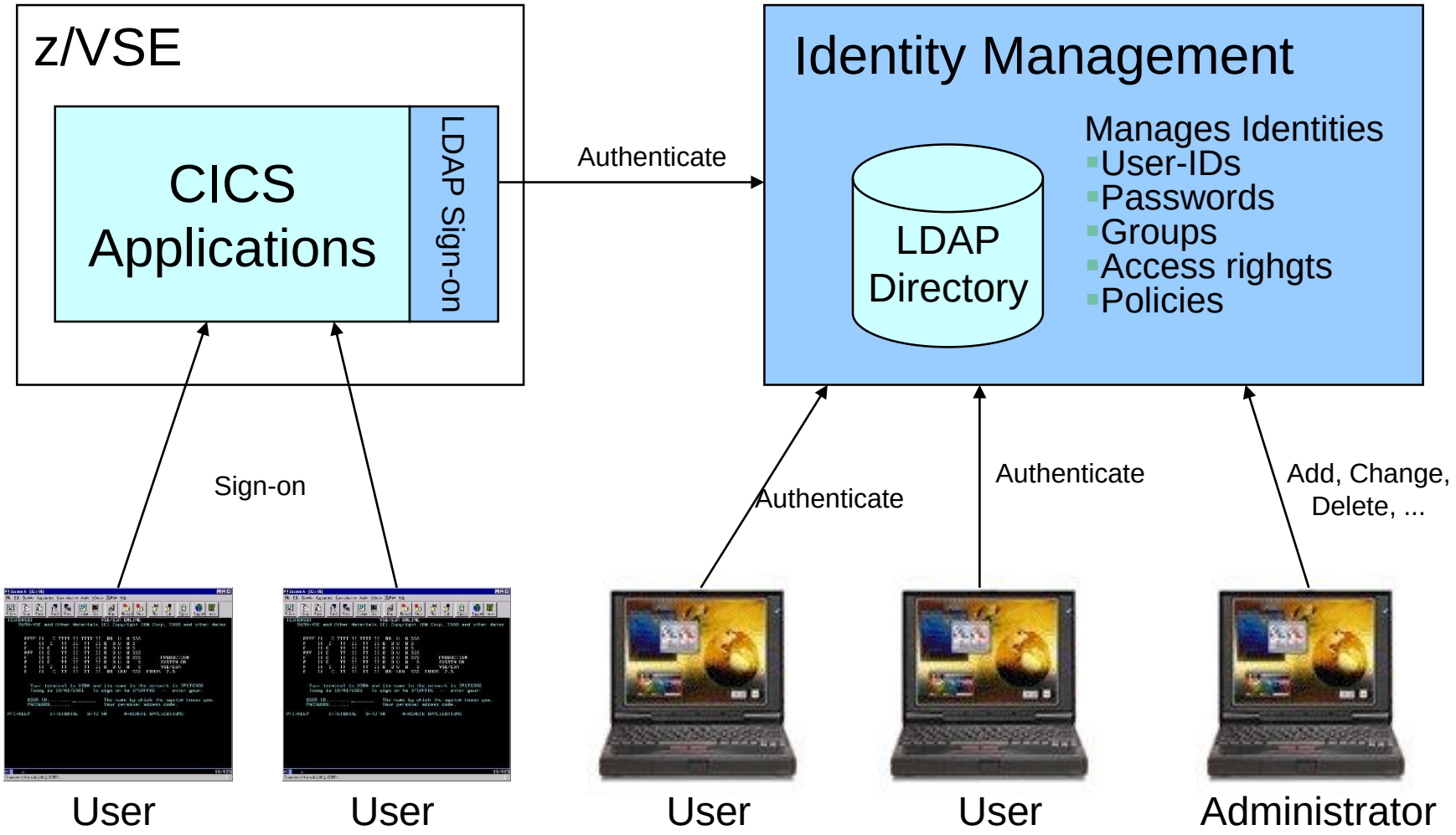
- **Provides exclusive information with the output of the BSTADMIN command**

```
STATUS|ST

AUDIT OPTIONS:
  ADMINISTRATOR ACCESSES TO RESOURCES ARE LOGGED

CLASS      ACTIVE     CMDAUDIT
-----      ------     --------
USER       YES        NO
GROUP      YES        NO
DATASET    YES        NO
...
```

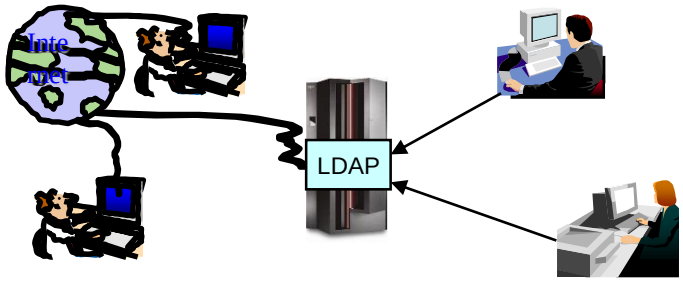
- **Grants the use of the BSTADMIN commands:**

```
LIST |LI <class-name> <profile-name>|* [GEN|NOGEN]
LISTG|LG <group-name>|*
LISTU|LU <user-id>
```

LDAP Signon Support



z/VSE 5.2: LDAP Tools



- **LDAP = Lightweight Directory Access Protocol**

- **z/VSE 4.2 added support for Sign-on using LDAP**
  - LDAP API implements a C language application interface to LDAP based on RFC 1823
  - The LDAP API implementation can be found in PRD1.BASE and it is referred to as IESLDAPH.H in z/VSE 4.2 System as C language header file

- **z/VSE V5.2 is now designed to give clients the flexibility to inspect and administrate the LDAP directory on the LDAP server from within the z/VSE system**

- **Batch tools are provided that support these LDAP functions on the LDAP directory:**
  - **LDAP search** to perform a search using specified filters
  - **LDAP add** to add an entry
  - **LDAP modify** to modify an entry
  - **LDAP delete** to delete one or more entries

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 Maintenance Dialogs have been connected to each other, leading you from User Definitions, to Group Maintenance 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

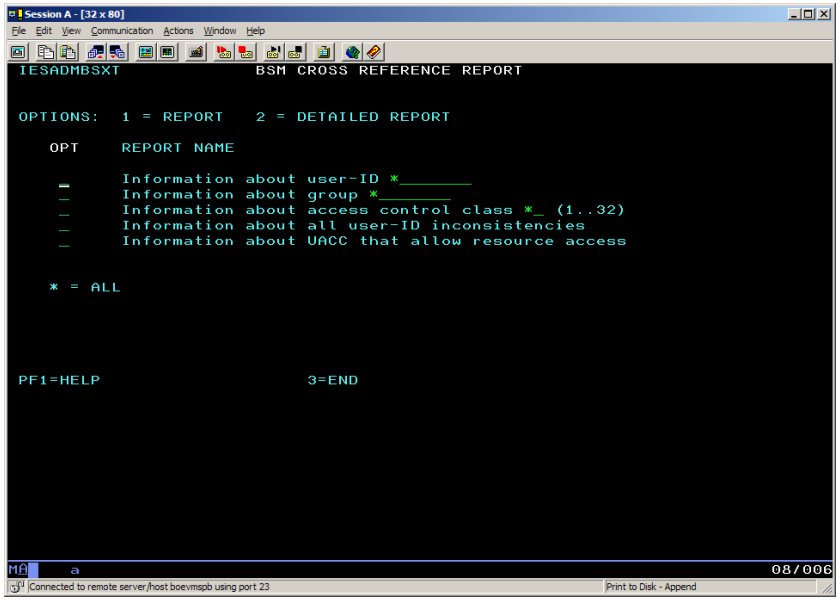
- Use the BSM Cross Reference Tool to find out where the user-ID is referenced (see separate foil)
- Perform a BSM Security Rebuild to activate the changes
- If you are using LDAP Authentication, you also need to update the user-ID in the LDAP mapping file via IESLDUMA

Group maintenance

- **Per default there are GROUP01 to GROUP64**
  - corresponding 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
  - z/VSE 5.2: BSM rejects the definition of new groups that have the same name as existing user IDs
- You can also use BSTADMIN to do this in batch.
- Perform a BSM Security Rebuild to activate the changes

BSM Cross Reference Tool

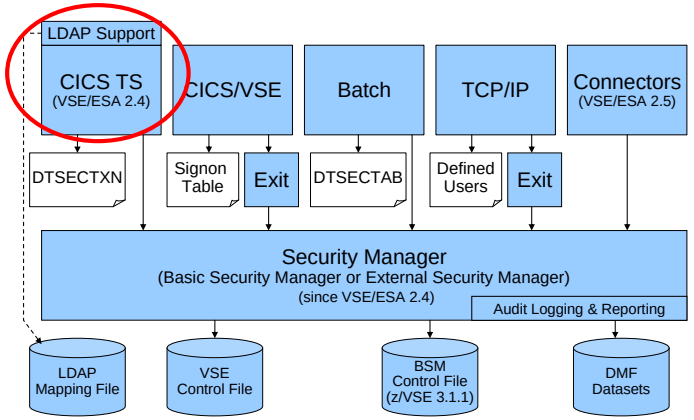
- The z/VSE BSM Cross Reference Tool is intended to help administrators control the profile definitions in the BSM control file.
- Example:
  - When you delete a user-ID, you can use it to ensure that you have removed the user-ID from all access lists and groups.
- The following functions are provided:
  - 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) → (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 resources**
  - 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)
ADD FCICSFCT FILEB UACC(NONE)
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 diagnostic 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

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

z/VSE 5.2: IDCAMS Command security

- IDCAMS tool provides a number of cluster management and catalog maintenance commands which can be destructive to data
  - To prevent data destruction, system administrators can restrict the usage of IDCAMS commands
- The administrator can control access to IDCAMS commands by using the 'IDCAMS.GENERAL' BSM resource profile of the resource class FACILITY
  - IDCAMS commands access control is designed for batch processing only
  - If batch security is not active (SYS SEC=NO) or IDCAMS function is executed in ICCF pseudo partition, then no security checks are performed

- The JCL sample below shows how to use BSTADMIN utility for defining the IDCAMS.GENERAL resource profile in BSM

```
// EXEC BSTADMIN
   ADD FACILITY IDCAMS.GENERAL UAC(READ)
   PERMIT FACILITY IDCAMS.GENERAL ID(USR1) ACCESS(UPD)
   PERMIT FACILITY IDCAMS.GENERAL ID(USR2) ACCESS(ALT)
   PERFORM DATASPACE REFRESH
   LIST FACILITY IDCAMS.GENERAL
/*
```

```
IESADMBSLE                    MAINTAIN SECURITY PROFILES
BSM RESOURCE CLASS: FACILITY     (START is Case Sensitive)     STATUS: ACTIVE
START....  DFHRCF.RSL24
OPTIONS:    1 = ADD          2 = CHANGE       5 = DELETE      6 = ACCESS LIST

   OPT    PROFILE NAME                          DESCRIPTION        UNIVERSAL AUDIT
                                               >                     ACCESS VALUE
    _      DFHRCF.RSL24                                                    12
    _      IBMVSE.JCL.ASSGN.PERM                                           12
    _      IBMVSE.JCL.LIBDEF.PERM                                          12
    _      IBMVSE.JCL.LIBDROP.PERM                                         12
    _      IBMVSE.JCL.OPTION.PARSTD                                        12
    _      IBMVSE.JCL.OPTION.STDLABEL                                      12
    6     *IDCAMS.GENERAL                                    2            12
```

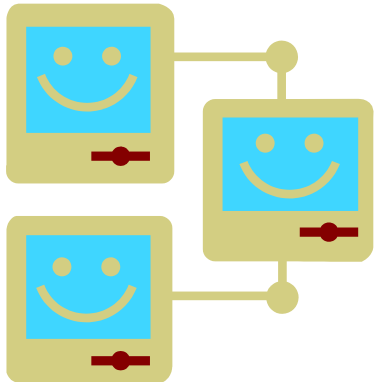
z/VSE 5.2: IDCAMS Command security

- **Users having *Read* authorization level are permitted to perform the following set of IDCAMS commands:**
  - LISTCAT - lists entries contained in a catalog
  - PRINT - lists a part or the whole VSAM file
  - BACKUP - produces a backup copy of one or more VSAM objects

- **Users having *Update* authorization level are permitted to perform commands:**
  - DEFINE CLUSTER|AIX|PATH|NONVSAM - defines cluster, alternate index or path
  - DELETE CLUSTER|AIX|PATH|NONVSAM - deletes cluster, alternate index or path
  - EXPORT/IMPORT - exports/imports cluster or alternate index
  - REPRO - copies data from one dataset to another
  - RESTORE - defines cluster (if required) and fills it with the data from the backup medium
  - BLDINDEX - builds one or more alternate indexes
  - VERIFY - verifies and corrects (if required) end-of-file information

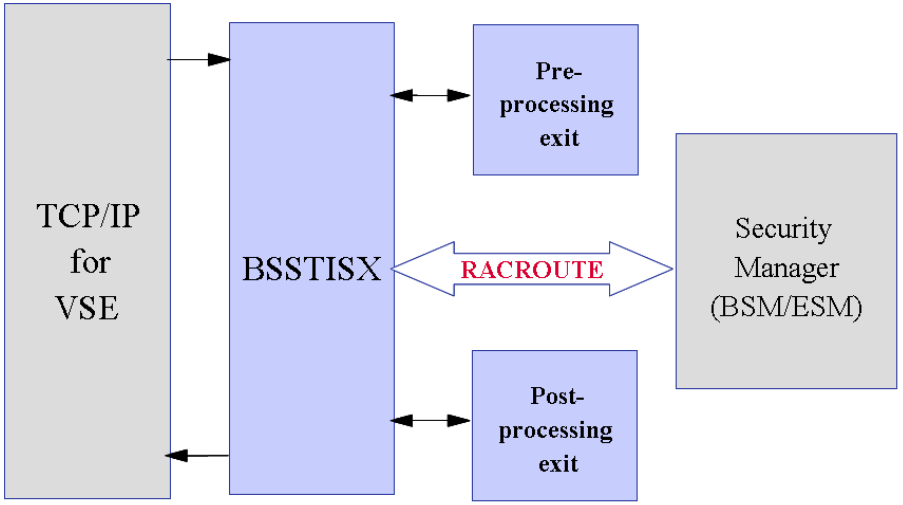
- **Users having *Alter* authorization level are permitted to perform commands:**
  - DEFINE MASTERCATALOG|USERCATALOG|SPACE - defines master catalog, user catalog, or space
  - DELETE MASTERCATALOG|USERCATALOG|SPACE - deletes master catalog, user catalog, or space
  - IMPORT DISCONNECT - disconnects user catalog from master catalog
  - EXPORT CONNECT - connects user catalog to master catalog
  - ALTER - changes attributes of catalog entries

TCP/IP Security



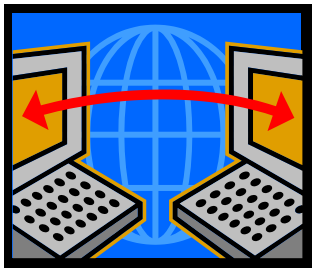
- **In general TCP/IP uses its own user id definitions**
  - Readable in initialization member (IPINITxx.L)
    - **`DEFINE USER,ID=user,PASSWORD=pwd`**
  - Duplicate user definitions

- **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



Cryptography and data encryption

Main areas of cryptography:



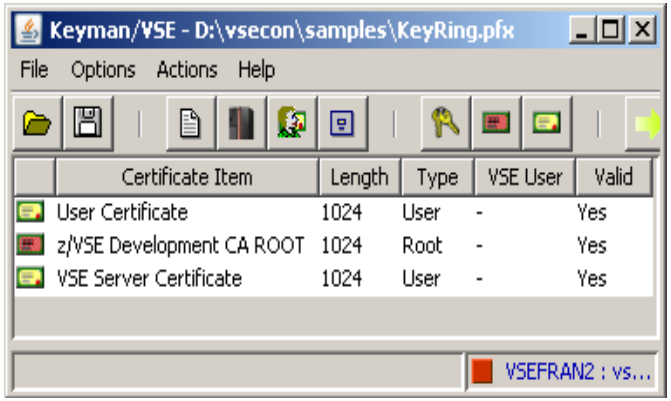
- **Encryption of data transmitted over network connections**
  - SSL, HTTPS
  - SecureFTP

- **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
  - TS1120/30/40 Encrypting Tape Drive
  - Encryption Facility for z/VSE

Key & Certificate Management

Cryptography 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

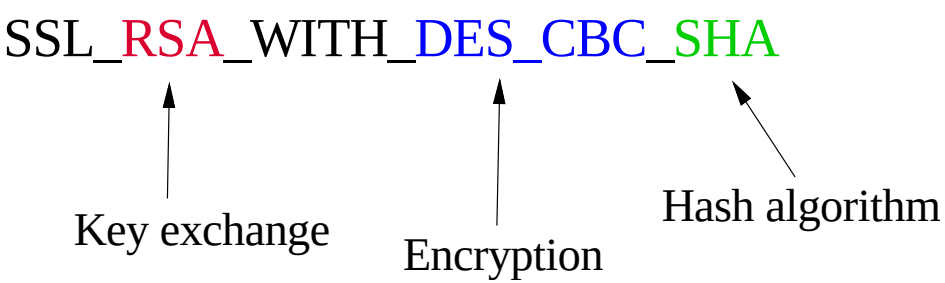
Certificates

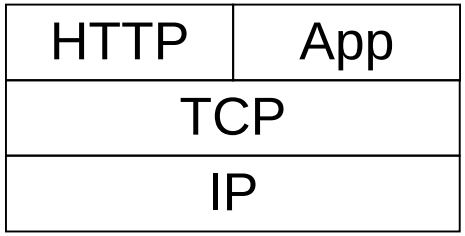
- **A certificate contains the following items**
  - The subject (name of the person)
  - The subject's public key
  - Period of validity
  - The issuer
  - Issuers signature

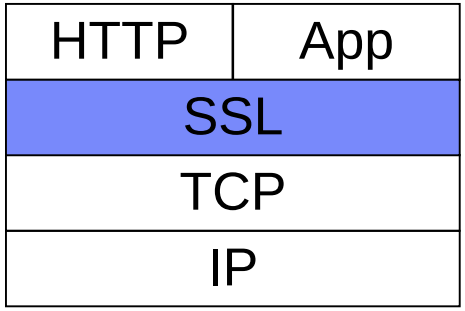
- **The issuer "signs" the certificate by encrypting a hash of the certificate content with his private key**
- **Everyone can check the sign by decrypting it with the issuers public key**
- **For production purposes, certificates are usually issued by a well known and trusted Certificate Authorities (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

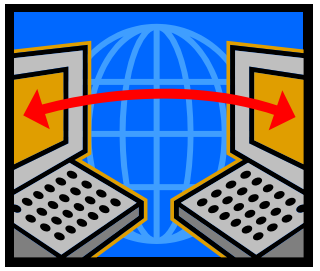
- **SSL provides a communication channel with message integrity, authentication, and confidentiality**
- **SSL is a widely used protocol**
  - Secure HTTP (HTTPS) is used very often in the Internet
- **SSL uses a TCP connection to transfer encrypted messages**
  - Uses asymmetric cryptography for session 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







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

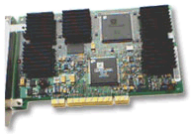
- **How to setup Secure FTP with VSE:**
  ftp://ftp.software.ibm.com/eserver/zseries/zos/vse/pdf3/How_to_setup_SecureFTP_with_VSE.pdf

Hardware Crypto Support on System z

z800, z900

PCICC(*)

PCICA



z890, z990

PCIXCC

CPACF

z9, z10

CEX2C CEX2A
configurable

PRNG,
protected-key CPACF

z196, z114

CEX3C CEX3A
configurable

CFB-mode

zEC12,
zBC12

CEX4C

CEX4A

CEX4P

z13

CEX5C

CEX5A

CEX5P

CCA Coprocessors
- RSA acceleration
- RSA key generation
- Random numbers

Accelerators
- RSA acceleration

EP11 Coprocessor
- PKCS#11
- Not exploited by VSE

On-board
crypto chip
- Symmetric encryption
- Hashing (SHA)

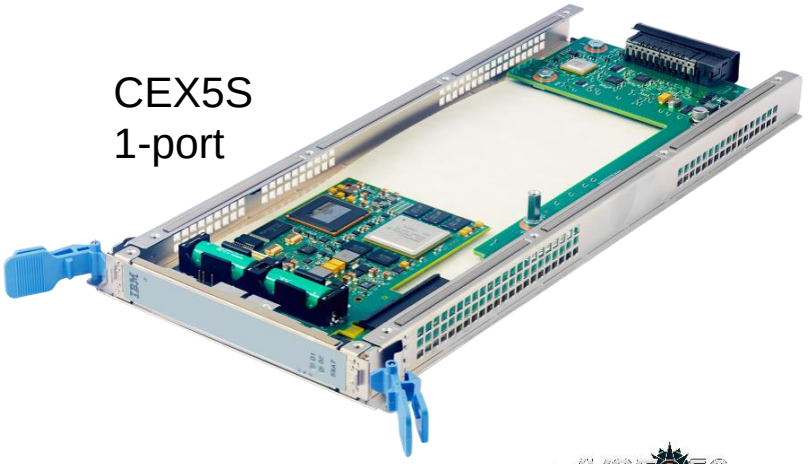
(*) PCICC was never supported by VSE

Crypto Express5S

- Exclusive to IBM z13
- One-port card, i.e. one AP (adjunct processor) per physical card
  - 2 cards min, 16 cards max per machine
- Seneca I/O cage (the 'S' in the name)
- Can be configured in one of three ways:
  - CEX5A: Accelerator
  - CEX5C: IBM Common Cryptographic Architecture (CCA) coprocessor
  - CEX5P: IBM Enterprise Public Key Cryptography Standards (PKCS) #11 (EP11) coprocessor
- Form factor comparison CEX3 / CEX4S/CEX5S:

CEX3
2-port

CEX5S
1-port



z/VSE Hardware Configuration

- **z/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 V5.1 plus PTFs – OpenSSL Support

- **What is OpenSSL?**
  - OpenSSL is an Open Source project providing an SSL implementation and key management utilities
  - Available for most Unix-style operating systems, MAC, Windows, and IBM System i (OS/400)
  - For details on OpenSSL refer to http://www.openssl.org/

- **Why OpenSSL on z/VSE?**
  - The TCP/IP stack from Connectivity Systems, Inc. has an own SSL implementation
  - What about the other two stacks:
    - IPv6/VSE from Barnard Systems, Inc.
    - Linux Fast Path (LFP) provided by IBM
  - All stacks could use one single SSL implementation: **OpenSSL**
  - OpenSSL is widely used in the industry
  - Latest RFC's implemented
  - One central place for access to crypto hardware, software updates, migration to higher versions

z/VSE V5.1 plus PTFs – OpenSSL Support

- **What is available on z/VSE?**
  - OpenSSL 1.0.1e runtime library (with PTF UD53983)
  - New component: z/VSE cryptographic services, 5686-CF9-17-51S
  - Available on z/VSE 5.1 plus PTFs
  - Software implementations for all algorithms with all key lengths
  - Hardware Crypto Support (Crypto Express cards and CPACF)
  - Programming APIs:
    - OS390 / z/OS compatible SSL API (gsk_initialize(), gsk_secure_soc_init(), etc.)
    - Subset of the OpenSSL API (LE/C)

- **OpenSSL Exploitation**
  - IPv6/VSE product exploits OpenSSL
    - **SSL Proxy Server** (BSTTPRXY)

      Proxies a clear text connection into an SSL/TLS connection and vice versa
    - **Automatic TLS Facility** (BSTTATLS)

      Automatically converts any application into SSL/TLS application

OpenSSL APARs and PTFs

http://www-03.ibm.com/systems/z/os/zvse/support/preventive.html#security

Security and system integrity related APARs/PTFs:

Last update: June 11, 2015

APAR Date	PTF	Contents
DY47610 2015/05/29	UD54118-52S	z/VSE V5.2: Security fixes for OpenSSL (Security issue with DH cipher suites)
DY47610 2015/05/29	UD54117-51S	z/VSE V5.1: Security fixes for OpenSSL (Security issue with DH cipher suites)
DY47602 2015/04/09	UD54106-52S	z/VSE V5.2: Security fixes for OpenSSL (CVE-2015-0286)
DY47602 2015/04/09	UD54105-51S	z/VSE V5.1: Security fixes for OpenSSL (CVE-2015-0286)
DY47591 2015/02/16	UD54091-52S	z/VSE V5.2: Security fixes for OpenSSL (CVE-2014-3572, CVE-2014-8275, CVE-2015-0204)
DY47591 2015/02/16	UD54090-51S	z/VSE V5.1: Security fixes for OpenSSL (CVE-2014-3572, CVE-2014-8275, CVE-2015-0204)
DY47581 2014/10/22	UD54072-52S	z/VSE V5.2: Security fixes for OpenSSL (CVE-2014-3567)
DY47581 2014/10/22	UD54071-51S	z/VSE V5.1: Security fixes for OpenSSL (CVE-2014-3567)
DY47561 2014/08/29	UD54054-52S	z/VSE V5.2: Security fixes for OpenSSL (CVE-2014-3509, CVE-2014-3511)
DY47561 2014/08/29	UD54053-51S	z/VSE V5.1: Security fixes for OpenSSL (CVE-2014-3509, CVE-2014-3511)
DY47545 2014/06/12	UD54037-52S	z/VSE V5.2: Security fixes for OpenSSL (CVE-2014-0224)
DY47545 2014/06/12	UD54036-51S	z/VSE V5.1: Security fixes for OpenSSL (CVE-2014-0224)
DY47534 2014/04/25	UD54027-52S	z/VSE V5.2: Security fixes for OpenSSL (CVE-2014-0160)
DY47532 2014/04/15	UD54020-51S	z/VSE V5.1: Security fixes for OpenSSL (CVE-2014-0160)
DY47516 2014/02/18	UD54005-51S	z/VSE V5.1: Security fixes for OpenSSL (CVE-2013-4353, CVE-2013-6449, CVE-2013-6450)

LE Multiplexer

- **The LE Multiplexer is used to specify the stack dependent phase implementing the TCP/IP socket API**
- **Skeleton EDCTCPMC in ICCF library 62 can be used as a template:**

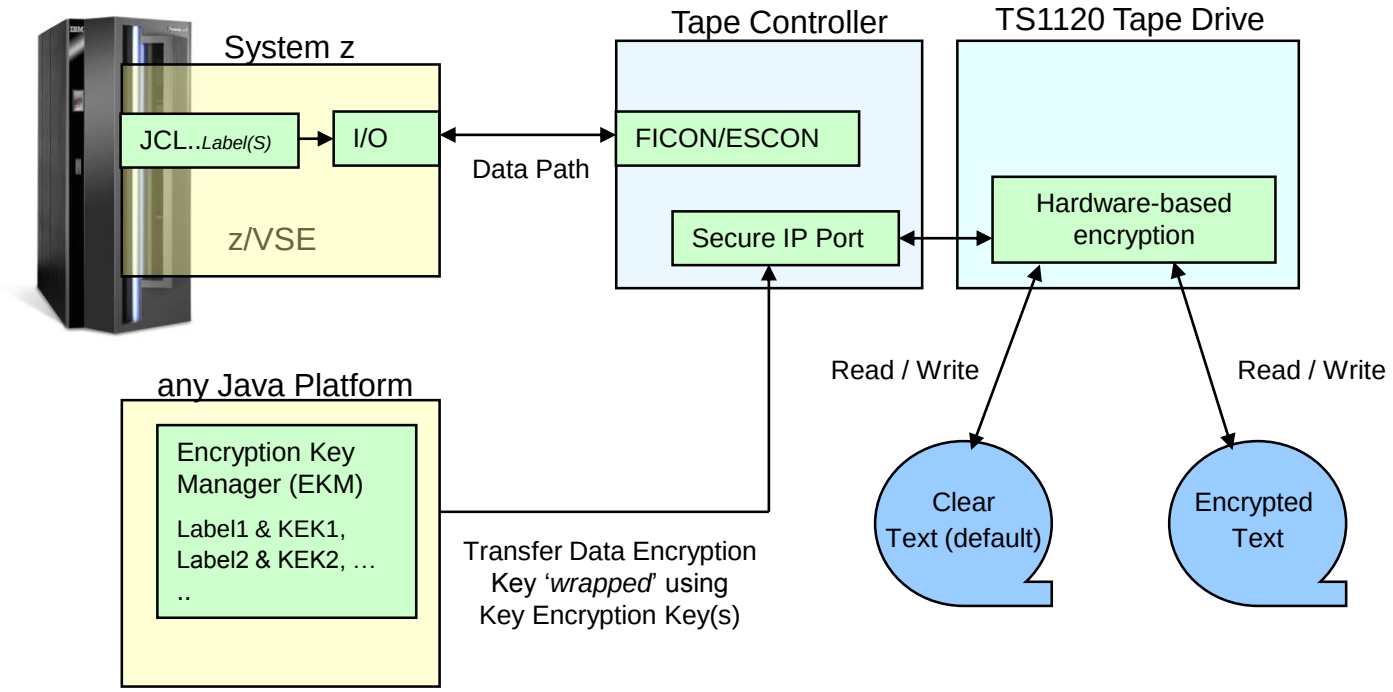
```
EDCTCPMC CSECT
EDCTCPMC AMODE ANY
EDCTCPMC RMODE ANY
*
         EDCTCPME SYSID='00',PHASE='$EDCTCPV'   <-- CSI
         EDCTCPME SYSID='01',PHASE='IJBLFPLE'   <-- LFP
         EDCTCPME SYSID='02',PHASE='BSTTTCP6'   <-- BSI
*
         END
```

- **z/VSE 5.2: New parameter SSLPHASE allows to specify the phase implementing the SSL API**
  - Now every combination of stack and SSL implementation (OpenSSL or CSI) can be used. (Default is phase name specified for PHASE)
  - Example: CSI stack with OpenSSL

```
EDCTCPME SYSID='00',PHASE='$EDCTCPV',SSLPHASE='IJBSSLLE'
```

Note: Only applicable for LE/C applications

IBM Tape Encryption – TS1120 & TS1130 & TS1140



encryption mode
(03=write)

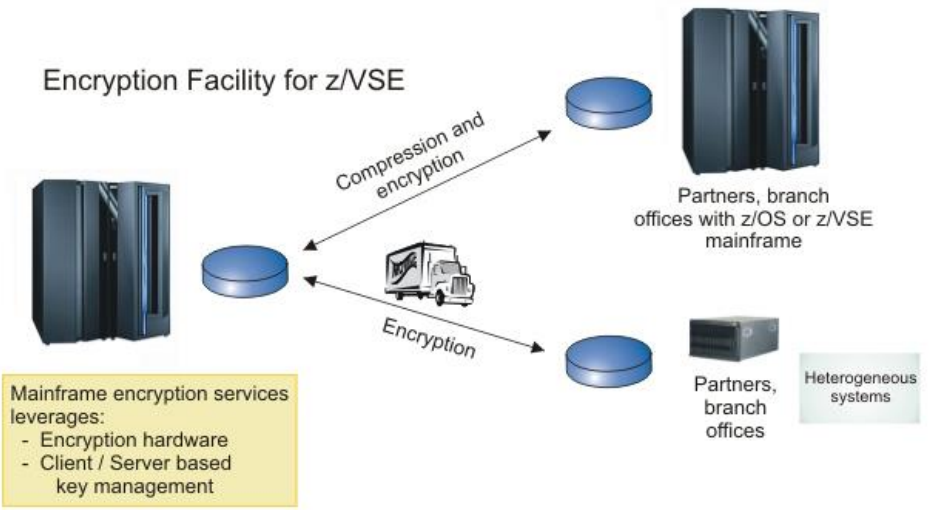
```
// JOB ENCRYPT
// ASSGN SYS005,480,03
// KEKL UNIT=480,KEKL1='MYKEKL1',KEM1=L,KEKL2='MYKEKL2',KEM2=L
// EXEC LIBR
  BACKUP LIB=PRD2 TAPE=SYS005
/*
/&
```

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

Technical articles on VSE homepage

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

How to setup hardware crypto and SSL with z/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: November 2010
  Joerg Schmidbauer, IBM
- How to setup SSL with CICS Web Support (PDF, 1.7MB)
  Updated: November 2010
  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, 1.2MB)
  Updated: November 2010
  Joerg Schmidbauer, IBM
- How to setup and use Keyman/VSE (PDF, 650KB)
  New: November 2010
  Joerg Schmidbauer, IBM
- How to setup cryptographic hardware for VSE (PDF, 1.4MB)
  Updated: December 2008
  Joerg Schmidbauer, IBM

Related Documentation

- 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 ?