# z/VSE Security Concepts and Update

Ingo Franzki
ifranzki@de.ibm.com

# Trademarks

The following are trademarks of the International Business Machines Corporation in the United States and / or other counties.

- CICS*
- DB2*
- DB2 Connect
- DB2 Universal Database
- e-business logo*
- Enterprise Storage Server
- HiperSockets
- IBM*
- IBM logo*
- IMS
- Intelligent Miner
- Multiprise*
- MQSeries*
- OS/390*
- S/390*
- SNAP/SHOT*
- Virtual Image Facility
- VM/ESA*
- VSE/ESA
- VisualAge*
- VTAM*
- WebSphere*
- xSeries
- z/Architecture
- z/VM
- z/VSE
- zSeries

* Registered trademarks of IBM Corporation

The following are trademarks or registered trademarks of other companies.

LINUX is a registered trademark of Linus Torvalds

Tivoli is a trademark of Tivoli Systems Inc.

Java and all Java-related trademarks and logos are trademarks of Sun Microsystems, Inc., in the United States and other countries

UNIX is a registered trademark of The Open Group in the United States and other countries.

Microsoft, Windows and Windows NT are registered trademarks of Microsoft Corporation.

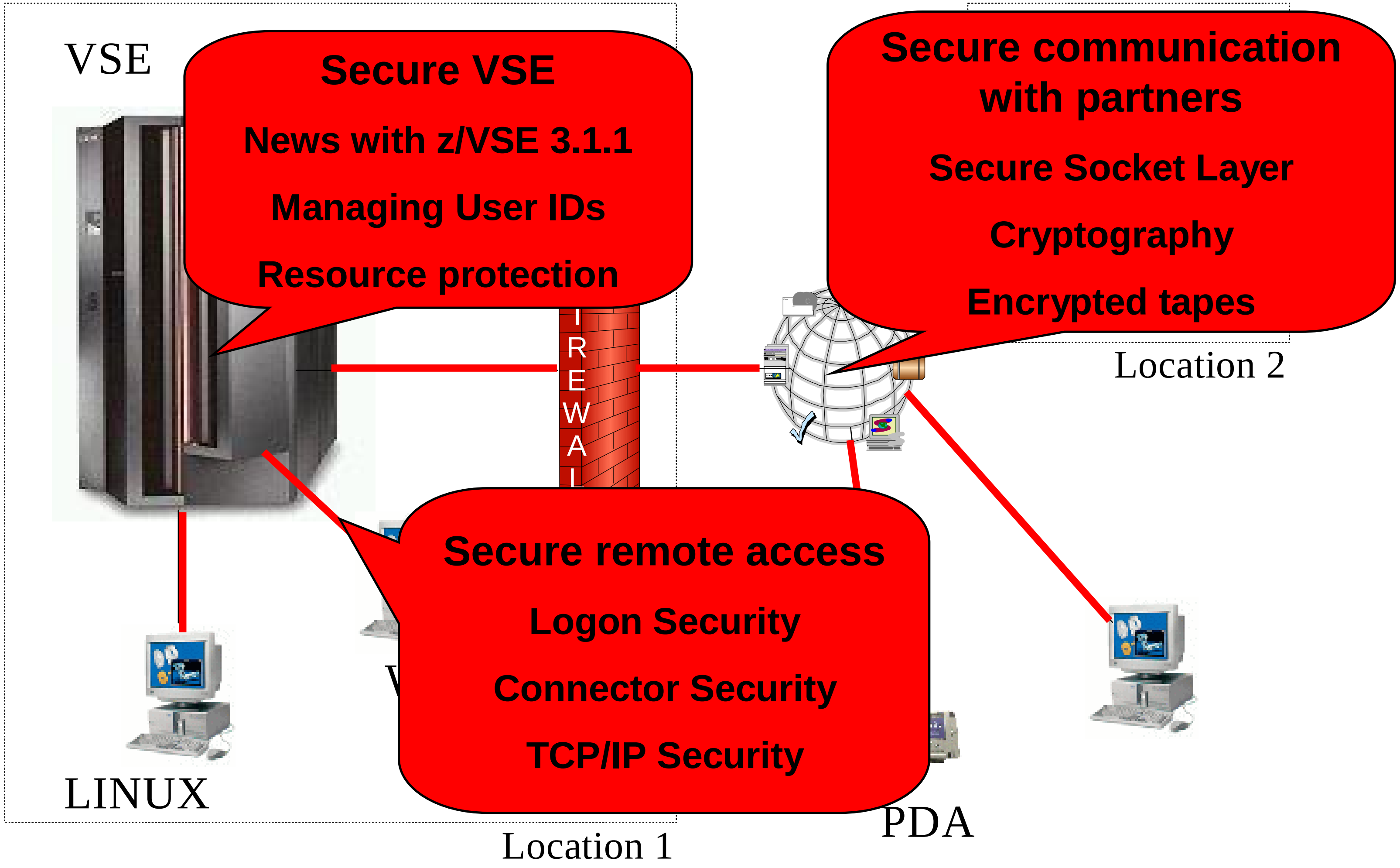
SET and Secure Electronic Transaction are trademarks owned by SET Secure Electronic Transaction LLC.

Intel is a registered trademark of Intel Corporation.

# 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

# Security in a heterogeneous environment



**Secure VSE**

**News with z/VSE 3.1.1**

**Managing User IDs**

**Resource protection**

**Secure communication with partners**

**Secure Socket Layer**

**Cryptography**

**Encrypted tapes**

**Secure remote access**

**Logon Security**

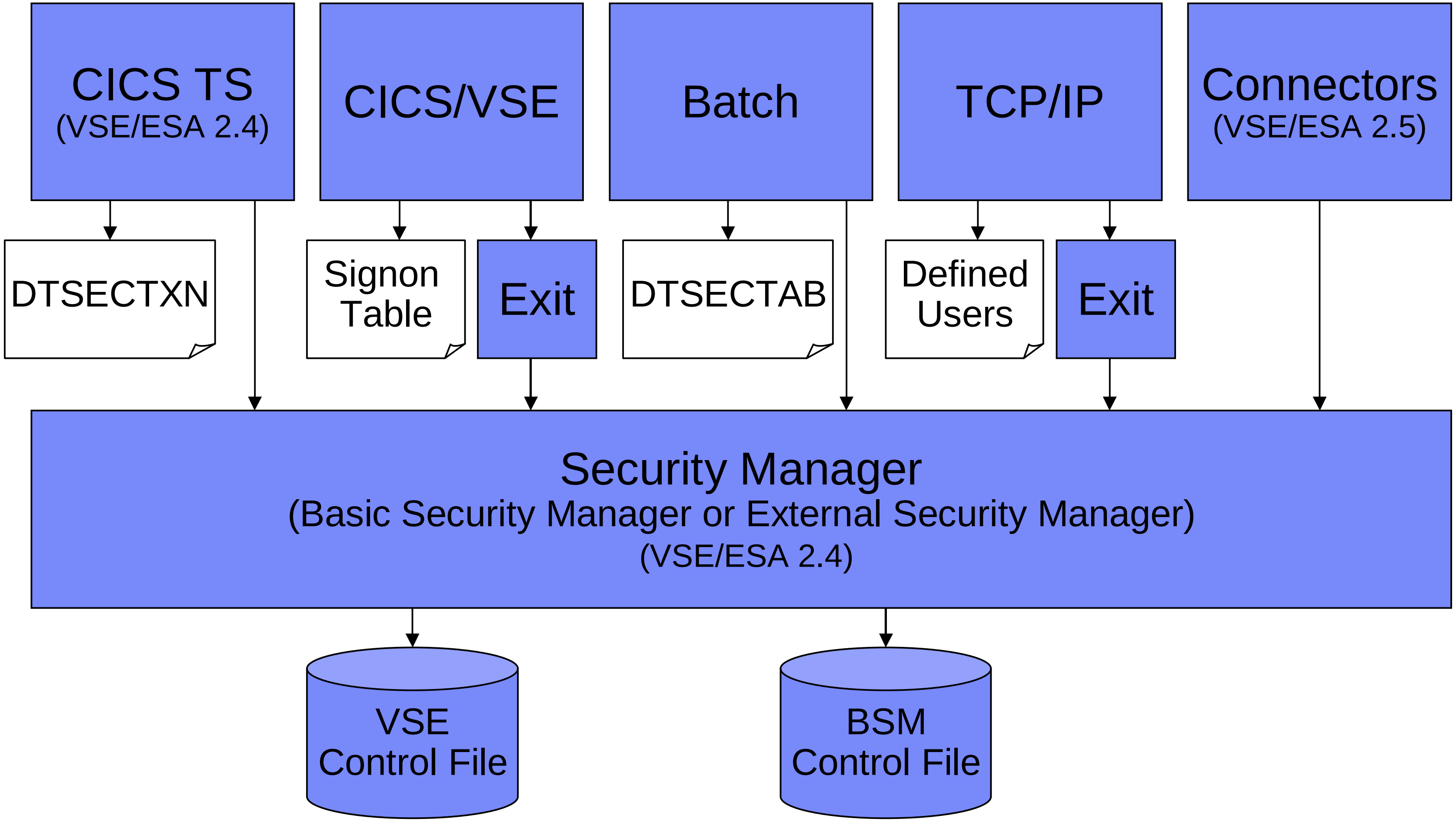
**Connector Security**

**TCP/IP Security**

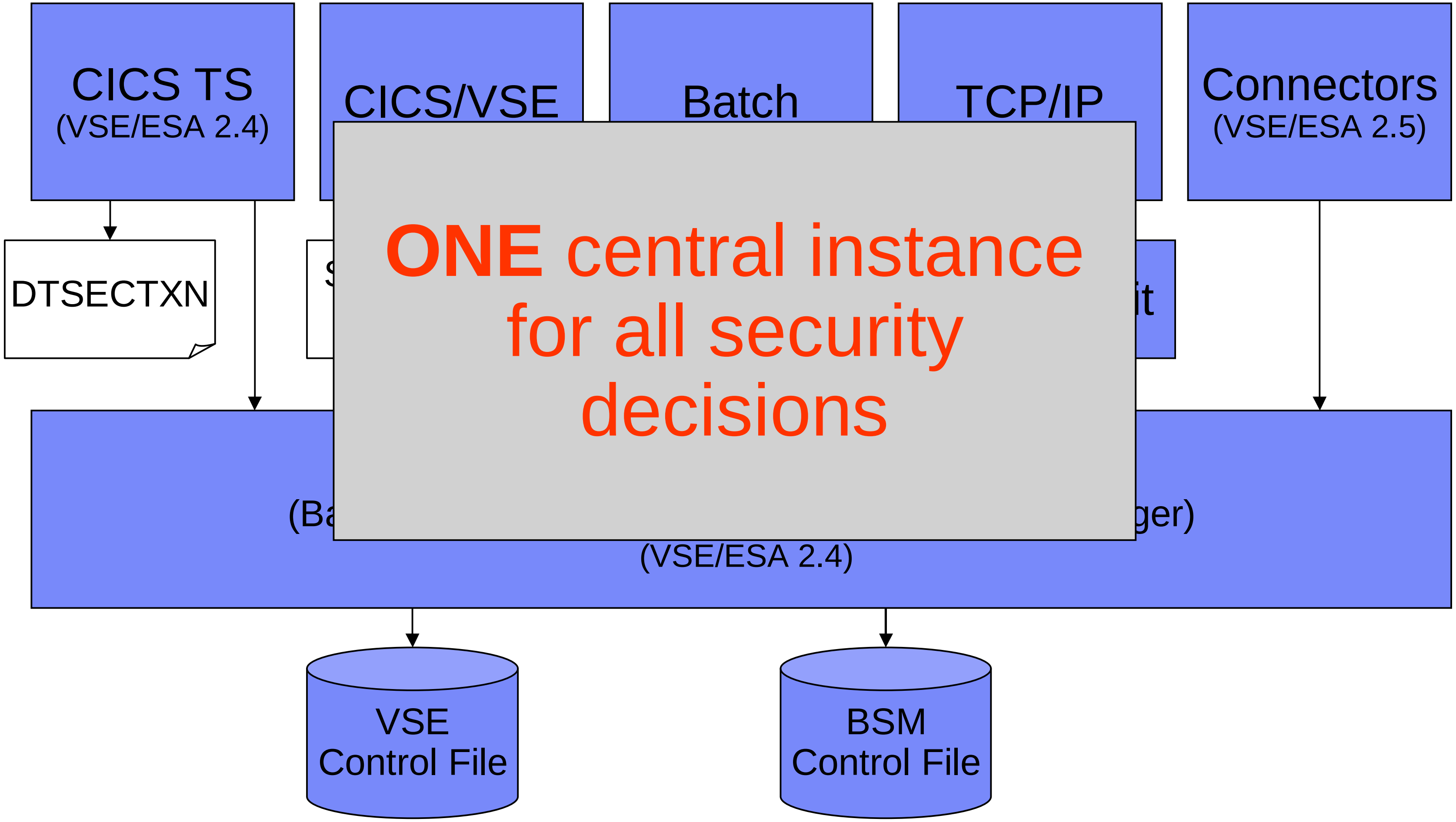
# Why secure VSE ?

- **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

# VSE Security Components



# VSE Security Components



**ONE** central instance for all security decisions

# Basic Security Manager – New with z/VSE 3.1.1

- User Groups
  - Users can be grouped into groups
  - Permissions can be given on groups or individual users
- Description field for all profiles (20 characters)
- New admin functions
  - BSTADMIN (console or batch)
  - Interactive Interface Dialogs
- New resource classes

| | |
|---|---|
| TCICSTRN | - Transactions (as on VSE/ESA 2.7) |
| MCICSPPT | - Application programs |
| FCICSFCT | - Files |
| JCICSJCT | - Journals |
| SCICSTST | - Temporary storage queues |
| DCICISDCT | - Transient data queues |
| ACICSPCT | - Transactions (CICS START) |
| APPL | - Applications |
| FACILITY | - Miscellaneous resources |

# Basic Security Manager – New with z/VSE 4.1

## § Audit-Logging and Reporting

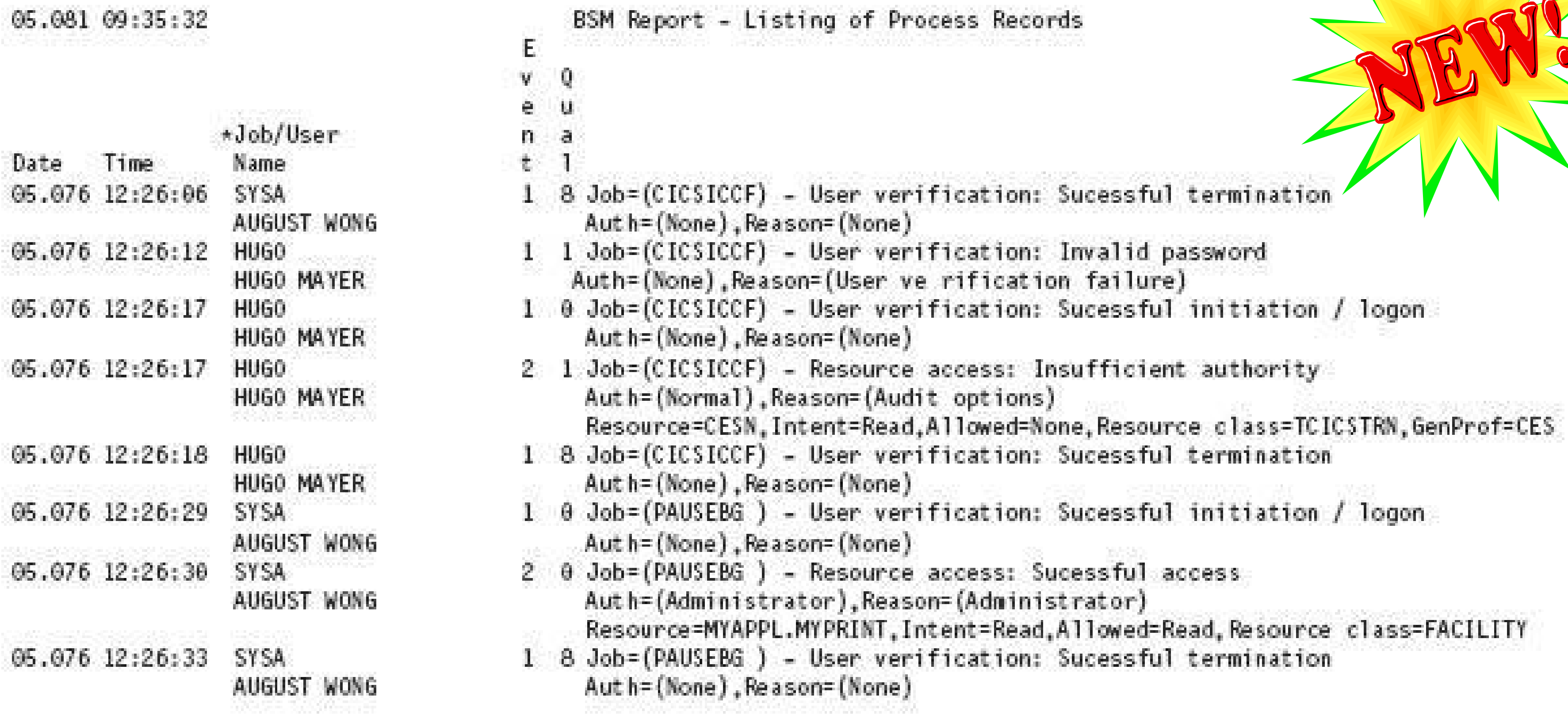
- All access attempts to protected resources can be logged
  - Allowed access as well as disallowed access
- Possible attacks can be detected
  - E.g. multiple logon attempts with invalid password
- You can comprehend who did when access which resource
- Analysis can be done using a reporting tool
  - Summary report
  - Detailed report of all access attempts
- Uses the CICS DMF Tool
  - Creates SMF records containing logging information

# Audit-Logging and Reporting - New with z/VSE 4.1

- **To activate logging for a specific resource, you need to specify the AUDIT option (BSTADMIN) on the resource profile**
  - AUDIT(***audit-level***)
    - **ALL**
      - Specifies that all authorized accesses and detected unauthorized access attempts should be logged.
    - **FAILURES**
      - Specifies that all detected unauthorized access attempts should be logged (the Default).
    - **SUCCESS**
      - Specifies that all access attempts that were authorized should be logged.
    - **NONE**
      - Specifies that no logging should be done.
- Note: You should use the auditing function with care. It will increase the BSM and DMF processing and might negatively affect the performance of your z/VSE system!

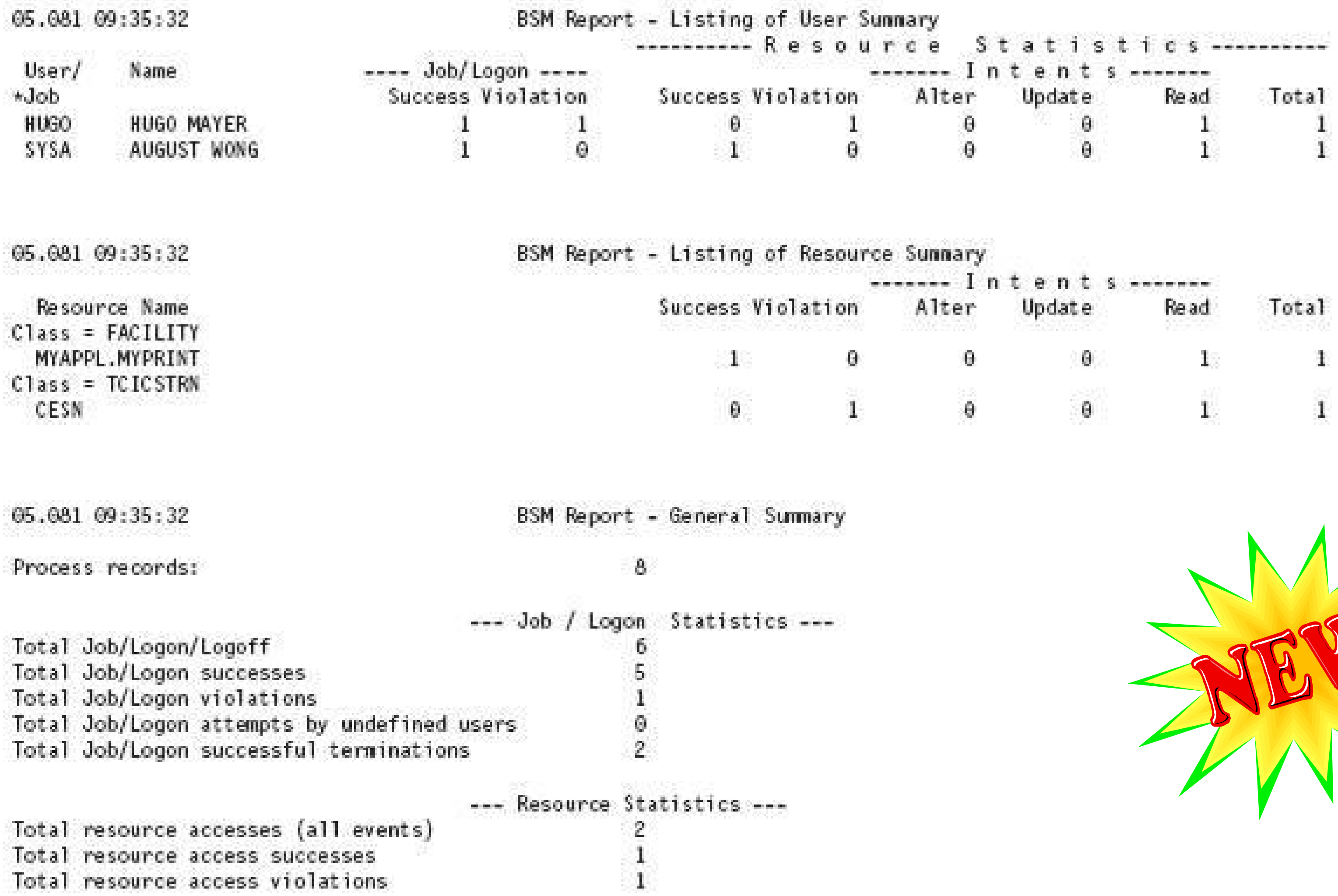
# Audit-Logging and Reporting - New with z/VSE 4.1

NEW!



```
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=Read,Allowed=None,Resource class=TCICSTRN,GenProf=CES
05.076 12:26:18   HUGO                 1  8 Job=(CICSICCF) - User verification: Sucessful termination
                  HUGO MAYER                Auth=(None),Reason=(None)
05.076 12:26:29   SYSA                 1  0 Job=(PAUSEBG ) - User verification: Sucessful initiation / logon
                  AUGUST WONG               Auth=(None),Reason=(None)
05.076 12:26:30   SYSA                 2  0 Job=(PAUSEBG ) - Resource access: Sucessful access
                  AUGUST WONG               Auth=(Administrator),Reason=(Administrator)
                                            Resource=MYAPPL.MYPRINT,Intent=Read,Allowed=Read,Resource class=FACILITY
05.076 12:26:33   SYSA                 1  8 Job=(PAUSEBG ) - User verification: Sucessful termination
                  AUGUST WONG               Auth=(None),Reason=(None)
```

# Audit-Logging and Reporting - New with z/VSE 4.1



```
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
```

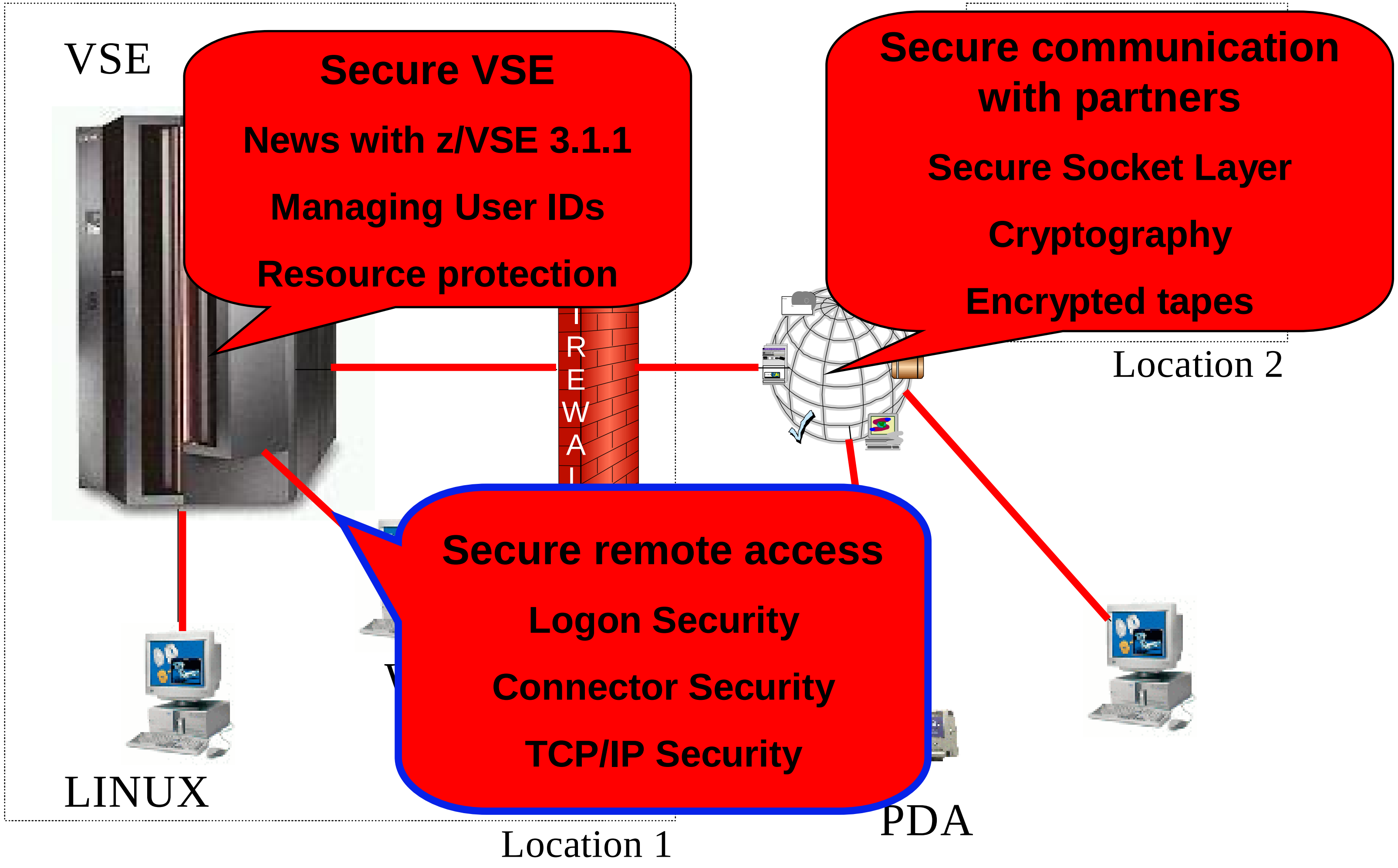
# CICS TS Security

- **Sign on Security**
  - Logon only possible for authorized users
  - Permissions for applications and resources based on user-id
- **Resource Security**
  - CICS Resources (e.g. files, applications, … ) can be protected
  - Permissions can be assigned very granularly
- **Definition within single resource definition (e.g. file FILEA and FILEB)**
  - Within 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`

# Batch Security

- **Only entitled users are allowed to execute jobs**
- **Jobs run under the specified user id**
  - Protects from disallowed access and/or modification of data
  - The job inherits the permissions from the user it is running under
- **ID statement or * $$ JOB specifies user id and password for a job**
  - Subsystems (LIBR, VSAM, ...) uses this user id to verify access permissions
  - Requites SYS SEC=YES in IPL Procedure

# Security in a heterogeneous environment



**Secure VSE**

**News with z/VSE 3.1.1**

**Managing User IDs**

**Resource protection**

**Secure communication with partners**

**Secure Socket Layer**

**Cryptography**

**Encrypted tapes**

**Secure remote access**

**Logon Security**

**Connector Security**

**TCP/IP Security**

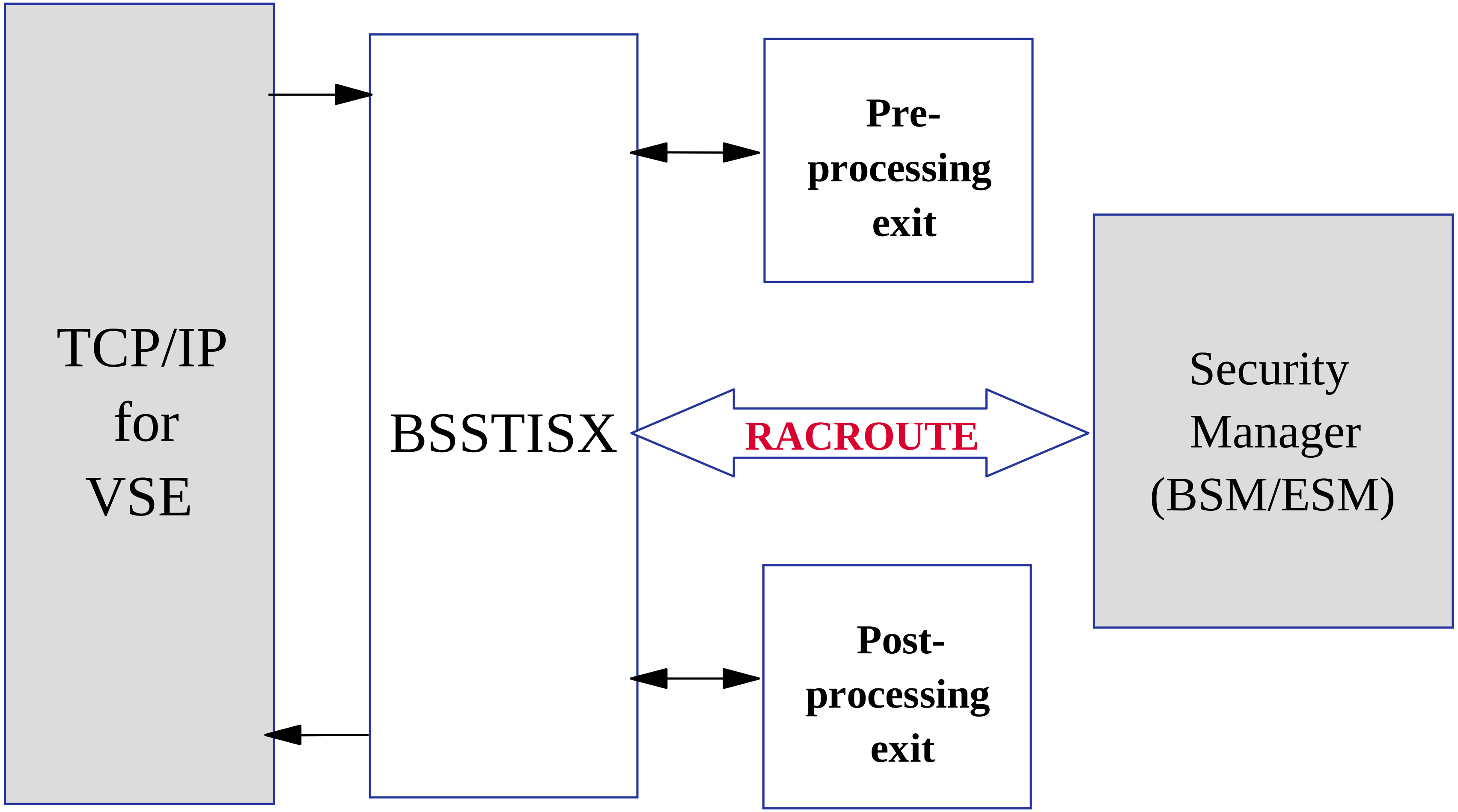
# Why secure remote access ?

- **Today most computers are part of a network**
  - Distributed processes require exchange of data between these systems
  - Data transfer must be secure and reliable
  - Other systems require access to VSE data and applications
  - Even in a company’s internal network, that is treated as relatively secure, you will find viruses and worms
  - The most dangerous attacks are those from inside the company (e.g. frustrated employees)
- **Prevent unauthorized access to VSE and data**
  - Requires to authenticate the user (logon)
  - Secure communication for confidential data
- **Using FTP you can access productions data**
  - E.g. VSAM, POWER Lists

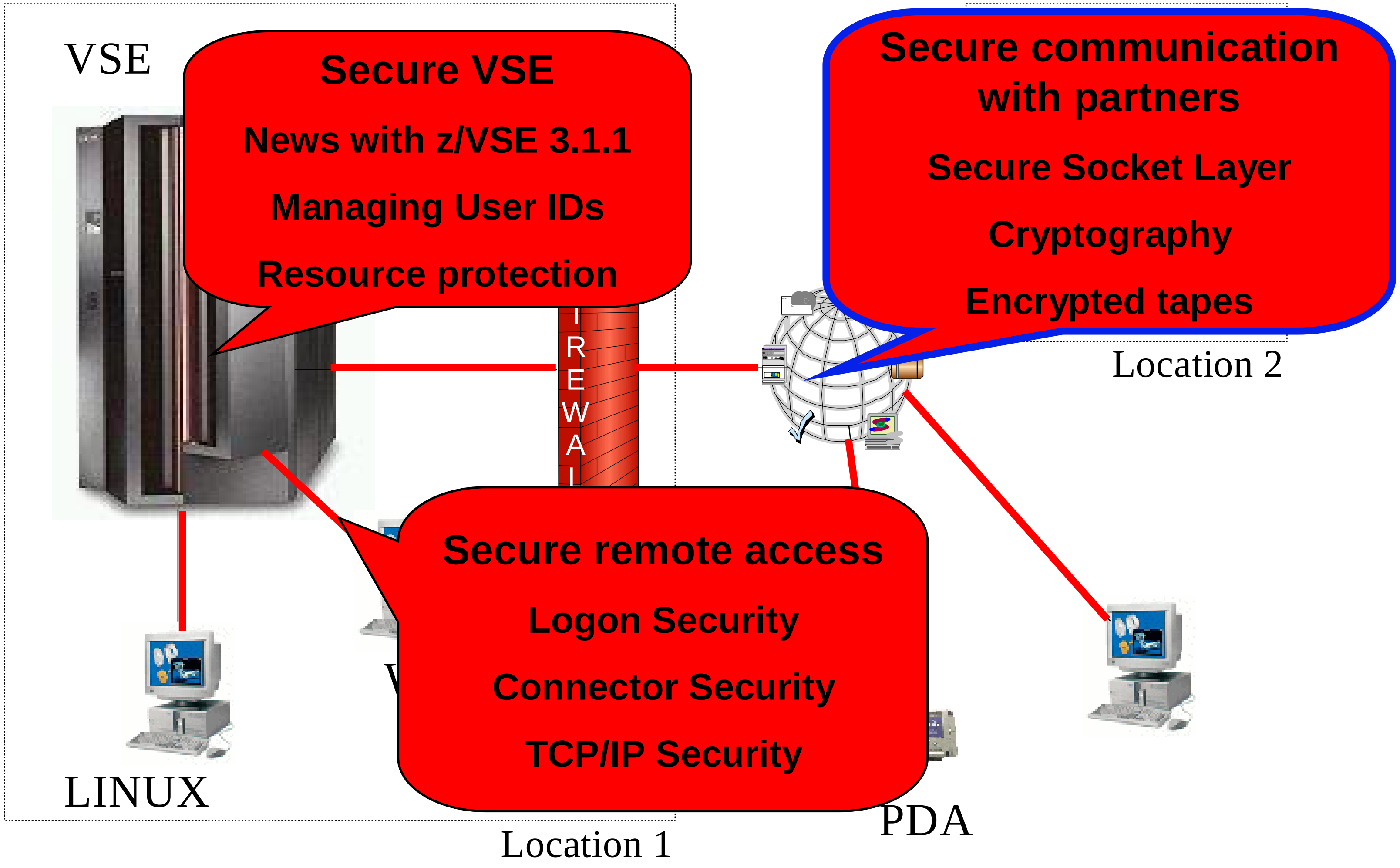
# TCP/IP Security

- **In general TCP/IP uses its own user id definitions**
  - DEFINE USER,ID=user,PASSWORD=pwd
  - Readable in initialization member (IPINITxx.L)
  - Duplicate user definitions
- **Security Exit available from IBM to check the user ids and resource access via Security Manager**
  - Checks user id during logon
  - Checks resource access permissions
- **The most attacks are today coming through TCP/IP**
  - It is important to focus on this area

# TCP/IP Security Exit



# Security in a heterogeneous environment



**Secure VSE**

**News with z/VSE 3.1.1**

**Managing User IDs**

**Resource protection**

**Secure communication with partners**

**Secure Socket Layer**

**Cryptography**

**Encrypted tapes**

**Secure remote access**

**Logon Security**

**Connector Security**

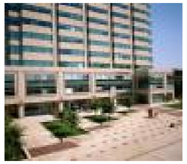
**TCP/IP Security**

# Customer Data Protection Requirements

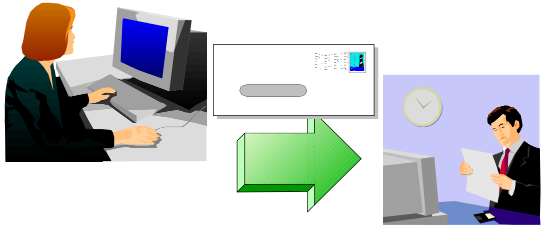
- Regulatory requirements driving need for greater data security, integrity, retention/auditability, and privacy
- Severe business impacts caused by loss or theft of data including financial liability, reputation damage, legal/compliance risk
- Increasing need to share data securely with business partners and maintain backups at remote locations
- Need to reduce complexity and improve processes around enterprise encryption management
- Need ability to cost effectively encrypt large quantities of tape data

Secondary Site

Business Partners



# Cryptography - what can it do for you?



- **Keeping secrets**
  - Alice wants to send Bob confidential information,
  - Charly should not be able to read it.
- **Proving identity**
  - Bob receives a message from Alice. How he can be sure that it is really from Alice?
- **Verifying information**
  - Bob receives a message from Alice. How he can be sure that the content has not been modified?

- **Encryption of data transmitted over TCP/IP connections**
  - SSL, HTTPS
  - SecureFTP
- **Encryption of data stored on disk or tape**
  - Encryption of backups or archives
  - Signing of data
  - Exchange of encrypted and/or signed data with customers or business partners

# 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
    - 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, 3DES and AES encryption and SHA-1 secure hash functions**
  - SecureFTP is integrated into TCP/IP for VSE with z/VSE V4.1 or as separate product

# Hardware Crypto Support on System z and VSE

by release

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

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

by server

CEX2C = Crypto Express2 in coprocessor mode
CEX2A = Crypto Express2 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 even TCP/IP applications**
  - But use of crypto hardware can be disabled via TCP/IP SOCKOPT phase

```
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.
```

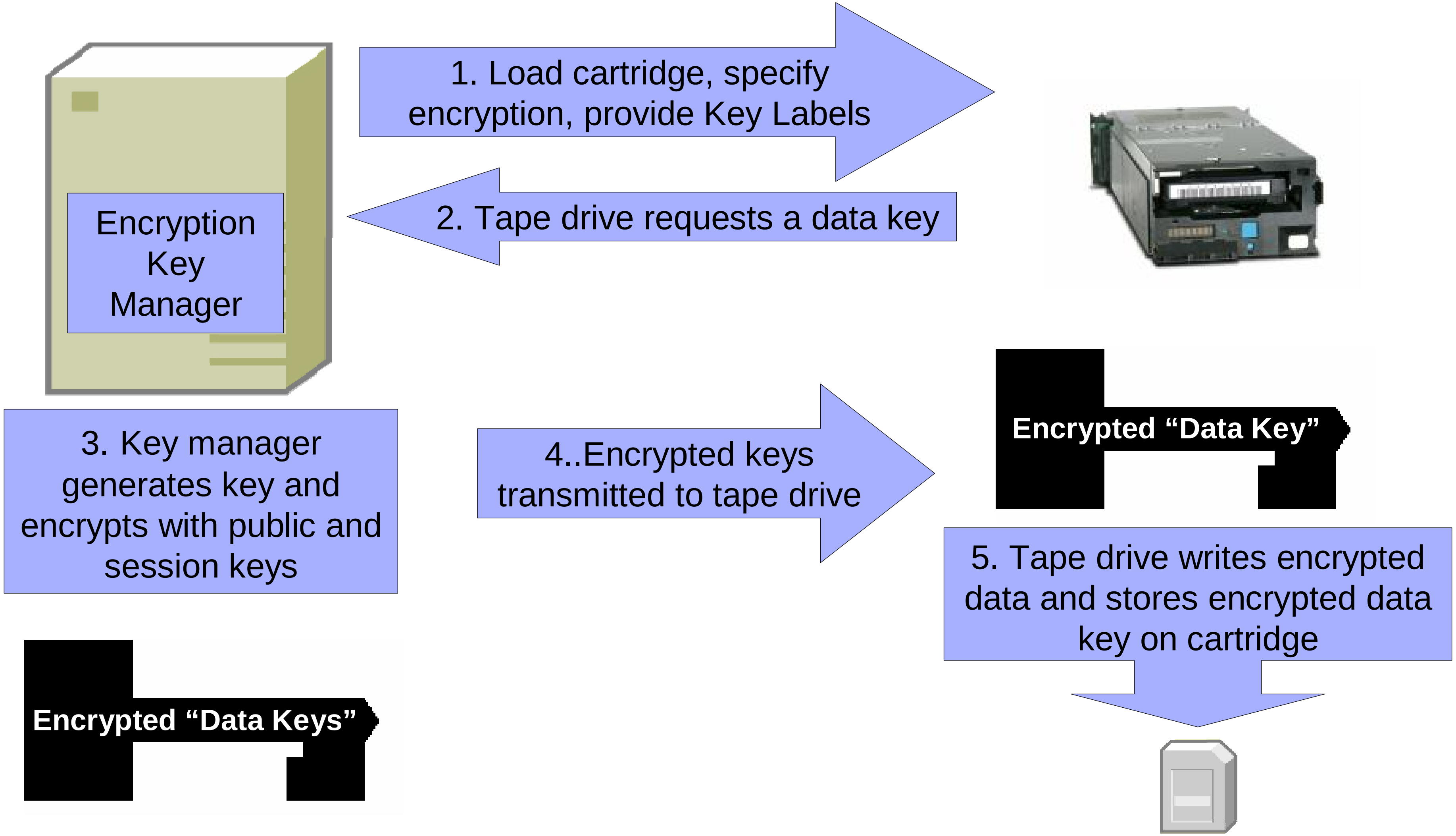
# Crypto HW exploitation in VSE

- **Pluggable crypto cards are used for RSA acceleration only**
  - RSA decrypt/encrypt for SSL session initiation
  - RSA encrypt for signing of certificates (CIALCREQ)
- **CPACF**
  - Acceleration of symmetric algorithms:
    DES, TDES, AES-128 (z9 only), SHA-1
  - Used at
    - SSL/SFTP data transfer
    - CIAL functions in TCP/IP
- **Usage is transparent for TCP/IP applications**
  - If Crypto HW is available, it will be used. If not available, the SW implementation (as part of TCP/IP) will be used
  - Crypto operations are faster by factors when using hardware acceleration

# IBM Tape Encryption – TS1120

- **The IBM System Storage TS1120 Tape Drive has been enhanced to provide drive based data encryption**
  - A new, separate IBM Encryption Key Manager component for the Java Platform (Encryption Key Manager) program is also being introduced
    - supports the generation and communication of encryption keys for the tape drives across the enterprise.
- **The announcement contains a Statement of Direction concerning z/VSE support:**
  - *z/VSE V3.1 support of the TS1120 Tape Drive with encryption is planned for first half 2007. It is also IBM's intent to support z/VSE V4.1 (when made available) using Systems Managed Encryption with the TS1120. z/VSE support will require the Encryption Key Manager component running on another operating system other than z/VSE using an out-of-band connection.*
- **For more information, please see the hardware announcement letter**
  - ENUS106-655

# IBM Tape Encryption – TS1120



1. Load cartridge, specify encryption, provide Key Labels

2. Tape drive requests a data key

Encryption Key Manager

3. Key manager generates key and encrypts with public and session keys

4..Encrypted keys transmitted to tape drive

Encrypted “Data Key”

5. Tape drive writes encrypted data and stores encrypted data key on cartridge

Encrypted “Data Keys”

# IBM Tape Encryption – TS1120

encryption mode
(03=write)

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

encoding mechanism
(L=Label, H=Hash)

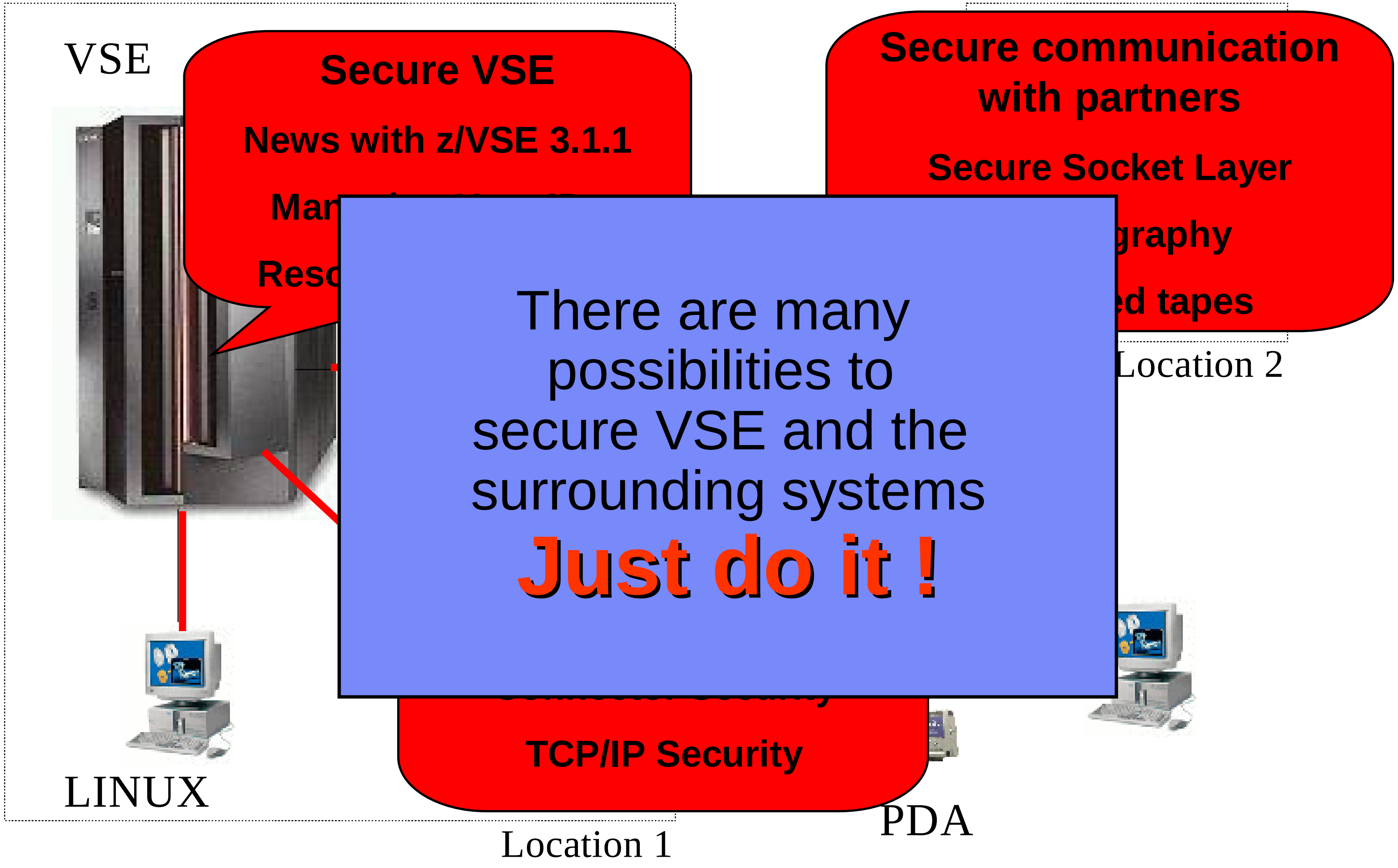
key label1
(name of the 1. KEK-key in EKM)

- The Data-Key can be encrypted using 2 different public keys (KEK = Key Encrypting Keys), to be able to send the tape to 2 different receivers
- More info can be found in the *z/VSE 4.1 Administration* manual (VSE Homepage)

# Other ways to encrypt your backups or tapes

- **Can be done 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 or OpenPGP)
    - 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

# Security in a heterogeneous environment



**Secure VSE**

**News with z/VSE 3.1.1**

**Man**

**Reso**

**Secure communication with partners**

**Secure Socket Layer**

**graphy**

**ed tapes**

**TCP/IP Security**

There are many possibilities to secure VSE and the surrounding systems

**Just do it !**

# Thank you for listening

Thank

You !

## Catch the WAVV

WAVV Conference
Green Bay, Wisconsin
May 18-22, 2007
Regency Suites Hotel

Register now: http://www.wavv.org