Security-Aspekte im z/VSE 3.1 (Batch/Online)

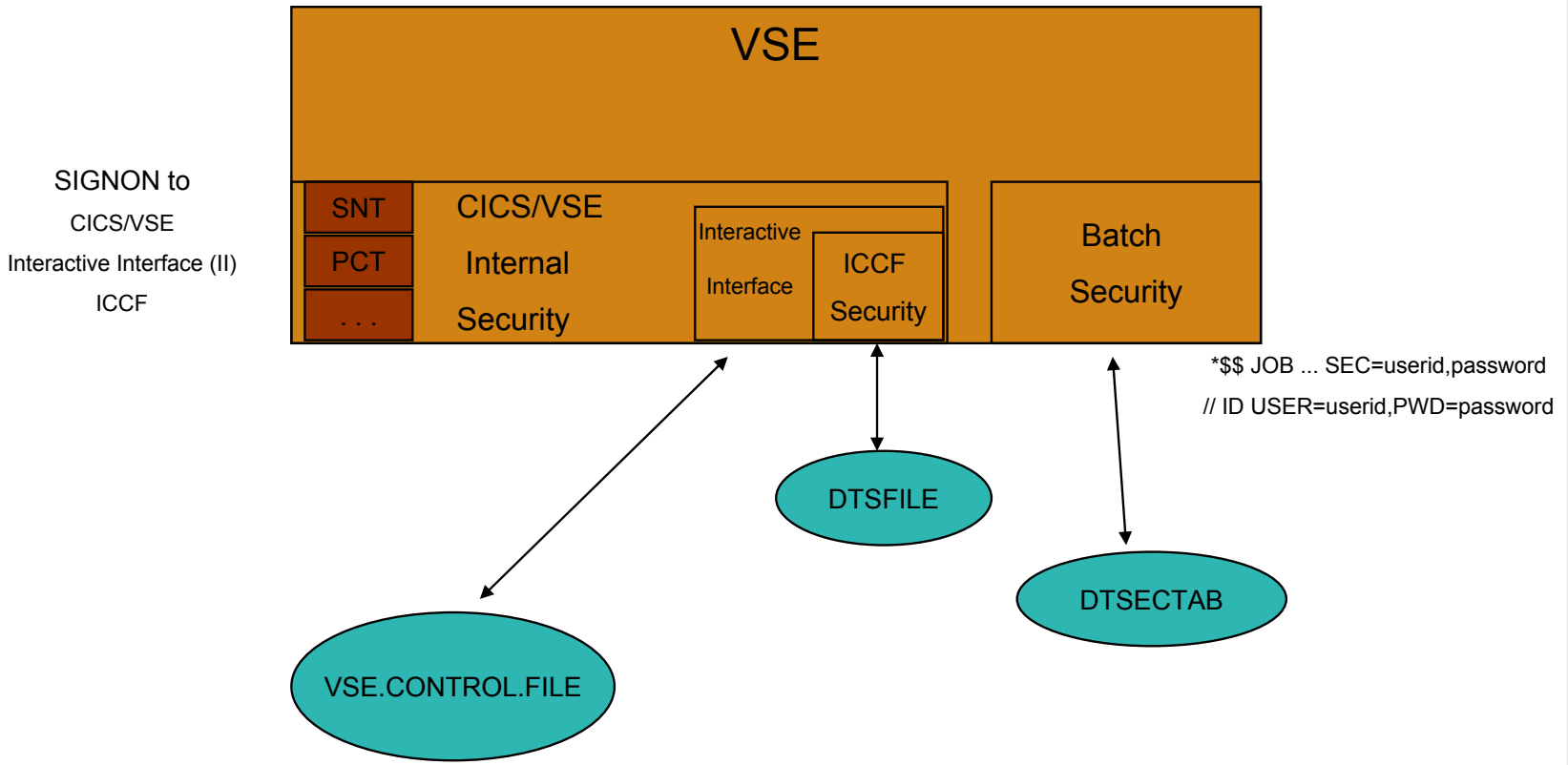
VM / VSE / Linux für zSeries

GSE-Herbsttagung 24. – 26. Okt. 2005

Dagmar Kruse und Hans Joachim Ebert
IBM Technical Sales zSeries
dkruse@de.ibm.com, eberthj@de.ibm.com

ON DEMAND BUSINESS™

VSE Security Structure with VSE/ESA 2.3 (or below)



CICS/VSE Internal Security

- **User IDs in CICS signon table (DFHSNT)**
- **CICS transaction security: 64 security keys**
  - 1 = public transaction
  - 64 = Interactice interface transaction
- **CICS resource security:**
  - 24 resource keys plus PUBLIC for resources
    - Application, Files, Journals, Temporary storage queues, Transient data queues,Transaction initiated by CICS START command

VSE Security Structure with VSE/ESA 2.3 (or below)

- **VSE.CONTROL.FILE:**
  - Repository file of **Interactive Interface**, it contains records auch as:
    - User profile records
    - Selection panel records
    - Application profile records
    - Synonym records
    - News records (messages displayed to users after they sign on)
    -
  - The user profile information provides coordination between CICS/VSE, VSE/ICCF and the Interactive Interface.

- **DTSFILE:**
  - Repository file of **ICCF,** it contains records for
    - ICCF User IDs (4 characters) and ICCF files

- **DTSECTAB:**
  - Repository file of **BATCH-Jobs,** it contains records for
  - User IDs (8 characters)
  - Access rights to libraries, sublibraries, members, VSAM-files

VSE Security Structure with VSE/ESA 2.4 – 2.7, z/VSE 3.1.0

- **CICS/VSE Security Structure is unchanged**

- **CICS TS Security:**
  - No internal security
  - RACROUTE calls to an external security manager (BSM/ESM) for decision of:
    - Signon of CICS users
    - CICS transactions
    - CICS resources
    - ...

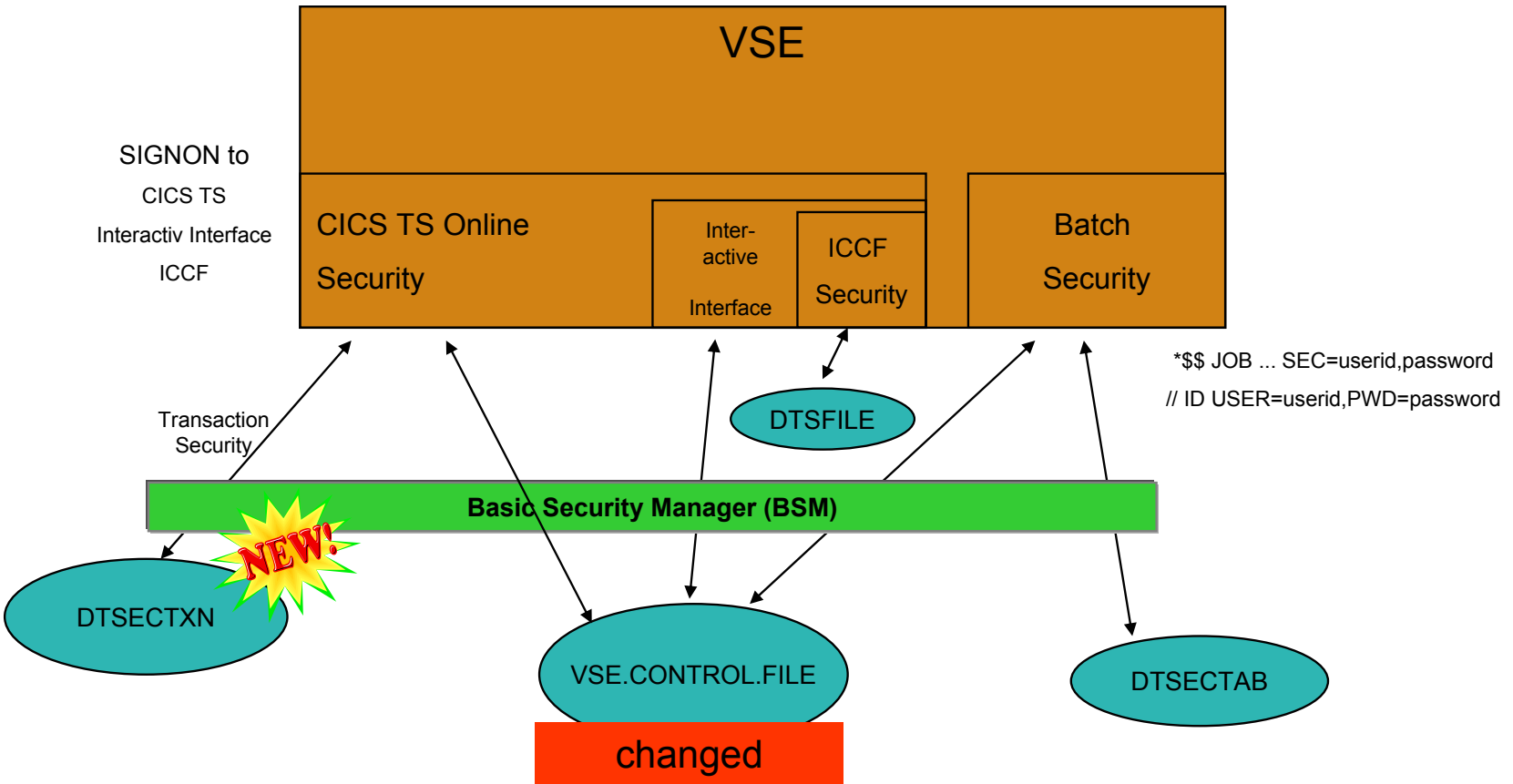
Basic Security Manager (BSM) with VSE/ESA 2.4 – 2.7, z/VSE 3.1.0

- **BSM is part of VSE Central Functions** – it's for free
  - Security Server in default partition FB
  - CICS TS protection for:
    - Sign on Security
    - Transaction Security (based on DTSECTXN)
  - RACROUTE interface to DTSECTAB resources
  - RACROUTE interface for TCP/IP Security Exit BSSTISX

If more security functions are needed:

- **External Security Manager (ESM)** – it's fee
  - CA-Top Secret, BIM Alert or other Vendor products

VSE Security Structure with VSE/ESA 2.4 – 2.7, z/VSE 3.1.0



Basic Security Manager (BSM) with VSE/ESA 2.4 – 2.7, z/VSE 3.1.0

- **VSE.CONTROL.FILE:**
  - VSAM KSDS File with new record format for user profiles to support User Ids for:
    - CICS TS signon
    - Interactive Interface,
    - ICCF (password propagation via Interactive Interface)
    - Batch job (exception: DUMMY and FORSEC)
  - **Migration from ‚old' VSE.CONTROLE.FILE and DFHSNT with Batch utility IESBLDUP**
  - Repository with
    - Batch utility IESUPDCF
    - Interactive Interface Dialog: 2.1.1

VSE Security Structure with VSE/ESA 2.4 – 2.7, z/VSE 3.1.0

- **DTSECTAB:**
  - Access rights to libraries, sublibraries, members, VSAM-files
  - Only User IDs FORSEC and DUMMY !
- **DTSECTXN:**
  - CICS transactions and their security class
  - BSM compares the security class of a transaction with the transaction security key(s) defined for a particular user in the corresponding user profile
  - **CICS does not allow access to transactions which are not defined in DTSECTXN**.
  - Migration from CICS/VSE TRANSEC value with REXX procedures
  - Repository with
    - DTSECTXN Macro
    - Interactive Interface dialog 2.8
- **ICCF Security with DTSFILE:**
  - User IDs (4 characters) and ICCF files
  - Same signon-password as Interactive Interface

Basic Security Manager:

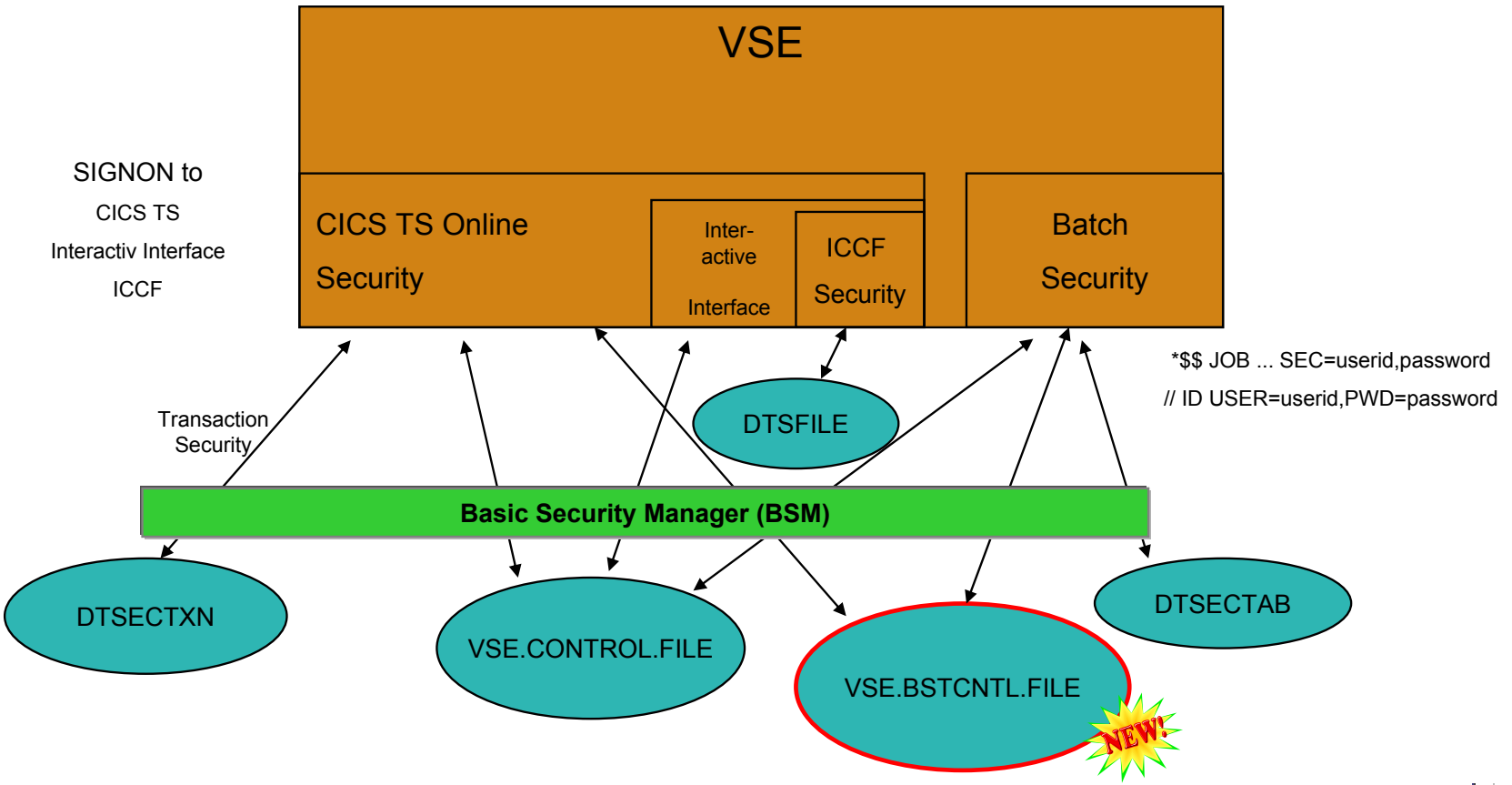
Up to z/VSE 3.1.0:

- Resource Classes (class_name)
  - **USER** for VSE.CONTROL.FILE
  - **DATASET** for DTSECTAB
  - **VSELIB, VSESLIB, VSEMEM** for DTSECTAB
  - **TCICSTRN (transaction class)** for DTSECTXN

z/VSE 3.1.1- Enhanced Security Concept (optional)

- **Resource Profiles**
  - **8 new Resource Classes (not only transaction class)**
- **Description field for all Profiles**
- **User Groups**
- **Administration of Password Rules**

VSE Security Structure with z/VSE 3.1.1
before Transaction Security Migration



Basic Security Manager - Repositories

- **VSE.CONTROLE.FILE, DTSECTAB:** unchanged

- **DTSECTXN:** (renamed and replaced by BSM Control File after transaction security migration)
  - Transaction security profiles
  - Define profiles with Dialog 2.8 on z/VSE 3.1.0 / Dialog 2.8.5 in z/VSE 3.1.1.
  - Has higher priority as BSM Control File

- **VSE.BSTCNTL.FILE: (BSM Contol file)**

  - Resource Profiles
  - User Groups
  - Password rules (remove IESIRCVT before using)
  - Better performance, because checking against a copy in data space

BSM Control File: VSE.BSTCNTL.FILE

- **Description field for all Resource Profiles (20 characters)**
- **BSM Resource Profiles (profile_name)**
  - Resource Classes (class_name)
    - TCICSTRN - Transactions (not new)
      - Relieves characterset limitations for the transaction names
      - Updates without reassembly
    - MCICSPPT - Application programs
    - FCICSFCT - Files
    - JCICSJCT - Journals
    - SCICSTST - Temporary storage queues
    - DCICISDCT - Transient data queues
    - ACICSPCT - Transactions (CICS START)

    - *APPL* - Applications, like CICS
    - *FACILITY* - Miscellaneous resources

  - Definition
    - Dialog: BSM Resource Profile Maintenance (2.8.1)
    - Batch utility BSTADMIN

BSM Control File: VSE.BSTCNTL.FILE

- **User Groups are stored in BSM Control File**
  - User IDs can be connected into a group
  - GROUP01, …, GROUP64
  - Replaces the security classes for CICS resources
  - Definition
    - Dialog: BSM Group Maintenance (2.8.2)
    - Batch utility BSTADMIN

Administration of VSE.BSMCNTL.FILE

- **BSTADMIN provides command to administer the profiles**
  - From the console in a PAUSE job
  - In a batch job
- **Commands**
  - ADD, CHANGE, DELETE
  - ADDGROUP, CHNGROUP, DELGROUP
  - CONNECT, REMOVE
  - LIST, LISTG, LISTU
  - PERFORM
  - STATUS
- **Security Maintenance Dialogs – 2.8.x**

Administration of Password Rules

- **No IPL for activating new password rules!**

- **Password rules can be changed by command**

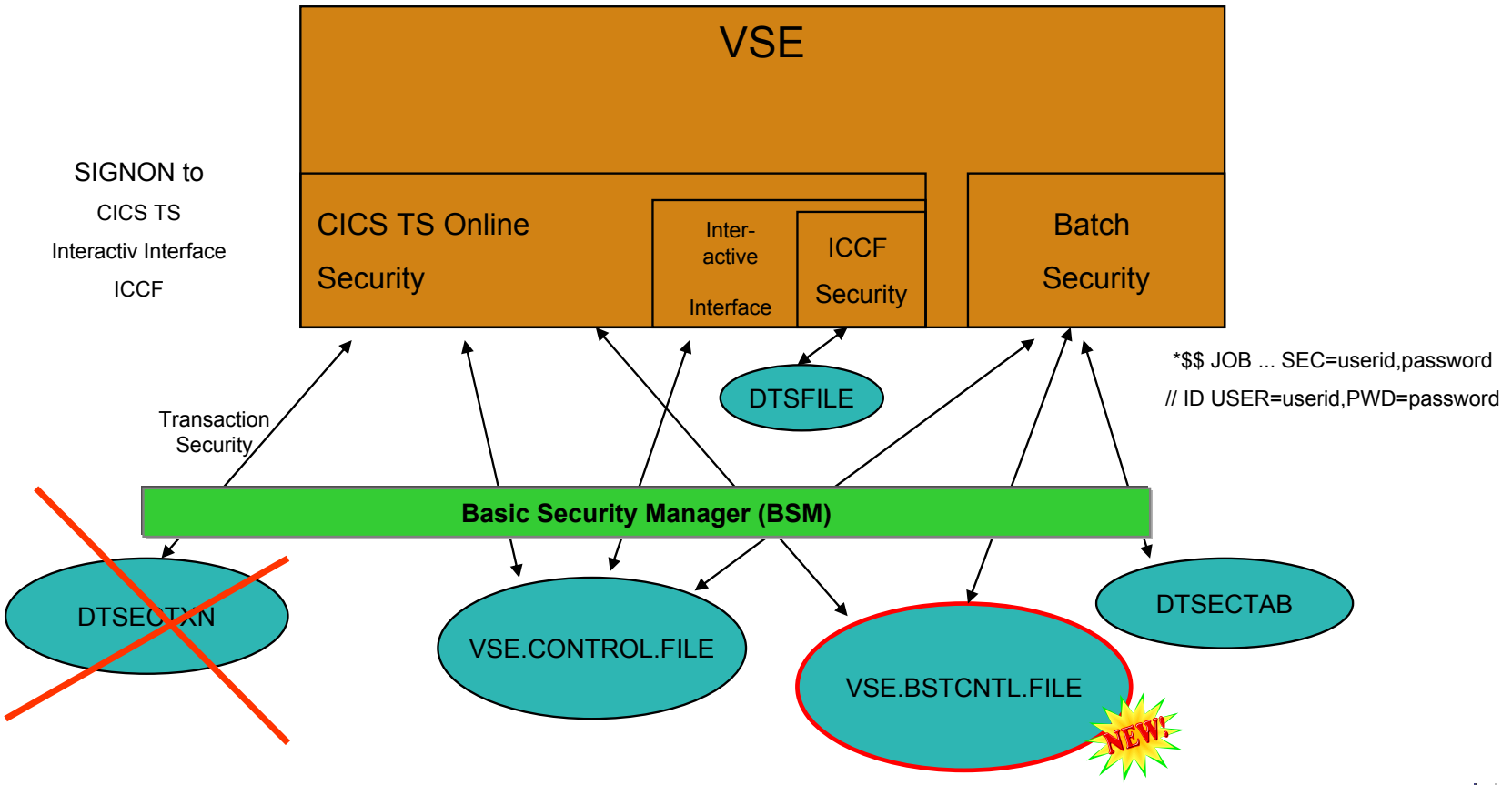
  Use BSTADMIN


```
PERFORM PASSWORD HISTORY|NOHISTORY
                 LENGTH(5)
                 REVOKE(4)
                 WARNING(3)
```

  - **HISTORY: a password history is maintained (the last 12 passwords)**
  - **LENGTH: minimum password length of password**
  - **WARNING: number of days a warning is displayed before password is expired**
  - **REVOKE: number of unsuccessful sign-on attempts before user id is revoked**

- Replaces IESIRCVT (in USERBG.PROC)
  - Remove all IESIRCVT from your z/VSE 3.1.1 !

VSE Security Structure with z/VSE 3.1.1
after Transaction Security Migration



Migrating to Enhanced Security Concept

- **Code of new Security Support is available with PTFs**

  (AF-PTF and Interactive Interface-PTFs)

BUT

do not migrate via RSL/PTF from z/VSE V3.1.0 !

Fast Service Upgrade is strongly recommended !!!

- **DTSECTXN should be no longer used !**

  ⟹ Use the new BSM Control File to protect CICS resources

Migrating Steps to Enhnaced Security Concept

- **Install z/VSE V.3.1.1 via FSU or Inital Installation**
- **Create group profiles from existing User-IDs**
  - User Maintenance Dialog 2.1.1 – press PF6
  - Creates a group for each security class (e.g. GROUP01) and connect existing users to it
- **Migrate DTSECTXN definitions (optional)**
  - Use Migrate Security Entries Dialog 2.8.5
- **Use the new resource classes**

→ Detailed description in **z/VSE Administration 3.1.1.**

Advantages for CICS TS users / administrators!

CICS TS Resource Security (new with z/VSE 3.1.1)

- **Most CICS TS resources can be protected now**
  - Protection via Resource Classes and Resource Profiles, held in VSE.BSTCNTL.FILE
    - (Transactions – as in previous releases)
    - Programs, Files, Journals, Temporary storage, Transient data, Start Transactions, VTAM Applications, miscellaneous resources
- **This is similar to Resource Level Checking under CICS/VSE**
  - RSLC(NO/YES) defined within a transaction
  - RSL(xx/PUblic) defined for
    - Users being allowed to access protected resources
    - Resources for being allowed to be accessed

CICS TS Resource Security (new) …

- **Resource security definitions under CICS TS**
  - DFHSIT

SEC=YES	Enables security
XTRAN=YES	Resource Class_name TCICSTRN
XDCT=YES	Resource Class_name DCICSDCT
XFCT=YES	Resource Class_name FCICSFCT
XJCT=YES	Resource Class_name JCICSJCT
XPCT=YES	Resource Class_name ACICSPCT for EXEC CICS Start TransIds
XPPT=YES	Resource Class_name MCICSPPT
XTST=YES	Resource Class_name SCICSTST

CICS TS Resource Security (new) …

- **Resource security definitions under CICS TS….**
  - 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) (resource_name = FILEA)
      - ADD FCICSFCT FILEB UACC(NONE) (resource_name = FILEB)
      - PERMIT FCICSFCT FILEA(GROUP01) ACCESS(UPDATE)
      - PERMIT FCICSFCT FILEB(GROUP01) ACCESS(READ)

Enhancement for Report Controller Faciliy (RCF) to browse reports

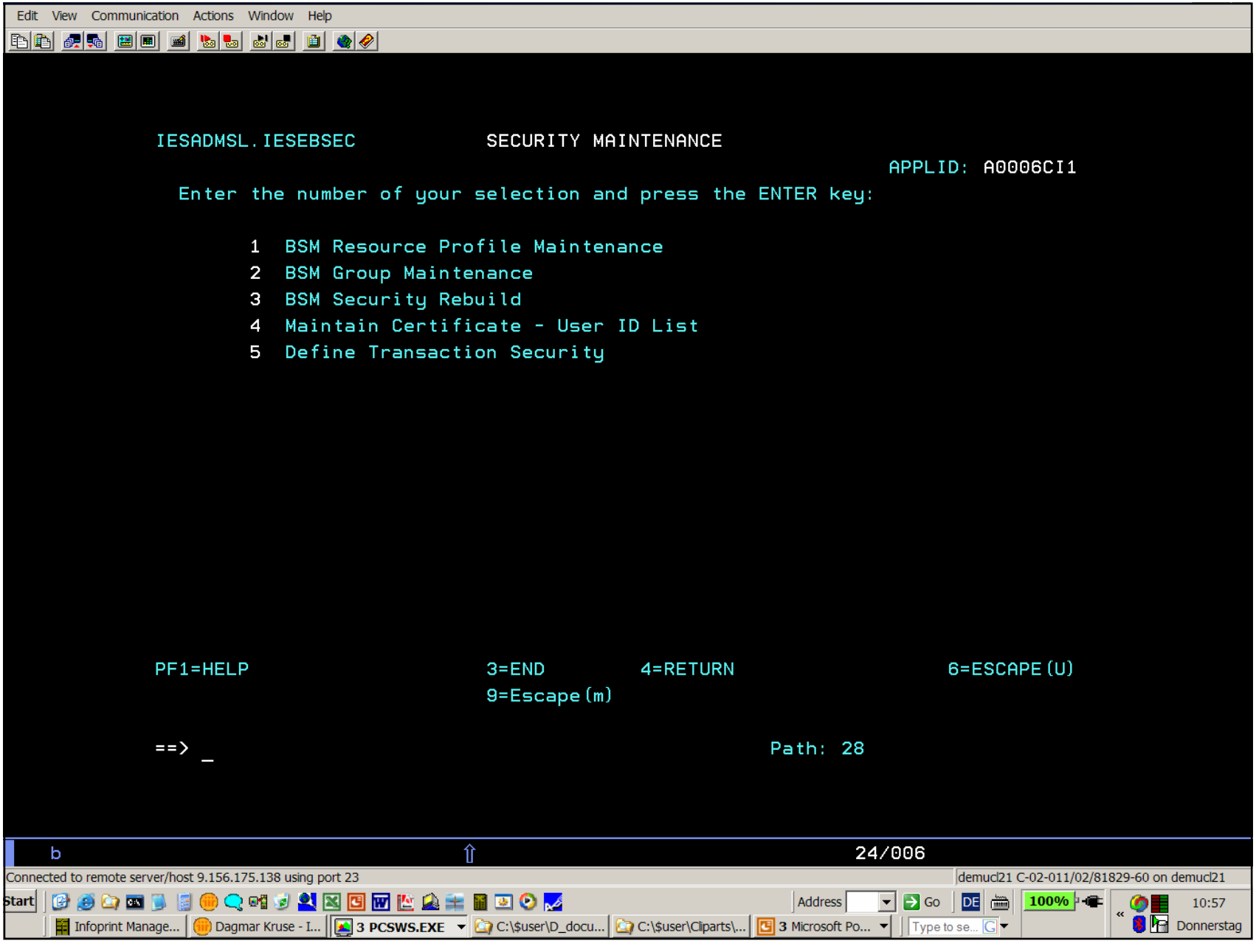
- **Access protection under CICS/VSE 2.3**
  - RSL for program DFHPSBRS – just 1 level of protection for all reports
  - All users with that RSLKEY can access all reports
- **Access protection under CICS TS 1.1.1**
  - RSL concept retained for compatibility reasons
    - Only with CICS TS APAR: PK11491
    - RSL keyword within SPOOLOPEN REPORT unchanged
  - For browsing purposes Profile_names **DFHRCF.BRSL01 – DFHRCF.BRSL24**
  - There are 24 levels for browse protection now – user must be authorized on access list of these related profiles DFHRCF.BRSLxx (RSLxx within SPOOLOPEN)
  - Protection based on report, not on browse program
- **Definition for RCF protection**
  - ADD FACILITY DFHRCF.BRSLnn UACC(NONE)
  - PERMIT FACILITY DFHRCF.BRSLnn ID(RCFGP01) ACCESS(READ)

Documentation

- **z/VSE Planning 3.1.1, SC33-8221-01**
- **z/VSE Administration 3.1.1, SC33-8224-01**
- **CICS TS Security Guide, SC33-1942-03**
- **RACROUTE documentation as part of the VSE Collection on**
  - DVD, SK3T-8348
  - CDROM, SK2T-0060
- **VSE Security documentation from Internet**
  - http://www-1.ibm.com/servers/eserver/zseries/zvse/documentation/security.html

Questions ?

Anhang


Edit View Communication Actions Window Help
IESADMSL.IESEBSEC SECURITY MAINTENANCE
APPLID: A0006CI1
Enter the number of your selection and press the ENTER key:
1 BSM Resource Profile Maintenance
2 BSM Group Maintenance
3 BSM Security Rebuild
4 Maintain Certificate - User ID List
5 Define Transaction Security
PF1=HELP 3=END 4=RETURN 6=ESCAPE(U)
9=Escape(m)
==> _
Path: 28
b
24/006
Connected to remote server/host 9.156.175.138 using port 23
demucl21 C-02-011/02/81829-60 on demucl21
Start
Address
Go
100%
10:57
Donnerstag
Infoprint Manage...
Dagmar Kruse - I...
3 PCSWS.EXE
C:\$user\D_docu...
C:\$user\Cliparts\...
3 Microsoft Po...
Type to se...