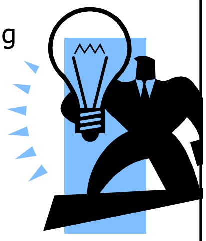
S17– Workshop - Security:

BSM-Konzept und Security im VSE

Dagmar Kruse (dkruse@de.ibm.com) IBM Deutschland GmbH

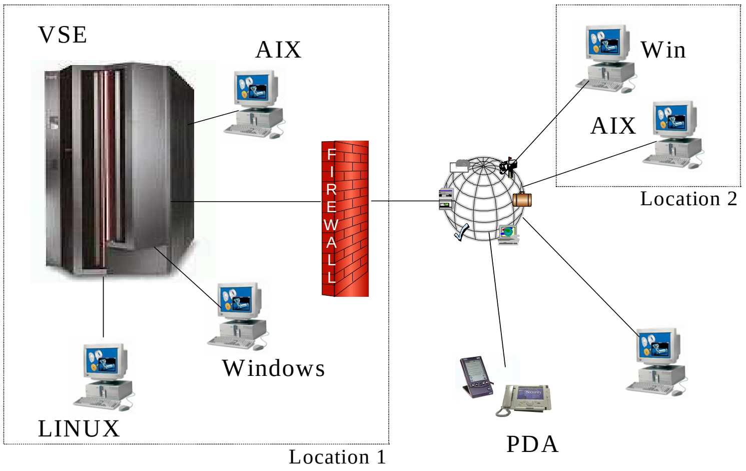
Heinz Peter Maassen (hp.maassen@lattwein.de) Lattwein GmbH

IT Sicherheit im Unternehmen

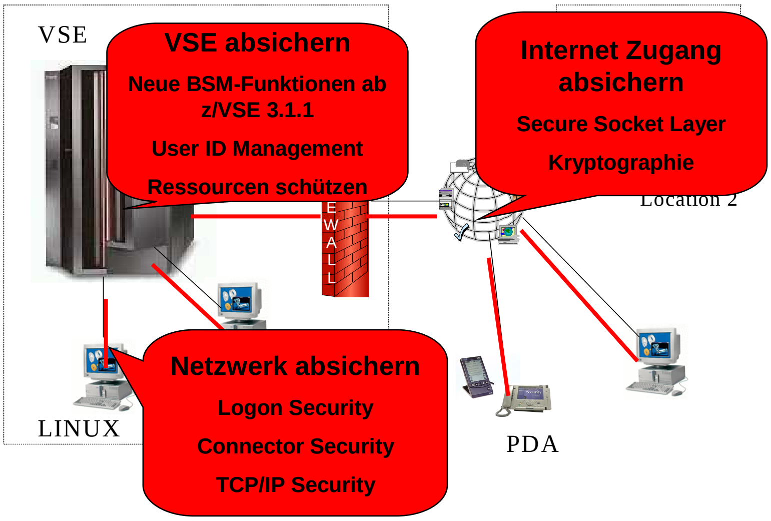


- Die Anforderungen an den Datenschutz steigen ständig
  - Datensicherheit
  - Datenintegrität
  - Audit-sicheres Speichern von Daten
- Die Attacken auf IT Systeme werden ständig mehr
  - Industrie-Spionage
  - Einbruchsversuche, Denial-of-Servcie Angriffe
  - Spam, Phishing, …
- Nichtbeachtung von Security-Anforderungen kann sehr teuer werden
  - Die Daten Ihres Unternehmens sind Ihre „(Über-) Lebensversicherung"
  - Schadensersatz-Forderungen bei Verlust von Kunden-Daten
  - Imageverlust kostet Kunden
- IT Sicherheit wird immer wichtiger
  - Es muss die gesamte IT-Landschaft betrachtet werden, nicht nur einzelne Systeme

IT Sicherheit in einem heterogenen Umfeld



IT Sicherheit in einem heterogenen Umfeld



VSE absichern

Neue BSM-Funktionen ab z/VSE 3.1.1

User ID Management

Ressourcen schützen

Internet Zugang absichern

Secure Socket Layer

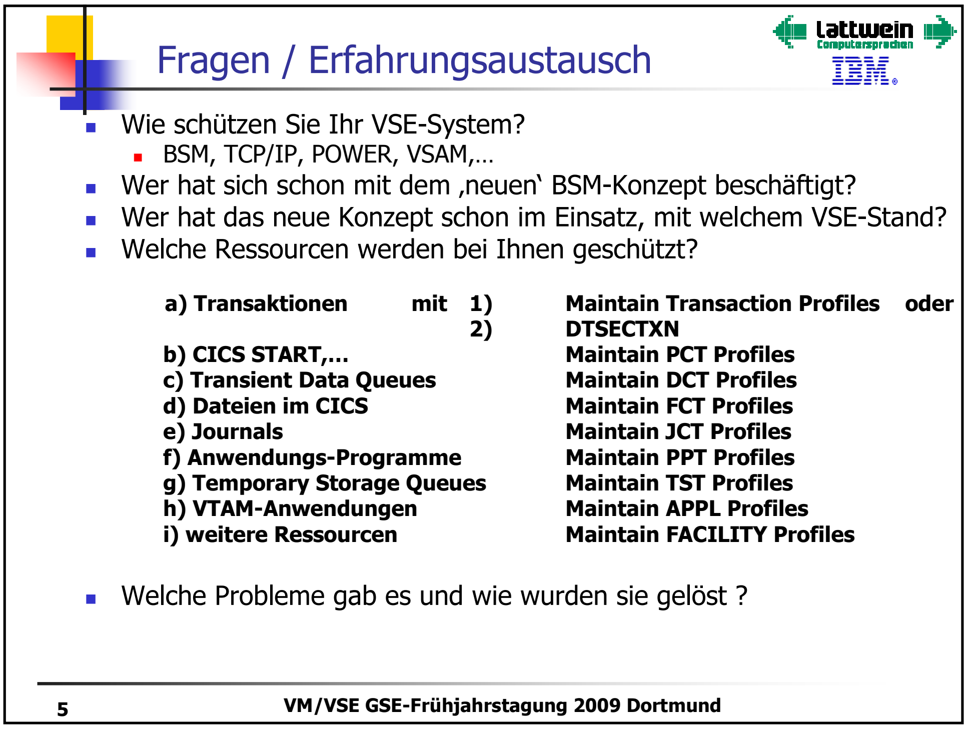
Kryptographie

Netzwerk absichern

Logon Security

Connector Security

TCP/IP Security

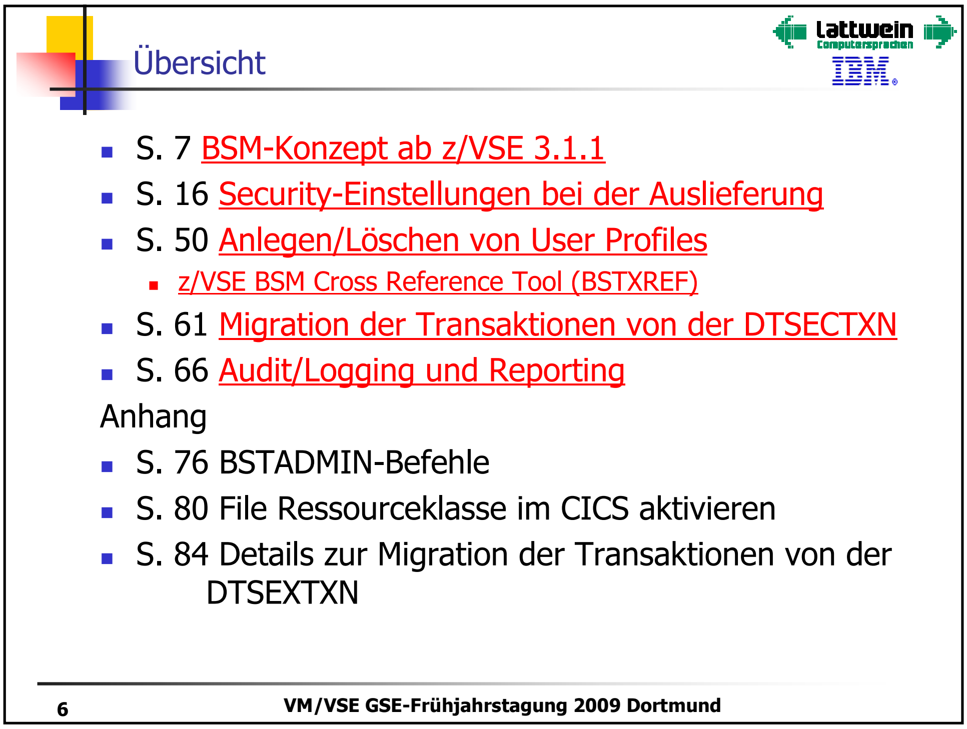


Fragen / Erfahrungsaustausch

- Wie schützen Sie Ihr VSE-System?
  - BSM, TCP/IP, POWER, VSAM,…
- Wer hat sich schon mit dem ‚neuen‛ BSM-Konzept beschäftigt?
- Wer hat das neue Konzept schon im Einsatz, mit welchem VSE-Stand?
- Welche Ressourcen werden bei Ihnen geschützt?

a) Transaktionen	**mit**	**1)**	**Maintain Transaction Profiles**	**oder**
		2)	**DTSECTXN**	
b) CICS START,…			**Maintain PCT Profiles**	
c) Transient Data Queues			**Maintain DCT Profiles**	
d) Dateien im CICS			**Maintain FCT Profiles**	
e) Journals			**Maintain JCT Profiles**	
f) Anwendungs-Programme			**Maintain PPT Profiles**	
g) Temporary Storage Queues			**Maintain TST Profiles**	
h) VTAM-Anwendungen			**Maintain APPL Profiles**	
i) weitere Ressourcen			**Maintain FACILITY Profiles**	

- Welche Probleme gab es und wie wurden sie gelöst ?



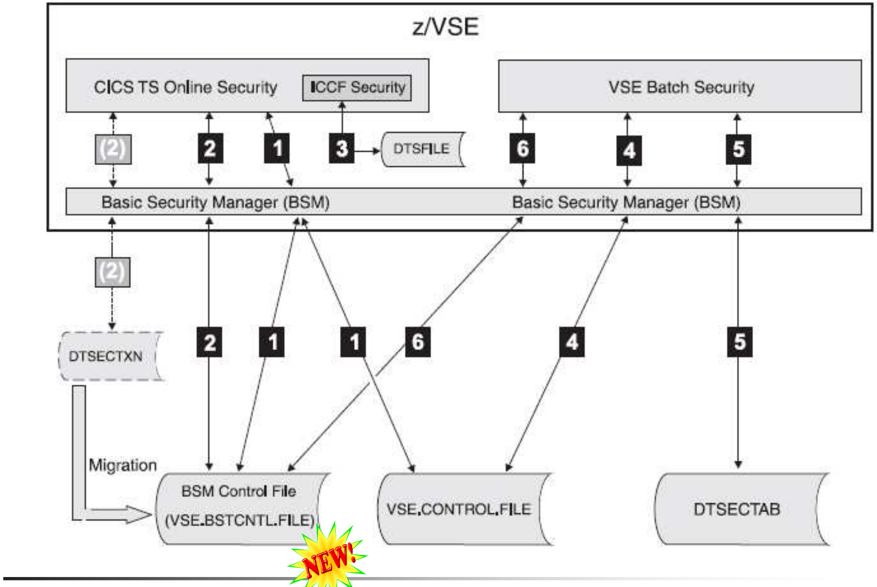
Übersicht

- S. 7 BSM-Konzept ab z/VSE 3.1.1
- S. 16 Security-Einstellungen bei der Auslieferung
- S. 50 Anlegen/Löschen von User Profiles
  - z/VSE BSM Cross Reference Tool (BSTXREF)
- S. 61 Migration der Transaktionen von der DTSECTXN
- S. 66 Audit/Logging und Reporting

Anhang

- S. 76 BSTADMIN-Befehle
- S. 80 File Ressourceklasse im CICS aktivieren
- S. 84 Details zur Migration der Transaktionen von der DTSEXTXN

BSM-Security-Konzept ab z/VSE 3.1.1



BSM-Security-Konzept ab z/VSE 3.1.1

1. Signon to CICS TS:
   - Userid- + PWD-Check : VSE.CONTROL.FILE
     erfolgreich ➔ BSM erstellt „user info block“
   - CICS APPLID-Check : VSE.BSTCNTL.FILE
     (falls Resource class „APPL‘“ aktiv ist)

2. Zugriff auf CICS-Ressourcen:
   - ACCESS- Check: VSE.BSTCNTL.FILE

   (Ausnahme (2), falls DTSECTXN vorhanden: Transaction-Security- Eintrag in DTSECTXN hat Vorrang)

BSM-Security-Konzept ab z/VSE 3.1.1

3. VSE/ICCF: Anwendung unter CICS TS:
   - Eigener Security-Check: DTSFILE

4. Signon aus dem Batch:
   - Userid- + PWD-Check : VSE.CONTOL.FILE
     erfolgreich ➔ BSM erstellt „user info block"

5. Zugriff auf DTSECTAB-Resourcen:
   - ACCESS- Check: DTSECTAB

6. Batch-Zugriff auf BSTCNTL-Resourcen:
   - ACCESS- Check: VSE.BSTCNTL.FILE

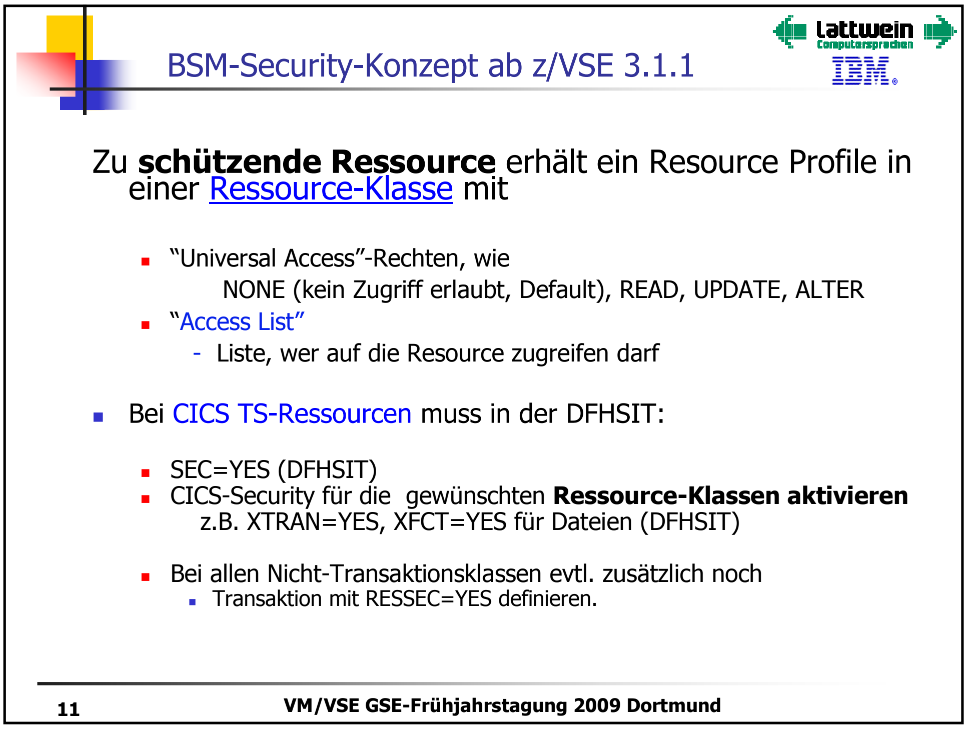
BSM-Security-Konzept ab z/VSE 3.1.1

- Erweiterung des RACROUT-Interfaces analog zum RACF im z/OS

- Neue RESSOURCE Klassen

TCICSTRN	- Transaktionen (bisher DTSECTXN)
MCICSPPT	- Anwendungs-Programme
FCICSFCT	- Dateien
JCICSJCT	- Journale
SCICSTST	- Temporary Storage Queues
DCICISDCT	- Transient Data Queues
ACICSPCT	- Transaktionen (CICS START)
APPL	- VTAM-Anwendungen (CICS1,CICS2,..)
FACILITY	- weitere Ressourcen (Spooling Files, RCF,…)

- Benutzer können in Gruppen eingeteilt werden
  - Berechtigungen können basierend auf der Gruppenzugehörigkeit vergeben werden
  - Vereinfacht das User-ID Management

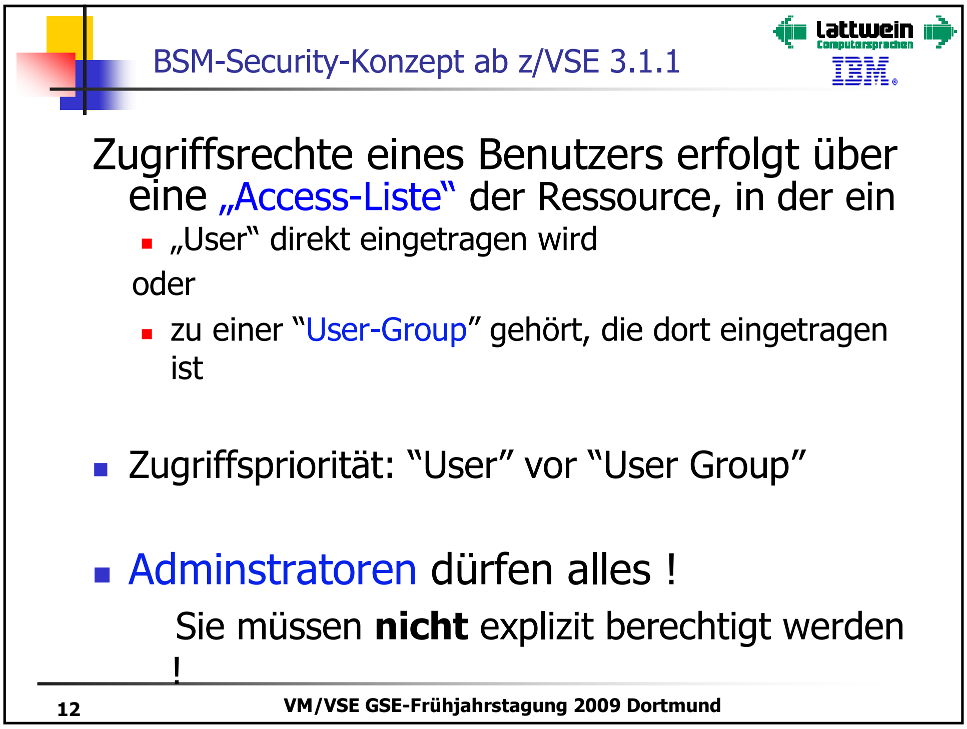


BSM-Security-Konzept ab z/VSE 3.1.1

Zu **schützende Ressource** erhält ein Resource Profile in einer Ressource-Klasse mit

- "Universal Access"-Rechten, wie
  NONE (kein Zugriff erlaubt, Default), READ, UPDATE, ALTER
- "Access List"
  - Liste, wer auf die Resource zugreifen darf

- Bei CICS TS-Ressourcen muss in der DFHSIT:
  - SEC=YES (DFHSIT)
  - CICS-Security für die gewünschten **Ressource-Klassen aktivieren**
    z.B. XTRAN=YES, XFCT=YES für Dateien (DFHSIT)
  - Bei allen Nicht-Transaktionsklassen evtl. zusätzlich noch
    - Transaktion mit RESSEC=YES definieren.



BSM-Security-Konzept ab z/VSE 3.1.1

Zugriffsrechte eines Benutzers erfolgt über eine „Access-Liste" der Ressource, in der ein

- „User" direkt eingetragen wird

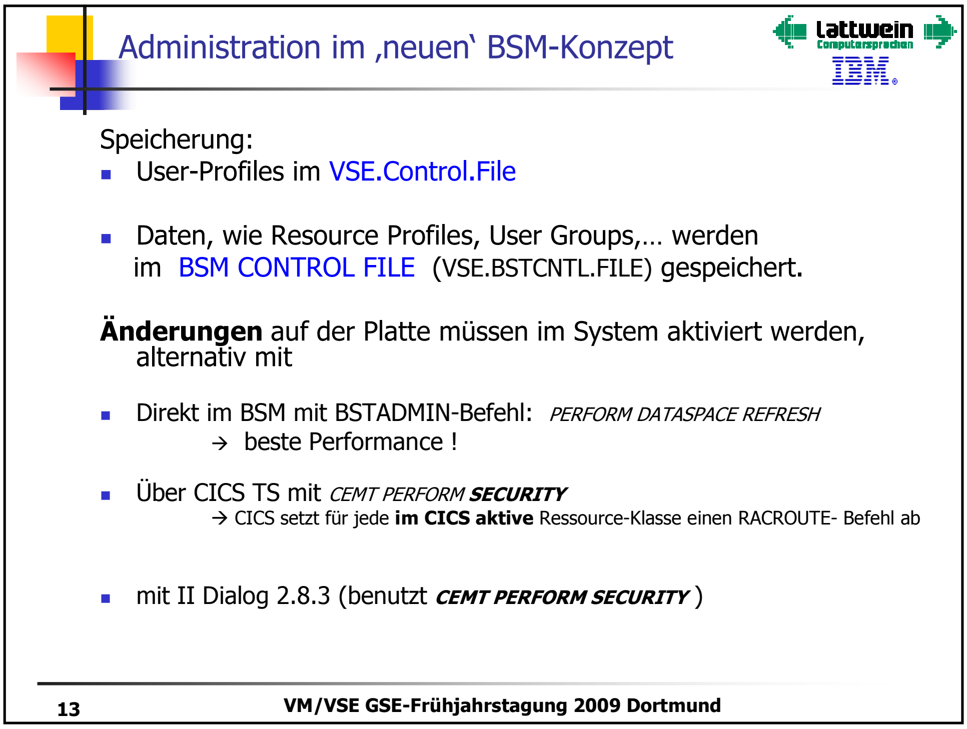
oder

- zu einer "User-Group" gehört, die dort eingetragen ist

- Zugriffspriorität: "User" vor "User Group"

- Adminstratoren dürfen alles !

  Sie müssen **nicht** explizit berechtigt werden !



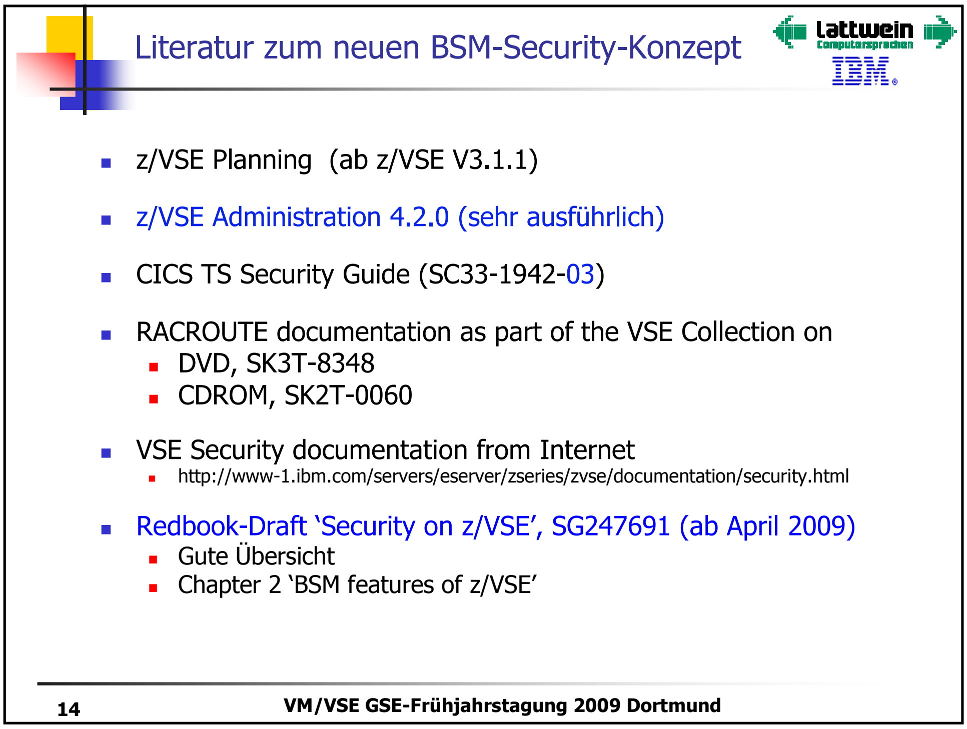
Administration im ‚neuen‘ BSM-Konzept

Speicherung:

- User-Profiles im VSE.Control.File
- Daten, wie Resource Profiles, User Groups,… werden im BSM CONTROL FILE (VSE.BSTCNTL.FILE) gespeichert.

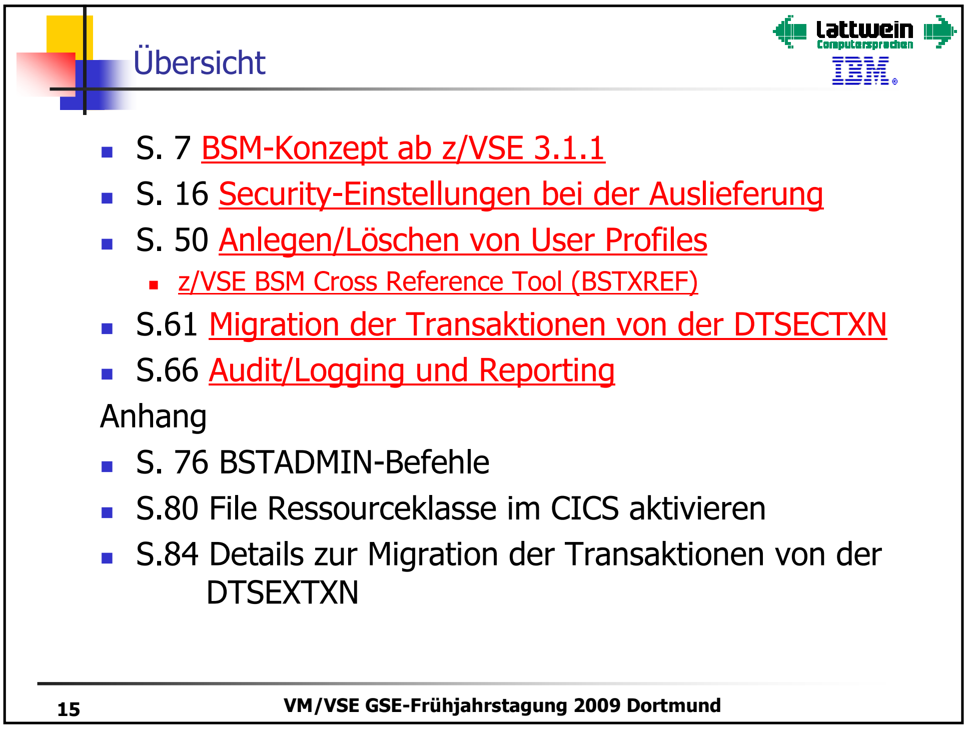
Änderungen auf der Platte müssen im System aktiviert werden, alternativ mit

- Direkt im BSM mit BSTADMIN-Befehl: *PERFORM DATASPACE REFRESH*
  → beste Performance !
- Über CICS TS mit *CEMT PERFORM **SECURITY***
  → CICS setzt für jede **im CICS aktive** Ressource-Klasse einen RACROUTE- Befehl ab
- mit II Dialog 2.8.3 (benutzt ***CEMT PERFORM SECURITY***)



Literatur zum neuen BSM-Security-Konzept

- z/VSE Planning (ab z/VSE V3.1.1)
- z/VSE Administration 4.2.0 (sehr ausführlich)
- 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
- Redbook-Draft ‘Security on z/VSE’, SG247691 (ab April 2009)
  - Gute Übersicht
  - Chapter 2 ‘BSM features of z/VSE’

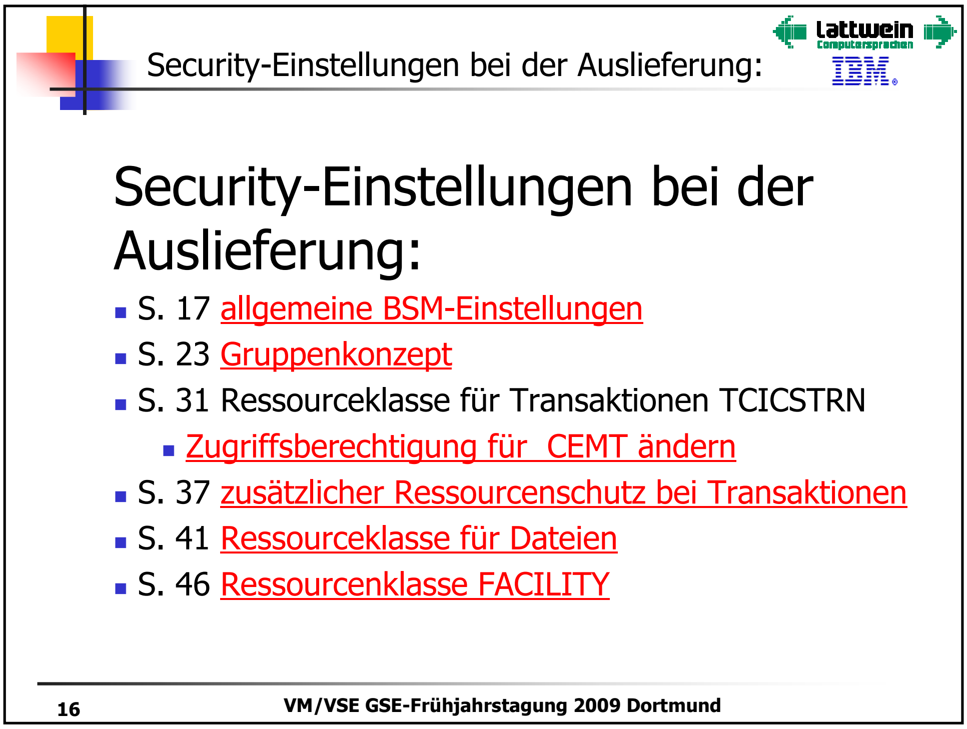


Übersicht

- S. 7 BSM-Konzept ab z/VSE 3.1.1
- S. 16 Security-Einstellungen bei der Auslieferung
- S. 50 Anlegen/Löschen von User Profiles
  - z/VSE BSM Cross Reference Tool (BSTXREF)
- S.61 Migration der Transaktionen von der DTSECTXN
- S.66 Audit/Logging und Reporting

Anhang

- S. 76 BSTADMIN-Befehle
- S.80 File Ressourceklasse im CICS aktivieren
- S.84 Details zur Migration der Transaktionen von der DTSEXTXN



Security-Einstellungen bei der Auslieferung:

Security-Einstellungen bei der Auslieferung:

- S. 17 allgemeine BSM-Einstellungen
- S. 23 Gruppenkonzept
- S. 31 Ressourceklasse für Transaktionen TCICSTRN
  - Zugriffsberechtigung für CEMT ändern
- S. 37 zusätzlicher Ressourcenschutz bei Transaktionen
- S. 41 Ressourceklasse für Dateien
- S. 46 Ressourcenklasse FACILITY

Security-Einstellungen bei der Auslieferung:

- Ab z/VSE 3.1.1 wird ein verändertes BSM-Security-Konzept ausgeliefert
- Das bisherige Konzept kann aber trotzdem noch weiter benutzt werden, aber **Erweiterungen** erfolgen nur noch für das neue Konzept!
- Was muss man **nach einer Neuinstallation** beachten?
- Wie sind die **Security-Settings** bei der Auslieferung?

Wir gehen es am Beispiel des z/VSE4.2 direkt nach der Neuinstallation durch:

- Überblick der gesetzten BSM-Security durch
  BSTADMIN- Befehl: ***STATUS***

Security-Einstellungen bei der Auslieferung

```
0 exec bstadmin
BG-0000 BST901A ENTER COMMAND OR END      Alle Änderungen über die
0 status                                  BSM-Commands werden ‚gelogged‘
BG 0000 CLASS     ACTIVE    CMDAUDIT
BG 0000 -----     ------    --------
BG 0000 USER      YES       NO   → User Profiles über VSE.CONTROL.FILE
BG 0000 GROUP     YES       NO   →  über VSE.BSTCNTL.FILE
BG 0000 DATASET   YES       NO
BG 0000 VSELIB    YES       NO        SYS SEC=(YES,NOTAPE)
BG 0000 VSESLIB   YES       NO         → über DTSECTAB
BG 0000 VSEMEM    YES       NO

BG 0000 TCICSTRN  YES       NO
BG 0000 ACICSPCT  YES       NO
BG 0000 DCICSDCT  YES       NO        CICS-Ressourcen:
BG 0000 FCICSFCT  YES       NO        BSM wird aber nur aktiv, wenn
BG 0000 JCICSJCT  YES       NO        es von CICS gerufen wird!
BG 0000 MCICSPPT  YES       NO
BG 0000 SCICSTST  YES       NO

BG 0000 APPL      YES       NO
BG 0000 FACILITY  YES       NO   →    CICS RCF, EXEC CICS SPOOL..
```

Security-Einstellungen bei der Auslieferung

```
BG 0000 PASSWORD PROCESSING OPTIONS:
BG 0000   12 GENERATIONS OF PREVIOUS PASSWORDS BEING MAINTAINED.
BG 0000   AFTER   5 CONSECUTIVE UNSUCCESSFUL PASSWORD ATTEMPTS,
BG 0000       A USERID WILL BE REVOKED.
BG 0000   PASSWORD EXPIRATION WARNING LEVEL IS   7 DAYS.
BG 0000   A PASSWORD CAN HAVE   3 TO   8 CHARACTERS.
BG 0000
BG 0000 AUDIT OPTIONS:
BG 0000   ADMINISTRATOR ACCESSES TO RESOURCES ARE NOT LOGGED
BG 0000
```

Änderung auf Logging mit EXEC BSTADMIN

- PERFOTM AUDIT ADMINACC

```
BG 0000 GENERAL OPTIONS:
BG 0000   NO USER ID IS REQUIRED TO USE BSTADMIN WITHOUT BATCH
                                                  SECURITY
BG 0000   BSTADMIN IS USING USER ID FORSEC   FOR AUTHORIZATION
BG 0000
```

Änderung mit EXEC BSTADMIN

- SETOPT CMDUSERID → BSTADMIN wird auch bei SEC=NO im IPL geschützt
- USERID USER(admin_user-id) PASSWORD(password) → userid ändern

Security-Einstellungen bei der Auslieferung

```
BG 0000
BG 0000 DATA SPACE STATUS:
BG 0000   CURRENT DATA SPACE SIZE IS      960K.
BG 0000   USAGE OF DATA SPACE STORAGE IS  18%.
BG 0000   DATA PART SIZE IS     171K.
BG 0000   SIZE OF PREVIOUS DATA SPACE WAS     960K.
BG 0000   USAGE OF PREVIOUS DATA SPACE WAS  18%.
BG 0000   DATA PART SIZE WAS     171K.
BG 0000 BST904I RETURN CODE OF STATUS IS 00
```

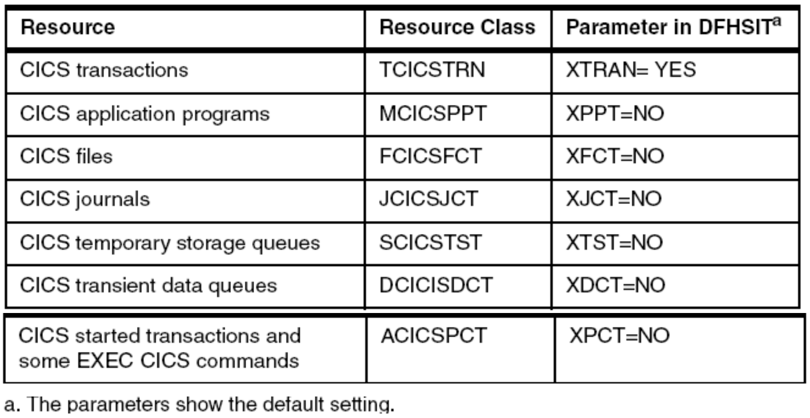
Data Space:

- SIZE-Änderung nur im BSM-Recovery-Mode mit
  - *PERFORM DATASPACE SIZE(nk|nM)*
- Inhalt aktualisieren / neue Definitionen aktivieren:
  - *PERFORM DATASPACE REFRESH*
- Data Space überprüfen mit
  - *Query DSPACE*

CICS-Security bei der Auslieferung

Wird in der DFSIT definiert :

- SEC=YES
- DFLTUSER=CICSUSER



Resource	Resource Class	Parameter in DFHSIT[a]
CICS transactions	TCICSTRN	XTRAN= YES
CICS application programs	MCICSPPT	XPPT=NO
CICS files	FCICSFCT	XFCT=NO
CICS journals	JCICSJCT	XJCT=NO
CICS temporary storage queues	SCICSTST	XTST=NO
CICS transient data queues	DCICISDCT	XDCT=NO
CICS started transactions and some EXEC CICS commands	ACICSPCT	XPCT=NO

a. The parameters show the default setting.

CICS Default User

- Im CICS läuft jede Transaktion über eine User-Id.
- Wenn kein Benutzer angemeldet ist, benutzt CICS per Default die User-ID, die in der DFTHSIT angegeben ist.
- DFLTUSER=CICSUSER wird ausgeliefert
  - darf CICS TS, aber nicht ICCF (Type 3)
  - Berechtigung im Interactiv Interface: `1=yes, 2=no`

```
NEWS....................... 1   Should user receive news items?
ESCAPE..................... 2   Can user escape to CICS?
CONFIRM DELETE............. 2   Does user want a confirmation message?
VSE PRIMARY SUBLIBRARY..... 2   Does user want a PRIMARY sublibrary?
SUBMIT TO BATCH............ 2   Can user submit to Batch?
```

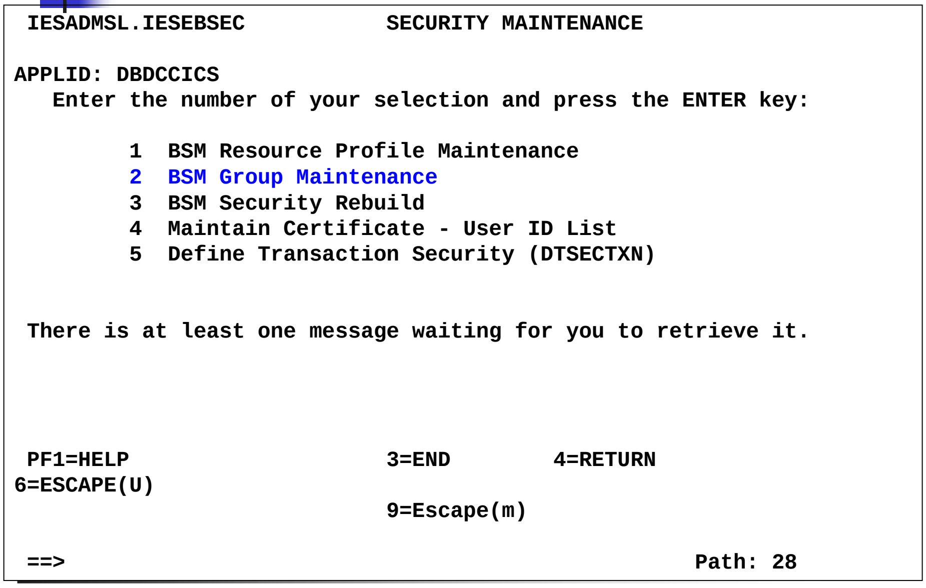
  - Ist nach Neuinstallation in GROUP01, GROUP60-GROUP64
  - Sollte auch in **GROUP01** und **GROUP61** bleiben.
    - braucht Berechtigung für Startup- und II-Transaktionen,
    - und falls File Security aktiviert ist (XFCT=YES) und Batch-Security genutzt wird, wird der CICSUSER auch für einige Systemdateien gebraucht
  - Darf keine Berechtigung für kritische Transaktionen wie CEMT,CEDA,USER,.. haben

- Benutzerzuordnung und Berechtigung der Gruppen muss gut überlegt werden!
- Welches Gruppenkonzept wird ausgeliefert?

Ausgeliefertes Gruppenkonzept

Ausgeliefertes Gruppenkonzept

Ausgeliefertes Gruppenkonzept



```
 IESADMSL.IESEBSEC            SECURITY MAINTENANCE

APPLID: DBDCCICS
   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 (DTSECTXN)


 There is at least one message waiting for you to retrieve it.




 PF1=HELP                     3=END        4=RETURN
6=ESCAPE(U)
                              9=Escape(m)

 ==>                                                  Path: 28
```

II Dialog 2.8.2 BSM Group Maintenance

Direkt nach der Installation zeigt der Dialog:

```
 IESADMBSLG                    MAINTAIN SECURITY PROFILES
BSM RESOURCE CLASS:    GROUP
START....
OPTIONS:   1 = ADD          2 = CHANGE       5 = DELETE       6 = USER LIST
                                              USERID
   OPT     GROUP NAME    DESCRIPTION          CONNECTED?
                                              ________
    _      GROUP01       TRANSEC CLASS MIGRAT
               …
    _      GROUP64       TRANSEC CLASS MIGRAT
```

Die Benutzergruppen GROUP01 – GROUP64 entsprechen
den Transaktions-Schlüsseln 01 – 64 im User-Profile

- Es können neue Gruppen erstellt werden, z.B. für Abteilung, …
- Benutzer in den Gruppen sind mit Option 6 USER LIST zu sehen

BSM Default-Gruppen-Konzept

GROUP01, GROUP60-GROUP64:

- Enthalten Profiles der Benutzer: PROG, OPER, CICSUSER, $SRV
  Administratoren sind nicht zugeordnet, da sie stets berechtigt sind !!
- Die zugehörigen User-Profiles haben Berechtigung für die **Transaktions-Schlüssel** 01, 60 – 64
  - Konsistent mit Definitionen im bisherigen BSM-Konzept
  - Die „Transaction Security Keys“ sind **nicht mehr relevant** im jetzigen BSM-Konzept über das BSM.Control.File (waren wichtig für DTSECTXN)
- Diese Gruppen sind für die Systempflege vorgesehen.
- restliche Gruppen enthalten noch KEINE Benutzer
- **Zugriffsberechtigungen** sind nur vergeben für:
  - GROUP01 bei CICS-Transaktionen (werden z.T. auch von II-Dialogen genutzt)
  - GROUP61 bei Transaktionen, die hauptsächlich von den II-Dialoge genutzt werden

BSM Gruppen-Einteilung: ZU BEACHTEN

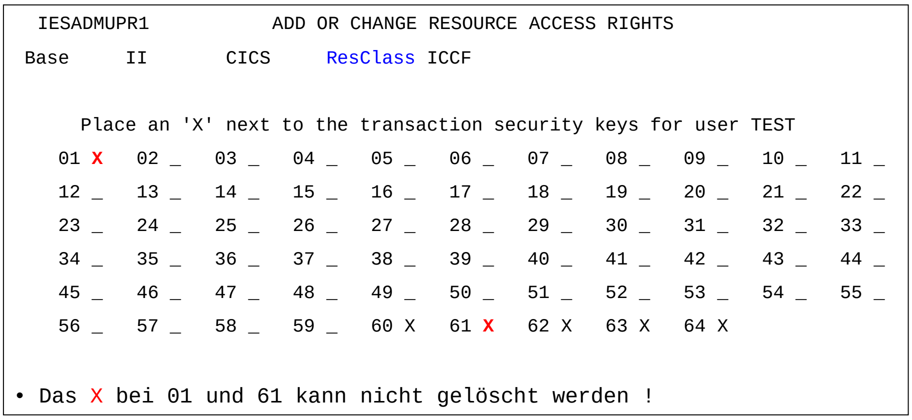
Achtung!

- Jeder Ihrer Benutzer hat die Transaktions-Schlüssel 01 und 61 !
  Diese können im II-Dialog ‚User Profile Maintenance' nicht gelöscht werden.
  ➔ Nach der Migration ist **jeder** Benutzer in den Gruppen GROUP01 **und** GROUP61
- Per Default haben die ausgelieferten **Transaktionen Zugriffsberechtigung** für die Benutzergruppen **GROUP01 bzw. GROUP61**
- Benutzer, die **ohne Anmeldung** ins CICS kommen können, haben die Berechtigung des Default-Users: CICSUSER
- Nach der Migration kann jeder Benutzer auch auf **kritische Transaktionen**, wie CEMT,USER,CEDA,… zugreifen, wenn Sie es nicht anpassen.
- **Unberechtigten** sollten Sie **keinen** Zugriff auf diese **kritische** Transaktionen geben!

➔ Zugriffsberechtigungen gut überlegen
und
Gruppeneinteilung anpassen!

II Dialog 2.1.1 Transaction Securtiy Keys

II-Dialog 2.1.1:User Profile Maintenance



```
  IESADMUPR1           ADD OR CHANGE RESOURCE ACCESS RIGHTS
Base     II       CICS     ResClass ICCF


     Place an 'X' next to the transaction security keys for user TEST
   01 X   02 _   03 _   04 _   05 _   06 _   07 _   08 _   09 _   10 _   11 _
   12 _   13 _   14 _   15 _   16 _   17 _   18 _   19 _   20 _   21 _   22 _
   23 _   24 _   25 _   26 _   27 _   28 _   29 _   30 _   31 _   32 _   33 _
   34 _   35 _   36 _   37 _   38 _   39 _   40 _   41 _   42 _   43 _   44 _
   45 _   46 _   47 _   48 _   49 _   50 _   51 _   52 _   53 _   54 _   55 _
   56 _   57 _   58 _   59 _   60 X   61 X   62 X   63 X   64 X
```

- Das X bei 01 und 61 kann nicht gelöscht werden !

Welche Transaktionen sind kritisch?

Transaktion	Default-Gruppen-Zuordnung	Ändern z.B. in
USER (Display Activity Dialog, send Message to **all** user)	GROUP61	GROUP63
CEMT	GROUP01	GROUP63
CEDA	GROUP01	GROUP63
CEDB	GROUP01	GROUP63
CEDX	GROUP01	GROUP63
CECI	GROUP01	GROUP63
CETR	GROUP01	GROUP63
CEDF	GROUP01	GROUP63
DITTo, ?? nicht unbedingt, wenn BATCH-Security genutzt wird	GROUP61	GROUP63
Weitere ??		

Group63 sollte CICSUSER nicht mehr enthalten!

Transaktion DITTO

- per Default darf **nur ein Administrator** die Transaktion DITT benutzen !!
- Geschützt bei aktiver Batch-Security durch DTSECTAB
  - IPL SYS SEC=(YES,NOTAPE) gibt es mind. Seit VSE/ESA 2.1
  - Nutzen Sie die BATCH-Security?
  - Bei einem TYPE 1 (2)- Benutzer bekommt man diese Fehlermeldung in der Ditto-Partition und das Terminal hängt:

```
Y1 0046 0S20I UNAUTHORIZED ACCESS REQUEST FOR: PRD1   .BASE    .DITTO
```

Zugriff kann **explizit erlaubt** werden, z.B für READ-Zugriff

- In DTSECTAB:

```
 *****   AVOID THAT ANYONE CAN MANIPULATE FILES USING DITTO
     DTSECTAB TYPE=MEMBER,                                        C
               NAME=PRD1.BASE.DITTO,                              C
               ACC=(1)
```

- Im User Profile:

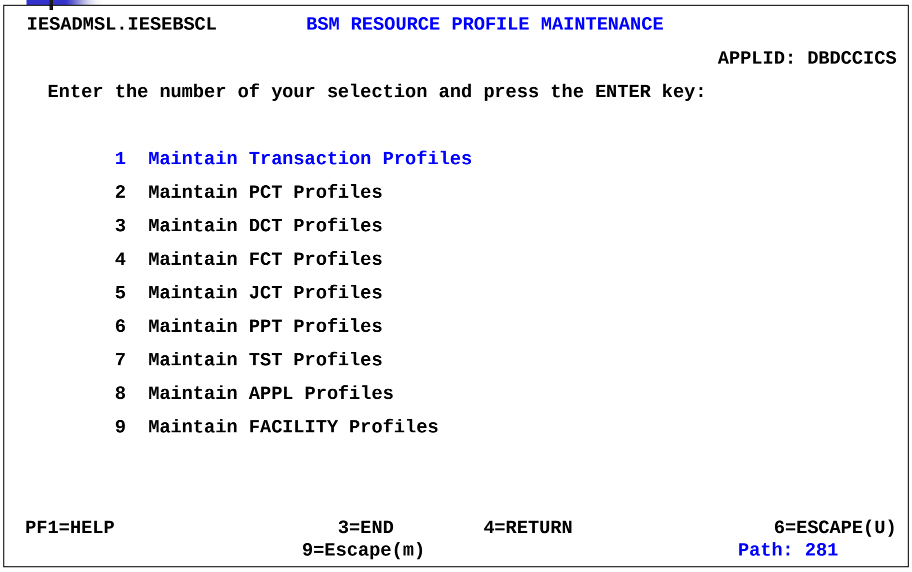
```
Specify the access rights for 1-32 DTSECTAB access control classes
    ( _=No access, 1=Connect, 2=Read, 3=Update, 4=Alter )
  01 2   02 _   03 _   04 _   05 _   06 _   07 _   08 _   09 _   10 _   11
```

TCICSTRN: Zugriff für CEMT ändern

Ressourceklasse für Transaktionen TCICSTRN

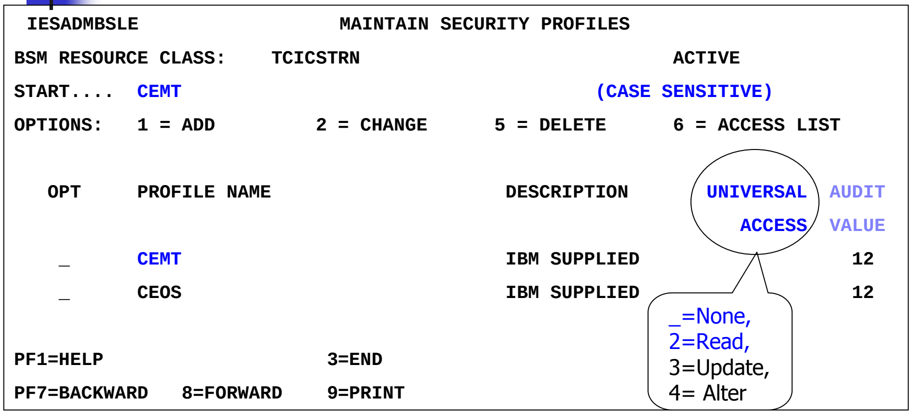
- Zugriffsberechtigung für **CEMT** ändern

II Dialog 2.8.1 BSM RESOURCE PROFILE MAINTENANCE



```
IESADMSL.IESEBSCL         BSM RESOURCE PROFILE MAINTENANCE
                                                          APPLID: DBDCCICS
  Enter the number of your selection and press the ENTER key:


        1  Maintain Transaction Profiles
        2  Maintain PCT Profiles
        3  Maintain DCT Profiles
        4  Maintain FCT Profiles
        5  Maintain JCT Profiles
        6  Maintain PPT Profiles
        7  Maintain TST Profiles
        8  Maintain APPL Profiles
        9  Maintain FACILITY Profiles



PF1=HELP                    3=END        4=RETURN                  6=ESCAPE(U)
                         9=Escape(m)                            Path: 281
```

II Dialog 2.8.1.1 kritische Transaktion: CEMT



```
 IESADMBSLE                  MAINTAIN SECURITY PROFILES
BSM RESOURCE CLASS:    TCICSTRN                            ACTIVE
START....  CEMT                                     (CASE SENSITIVE)
OPTIONS:   1 = ADD         2 = CHANGE      5 = DELETE      6 = ACCESS LIST

   OPT     PROFILE NAME                     DESCRIPTION      UNIVERSAL  AUDIT
                                                                ACCESS  VALUE
    _      CEMT                             IBM SUPPLIED                  12
    _      CEOS                             IBM SUPPLIED                  12

PF1=HELP                     3=END
PF7=BACKWARD   8=FORWARD     9=PRINT
```

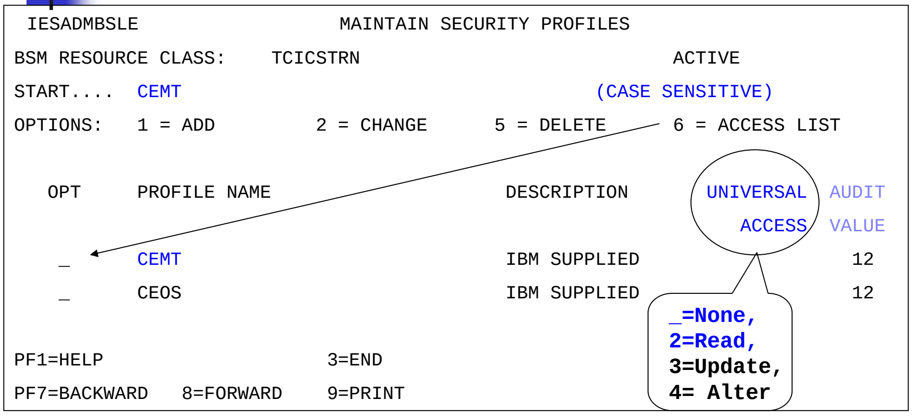
AUDIT VALUE: 12 = Failure(READ), d.h. protokolliert werden nur unberechtigte Zugriffe

audit level: _=None, 1=Failure, 2=Success, 3=All

access level: 2=Read, 3=Update, 4= Alter, _ for the default

CEMT: Universal Access= None, also **höchstens ACCESS LIST-Benutzer** haben Zugriffsberechtigung

II Dialog 2.8.1.1 kritische Transaktion: CEMT



```
 IESADMBSLE                  MAINTAIN SECURITY PROFILES
BSM RESOURCE CLASS:    TCICSTRN                            ACTIVE
START....  CEMT                                     (CASE SENSITIVE)
OPTIONS:   1 = ADD         2 = CHANGE      5 = DELETE      6 = ACCESS LIST

   OPT     PROFILE NAME                     DESCRIPTION      UNIVERSAL  AUDIT
                                                                ACCESS  VALUE
    _      CEMT                             IBM SUPPLIED                  12
    _      CEOS                             IBM SUPPLIED                  12

PF1=HELP                     3=END
PF7=BACKWARD   8=FORWARD     9=PRINT
```

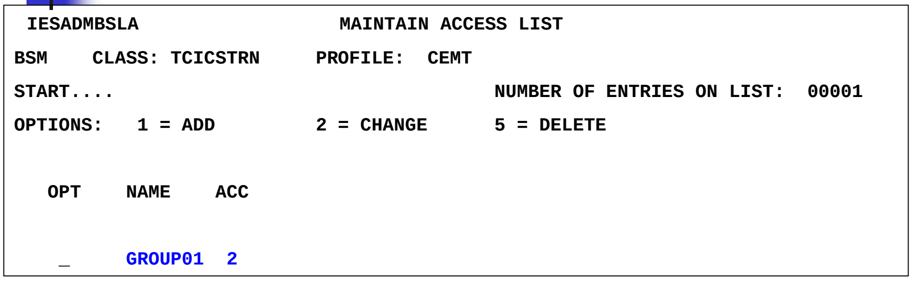
CEMT: Universal Access= None, also höchstens ACCESS LIST-Benutzer haben Zugriffsberechtigung

AUDIT VALUE: 12 = Failure(READ), d.h. protokolliert nur werden unberechtigte Zugriffe

audit level: _=None, 1=Failure, 2=Success, 3=All

access level: 2=Read, 3=Update, 4= Alter, _ for the default

II Dialog 2.8.1.1: CEMT- ACCESS LIST



```
 IESADMBSLA                  MAINTAIN ACCESS LIST
BSM    CLASS: TCICSTRN     PROFILE:  CEMT
START....                                 NUMBER OF ENTRIES ON LIST:  00001
OPTIONS:    1 = ADD           2 = CHANGE      5 = DELETE


   OPT    NAME    ACC


    _      GROUP01   2
```

ACCESS RIGHTS: _=None, 2=Read, 3=Update, 4=Alter

CEMT: GROUP01 haben Zugriff (=READ), d.h. evtl. alle Benutzer Ihres Systems!

➔ Berechtigungen überprüfen!!!

Dialog hat keine Refresh-Funktion, daher am besten

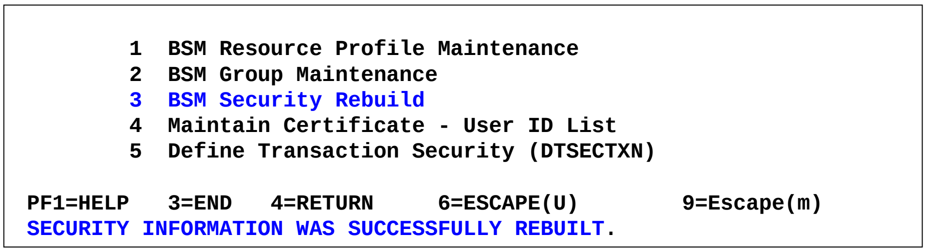
1. ADD von Gruppe mit besonders authorisierten Benutzern, wie PROG,OPERATOR,... , z.B. GROUP63 mit READ-Zugriff
2. DELETE GROUP01

Aktivieren der Security-Definitionen

Neue Definitionen müssen noch aktiviert werden!

Alternativen:

- Direkt im BSM mit BSTADMIN-Befehl: PERFORM DATASPACE REFRESH
- Aus dem CICS TS mit CEMT PERFORM SECURITY
- mit II Dialog 2.8.3 (benutzt CEMT PERFORM SECURITY)



```
          1  BSM Resource Profile Maintenance
          2  BSM Group Maintenance
          3  BSM Security Rebuild
          4  Maintain Certificate - User ID List
          5  Define Transaction Security (DTSECTXN)

PF1=HELP   3=END   4=RETURN    6=ESCAPE(U)       9=Escape(m)
SECURITY INFORMATION WAS SUCCESSFULLY REBUILT.
```

Ressourcenschutz der Transaktionen

Ressourcenschutz der Transaktionen

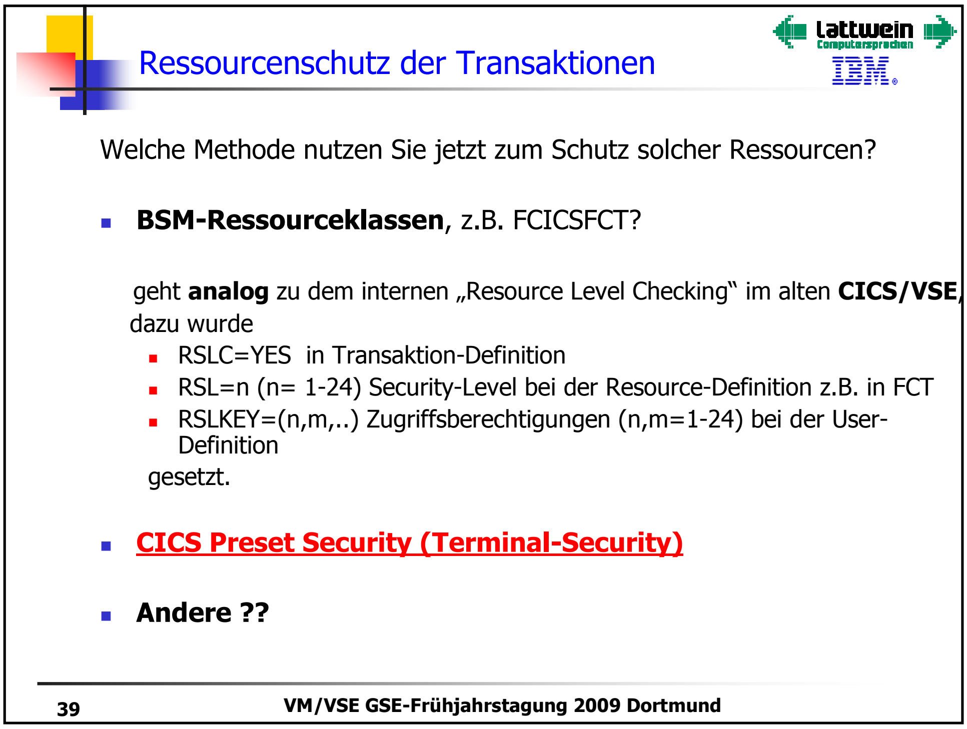
Ressourcenschutz der Transaktionen

- Default-Zugriff über Transaktionen
  (RESSEC= NO bei der Definition)

  Wer die Transaktion benutzen darf, **darf auch** auf alle aufgerufenen **Ressourcen** zugreifen !

Reicht dieser Schutz aus?

- Sollten Sie zusätzlich die Ressourcen, die von der Transaktion genutzt werden, schützen?
  - Gehaltsdatei
  - Adressen-Dateien
  - …



Ressourcenschutz der Transaktionen

Welche Methode nutzen Sie jetzt zum Schutz solcher Ressourcen?

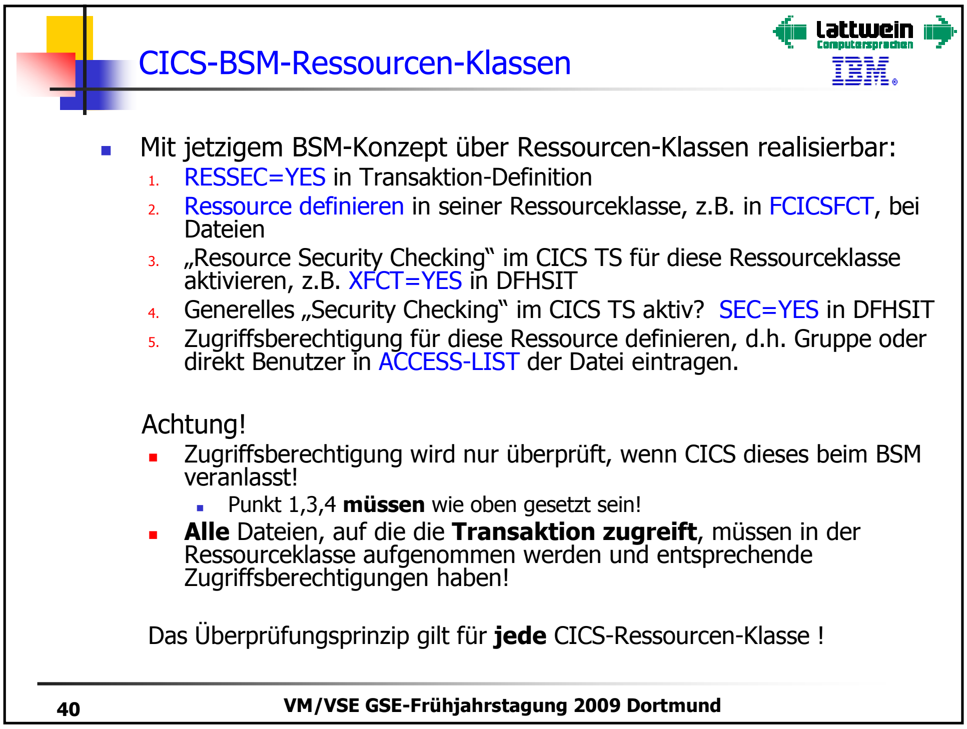
- **BSM-Ressourceklassen**, z.B. FCICSFCT?

  geht **analog** zu dem internen „Resource Level Checking" im alten **CICS/VSE**, dazu wurde
  - RSLC=YES in Transaktion-Definition
  - RSL=n (n= 1-24) Security-Level bei der Resource-Definition z.B. in FCT
  - RSLKEY=(n,m,..) Zugriffsberechtigungen (n,m=1-24) bei der User-Definition

  gesetzt.

- **CICS Preset Security (Terminal-Security)**

- **Andere ??**



CICS-BSM-Ressourcen-Klassen

- Mit jetzigem BSM-Konzept über Ressourcen-Klassen realisierbar:
  1. RESSEC=YES in Transaktion-Definition
  2. Ressource definieren in seiner Ressourceklasse, z.B. in FCICSFCT, bei Dateien
  3. „Resource Security Checking" im CICS TS für diese Ressourceklasse aktivieren, z.B. XFCT=YES in DFHSIT
  4. Generelles „Security Checking" im CICS TS aktiv? SEC=YES in DFHSIT
  5. Zugriffsberechtigung für diese Ressource definieren, d.h. Gruppe oder direkt Benutzer in ACCESS-LIST der Datei eintragen.

Achtung!

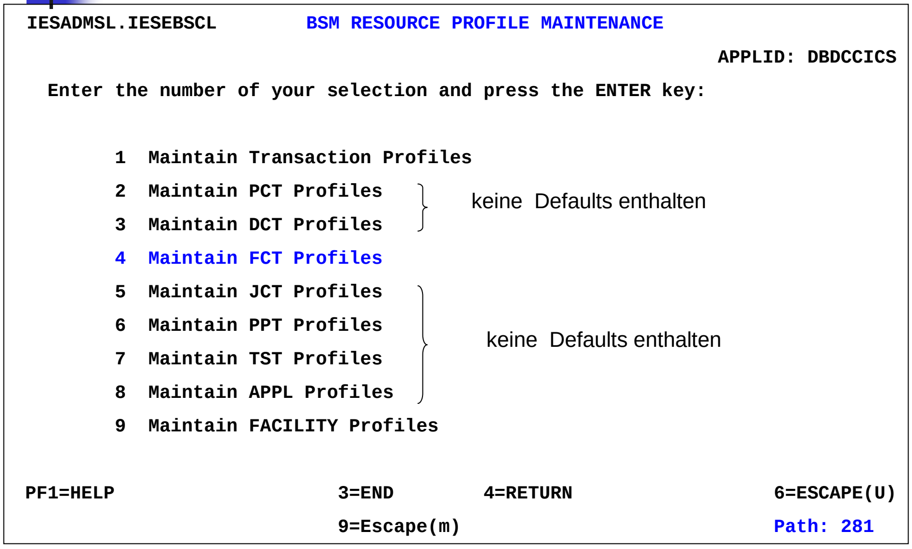
- Zugriffsberechtigung wird nur überprüft, wenn CICS dieses beim BSM veranlasst!
  - Punkt 1,3,4 **müssen** wie oben gesetzt sein!
- **Alle** Dateien, auf die die **Transaktion zugreift**, müssen in der Ressourceklasse aufgenommen werden und entsprechende Zugriffsberechtigungen haben!

Das Überprüfungsprinzip gilt für **jede** CICS-Ressourcen-Klasse !

Ressourceklasse für Dateien

Ressourceklasse für Dateien

II Dialog 2.8.1 BSM RESOURCE PROFILE MAINTENANCE

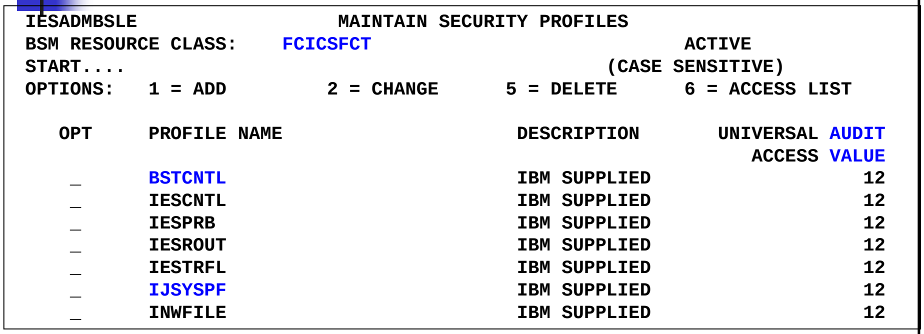


```
IESADMSL.IESEBSCL        BSM RESOURCE PROFILE MAINTENANCE
                                                      APPLID: DBDCCICS
  Enter the number of your selection and press the ENTER key:


        1  Maintain Transaction Profiles
        2  Maintain PCT Profiles
        3  Maintain DCT Profiles
        4  Maintain FCT Profiles
        5  Maintain JCT Profiles
        6  Maintain PPT Profiles
        7  Maintain TST Profiles
        8  Maintain APPL Profiles
        9  Maintain FACILITY Profiles


PF1=HELP                    3=END        4=RETURN                 6=ESCAPE(U)
                            9=Escape(m)                           Path: 281
```

keine Defaults enthalten

keine Defaults enthalten

II Dialog 2.8.2: Maintain FCT Profiles



```
IESADMBSLE                    MAINTAIN SECURITY PROFILES
BSM RESOURCE CLASS:    FCICSFCT                             ACTIVE
START....                                            (CASE SENSITIVE)
OPTIONS:    1 = ADD          2 = CHANGE       5 = DELETE       6 = ACCESS LIST

   OPT      PROFILE NAME                      DESCRIPTION        UNIVERSAL AUDIT
                                                                    ACCESS VALUE
    _       BSTCNTL                           IBM SUPPLIED                    12
    _       IESCNTL                           IBM SUPPLIED                    12
    _       IESPRB                            IBM SUPPLIED                    12
    _       IESROUT                           IBM SUPPLIED                    12
    _       IESTRFL                           IBM SUPPLIED                    12
    _       IJSYSPF                           IBM SUPPLIED                    12
    _       INWFILE                           IBM SUPPLIED                    12
```

- nur relevant, wenn in DFHSIT: XFCT=YES
- Universal Access= None, also nur Zugriffsberechtigung über ACCESS LIST + Administrator
- AUDIT VALUE: 12 = protokolliert werden nur unberechtigte Zugriffe

- Dateien BSTCNTL,IJSYSPF: z. Z. noch keine ACCESS LIST!
- Anderen Dateien haben GROUP01,GROUP61 jeweils mit 3=Update-Berechtigung

FCICSFCT für CICS Dateien aktivieren

Welche Probleme können beim Aktivieren der File-Securtiy entstehen (in DFHSIT: **XFCT=YES**) ?

Ausgangssituation:

Keiner hat Zugriffsberechtigung im CICS für

BSTCNT	BSM Control File
IJSYSPF	PTF FILE

GROUP01, GROUP61 haben Update-Berechtigung für

IESCNTL	VSE Control File
IESPRB	Online Problem Detrmination
IESROUT	Message Routing File
IESTRFL	Text Repository File (Help-Text)
INWFILE	Host Transfer File

FCICSFCT für CICS Dateien aktivieren

- Shutdown-Problem mit BSTCNTL und IJSYSPF:

  ➔ CICSUSER braucht READ-Zugriff geben

```
F5 0101 BST120I USER(CICSUSER)
        BST120I   A0006CI2.BSTCNTL CL(FCICSFCT)
        BST120I   INSUFFICIENT ACCESS AUTHORITY
        BST120I   FROM BSTCNTL
        BST120I   ACCESS INTENT(READ    ) ACCESS ALLOWED(NONE    )
F5 0101 BST120I USER(CICSUSER)
        BST120I   A0006CI2.IJSYSPF CL(FCICSFCT)
        BST120I   INSUFFICIENT ACCESS AUTHORITY
        BST120I   FROM IJSYSPF
        BST120I   ACCESS INTENT(READ    ) ACCESS ALLOWED(NONE
```

Lösung: PTF PK81238 (kommt mit z/VSE 4.2.1)

- BSTCNTL : Read-Zugriff (2) für GROUP01
- IJSYSPF : Update-Zugriff (3) für GROUP01, GROUP61

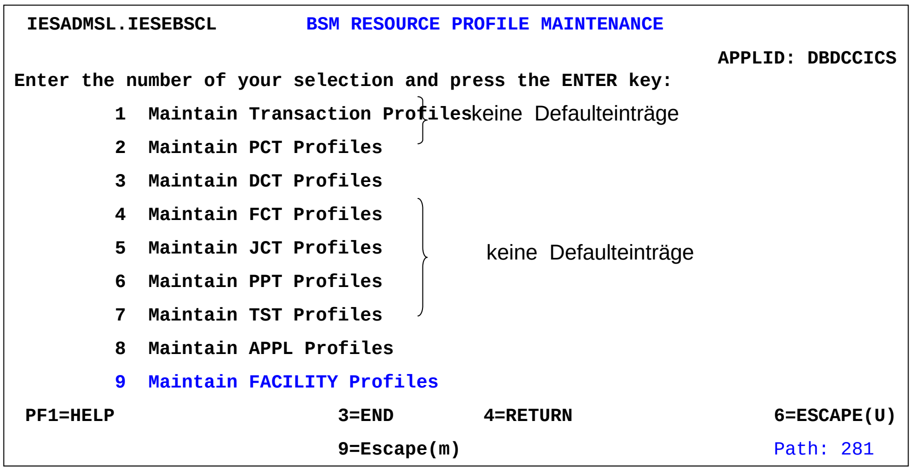
  Vorgehensweise für lokalen Fix, s. Anhang

Ressourceklasse FACILITY

Ressourcenklasse FACILITY

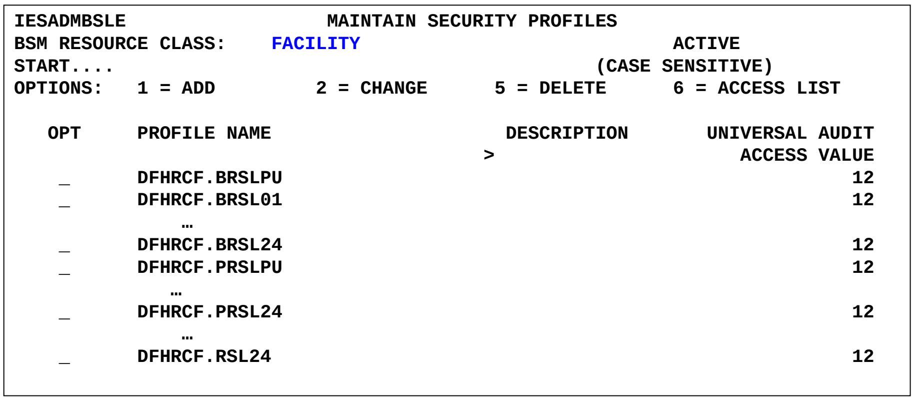
II Dialog 2.8.1 BSM RESOURCE PROFILE MAINTENANCE

„Security Checking“ für FACILITY ist per Default aktiv !



```
 IESADMSL.IESEBSCL         BSM RESOURCE PROFILE MAINTENANCE
                                                              APPLID: DBDCCICS
Enter the number of your selection and press the ENTER key:
         1  Maintain Transaction Profiles   keine  Defaulteinträge
         2  Maintain PCT Profiles
         3  Maintain DCT Profiles
         4  Maintain FCT Profiles
         5  Maintain JCT Profiles              keine  Defaulteinträge
         6  Maintain PPT Profiles
         7  Maintain TST Profiles
         8  Maintain APPL Profiles
         9  Maintain FACILITY Profiles
 PF1=HELP                    3=END        4=RETURN                   6=ESCAPE(U)
                             9=Escape(m)                             Path: 281
```

II Dialog 2.8.2: Maintain FACILITY Profiles



```
IESADMBSLE                  MAINTAIN SECURITY PROFILES
BSM RESOURCE CLASS:     FACILITY                         ACTIVE
START....                                         (CASE SENSITIVE)
OPTIONS:    1 = ADD         2 = CHANGE      5 = DELETE      6 = ACCESS LIST

   OPT      PROFILE NAME                     DESCRIPTION        UNIVERSAL AUDIT
                                           >                       ACCESS VALUE
    _       DFHRCF.BRSLPU                                                    12
    _       DFHRCF.BRSL01                                                    12
                …
    _       DFHRCF.BRSL24                                                    12
    _       DFHRCF.PRSLPU                                                    12
               …
    _       DFHRCF.PRSL24                                                    12
                …
    _       DFHRCF.RSL24                                                     12
```

Diese Ressourcen werden benötigt für Programme mit
EXEC CICS SPOOLOPEN / SPOOLREAD / SPOOLWRITE / SPOOLCLOSE
und für CICS Report Control Facility.

Übersicht

- S. 7 BSM-Konzept ab z/VSE 3.1.1
- S. 16 Security-Einstellungen bei der Auslieferung
- S. 50 Anlegen/Löschen von User Profiles
  - z/VSE BSM Cross Reference Tool (BSTXREF)
- S. 61 Migration der Transaktionen von der DTSECTXN
- S. 66 Audit/Logging und Reporting

Anhang

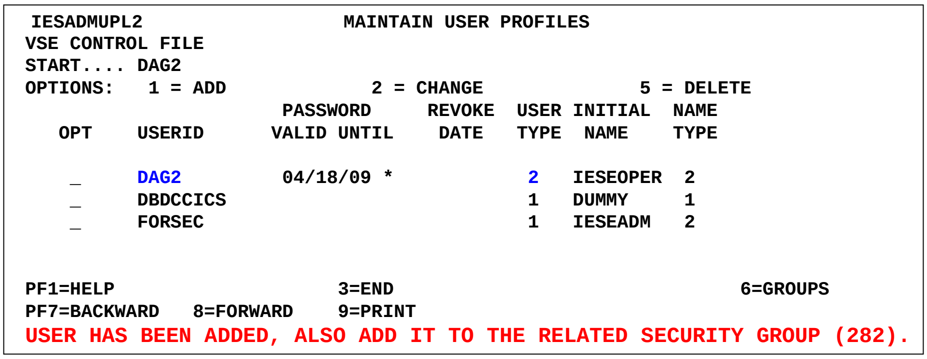
- S. 76 BSTADMIN-Befehle
- S. 80 File Ressourceklasse im CICS aktivieren
- S. 84 Details zur Migration der Transaktionen von der DTSEXTXN

Anlegen/Löscher User Profile

Anlegen/Löschen von User Profiles

- z/VSE BSM Cross Reference Tool (BSTXREF)

Neuen Benutzer angelegt mit II-Dialog 2.1.1



```
 IESADMUPL2                      MAINTAIN USER PROFILES
VSE CONTROL FILE
START.... DAG2
OPTIONS:   1 = ADD                2 = CHANGE                5 = DELETE
                       PASSWORD      REVOKE  USER INITIAL  NAME
   OPT     USERID     VALID UNTIL     DATE   TYPE  NAME    TYPE

    _      DAG2        04/18/09 *              2   IESEOPER  2
    _      DBDCCICS                            1   DUMMY     1
    _      FORSEC                              1   IESEADM   2


PF1=HELP                    3=END                               6=GROUPS
PF7=BACKWARD   8=FORWARD    9=PRINT
USER HAS BEEN ADDED, ALSO ADD IT TO THE RELATED SECURITY GROUP (282).
```

- Userid DAG2 ist jetzt im **VSE CONTROL FILE**
- Braucht noch Ressource-Berechtigungen:
  - über entsprechenden Gruppen
  - direkt eingetragen in die Access-Liste der benötigten Ressourcen

•Alternative zu Dialog 2.1.1: mit Batch-Utility IESUPCF (ICCF-Lib 59)

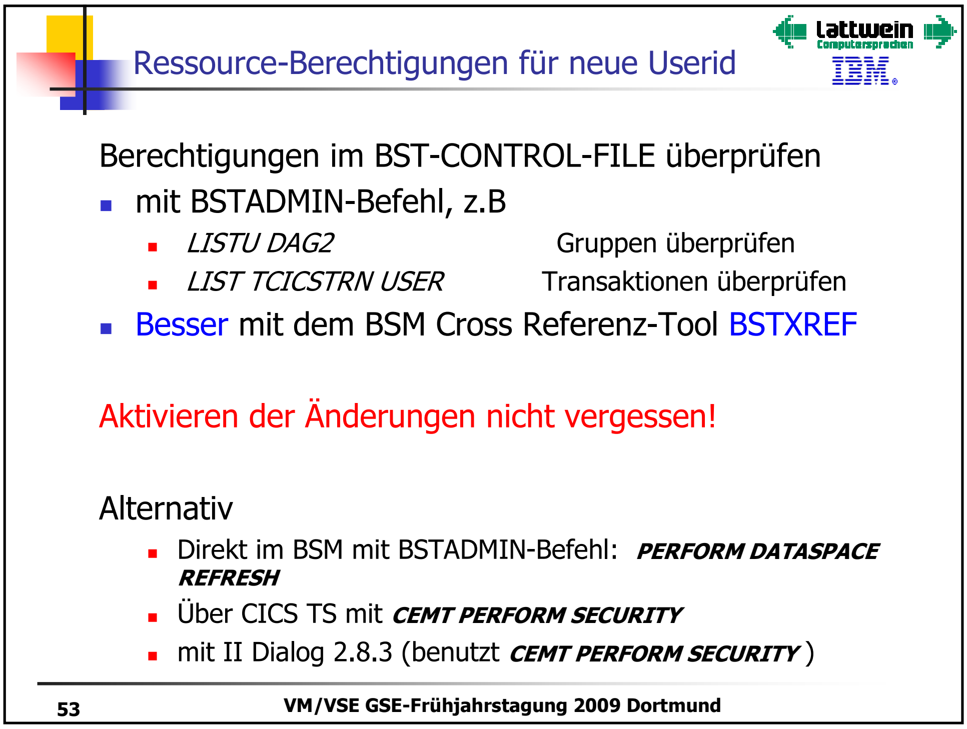
Ressource-Berechtigungen für neue Userid

Userid bei den entsprechenden Gruppen hinzufügen:

- II-Dialog 281 mit PF6 GROUPS (besser nicht!)
  - Unterstützt **nur Gruppenkonzept:**
    - GROUP01 – GROUP64 entsprechend dem Transaction Security Keys 01 – 64 im User-Profile
  - Für alle Benutzer wird Gruppeneinteilung gemacht
  - sollte **nur einmalig** bei der Migration genutzt werden
  - Sonst sind zwischenzeitlich gemachte Gruppen-Definitionen überschreiben
- über II-Dialog 282 BSM Group Maintenance
  - GROUP01 für CICS-Transaktionen
  - GROUP61 für Nutzung der II-Dialoge
- Per EXEC BSTADMIN *CONNECT GROUP01 DAG2*

Oder direkt in Access-Liste der benötigten Ressourcen, wenn sinnvoll

- per Batch mit EXEC BSTADMIN
  PERMIT TCICSTRN USER ID(DAG2) ACCESS(READ)
- II-DIALOG 2.8.1 BSM Resource Profile Maintenance



Ressource-Berechtigungen für neue Userid

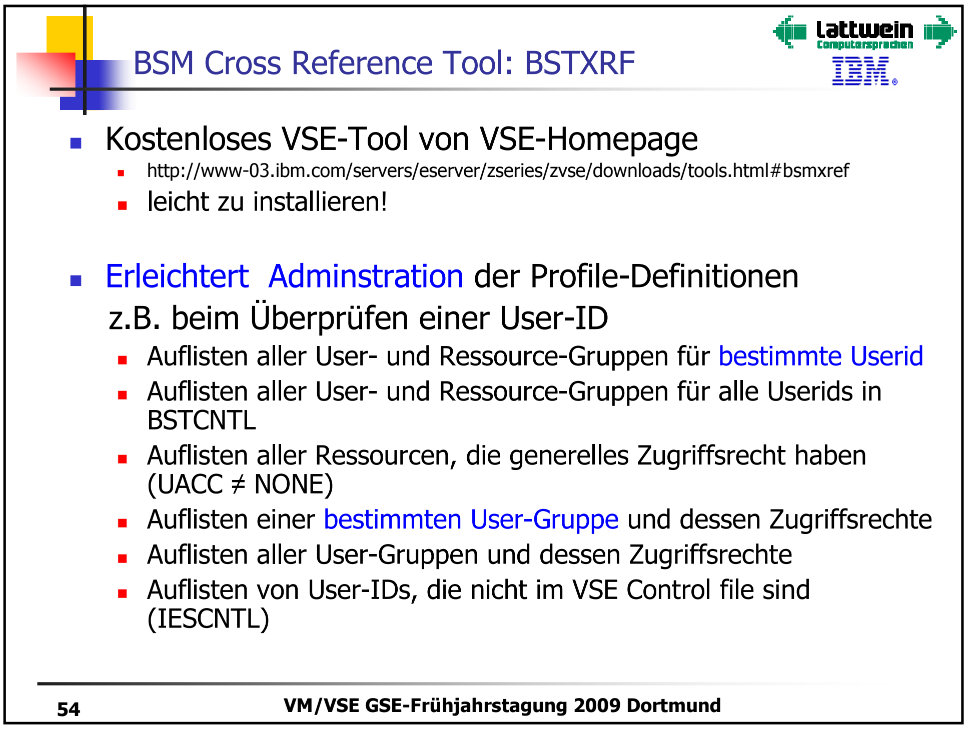
Berechtigungen im BST-CONTROL-FILE überprüfen

- mit BSTADMIN-Befehl, z.B
  - *LISTU DAG2* Gruppen überprüfen
  - *LIST TCICSTRN USER* Transaktionen überprüfen
- Besser mit dem BSM Cross Referenz-Tool BSTXREF

Aktivieren der Änderungen nicht vergessen!

Alternativ

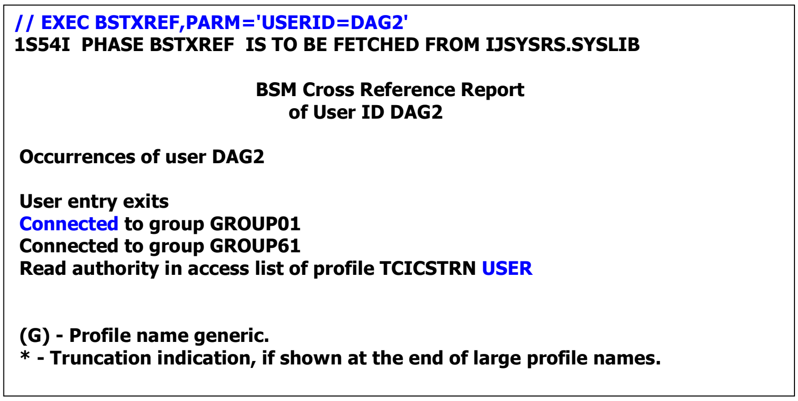
- Direkt im BSM mit BSTADMIN-Befehl: ***PERFORM DATASPACE REFRESH***
- Über CICS TS mit ***CEMT PERFORM SECURITY***
- mit II Dialog 2.8.3 (benutzt ***CEMT PERFORM SECURITY***)



BSM Cross Reference Tool: BSTXRF

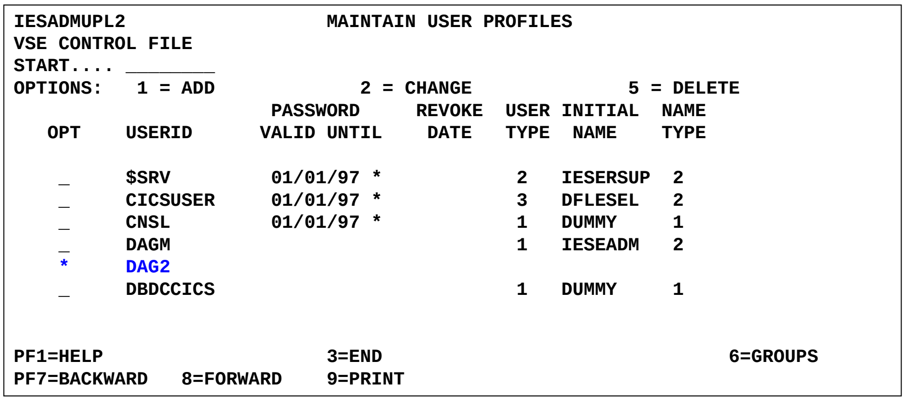
- Kostenloses VSE-Tool von VSE-Homepage
  - http://www-03.ibm.com/servers/eserver/zseries/zvse/downloads/tools.html#bsmxref
  - leicht zu installieren!
- Erleichtert Adminstration der Profile-Definitionen
  z.B. beim Überprüfen einer User-ID
  - Auflisten aller User- und Ressource-Gruppen für bestimmte Userid
  - Auflisten aller User- und Ressource-Gruppen für alle Userids in BSTCNTL
  - Auflisten aller Ressourcen, die generelles Zugriffsrecht haben (UACC ≠ NONE)
  - Auflisten einer bestimmten User-Gruppe und dessen Zugriffsrechte
  - Auflisten aller User-Gruppen und dessen Zugriffsrechte
  - Auflisten von User-IDs, die nicht im VSE Control file sind (IESCNTL)

BSTXREF-Beispiel: DAG2



```
// EXEC BSTXREF,PARM='USERID=DAG2'
1S54I  PHASE BSTXREF  IS TO BE FETCHED FROM IJSYSRS.SYSLIB

                              BSM Cross Reference Report
                                   of User ID DAG2

Occurrences of user DAG2

User entry exits
Connected to group GROUP01
Connected to group GROUP61
Read authority in access list of profile TCICSTRN USER


(G) - Profile name generic.
* - Truncation indication, if shown at the end of large profile names.
```

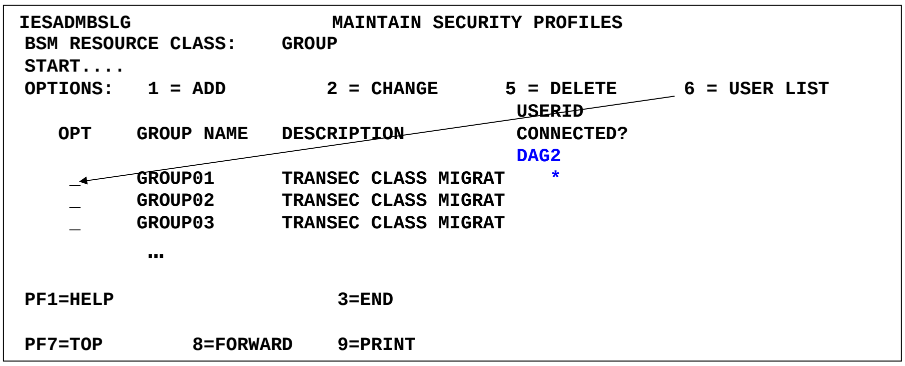
Benutzer gelöscht mit II-Dialog 2.1.1



```
IESADMUPL2                   MAINTAIN USER PROFILES
VSE CONTROL FILE
START.... ________
OPTIONS:   1 = ADD             2 = CHANGE              5 = DELETE
                       PASSWORD     REVOKE  USER INITIAL  NAME
   OPT     USERID     VALID UNTIL    DATE   TYPE  NAME    TYPE

    _      $SRV        01/01/97 *            2   IESERSUP  2
    _      CICSUSER    01/01/97 *            3   DFLESEL   2
    _      CNSL        01/01/97 *            1   DUMMY     1
    _      DAGM                              1   IESEADM   2
    *      DAG2
    _      DBDCCICS                          1   DUMMY     1


PF1=HELP                     3=END                                6=GROUPS
PF7=BACKWARD   8=FORWARD     9=PRINT
```

Benutzer sollte auch aus den Gruppen-/Userlisten gelöscht werden

Benutzer aus Gruppen löschen mit II-Dialog 2.8.2



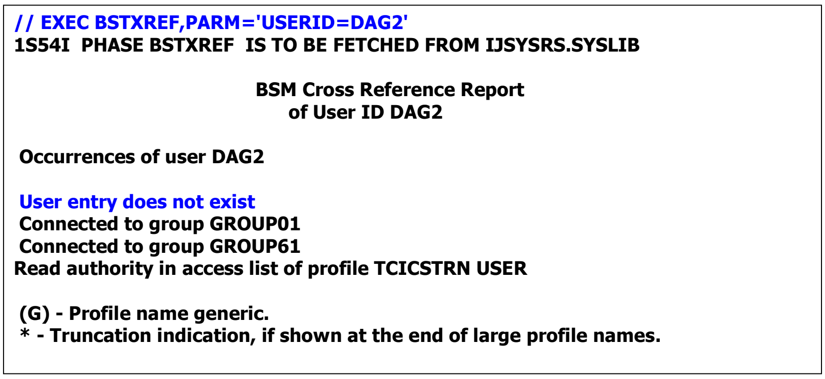
```
IESADMBSLG                   MAINTAIN SECURITY PROFILES
 BSM RESOURCE CLASS:    GROUP
 START....
 OPTIONS:   1 = ADD        2 = CHANGE      5 = DELETE      6 = USER LIST
                                            USERID
    OPT    GROUP NAME   DESCRIPTION         CONNECTED?
                                            DAG2
     _      GROUP01      TRANSEC CLASS MIGRAT    *
     _      GROUP02      TRANSEC CLASS MIGRAT
     _      GROUP03      TRANSEC CLASS MIGRAT
             ...

 PF1=HELP                    3=END

 PF7=TOP        8=FORWARD    9=PRINT
```

Effektiver ist aber:

- Auflisten aller User- und Resource-Gruppen für die Userid DAG2 mit dem BSM Cross Referenz-Tool BSTXREF

- Löschen mit BSTADMIN-Befehl

BSTXREF-Beispiel: DAG2 nach Löschen der Userid



```
// EXEC BSTXREF,PARM='USERID=DAG2'
1S54I  PHASE BSTXREF  IS TO BE FETCHED FROM IJSYSRS.SYSLIB

                    BSM Cross Reference Report
                        of User ID DAG2

 Occurrences of user DAG2

 User entry does not exist
 Connected to group GROUP01
 Connected to group GROUP61
Read authority in access list of profile TCICSTRN USER

 (G) - Profile name generic.
 * - Truncation indication, if shown at the end of large profile names.
```

BSTADMIN-Beispiel: Löschen von DAG2 aus Profiles

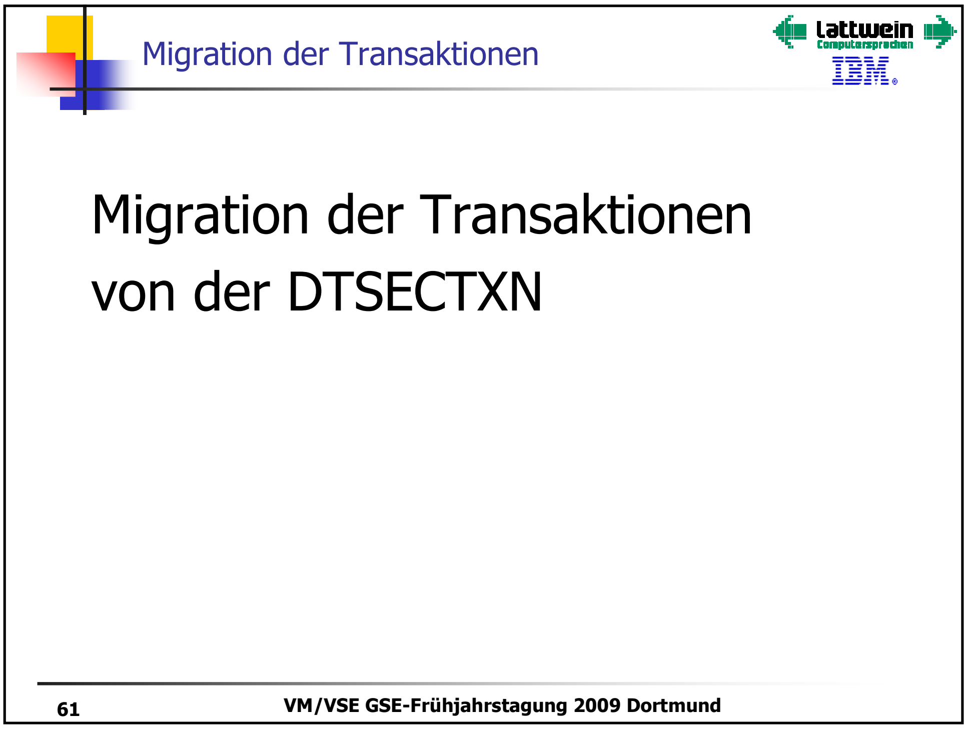
```
* $$ JOB JNM=BSTADMIN,CLASS=4,DISP=D
// JOB BSTADMIN
// ID USER=FORSEC,PWD=FORSEC
// EXEC BSTADMIN
REMOVE GROUP01 DAG2
REMOVE GROUP61 DAG2
*
PERMIT TCICSTRN USER ID(DAG2) DELETE
/*
/&
* $$ EOJ
```

Übersicht

- S. 7 BSM-Konzept ab z/VSE 3.1.1
- S. 16 Security-Einstellungen bei der Auslieferung
- S. 50 Anlegen/Löschen von User Profiles
  - z/VSE BSM Cross Reference Tool (BSTXREF)
- S. 61 Migration der Transaktionen von der DTSECTXN
- S. 66 Audit/Logging und Reporting

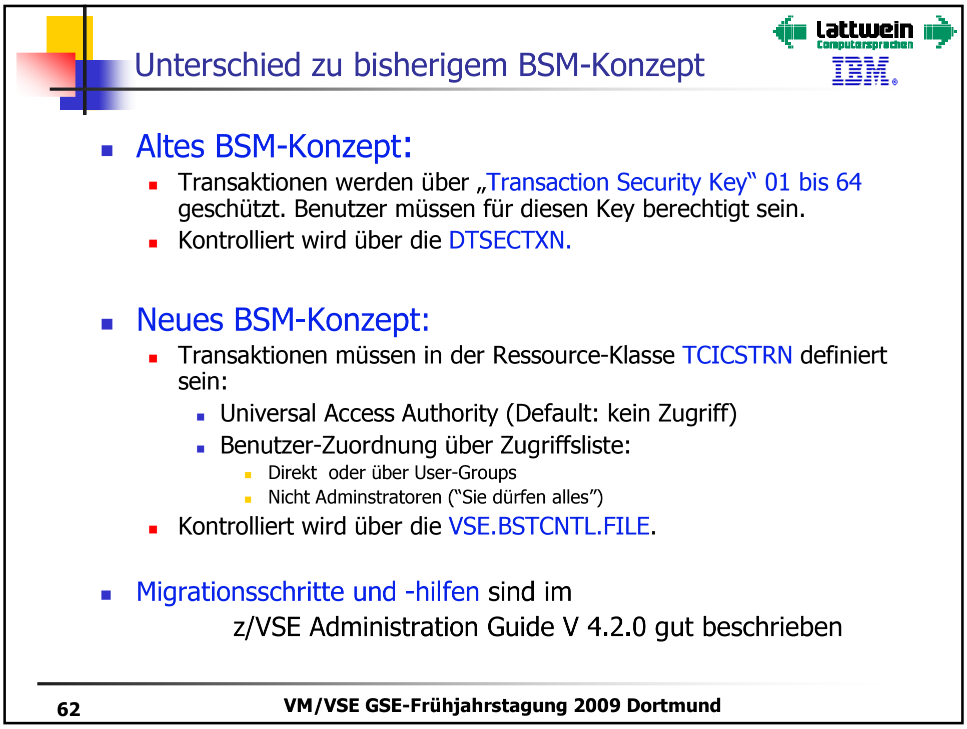
Anhang

- S. 76 BSTADMIN-Befehle
- S. 80 File Ressourceklasse im CICS aktivieren
- S. 84 Details zur Migration der Transaktionen von der DTSEXTXN



Migration der Transaktionen

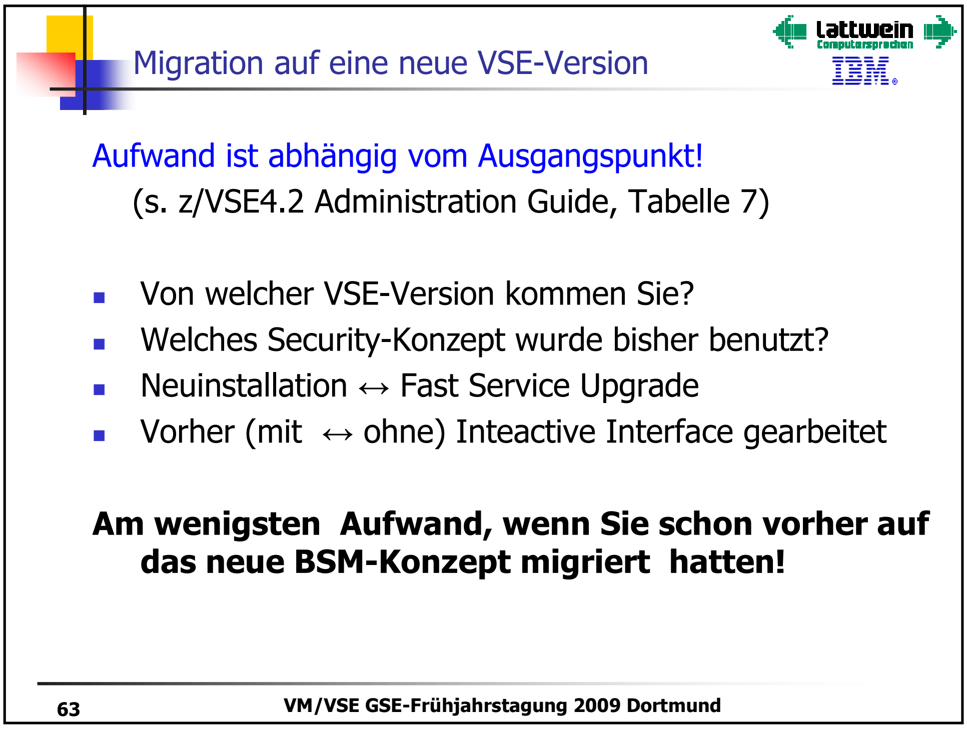
Migration der Transaktionen von der DTSECTXN



Unterschied zu bisherigem BSM-Konzept

- Altes BSM-Konzept:
  - Transaktionen werden über „Transaction Security Key" 01 bis 64 geschützt. Benutzer müssen für diesen Key berechtigt sein.
  - Kontrolliert wird über die DTSECTXN.
- Neues BSM-Konzept:
  - Transaktionen müssen in der Ressource-Klasse TCICSTRN definiert sein:
    - Universal Access Authority (Default: kein Zugriff)
    - Benutzer-Zuordnung über Zugriffsliste:
      - Direkt oder über User-Groups
      - Nicht Adminstratoren ("Sie dürfen alles")
  - Kontrolliert wird über die VSE.BSTCNTL.FILE.
- Migrationsschritte und -hilfen sind im

  z/VSE Administration Guide V 4.2.0 gut beschrieben

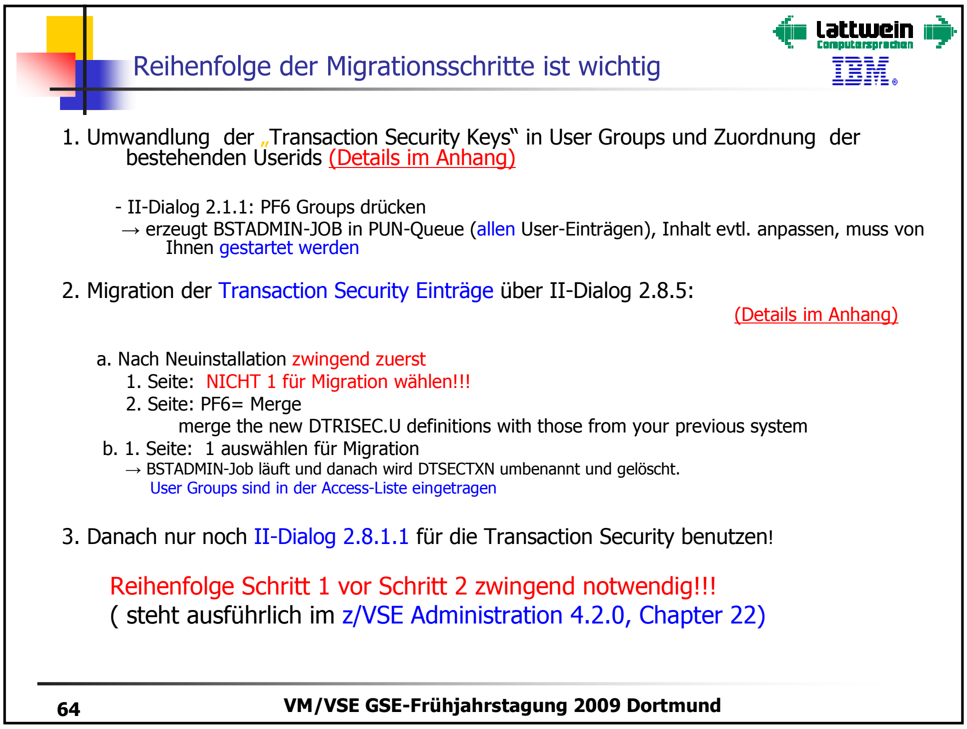


Migration auf eine neue VSE-Version

Aufwand ist abhängig vom Ausgangspunkt!
(s. z/VSE4.2 Administration Guide, Tabelle 7)

- Von welcher VSE-Version kommen Sie?
- Welches Security-Konzept wurde bisher benutzt?
- Neuinstallation ↔ Fast Service Upgrade
- Vorher (mit ↔ ohne) Inteactive Interface gearbeitet

Am wenigsten Aufwand, wenn Sie schon vorher auf das neue BSM-Konzept migriert hatten!



Reihenfolge der Migrationsschritte ist wichtig

1. Umwandlung der „Transaction Security Keys“ in User Groups und Zuordnung der bestehenden Userids (Details im Anhang)

   - II-Dialog 2.1.1: PF6 Groups drücken
   → erzeugt BSTADMIN-JOB in PUN-Queue (allen User-Einträgen), Inhalt evtl. anpassen, muss von Ihnen gestartet werden

2. Migration der Transaction Security Einträge über II-Dialog 2.8.5:
   (Details im Anhang)

   a. Nach Neuinstallation zwingend zuerst
      1. Seite: NICHT 1 für Migration wählen!!!
      2. Seite: PF6= Merge
         merge the new DTRISEC.U definitions with those from your previous system
   b. 1. Seite: 1 auswählen für Migration
      → BSTADMIN-Job läuft und danach wird DTSECTXN umbenannt und gelöscht.
      User Groups sind in der Access-Liste eingetragen

3. Danach nur noch II-Dialog 2.8.1.1 für die Transaction Security benutzen!

Reihenfolge Schritt 1 vor Schritt 2 zwingend notwendig!!!
(steht ausführlich im z/VSE Administration 4.2.0, Chapter 22)

Übersicht

- S. 7 BSM-Konzept ab z/VSE 3.1.1
- S. 16 Security-Einstellungen bei der Auslieferung
- S. 50 Anlegen/Löschen von User Profiles
  - z/VSE BSM Cross Reference Tool (BSTXREF)
- S. 61 Migration der Transaktionen von der DTSECTXN
- S. 66 Audit/Logging und Reporting

Anhang

- S. 76 BSTADMIN-Befehle
- S. 80 File Ressourceklasse im CICS aktivieren
- S. 84 Details zur Migration der Transaktionen von der DTSEXTXN

Audit/Logging und Reporting

Audit/Logging und Reporting mit dem BSM Report Writer

Audit/Logging und Reporting

Logging der im BSM Control File gespeicherten Ressourcen

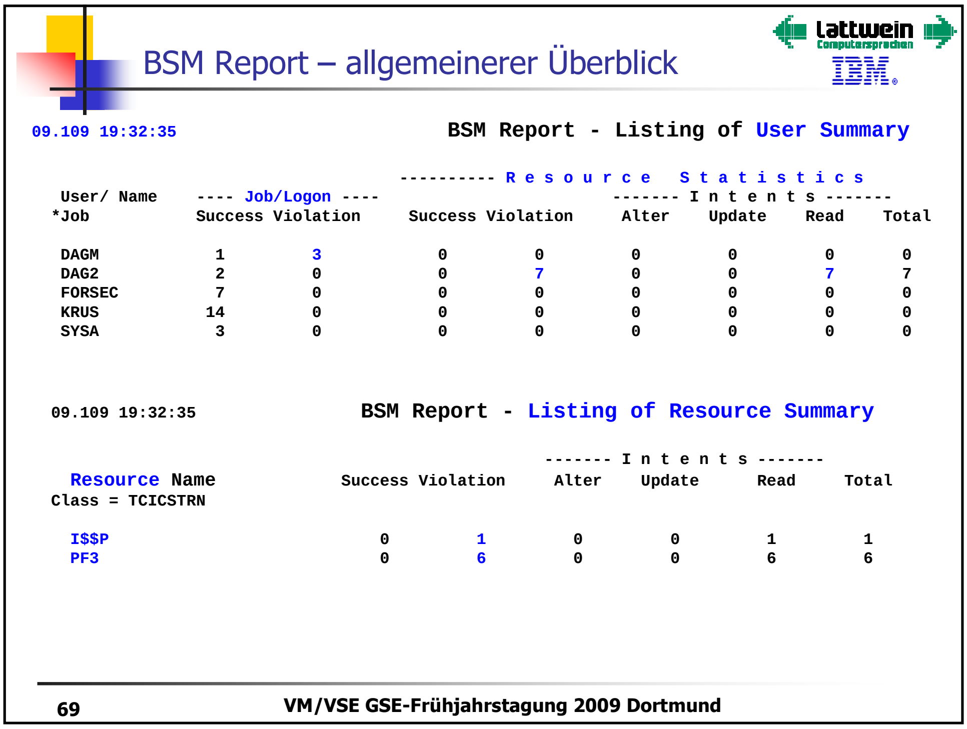
- Alle Zugriffe auf geschützte Ressourcen können protokolliert werden
  - Sowohl erlaubte als auch unerlaubte Zugriffe
- Versuchte Angriffe können erkannt werden
  - z.B. mehrfache Logon-Versuche mit falschem Passwort
- Man kann nachvollziehen, wer wann welche Ressource im Zugriff hatte

- Auswertung mit Hilfe eines Report-Tools
  - BSM Report Writer (BSMRPWTR) (s. ICCF-lib 59)
  - Detaillierte Auflistung aller Zugriffe – Allgemeinere Überblick- Kurzfassung am Ende (diese zuerst ansehen!)
- Benutzt das CICS DMF Tool
  - Erstellt SMF Records für Protokoll-Informationen

- **Implementierung und Report-Erstellung ist sehr einfach !**
- Gute Beschreibung im Redbook-Draft: 'Security on z/VSE', SG247691

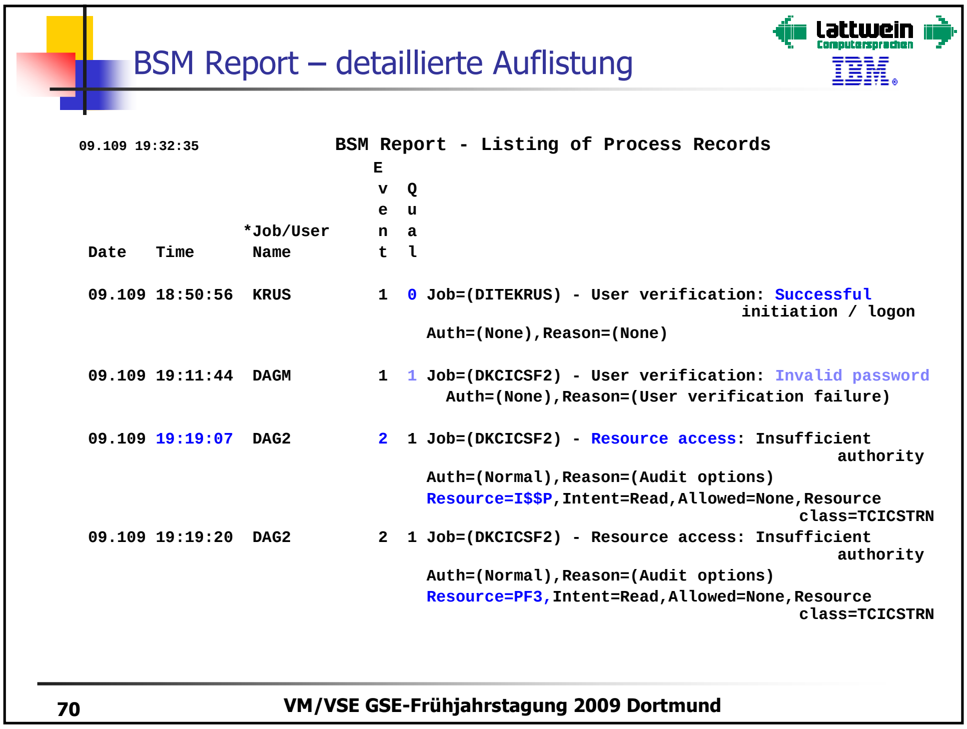
BSM Report – Kurzfassung

```
09.109 19:32:35                           BSM Report - General
   Summary

  Process records:                                    60

                                       --- Job / Logon
   Statistics ---
  Total Job/Logon/Logoff                              52
  Total Job/Logon successes                           27
  Total Job/Logon violations                           3
  Total Job/Logon attempts by undefined users          0
  Total Job/Logon successful terminations             22

                                       --- Resource Statistics --
   -
  Total resource accesses (all events)                 7
  Total resource access successes                      0
  Total resource access violations                     7
```



BSM Report – allgemeinerer Überblick

```
09.109 19:32:35                       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

 DAGM                1         3         0         0         0         0        0        0
 DAG2                2         0         0         7         0         0        7        7
 FORSEC              7         0         0         0         0         0        0        0
 KRUS               14         0         0         0         0         0        0        0
 SYSA                3         0         0         0         0         0        0        0


09.109 19:32:35                   BSM Report - Listing of Resource Summary

                                                   ------- I n t e n t s -------
  Resource Name                 Success Violation   Alter    Update    Read     Total
Class = TCICSTRN

  I$$P                              0         1         0         0        1        1
  PF3                               0         6         0         0        6        6
```

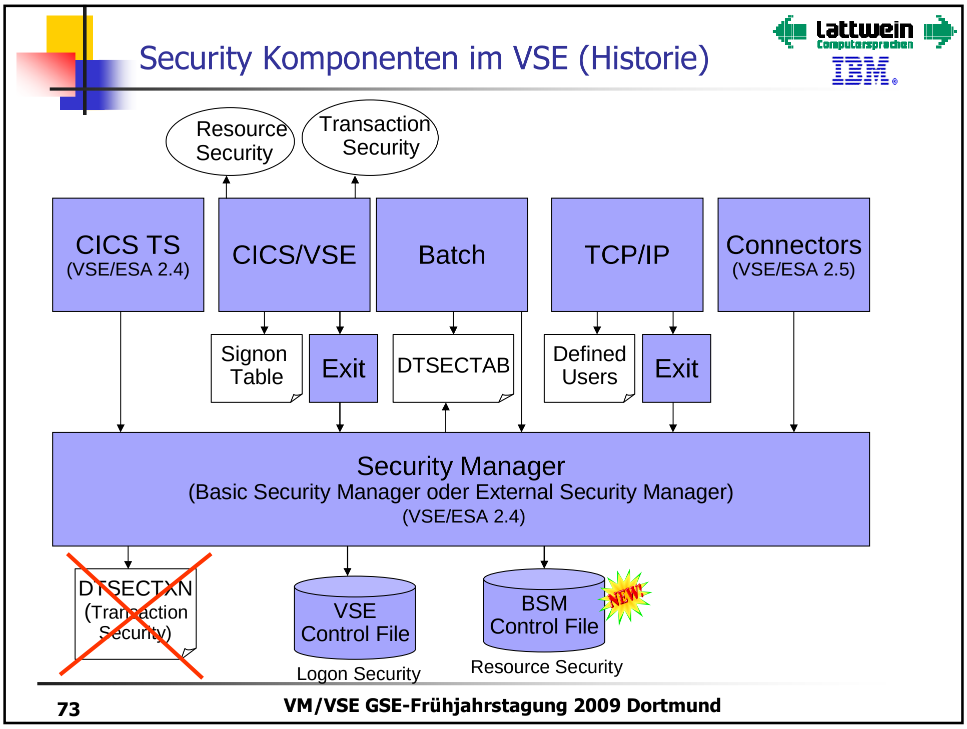


BSM Report – detaillierte Auflistung

```
09.109 19:32:35                BSM Report - Listing of Process Records
                                          E
                                          v  Q
                                          e  u
                         *Job/User        n  a
 Date     Time            Name            t  l

 09.109 18:50:56  KRUS            1  0 Job=(DITEKRUS) - User verification: Successful
                                                                initiation / logon
                                       Auth=(None),Reason=(None)

 09.109 19:11:44  DAGM            1  1 Job=(DKCICSF2) - User verification: Invalid password
                                         Auth=(None),Reason=(User verification failure)

 09.109 19:19:07  DAG2            2  1 Job=(DKCICSF2) - Resource access: Insufficient
                                                                          authority
                                       Auth=(Normal),Reason=(Audit options)
                                       Resource=I$$P,Intent=Read,Allowed=None,Resource
                                                                      class=TCICSTRN
 09.109 19:19:20  DAG2            2  1 Job=(DKCICSF2) - Resource access: Insufficient
                                                                          authority
                                       Auth=(Normal),Reason=(Audit options)
                                       Resource=PF3,Intent=Read,Allowed=None,Resource
                                                                      class=TCICSTRN
```

Vielen Dank für Ihre Aufmerksamkeit

Anhang



Security Komponenten im VSE (Historie)

Resource Security

Transaction Security

CICS TS (VSE/ESA 2.4)

CICS/VSE

Batch

TCP/IP

Connectors (VSE/ESA 2.5)

Signon Table

Exit

DTSECTAB

Defined Users

Exit

Security Manager
(Basic Security Manager oder External Security Manager)
(VSE/ESA 2.4)

~~DTSECTXN (Transaction Security)~~

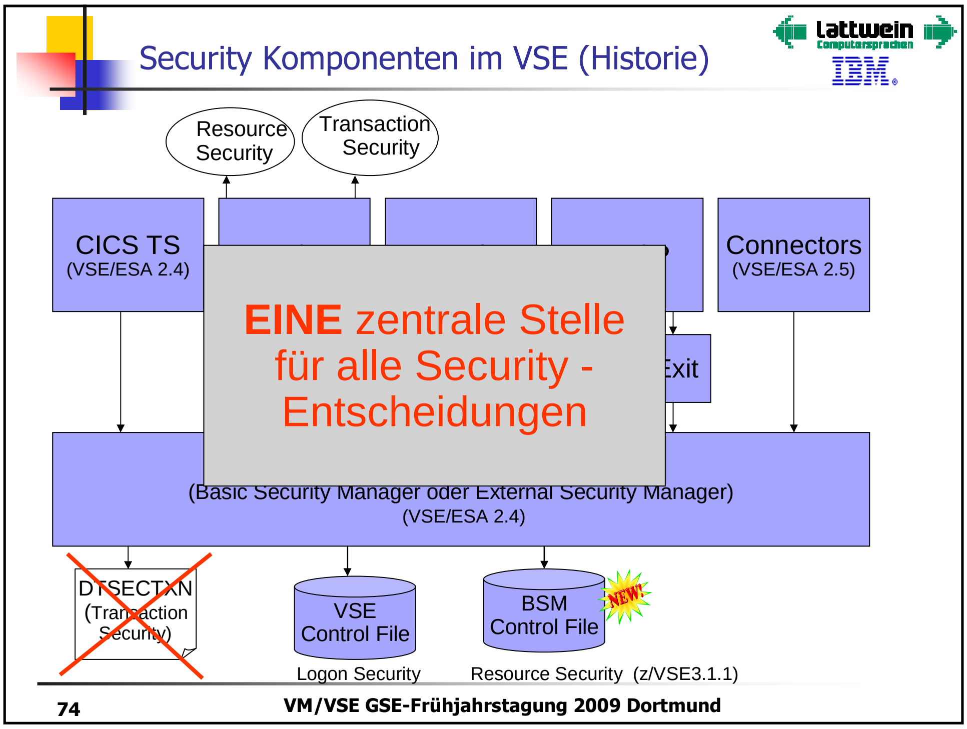
VSE Control File

Logon Security

BSM Control File

NEW!

Resource Security



Security Komponenten im VSE (Historie)

Resource Security

Transaction Security

CICS TS (VSE/ESA 2.4)

Connectors (VSE/ESA 2.5)

Exit

EINE zentrale Stelle für alle Security - Entscheidungen

(Basic Security Manager oder External Security Manager)
(VSE/ESA 2.4)

~~DTSECTXN (Transaction Security)~~

VSE Control File

Logon Security

BSM Control File

NEW!

Resource Security (z/VSE3.1.1)

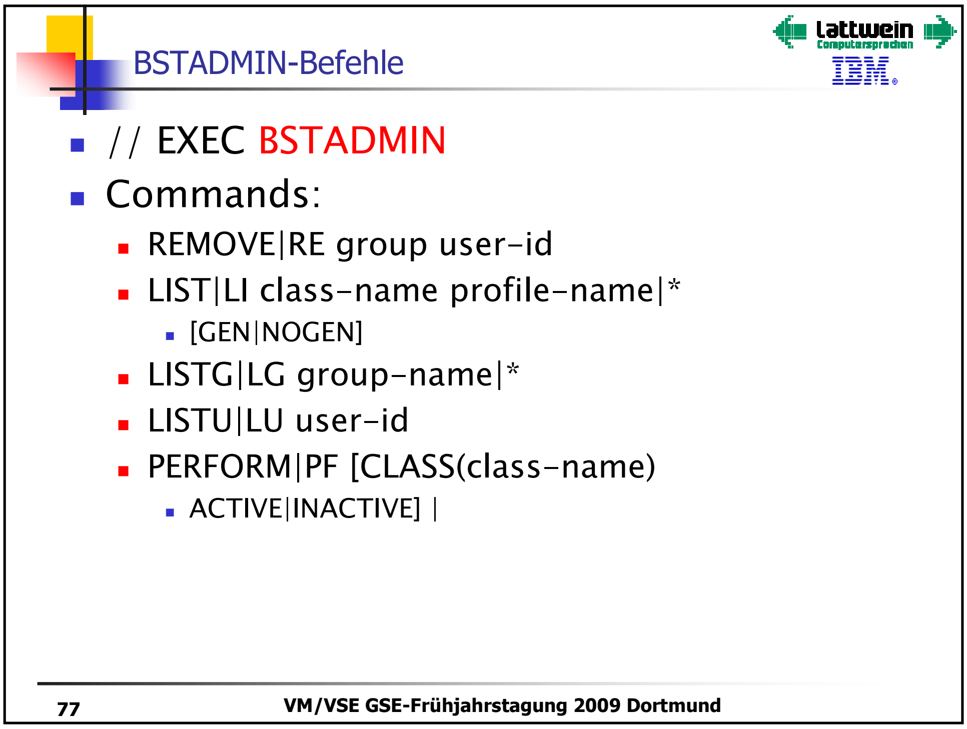
BSTADMIN-Befehle

// EXEC BSTADMIN

- Commands:
  - ADD|AD class-name profile-name
    - [GEN|NOGEN] [UACC(uacc)]
    - [DATA('installation-data')]
  - CHANGE|CH class-name profile-name [GEN|NOGEN] [UACC(uacc)]
    - [DATA('installation-data')]
  - DELETE|DE class-name profile-name
    - [GEN|NOGEN]

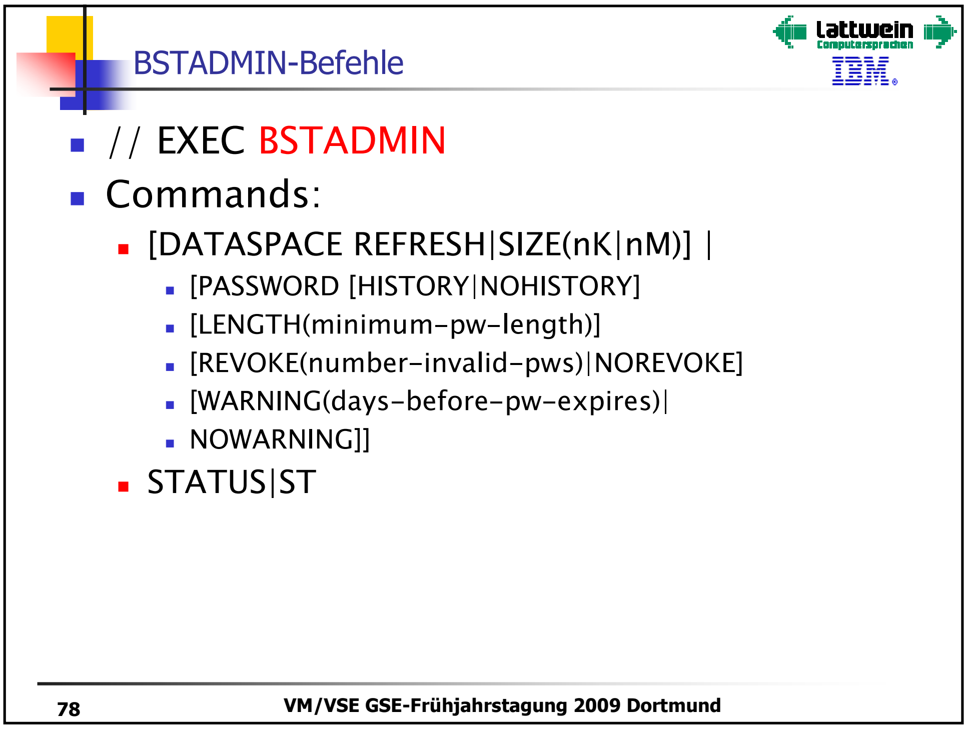
BSTADMIN-Befehle

- // EXEC BSTADMIN
- Commands:
  - PERMIT|PE
    - class-name profile-name [GEN|NOGEN]
    - ID(name)
    - ACCESS(access)|DELETE
  - ADDGROUP|AG group
    - [DATA('installation-data')]
  - CHNGROUP|CG group
    - [DATA('installation-data')]
  - DELGROUP|DG group
  - CONNECT|CO group user-id



BSTADMIN-Befehle

- // EXEC BSTADMIN
- Commands:
  - REMOVE|RE group user-id
  - LIST|LI class-name profile-name|*
    - [GEN|NOGEN]
  - LISTG|LG group-name|*
  - LISTU|LU user-id
  - PERFORM|PF [CLASS(class-name)
    - ACTIVE|INACTIVE] |



BSTADMIN-Befehle

- // EXEC BSTADMIN
- Commands:
  - [DATASPACE REFRESH|SIZE(nK|nM)] |
    - [PASSWORD [HISTORY|NOHISTORY]
    - [LENGTH(minimum-pw-length)]
    - [REVOKE(number-invalid-pws)|NOREVOKE]
    - [WARNING(days-before-pw-expires)|
    - NOWARNING]]
  - STATUS|ST

FCICSFCT für CICS Dateien aktivieren

- Shutdown-Problem mit BSTCNTL und IJSYSPF:

  ➔ CICSUSER braucht READ-Zugriff geben

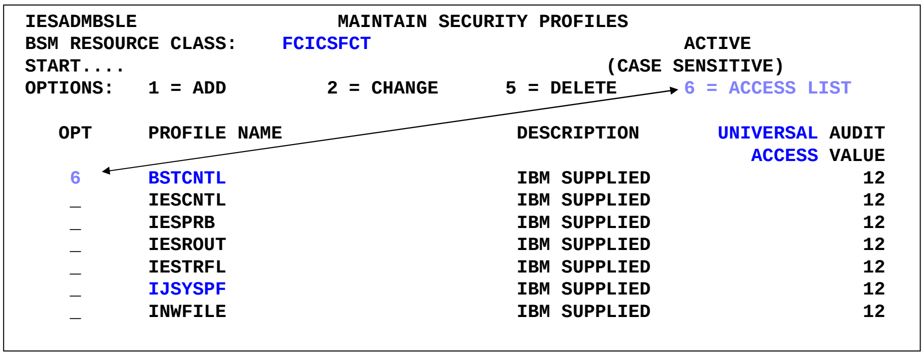
```
 F5 0101 BST120I USER(CICSUSER)
         BST120I   A0006CI2.BSTCNTL CL(FCICSFCT)
         BST120I   INSUFFICIENT ACCESS AUTHORITY
         BST120I   FROM BSTCNTL
         BST120I   ACCESS INTENT(READ    ) ACCESS ALLOWED(NONE
   )
F5 0101 BST120I USER(CICSUSER)
         BST120I   A0006CI2.IJSYSPF CL(FCICSFCT)
         BST120I   INSUFFICIENT ACCESS AUTHORITY
         BST120I   FROM IJSYSPF
         BST120I   ACCESS INTENT(READ    ) ACCESS ALLOWED(NONE
```

Lösung: PTF PK81238 (kommt mit z/VSE 4.2.1)

- BSTCNTL : Read-Zugriff (2) für GROUP01
- IJSYSPF :   Update-Zugriff (3) für GROUP01, GROUP61

Zugriff für GROUP01 bei Datei BSTCNTL

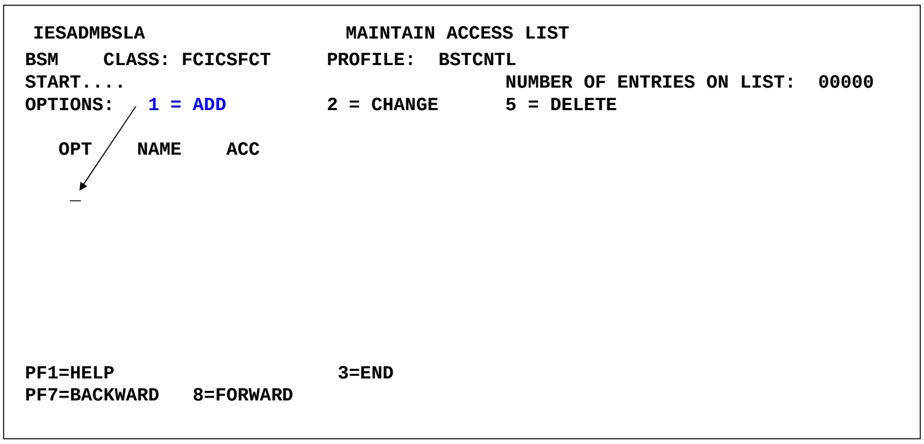
Bisher hat KEINER Zugriffsrecht, daher mit Auswahl 6 die Gruppen-/User-Liste hinzufügen.



```
IESADMBSLE                   MAINTAIN SECURITY PROFILES
BSM RESOURCE CLASS:    FCICSFCT                              ACTIVE
START....                                             (CASE SENSITIVE)
OPTIONS:    1 = ADD          2 = CHANGE       5 = DELETE      6 = ACCESS LIST

   OPT      PROFILE NAME                       DESCRIPTION         UNIVERSAL AUDIT
                                                                      ACCESS VALUE
    6       BSTCNTL                            IBM SUPPLIED                    12
    _       IESCNTL                            IBM SUPPLIED                    12
    _       IESPRB                             IBM SUPPLIED                    12
    _       IESROUT                            IBM SUPPLIED                    12
    _       IESTRFL                            IBM SUPPLIED                    12
    _       IJSYSPF                            IBM SUPPLIED                    12
    _       INWFILE                            IBM SUPPLIED                    12
```

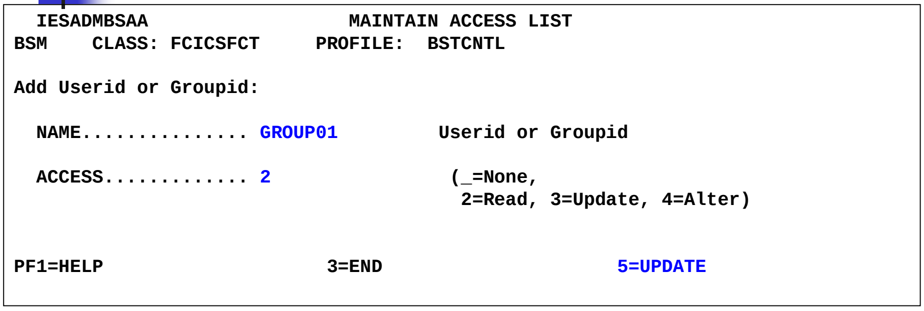
ACCESS-LIST bei Datei BSTCNTL

Mit Auswahl 1 eine Gruppe oder User hinzufügen



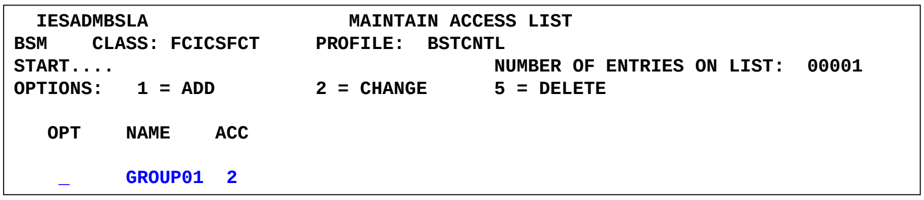
```
  IESADMBSLA                          MAINTAIN ACCESS LIST
 BSM     CLASS: FCICSFCT      PROFILE:   BSTCNTL
 START....                                      NUMBER OF ENTRIES ON LIST:   00000
 OPTIONS:     1 = ADD           2 = CHANGE       5 = DELETE

    OPT      NAME     ACC

    _




 PF1=HELP                            3=END
 PF7=BACKWARD    8=FORWARD
```

ACCESS-LIST bei Datei BSTCNTL



```
   IESADMBSAA                          MAINTAIN ACCESS LIST
 BSM     CLASS: FCICSFCT      PROFILE:   BSTCNTL

 Add Userid or Groupid:

   NAME............... GROUP01          Userid or Groupid

   ACCESS............. 2                 (_=None,
                                          2=Read, 3=Update, 4=Alter)


 PF1=HELP                           3=END                        5=UPDATE
```

Änderung aktivieren durch PF5:

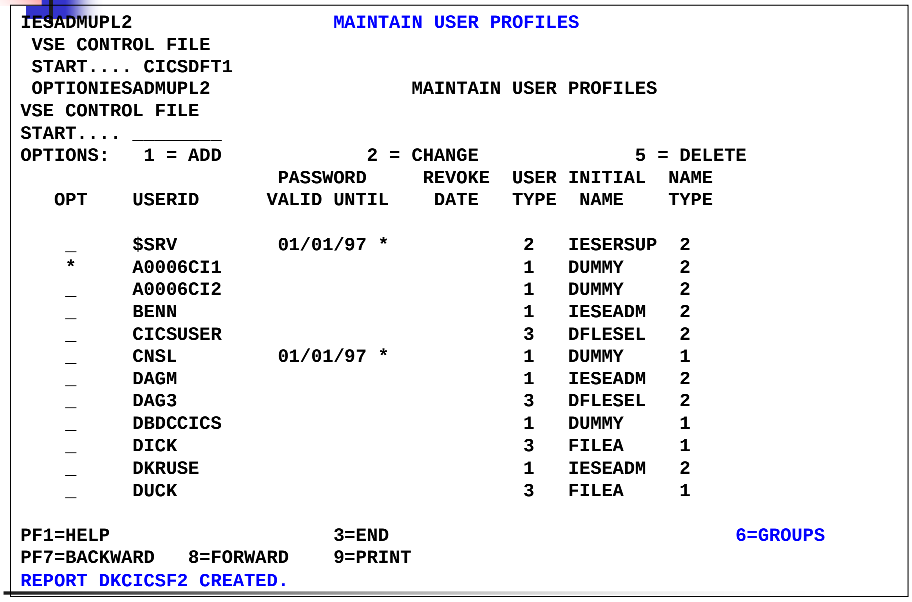


```
   IESADMBSLA                          MAINTAIN ACCESS LIST
 BSM     CLASS: FCICSFCT      PROFILE:   BSTCNTL
 START....                                      NUMBER OF ENTRIES ON LIST:   00001
 OPTIONS:    1 = ADD           2 = CHANGE       5 = DELETE

    OPT      NAME     ACC

     _       GROUP01   2
```

Migration der Transaktionen

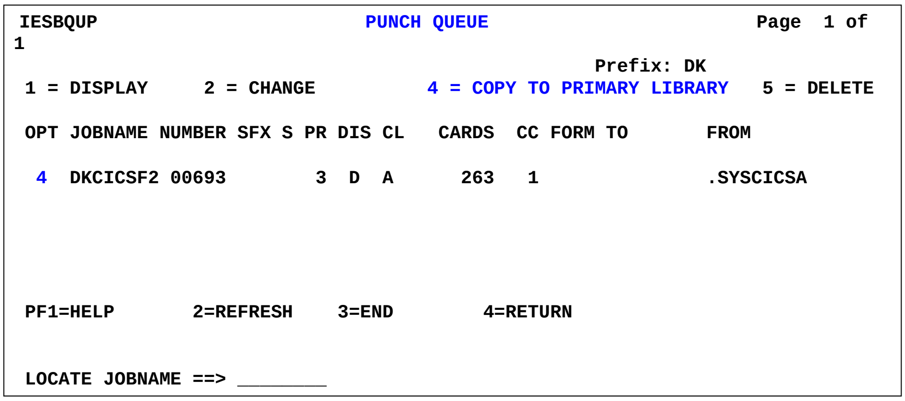
Details zur Migration der Transaktionen
von der DTSECTXN

Migration auf neues Konzept: Details zu 1.



```
IESADMUPL2                  MAINTAIN USER PROFILES
 VSE CONTROL FILE
 START.... CICSDFT1
 OPTIONIESADMUPL2                   MAINTAIN USER PROFILES
VSE CONTROL FILE
START.... ________
OPTIONS:   1 = ADD           2 = CHANGE               5 = DELETE
                     PASSWORD     REVOKE  USER INITIAL  NAME
   OPT     USERID   VALID UNTIL    DATE   TYPE  NAME    TYPE

    _      $SRV      01/01/97 *            2   IESERSUP  2
    *      A0006CI1                        1   DUMMY     2
    _      A0006CI2                        1   DUMMY     2
    _      BENN                            1   IESEADM   2
    _      CICSUSER                        3   DFLESEL   2
    _      CNSL      01/01/97 *            1   DUMMY     1
    _      DAGM                            1   IESEADM   2
    _      DAG3                            3   DFLESEL   2
    _      DBDCCICS                        1   DUMMY     1
    _      DICK                            3   FILEA     1
    _      DKRUSE                          1   IESEADM   2
    _      DUCK                            3   FILEA     1

PF1=HELP                    3=END                                6=GROUPS
PF7=BACKWARD   8=FORWARD    9=PRINT
REPORT DKCICSF2 CREATED.
```

Migration auf neues Konzept: Details zu 1.



```
IESBQUP                        PUNCH QUEUE                        Page  1 of
1
                                                      Prefix: DK
 1 = DISPLAY     2 = CHANGE          4 = COPY TO PRIMARY LIBRARY    5 = DELETE

 OPT JOBNAME NUMBER SFX S PR DIS CL   CARDS  CC FORM TO       FROM

  4  DKCICSF2 00693        3  D  A      263   1               .SYSCICSA




 PF1=HELP       2=REFRESH    3=END        4=RETURN


 LOCATE JOBNAME ==> ________
```

Migration auf neues Konzept: Details zu 1.

Report überprüfen, anpassen und abschicken!

```
// JOB IESTBGRI
* CREATED BY IESXSPR FROM IESCNTL      DATE: 04/05/09 TIME: 06:26:50
// EXEC BSTADMIN
* ADD TRANSEC CLASS MIGRATION GROUPS IN CASE NOT EXIST
 ADDGROUP GROUP01    DATA('TRANSEC CLASS MIGRAT')
 ADDGROUP GROUP02    DATA('TRANSEC CLASS MIGRAT')
 ADDGROUP GROUP03    DATA('TRANSEC CLASS MIGRAT')
…
 ADDGROUP GROUP64    DATA('TRANSEC CLASS MIGRAT')
…
* CONNECT NON ADMIN USERS TO THE GROUPS
CONNECT GROUP01   CICSUSER
CONNECT GROUP60   CICSUSER
CONNECT GROUP61   CICSUSER
CONNECT GROUP62   CICSUSER
CONNECT GROUP63   CICSUSER
CONNECT GROUP64   CICSUSER
* CNSL      IS SYSTEM ADMINISTRATOR. NOT CONNECTED TO ANY GROUP
* DAGM      IS SYSTEM ADMINISTRATOR. NOT CONNECTED TO ANY GROUP
…
* VCSRV     IS SYSTEM ADMINISTRATOR. NOT CONNECTED TO ANY GROUP
 PERFORM DATASPACE REFRESH
/*
```

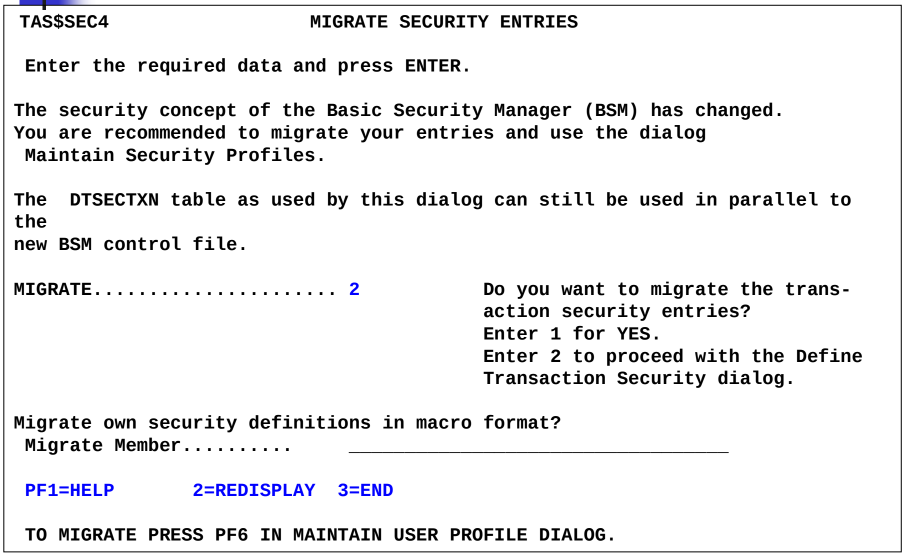
Migration auf neues Konzept: Details zu 1.

Nach Neuinstallation ist bei der Migration Return Code = 8 in Ordnung!

```
// JOB IESTBGRI
* CREATED BY IESXSPR FROM IESCNTL      DATE: 04/05/09
   TIME: 06:26:50
// EXEC BSTADMIN
1S54I  PHASE BSTADMIN IS TO BE FETCHED FROM
   IJSYSRS.SYSLIB
* ADD TRANSEC CLASS MIGRATION GROUPS IN CASE NOT EXIST
ADDGROUP GROUP01    DATA('TRANSEC CLASS MIGRAT,)
BST921I COMMAND FAILED, DUPLICATE ENTRY
BST904I RETURN CODE OF ADDGROUP IS 08
…
CONNECT GROUP01   CICSUSER
BST921I COMMAND FAILED, DUPLICATE ENTRY
BST904I RETURN CODE OF CONNECT IS 08
…
```

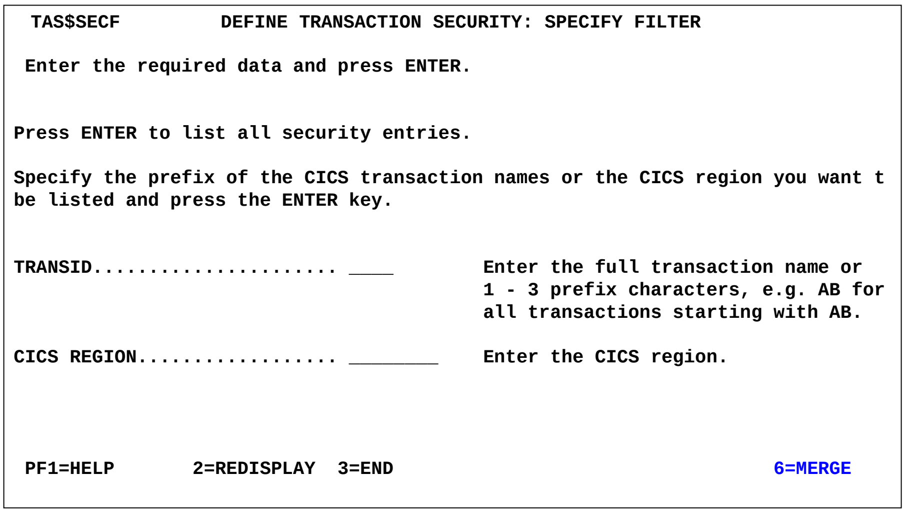
Damit sind Ihre Benutzer den entsprechenden Gruppen zugeordnet!

Migration auf neues Konzept: Details zu 2.



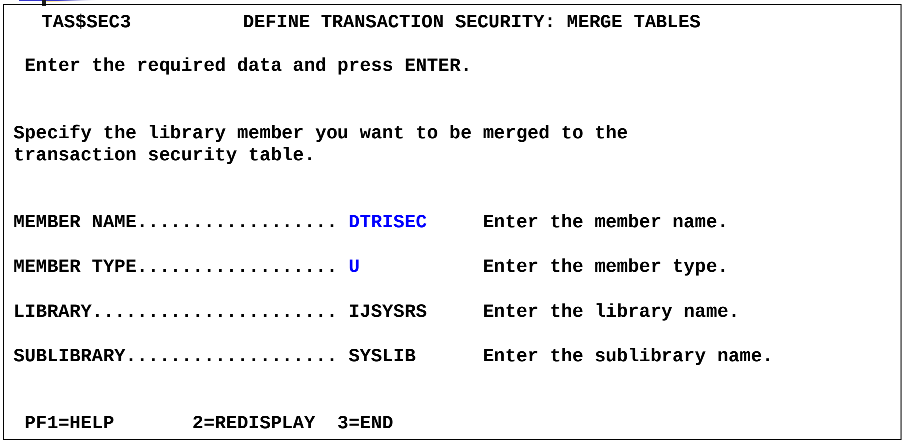
```
TAS$SEC4                         MIGRATE SECURITY ENTRIES

 Enter the required data and press ENTER.

The security concept of the Basic Security Manager (BSM) has changed.
You are recommended to migrate your entries and use the dialog
 Maintain Security Profiles.

The  DTSECTXN table as used by this dialog can still be used in parallel to
the
new BSM control file.

MIGRATE..................... 2           Do you want to migrate the trans-
                                         action security entries?
                                         Enter 1 for YES.
                                         Enter 2 to proceed with the Define
                                         Transaction Security dialog.

Migrate own security definitions in macro format?
 Migrate Member..........     __________________________________

 PF1=HELP       2=REDISPLAY  3=END

 TO MIGRATE PRESS PF6 IN MAINTAIN USER PROFILE DIALOG.
```

Migration auf neues Konzept: Details zu 2.



```
 TAS$SECF          DEFINE TRANSACTION SECURITY: SPECIFY FILTER

 Enter the required data and press ENTER.


Press ENTER to list all security entries.

Specify the prefix of the CICS transaction names or the CICS region you want t
be listed and press the ENTER key.


TRANSID..................... ____        Enter the full transaction name or
                                         1 - 3 prefix characters, e.g. AB for
                                         all transactions starting with AB.

CICS REGION................. ________    Enter the CICS region.




 PF1=HELP      2=REDISPLAY  3=END                                  6=MERGE
```

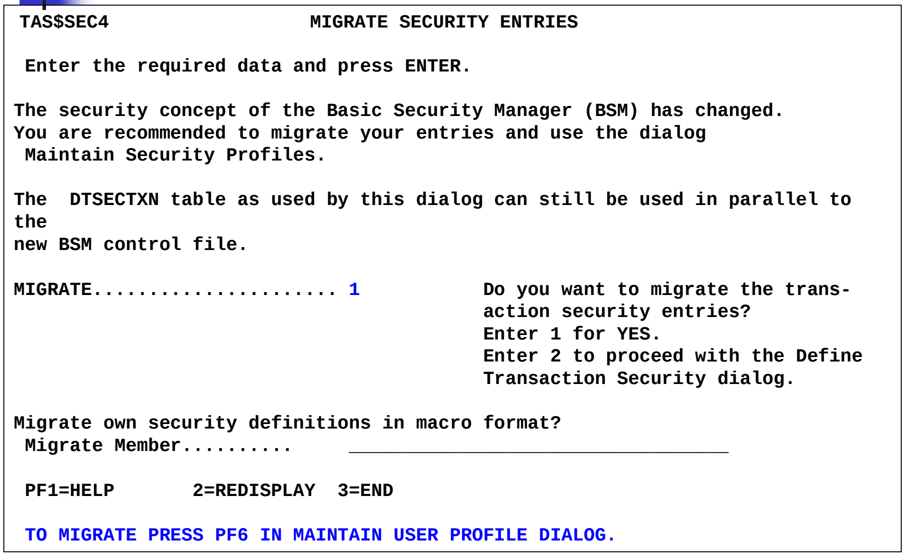
Migration auf neues Konzept: Details zu 2.



```
  TAS$SEC3          DEFINE TRANSACTION SECURITY: MERGE TABLES

 Enter the required data and press ENTER.


Specify the library member you want to be merged to the
transaction security table.


MEMBER NAME................. DTRISEC     Enter the member name.

MEMBER TYPE................. U           Enter the member type.

LIBRARY..................... IJSYSRS     Enter the library name.

SUBLIBRARY.................. SYSLIB      Enter the sublibrary name.


 PF1=HELP      2=REDISPLAY  3=END
```

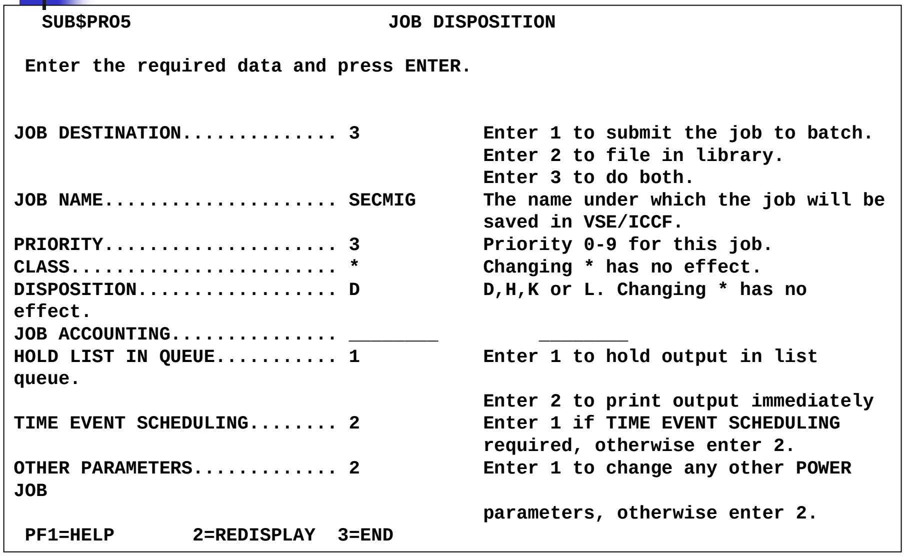
- Enter drücken und danach PF3
- Wieder zu II-Dialog 2.8.5

Migration auf neues Konzept: Details zu 2.



```
 TAS$SEC4                   MIGRATE SECURITY ENTRIES

  Enter the required data and press ENTER.

 The security concept of the Basic Security Manager (BSM) has changed.
 You are recommended to migrate your entries and use the dialog
  Maintain Security Profiles.

 The  DTSECTXN table as used by this dialog can still be used in parallel to
 the
 new BSM control file.

 MIGRATE..................... 1           Do you want to migrate the trans-
                                          action security entries?
                                          Enter 1 for YES.
                                          Enter 2 to proceed with the Define
                                          Transaction Security dialog.

 Migrate own security definitions in macro format?
  Migrate Member..........     __________________________________

  PF1=HELP       2=REDISPLAY  3=END

  TO MIGRATE PRESS PF6 IN MAINTAIN USER PROFILE DIALOG.
```

Migration auf neues Konzept: Details zu 2.



```
   SUB$PRO5                         JOB DISPOSITION

  Enter the required data and press ENTER.


 JOB DESTINATION............. 3           Enter 1 to submit the job to batch.
                                          Enter 2 to file in library.
                                          Enter 3 to do both.
 JOB NAME.................... SECMIG      The name under which the job will be
                                          saved in VSE/ICCF.
 PRIORITY.................... 3           Priority 0-9 for this job.
 CLASS....................... *           Changing * has no effect.
 DISPOSITION................. D           D,H,K or L. Changing * has no
 effect.
 JOB ACCOUNTING.............. ________            ________
 HOLD LIST IN QUEUE.......... 1           Enter 1 to hold output in list
 queue.
                                          Enter 2 to print output immediately
 TIME EVENT SCHEDULING........ 2          Enter 1 if TIME EVENT SCHEDULING
                                          required, otherwise enter 2.
 OTHER PARAMETERS............ 2           Enter 1 to change any other POWER
 JOB
                                          parameters, otherwise enter 2.
  PF1=HELP       2=REDISPLAY  3=END
```

Migration auf neues Konzept: Details zu 2.

Console-Output:

```
BG 0001 1Q47I   BG SECMIG 00703 FROM (SYSA) , TIME= 8:05:36
BG 0000 // JOB SECMIG  MIGRATE SECURITY ENTRIES
        DATE 04/05/2009, CLOCK 08/05/36
BG 0000 * MIGRATE DTRISEC.Z TABLE USED BY THE DIALOG
BG 0000 * MIGRATE DTSECTXM.A WITH MIXED CASE MACRO DEFINITIONS
BG 0000 * RENAME THE OLD DEFINITION MEMBERS
BG 0000 * NOW LOAD INITIAL BSTADMIN DEFINITIONS
BG 0000 * NOW LOAD MIGRATED BSTADMIN DEFINITIONS
BG 0000 * REBUILD THE DATASPACE
BG 0000 * IF OK, DELETE THE OLD DTSECTXN PHASE
MSG F2,DATA=CEMT PERF SECURITY REBUILD
AR 0015 1I40I  READY
F2 0164 DFHXS1105 DBDCCICS Resource profiles for class TCICSTRN have been
        built.
F2 0164
         Security
         Rebuild
         RESPONSE: NORMAL TIME:  08.05.45  DATE: 04.05.09
         SYSID=CIC1 APPLID=DBDCCICS
BG 0000 EOJ SECMIG    MAX.RETURN CODE=0008
        DATE 04/05/2009, CLOCK 08/05/44, DURATION   00/00/08
```

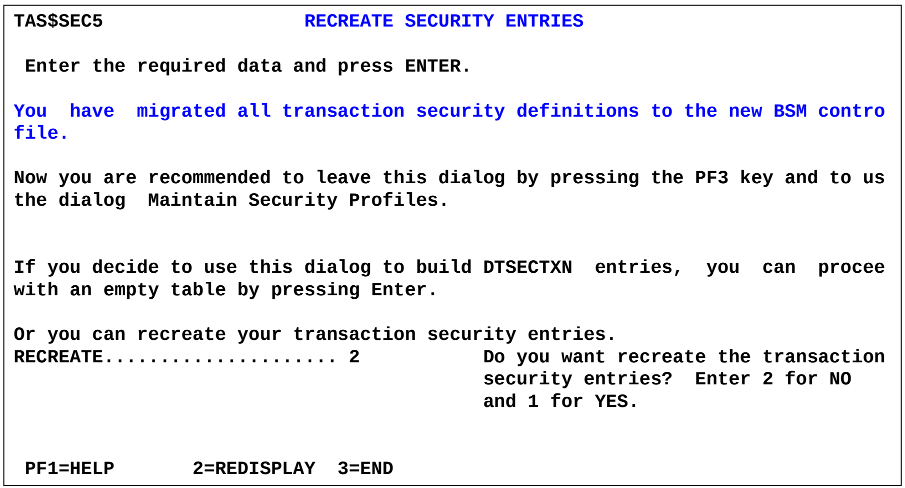
Migration auf neues Konzept: Details zu 2.

SECMIG mit RC=8 ist ok, da nach Neuinstalltion:

```
L082I MEMBER DTRISEC.Z NOT FOUND IN SUBLIBRARY PRD2.SAVE
L113I RETURN CODE OF DELETE IS  4
1S55I  LAST RETURN CODE WAS 0008
…
ADDGROUP GROUP01 DA('TRANSEC CLASS MIGRAT')
BST921I COMMAND FAILED, DUPLICATE ENTRY
BST904I RETURN CODE OF ADDGROUP IS 08
…
 * INITIAL DEFAULT FILE SETUP                ← bei den ADD-Statemnts!
ADD FCICSFCT 'BSTCNTL' UACC(NONE) DATA('IBM SUPPLIED')
BST921I COMMAND FAILED, DUPLICATE ENTRY
BST904I RETURN CODE OF ADD IS 08
…
PERMIT FACILITY DFHRCF.BRSLPU ID(GROUP01) ACCESS(UPDATE)
BST904I RETURN CODE OF PERMIT IS 00
```

Migration auf neues Konzept: Details zu 2.

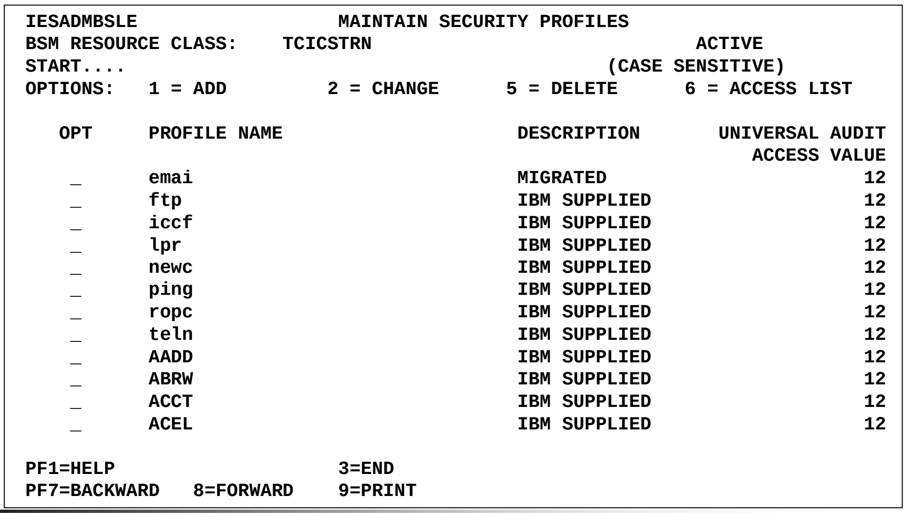
II Dialog 285 nach der Migration nicht mehr benutzen!



```
TAS$SEC5                    RECREATE SECURITY ENTRIES

 Enter the required data and press ENTER.

You  have  migrated all transaction security definitions to the new BSM contro
file.

Now you are recommended to leave this dialog by pressing the PF3 key and to us
the dialog  Maintain Security Profiles.


If you decide to use this dialog to build DTSECTXN  entries,  you  can  procee
with an empty table by pressing Enter.

Or you can recreate your transaction security entries.
RECREATE..................... 2          Do you want recreate the transaction
                                          security entries?  Enter 2 for NO
                                          and 1 for YES.


 PF1=HELP       2=REDISPLAY   3=END
```

Migration auf neues Konzept: Details zu 2.

II Dialog 2811 benutzen:



```
 IESADMBSLE                    MAINTAIN SECURITY PROFILES
 BSM RESOURCE CLASS:    TCICSTRN                              ACTIVE
 START....                                            (CASE SENSITIVE)
 OPTIONS:    1 = ADD         2 = CHANGE        5 = DELETE       6 = ACCESS LIST

    OPT      PROFILE NAME                     DESCRIPTION        UNIVERSAL AUDIT
                                                                    ACCESS VALUE
     _       emai                             MIGRATED                        12
     _       ftp                              IBM SUPPLIED                    12
     _       iccf                             IBM SUPPLIED                    12
     _       lpr                              IBM SUPPLIED                    12
     _       newc                             IBM SUPPLIED                    12
     _       ping                             IBM SUPPLIED                    12
     _       ropc                             IBM SUPPLIED                    12
     _       teln                             IBM SUPPLIED                    12
     _       AADD                             IBM SUPPLIED                    12
     _       ABRW                             IBM SUPPLIED                    12
     _       ACCT                             IBM SUPPLIED                    12
     _       ACEL                             IBM SUPPLIED                    12

 PF1=HELP                    3=END
 PF7=BACKWARD    8=FORWARD   9=PRINT
```