

z/VSE und CICS: Hints & Tipps

Dagmar Kruse,
IBM München

Heinz Peter Maassen,
Lattwein GmbH

Wie beenden Sie CICS TS?

- | CEMT Perform Shutdown

oder

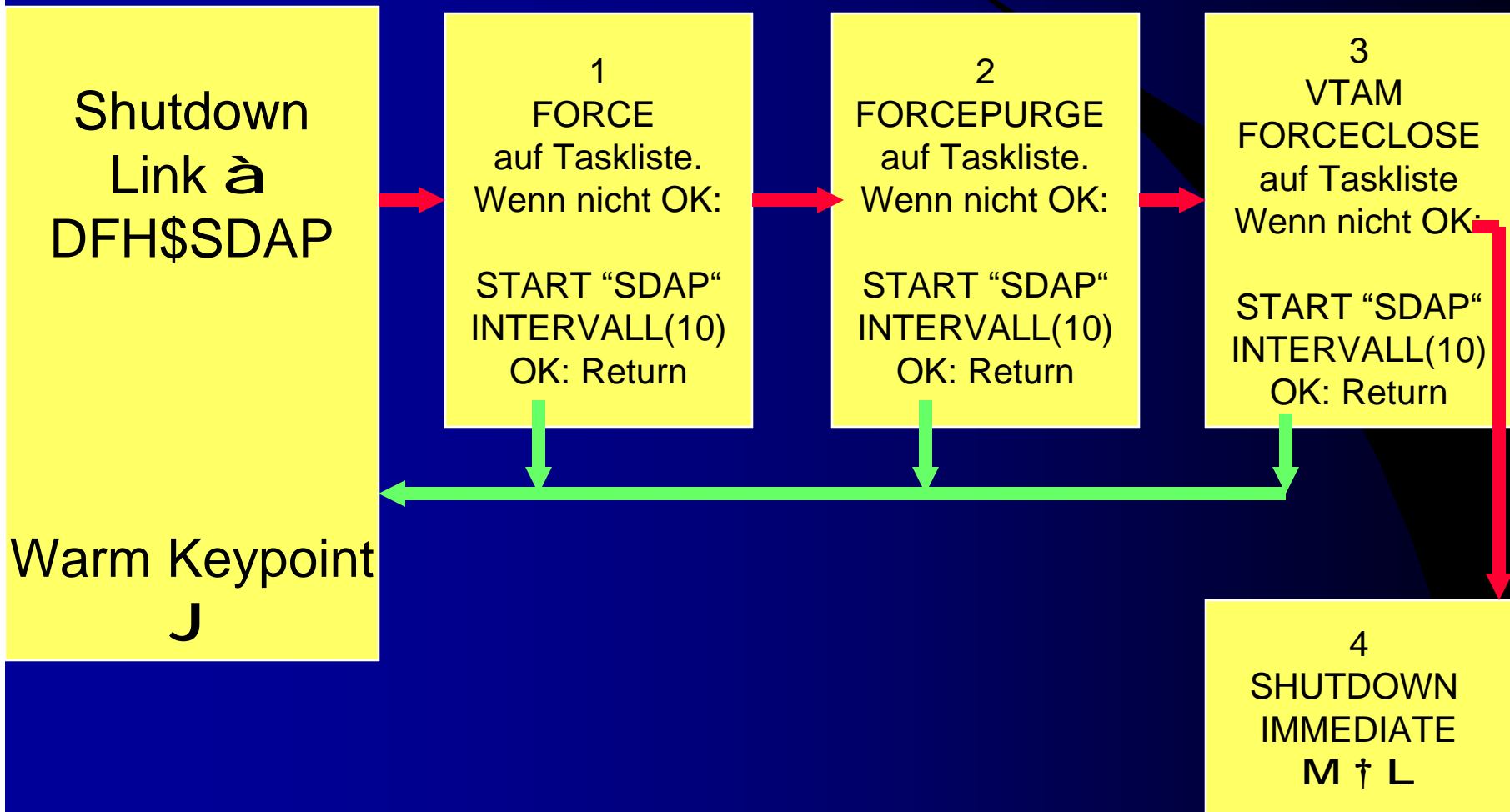
- | CEMT Perform Shutdown Immediate

?

CICS TS Shutdown Programm: DFH\$SDAP

- | CICS TS stellt ein **ShutDown Assist Programm** bereit, **DFH\$SDAP** (siehe: PRD1.BASE). Dieses Programm läuft im 1.Step beim Shutdown ab. **DFH\$SDAP** versucht CICS TS normal zu beenden. Oftmals wird dies durch Dialogprogramme (Langläufer) verhindert, die noch nicht beendet wurden. Das Programm läuft in 4 Stufen mit einer Wartezeit von 10 Sekunden ab:
 - | (1) FORCE (2) FORCEPURGE
 - | (3) VTAM FORCECLOSE (4) SHUTDOWN IMMEDIATE

CICS TS Shutdown: DFH\$SDAP



CICS TS Shutdown: DFH\$SDAP

- | Die laufenden Tasks werden gepurged, wenn diese mit PURGE, FORCEPURGE oder VTAM FORCECLOSE beendet werden und sollten normal über den BACKOUT laufen. Werden alle Transaktionen erfolgreich beendet, bevor der SHUTDOWN IMMEDIATE ausgeführt wird, so wird ein "Warm Keypoint" erzeugt.
- | Man kann die Zeitverzögerung bei DELAY Intervall an die eigene Systemumgebung anpassen. Dem VTAM FORCECLOSE Befehl sollte ein genügend großer Zeitabschnitt definiert werden, damit dieser ausgeführt werden kann. Falls das Zeitfenster zu klein ist, wird anschließend kein Warmstart durchgeführt.

CICS TS Shutdown

- I Der Source Code für dieses Beispiel wird nur für Assembler bereitgestellt. Man muss das Programm mit DFHEAP1\$ precompilieren, assemblieren und linken. Anschließend sollte das Programm über RDO definiert werden und als Transaktion SDAP eingetragen werden. Für die Transaktion SDAP sollte das SHUTDOWN Attribut als ENABLED gesetzt sein.
- I Damit das Programm DFH\$SDAP aufgerufen wird, muss ein Eintrag in der DFHPLTSD im 1. Teil eingetragen werden.

CICS TS Shutdown: DFH\$SDAP

```
CEDA DEFINE TRANSACTION(SDAP) GROUP(SDGROUP)  
PROGRAM(DFH$SDAP) TWASIZE(0) PROFILE(DFHCICST)  
STATUS(Enabled) TASKDATALOC(BELOW) TASKDATAKEY(USER)  
SHUTDOWN(ENABLED)
```

```
CEDA DEFINE PROGRAM(DFH$SDAP) GROUP(SDGROUP)  
LANGUAGE(ASSEMBLER) RELOAD(NO) RESIDENT(NO)  
STATUS(ENABLED) RSL(PUBLIC) DATALOCATION(BELOW)  
EXECKEY(USER)
```

CICS TS Shutdown: DFH\$SDAP

DFHSIT oder Overwrite:

PLTSD=SD

Suffix Shutdown PLT

DFHPLTSD

.....

DFHPLT TYPE=ENTRY,PROGRAM=DFH0STAT CALL Statistics Print *

DFHPLT TYPE=ENTRY,PROGRAM=DFH\$SDAP SHUTDOWN APPLICATIONS *

* DFHPLT TYPE=ENTRY,PROGRAM=DFHDELIM *

CICS TS Shutdown: DFH\$SDAP

- | Erweiterung für CICS Web Support.
- | Im DFH\$SDAP einen weiteren Befehl einfügen zum Beenden von CICS Web Support:

```
| EXEC CICS SET TCPIPSERVICE(*) IMMCLOSE  
RESP(RESP)
```

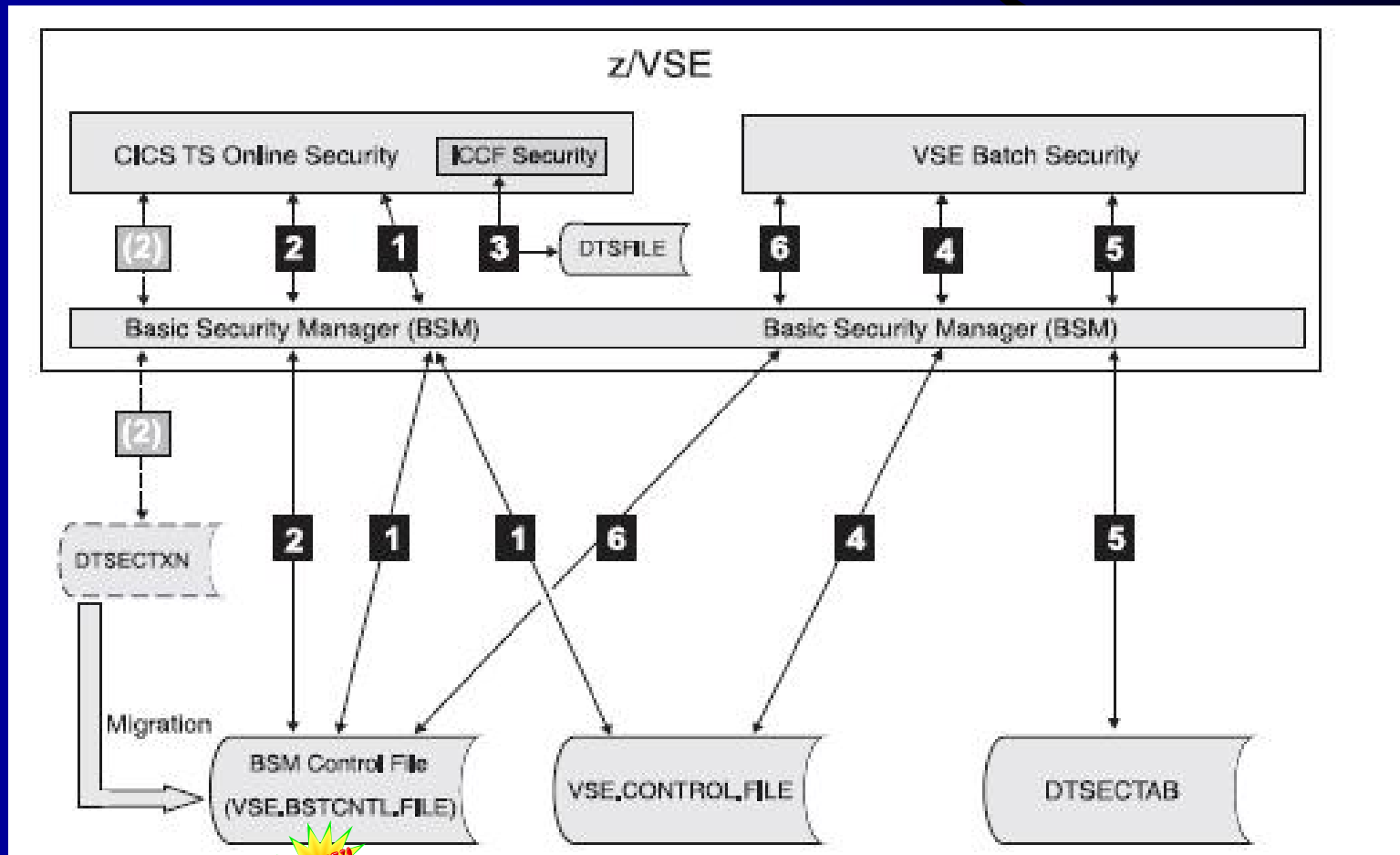
- | Damit werden die Listener vom CWS gestoppt.

CICS TS Security ab z/VSE 3.1.1

- | Neues Konzept des Basic Security Managers (BSM)
- | Praktische Hinweise

Neues Security-Konzept

ab z/VSE 3.1.1



Neues 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)

Neues Security-Konzept ab z/VSE 3.1.1

3. VSE/ICCF: Anwendung unter CICS TS:

- Eigener Security-Check: DTSDFILE

4. Signon aus dem Batch:

- Userid- + PWD-Check : VSE.CONTROL.FILE
erfolgreich è BSM erstellt „user info block“

5. Zugriff auf DTSECTAB-Ressourcen:

- ACCESS- Check: DTSECTAB

6. Batch-Zugriff auf BSTCNTL-Ressourcen:

- ACCESS- Check: VSE.BSTCNTL.FILE

Neues Security-Konzept

ab z/VSE 3.1.1

I mögliche **Resource-Klassen** (**class_name**) in BSTCNTL

- | | |
|-----------|---|
| TCICSTRN | - Transactions (s. DTSECTXN) |
| MCICSPPT | - Application programs |
| FCICSFCT | - Files |
| JCICSJCT | - Journals |
| SCICSTST | - Temporary storage queues |
| DCICISDCT | - Transient data queues |
| ACICSPCT | - CICS started Transactions |
| | |
| APPL | - VTAM-Applications |
| FACILITY | - Miscellaneous resources (Spooling Files, RCF,...) |

è Das neue Konzept ist sehr zu empfehlen:

- kann mehr Schutz bieten
- schneller als über DTSECTXN (nutzt Data Spaces)
- Transaktionen auf neues Konzept umstellen
 - | Security über DTSECTXN wird noch unterstützt (Kompatibilität)
- einfachere Wartung (z.B. auch bei VSE-Upgrades)

Neues Security-Konzept

ab z/VSE 3.1.1

- I DFHSIT: die Security für die gewünschten Resource-Klassen auf "YES" setzen

– SEC=YES	Enables security
– XTRAN=YES	Resource Class_name TCICSTRN
– XPPT=NO	Resource Class_name MCICSPPT
– XFCT=NO	Resource Class_name FCICSFCT
– XJCT=NO	Resource Class_name JCICSJCT
– XTST=NO	Resource Class_name SCICSTST
– XDCT=NO	Resource Class_name DCICSDCT
– XPCT=NO	Resource Class_name ACICSPCT for EXEC CICS Start Translds

Neues Security-Konzept

ab z/VSE 3.1.1

I Zu schützende Resource muss

- in einer **Resource Class** definiert sein

- Eine 'Universal Access Authority' haben:

NONE (default), READ, UPDATE, ALTER

- besitzt eine **Access List**

è Das ist dann das '**Resource Profile**' (II-Dialog 281)

Neues Security-Konzept

ab z/VSE 3.1.1

| Der **Benutzer** bekommt Zugriffsrecht:

– Über die „**Access List**“ der Resource (II-Dialog 281)

| User wird direkt dort eingetragen

oder

| gehört zu einer „**User Group**“, die dort eingetragen ist

– User in “User Group” eintragen (II-Dialog 282)

Administrator dürfen alles,
sie müssen nicht explizit eingetragen
werden!

Neues Security-Konzept

ab z/VSE 3.1.1

I Aktivieren der gewünschten Security:

- Änderungen müssen dem Basic Security Manager (BSM) übergeben und dort aktiviert werden:

```
// EXEC BSTADMIN
```

Befehle, s. z/VSE Administration Guide, Kapitel 8

- I Daten, wie Resource Profiles, User Groups,... werden im **VSE.BSTCNTL.FILE** gespeichert.

Neues Security-Konzept

ab z/VSE 3.1.1

I Was wird durch den BSM z. Z. geschützt?

```
r rdr,pausebg
```

```
BG-0000 // PAUSE
```

```
0 exec bstadmin
```

```
BG-0000 BST901A ENTER COMMAND OR END
```

```
0 status
```

```
BG 0000 USER          ACCESS
```

```
BG 0000 ----          ----
```

```
BG 0000 USER          YES
```

```
BG 0000 DATASET       YES
```

```
BG 0000 VSELIB        YES
```

```
BG 0000 VESLIB        YES
```

```
BG 0000 VSEMEM        YES
```

```
BG 0000 TCICSTRN      YES
```

```
BG 0000 ACICSPCT      YES
```

```
BG 0000 DCICSDCT      YES
```

Neues Security-Konzept

ab z/VSE 3.1.1

...

BG 0000 FCICSFCT YES

BG 0000 JCICSJCT YES

BG 0000 MCICSPPT YES

BG 0000 SCICSTST YES

BG 0000 APPL YES

BG 0000 FACILITY YES

BG 0000

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

...

Neues Security-Konzept

ab z/VSE 3.1.1

...

```
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              170K.
BG 0000   SIZE OF PREVIOUS DATA SPACE WAS  960K.
BG 0000   USAGE OF PREVIOUS DATA SPACE WAS 18%.
BG 0000   DATA PART SIZE WAS              170K.
BG 0000
BG 0000 BST904I RETURN CODE OF STATUS IS 00
```

Transactionen im neuen Security-Konzept

I Altes Konzept:

- Transaktionen werden über **Transaction Security Key 01 bis 64** geschützt. Benutzer müssen für diesen Key berechtigt sein.
- Kontrolliert wird über die **DTSECTXN**.

I Neues Konzept:

- Transaktionen müssen in der Resource-Klasse **TCICSTRN** definiert sein:
 - I Universal Access Authority (Default: NONE)
 - I Benutzer-Zuordnung über Access-Liste:
 - Direkt oder über User Groups
 - Nicht Administratoren (“Sie dürfen alles”)
- Kontrolliert wird über die **VSE.BSTCNTL.FILE**.

Transactionen im neuen Security-Konzept

I Nach der Migration ins neue Konzept:

- Die User Groups **GROUP01 – GROUP64** entsprechen diesen Transaction Security **Keys 01 - 64**.
 - I GROUP01 enthält alle Benutzer die zum ehemaligen Transaktions-Schlüssel 01 zugelassen waren (außer Administratoren, z.B. PROG, OPER, CICSUSER und \$SRV).
- Es können neue Gruppen erstellt werden, es ist aber ratsam die Gruppen **GROUP01-GROUP64 zu behalten**.

Migration der Transaktionen ins neue Security-Konzept

1. Umwandlung der **Transaction Security Keys** in **User Groups** und **Zuordnung der bestehenden Userids:**

- 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. **Danach Migration der Transaction Security Einträge**

- II-Dialog 2.8.5: 1 auswählen

→ 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 3.1.1, Chapter 8**)

Migration zum neuen Security-Konzept ab z/VSE 3.1.1

Hier der generierte Job:

```
// JOB IESTBGRI
* CREATED BY IESXSPR FROM IESCNTL      DATE: 03/24/07
// EXEC BSTADMIN
* ADD TRANSEC CLASS MIGRATION GROUPS IN CASE NOT EXIST
  ADDGROUP GROUP01      DATA('TRANSEC CLASS MIGRAT')
  ADDGROUP GROUP02      DATA('TRANSEC CLASS MIGRAT')
  ...
  ADDGROUP GROUP64      DATA('TRANSEC CLASS MIGRAT')
* CONNECT NON ADMIN USERS TO THE GROUPS
* $LPR      IS SYSTEM ADMINISTRATOR. NOT CONNECTED TO ANY GROUP
  CONNECT GROUP01      $SRV
  CONNECT GROUP60      $SRV
  CONNECT GROUP61      $SRV
  CONNECT GROUP62      $SRV
  CONNECT GROUP63      $SRV
  CONNECT GROUP64      $SRV
  . . . .
```

Migration zum neuen Security-Konzept ab z/VSE 3.1.1

```
CONNECT GROUP01 LATTW
CONNECT GROUP02 LATTW
CONNECT GROUP03 LATTW
CONNECT GROUP04 LATTW
CONNECT GROUP05 LATTW
CONNECT GROUP06 LATTW
CONNECT GROUP64 LWSN
* MAAS IS SYSTEM ADMINISTRATOR
CONNECT GROUP01 OPER
CONNECT GROUP60 OPER
CONNECT GROUP61 OPER
CONNECT GROUP62 OPER
CONNECT GROUP63 OPER
CONNECT GROUP64 OPER
CONNECT GROUP60 VERW
CONNECT GROUP61 VERW
CONNECT GROUP62 VERW
CONNECT GROUP63 VERW
CONNECT GROUP64 VERW
PERFORM DATASPACE REFRESH
```

/*

Security-Konzept - Literatur

- | z/VSE Planning 3.1.1, 4.1.0
- | z/VSE Administration 3.1.1, 4.1.0 (ist ausführlicher)
- | 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>

CICS TS Security

I alter II-Dialog 2.8 war (vor z/VSE 3.1.1):

```
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 to 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.

CICS TS Security ab z/VSE 3.1.1

I II Dialog 2.8 zeigt jetzt:

IESADMSL.IESEBSEC

SECURITY MAINTENANCE

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)

CICS TS Security ab z/VSE 3.1.1

I II-Dialog 2.8.5 ist für DTSECTXN:

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 transaction security entries?

Enter 1 for YES.

Enter 2 to proceed with the Define Transaction Security dialog.

Der alte Dialog erscheint.

CICS TS Security ab z/VSE 3.1.1

Nach der Migration zeigt II-Dialog 2.8.5:

TAS\$SEC5

RECREATE SECURITY ENTRIES

Enter the required data and press ENTER.

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

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

If you decide to use this dialog based on DTSECTXN, you can proceed 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.

CICS TS Security ab z/VSE 3.1.1

I II Dialog 2.8 (SECURITY MAINTENANCE):

- 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)

CICS TS Security ab z/VSE 3.1.1

I II Dialog 2.8.1 hat folgende Auswahl:

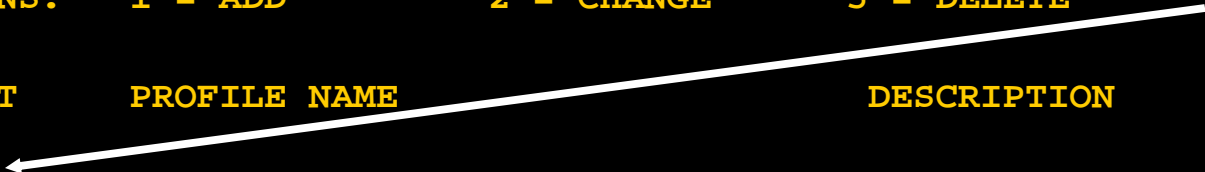
- 1 **Maintain Transaction Profiles**
- 2 Maintain PCT Profiles
- 3 Maintain DCT Profiles
- 4 Maintain FCT Profiles
- 5 Maintain JCT Profiles
- 6 Maintain PPT Profiles
- 7 Maintain TST Profiles
- 8 Maintain APPL Profiles
- 9 Maintain FACILITY Profiles

CICS TS Security ab z/VSE 3.1.1

I Verwalten der Transaktion Profile:

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

  OPT      PROFILE NAME      DESCRIPTION      UNIVERSAL
  OPT      PROFILE NAME      DESCRIPTION      ACCESS
  6        ICCF              MIGRATED
  -        ICIC              MIGRATED
  -        ICVA              MIGRATED
  -        ICVM              MIGRATED
  -        ICVP              MIGRATED
  -        ICVS              MIGRATED
  -        IE$L              MIGRATED
```




CICS TS Security ab z/VSE 3.1.1

- Mit Auswahl 6 kann man die Gruppen / User Liste zu einer Transaktion anzeigen.

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

OPT      NAME      ACC
1        GROUP01   2
```



CICS TS Security ab z/VSE 3.1.1

I II Dialog 2.8 zeigt uns die Auswahl zur Benutzer-Gruppenverwaltung:

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

CICS TS Security ab z/VSE 3.1.1

- Im II Dialog 2.8.2 werden alle Gruppen angezeigt. Hier nur diejenigen, die Benutzer definiert haben.

```
OPTIONS:      1 = ADD                2 = CHANGE                5 = DELETE                6 = USER LIST
              USERID
              CONNECTED?
OPT   GROUP NAME   DESCRIPTION
--
6     CI31TEST     CICSTEST Group
--
6     GROUP01     TRANSEC CLASS MIGRAT
--
6     GROUP02     TRANSEC CLASS MIGRAT
--
6     GROUP61     TRANSEC CLASS MIGRAT
--
6     GROUP62     TRANSEC CLASS MIGRAT
--
6     GROUP63     TRANSEC CLASS MIGRAT
--
6     GROUP64     TRANSEC CLASS MIGRAT
--
6     PROG        Programmer
--
6     SYST        System Group
```

CICS TS Security ab z/VSE 3.1.1

- | Mit Auswahl - 6 sehen wird die Gruppenliste, Benutzer können hinzugefügt oder gelöscht werden.

START.....

OPTIONS: 1 = ADD 5 = DELETE

OPT	USERID
—	BELL
—	CICSUSER
—	HOER
—	LWHD
—	LWSN
—	MAAS
—	OPER
—	PRIC
—	PRIN
—	SYSA

CICS TS Security ab z/VSE 3.1.1

- I II Dialog 2.8.2 - 6 –1 Hinzufügen eines Benutzers:

Connect Userid to group:

GROUP NAME.....	GROUP01	Group name
USERID.....	BEL2	4 - 8 characters

CICS TS Security ab z/VSE 3.1.1

II Dialog 2.8.2: In welchen Gruppen ist die Userid „DAGO“ enthalten?

```
IESADMBSLG                                MAINTAIN SECURITY PROFILES
BSM RESOURCE CLASS:                        GROUP
START....
OPTIONS:      1 = ADD                      2 = CHANGE                      5 = DELETE
                                                    USERID
OPT           GROUP NAME                   DESCRIPTION                       CONNECTED?
                                                    DAGO
-            CIDBDCGR                       a0006ci1
-            CIPRODGR                       a0006ci2                          *
-            GROUP01                       TRANSEC CLASS MIGRAT                *
-            GROUP02                       TRANSEC CLASS MIGRAT
-            GROUP03                       TRANSEC CLASS MIGRAT
-            GROUP04                       TRANSEC CLASS MIGRAT
-            GROUP05                       TRANSEC CLASS MIGRAT
```

CICS TS Security ab z/VSE 3.1.1

- I II Dialog 2.8.3 Aktivieren der Security-Definitionen geht auch mit **CEMT PER Security**

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

SECURITY INFORMATION WAS SUCCESSFULLY REBUILT.

CICS TS Security ab z/VSE 3.1.1

- I Verwenden Sie RCF ?
- I Dann müssen im z/VSE 3.1.1 die PTFs **UK14161** (in z/VSE 3.1.2 enthalten) und **UK19662*** installiert sein.
- I Danach muss in der ICCF Library 59 das Skeleton SKRCFSEC ausgeführt werden, um die Security für RCF zu definieren.

* PreReqs: UK14212 (in z/VSE3.1.2 enthalten), UK18593

CICS TS Security ab z/VSE 3.1.1

```
* $$ JOB JNM=SKRCFSEC,DISP=D,CLASS=0
// JOB SKRCFSEC SECURITY SETUP CICS RCF
// DLBL BSTCNTL,'VSE.BSTCNTL.FILE',,VSAM,CAT=VSESPUC
// EXEC BSTADMIN

* INITIAL FACILITIES FOR REPORT CONTROLLER
ADD FACILITY DFHRCF.RSLPU UACC(NONE)
ADD FACILITY DFHRCF.RSL01 UACC(NONE) ( bis - PRSL24)
PERMIT FACILITY DFHRCF.RSLPU ID(GROUP01)ACCESS(UPDATE)
PERMIT FACILITY DFHRCF.RSL01 ID(GROUP01)ACCESS(UPDATE)
ADD FACILITY DFHRCF.BRSLPU UACC(NONE)
ADD FACILITY DFHRCF.BRSL01 UACC(NONE) (bis - PRSL24)
PERMIT FACILITY DFHRCF.BRSLPU ID(GROUP01) ACCESS(UPDATE)
PERMIT FACILITY DFHRCF.BRSL01 ID(GROUP01) ACCESS(UPDATE)
```

CICS TS Security ab z/VSE 3.1.1

```
ADD FACILITY DFHRCF.PRSLPU UACC(NONE)
ADD FACILITY DFHRCF.PRSL01 UACC(NONE)      (bis - PRSL24)
PERMIT FACILITY DFHRCF.PRSLPU ID(GROUP01) ACCESS(UPDATE)
PERMIT FACILITY DFHRCF.PRSL01 ID(GROUP01) ACCESS(UPDATE)
/*
* REBUILD THE DATASPACE
// EXEC BSTADMIN
    PERFORM DATASPACE REFRESH
/*
/ &
```

CICS TS Security ab z/VSE 3.1.1

- I Diese PTFs sind auch zu installieren, wenn man eigene Programme hat die mit EXEC CICS ...

- I SPOOLOPEN / SPOOLREAD
SPOOLWRITE / SPOOLCLOSE

arbeiten.

Anhang

BSTADMIN

| // 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

I 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

| 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

| // 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

BSTADMIN

```
* $$ JOB JNM=SKRCFSEC,DISP=D,CLASS=0
// JOB SKRCFSEC SECURITY SETUP CICS RCF
// DLBL BSTCNTL,'VSE.BSTCNTL.FILE',,VSAM,CAT=VSESPUC
// EXEC BSTADMIN
```

```
* Add Generic Transaction ABC and associate GROUP03
ADD TCICSTRN ABC GEN
PERMIT TCICSTRN ABC GEN ID(GROUP03) ACCESS(READ)
/*
```

```
* REBUILD THE DATASPACE
// EXEC BSTADMIN
    PERFORM DATASPACE REFRESH
/*
/&
* $$ EOJ
```