VSE/ESA V2.4 Security

VM and VSE Technical Conference in Orlando
May 24th - 27th, 1999

34D / 34E

Helmut Hellner
VSE/ESA Development
Internet id: hhellner@de.ibm.com

(c) 1999 IBM Corporation

PDF created with FinePrint pdfFactory trial version http://www.fineprint.com

Contents

- Basics
- BSM
  - User IDs
  - Protecting Resources
  - Security Server
- Hints and Tips
  - Migration
  - Recovery
  - others
- Summary

(c) 1999 IBM Corporation

PDF created with FinePrint pdfFactory trial version http://www.fineprint.com

Basics

(c) 1999 IBM Corporation

PDF created with FinePrint pdfFactory trial version http://www.fineprint.com

Security Changes - Why?

- VSE/ESA 2.4 introduces the CICS Transaction Server for VSE/ESA 1.1 (CICS TS 1.1)
- CICS TS 1.1 has no CICS internal security
- Instead of it CICS TS 1.1 issues RACROUTE requests

(c) 1999 IBM Corporation

PDF created with FinePrint pdfFactory trial version http://www.fineprint.com

RACROUTE

- RACROUTE macro is the external security interface of the System Authorization Facility (SAF)
  - To be used by resource manager, subsystems, and security managers
  - RACROUTE macro and its related mapping macros are part of the generation feature
  - The RACROUTE return code consists of 3 parts
    - SAF router return code from R15
    - Security manager return code
    - Security manager reason code

(c) 1999 IBM Corporation

PDF created with FinePrint pdfFactory trial version http://www.fineprint.com

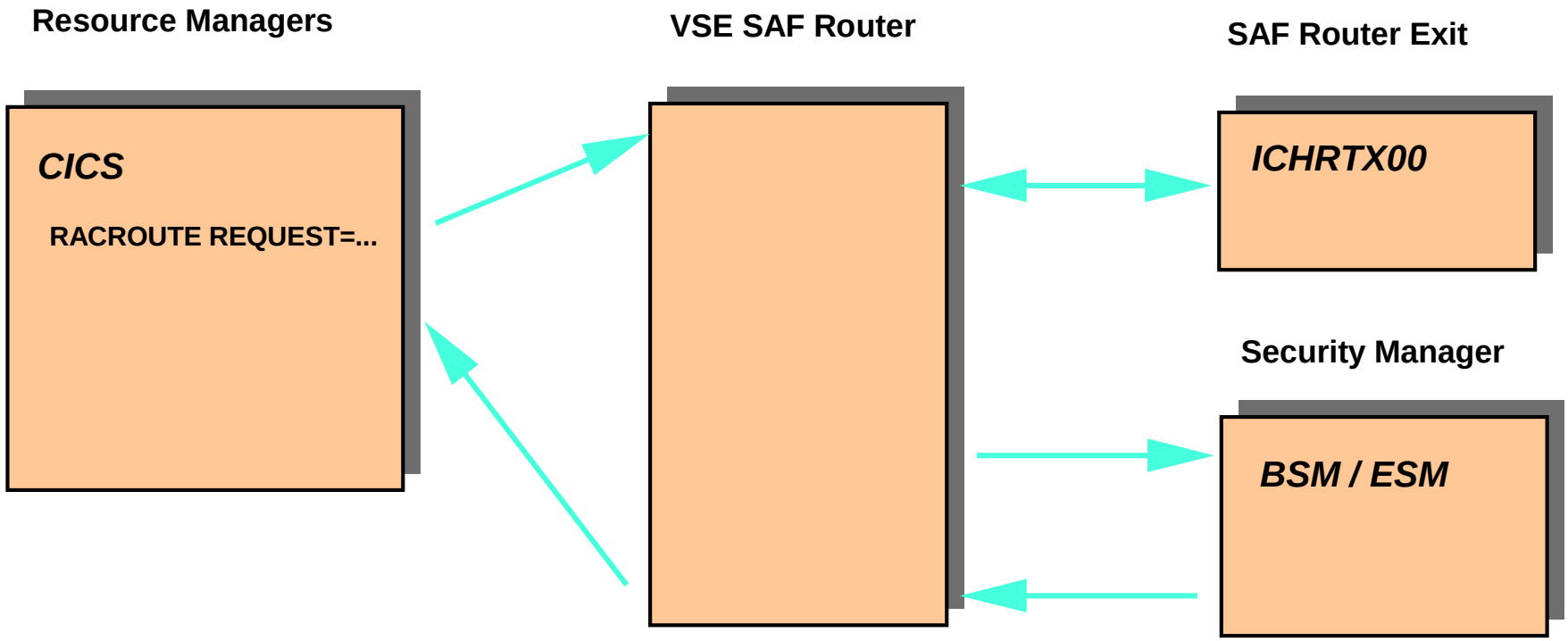
System Authorization Facility (SAF)

- The SAF is a centralized system security component
  - A RACROUTE request invokes the VSE SAF router
  - The VSE SAF router
    - Routes the requests to the installation exit ICHRTX00 and/or to the security manager
    - Creates security tokens
    - Builds default control blocks
  - The SAF in VSE/ESA is ported from OS/390

(c) 1999 IBM Corporation

PDF created with FinePrint pdfFactory trial version http://www.fineprint.com

SAF Overview



System Authorization Facility (SAF) for VSE/ESA 2.4.0

(c) 1999 IBM Corporation

PDF created with FinePrint pdfFactory trial version http://www.fineprint.com

Security Managers

- Basic Security Manager (BSM)
  - For no additional charge
  - Provides signon, transaction, and DTSECTAB security
  - It is activated by default, if no ESM is started
- External Security Manager (ESM) distributed by IBM
  - CA-Top Secret for VSE/ESA
- External Security Manager from any vendor

(c) 1999 IBM Corporation

PDF created with FinePrint pdfFactory trial version http://www.fineprint.com

Common Security Startup

- The security manager has to be initialized before other partitions or POWER are active
  - Exception: OCCF partition at unattended nodes
- The security server partition must be static
- BSSINIT will fail, if there are other partitions active

(c) 1999 IBM Corporation

PDF created with FinePrint pdfFactory trial version http://www.fineprint.com

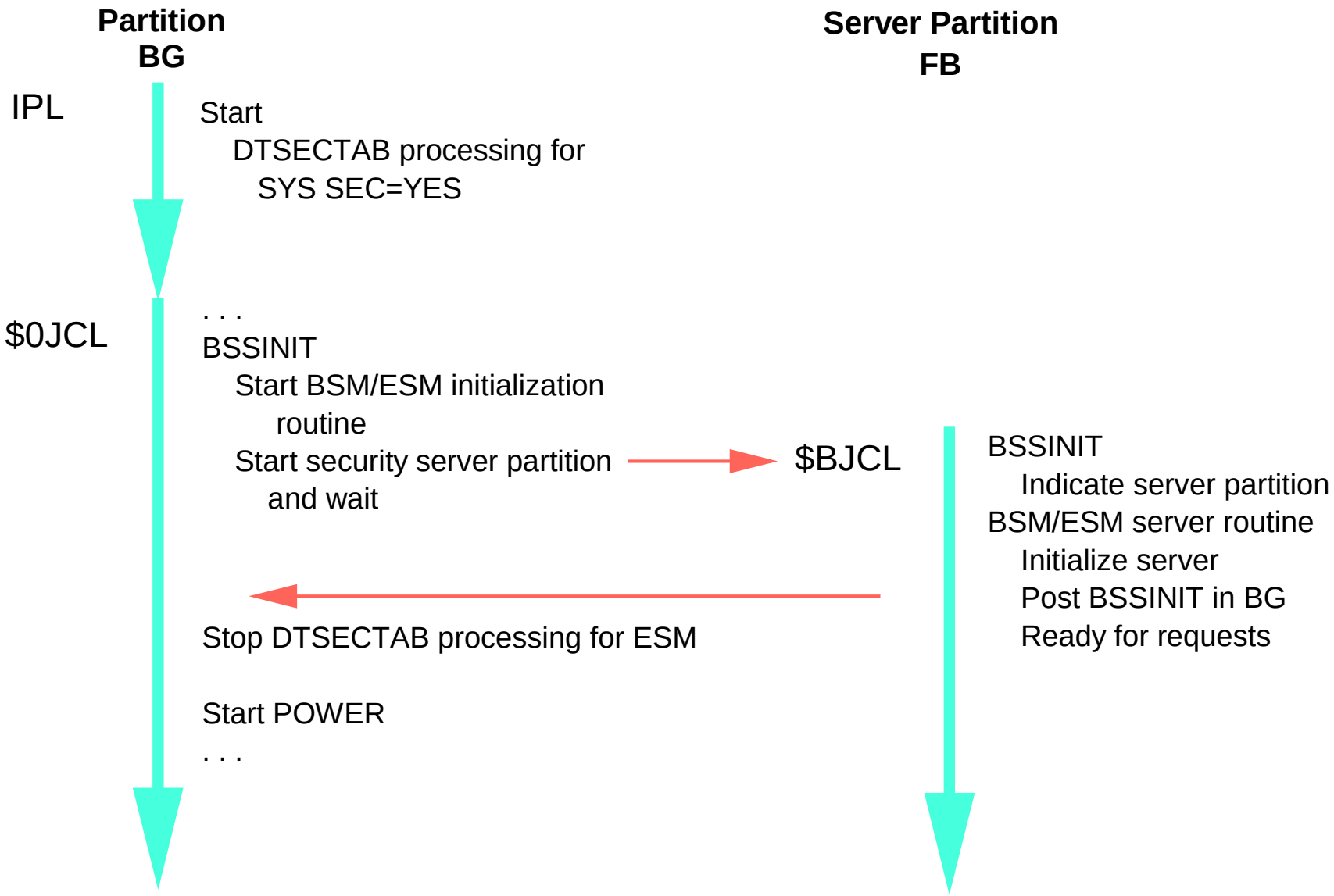
Common Security Startup ...

- To start an ESM specify SYS ESM=phasename in the IPL procedure
- If no ESM start is requested, the BSM comes up
- SYS SEC=YES/NO is still supported
- For SYS SEC=YES and ESM a DTSECTAB protection is active until the ESM is initialized

(c) 1999 IBM Corporation

PDF created with FinePrint pdfFactory trial version http://www.fineprint.com

Common Security Startup ...



(c) 1999 IBM Corporation

PDF created with FinePrint pdfFactory trial version http://www.fineprint.com

IBM distributed ESM

- For customers who need more security functions than the BSM provides
- IBM distributes CA-Top Secret for VSE/ESA (TSS) as ESM on extended base tape
  - Not for free - needs IBM key to fully activate it
  - TSS service via IBM PTFs using MSHP
  - Requires CA90 with a new service level
  - Use Common security startup
  - Exploits security server partition specified at SYS SECSERV= (default = FB)
- For additional information see product documentation

(c) 1999 IBM Corporation

PDF created with FinePrint pdfFactory trial version http://www.fineprint.com

Basic Security Manager
BSM

(c) 1999 IBM Corporation

PDF created with FinePrint pdfFactory trial version http://www.fineprint.com

BSM Scope

- Provide RACROUTE support for CICS signon, batch signon, and transaction security
- Support also the old SVC-based security calls (e.g. SECHECK)
- Following RACROUTE resource classes are covered
  - USER
  - DATASET
  - VSELIB
  - VSESLIB
  - VSEMEM
  - TCICSTRN

(c) 1999 IBM Corporation

PDF created with FinePrint pdfFactory trial version http://www.fineprint.com

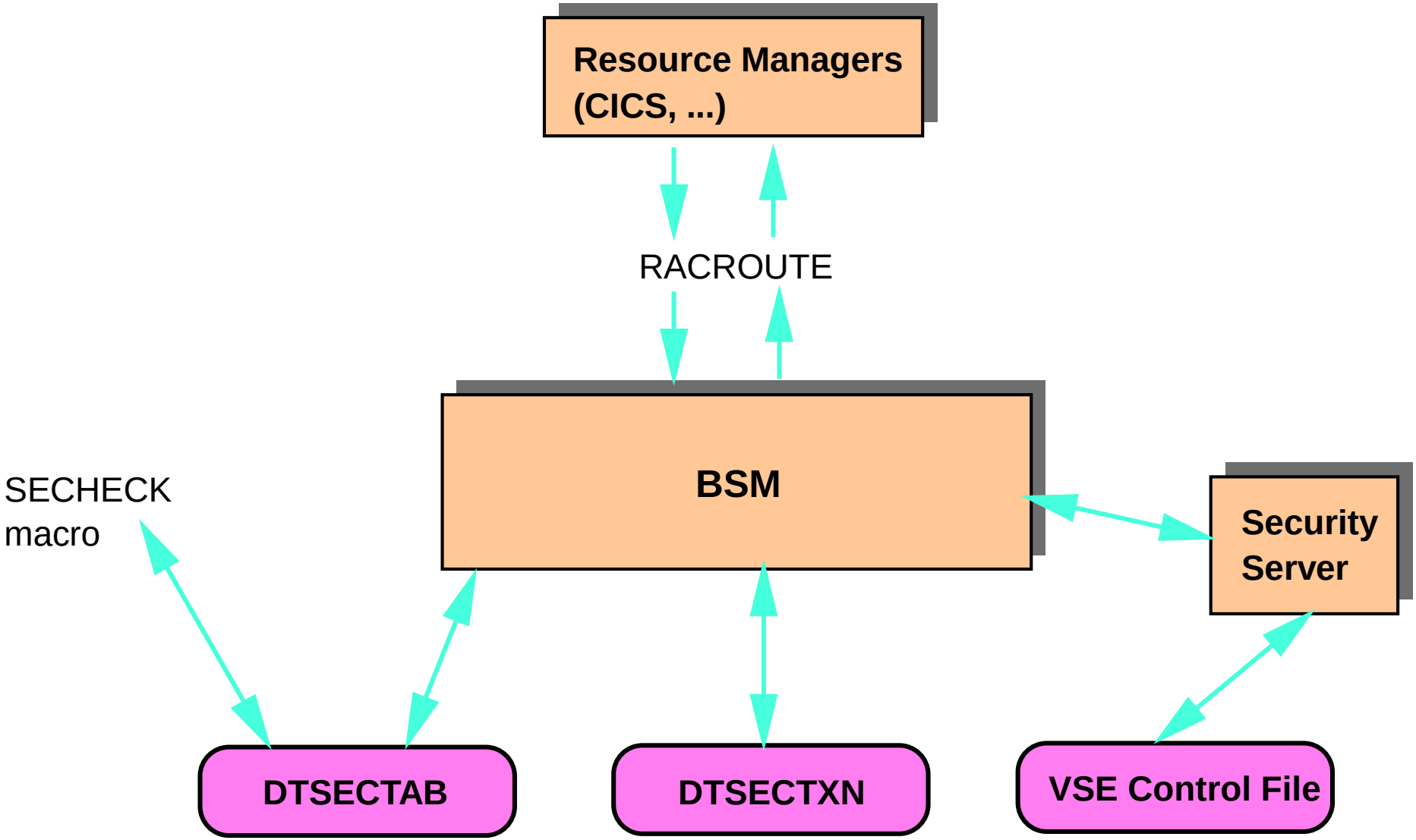
BSM Repositories

- VSE Control File
  - Central repository for all user profiles
  - Used for CICS and batch (SYS SEC=YES) signon
  - VSAM file
- DTSECTAB
  - Contains resources like files, libraries, sublibraries, and sublibrary members
  - Only two user IDs are still needed in DTSECTAB (FORSEC, DUMMY)
- DTSECTXN (new)
  - Keeps the transaction security profiles

(c) 1999 IBM Corporation

PDF created with FinePrint pdfFactory trial version http://www.fineprint.com

BSM Overview



(c) 1999 IBM Corporation

PDF created with FinePrint pdfFactory trial version http://www.fineprint.com

BSM User IDs

(c) 1999 IBM Corporation

PDF created with FinePrint pdfFactory trial version http://www.fineprint.com

BSM User Profiles

- DTSECTAB
  - Activated via SYS SEC=YES
  - Compatible to previous releases
  - Contains only 2 user IDs for ASI procedures during startup
  - Includes **no** CICS information
- VSE Control File (IESCNTL)
  - Central repository for user IDs
  - All CICS users must be defined here
  - User IDs of the CICS startup jobs must be defined here

(c) 1999 IBM Corporation

PDF created with FinePrint pdfFactory trial version http://www.fineprint.com

BSM User Profiles ...

- Passwords
  - 3 to 8 characters (DTSECTAB limited to 6)
  - ID statement, $$ JOB statement support 8 characters
- Special user rights
  - AUTH, BTRANS, READDIR, MCONS

(c) 1999 IBM Corporation

PDF created with FinePrint pdfFactory trial version http://www.fineprint.com

BSM User Profiles ...

- Access rights for DTSECTAB defined resources
  - CONnect, READ, UPDate, ALTer
  - Authorization via UACC at resource profile
  - Authorization per class at user profile
  - 32 access classes
- Transactions
  - Only for users defined in VSE Control File
  - 64 transaction classes

(c) 1999 IBM Corporation

PDF created with FinePrint pdfFactory trial version http://www.fineprint.com

BSM User Identification

- Search sequence for user IDs
  - First searched in DTSECTAB
  - If not found, then searched in VSE Control File (using RACROUTE)
  - Exception: user ID FORSEC
    - During IPL searched in DTSECTAB first
    - After IPL complete, searched only in the VSE Control File

(c) 1999 IBM Corporation

PDF created with FinePrint pdfFactory trial version http://www.fineprint.com

BSM User ID and CICS Prefixing

- CICS prefixing can be used to differentiate between two or more CICS Transaction Servers running on one VSE/ESA system
- The CICS prefix is identical with the user ID of the CICS startup job
  - If no user ID was specified FORSEC will be used as default
  - FORSEC will be replaced
    - For SYS SEC=YES by a user ID specified in $$ JOB or ID statement
    - For SYS SEC=NO by a user ID specified in the ID statement (w/o password)

(c) 1999 IBM Corporation

PDF created with FinePrint pdfFactory trial version http://www.fineprint.com

BSM ID Statements Without Password

- SYS SEC=YES specified
  - During ASI procedure, no password required
    - FORSEC password in DTSECTAB not used
  - Special task user IDs
    - An administrator can submit a job with an // ID statement containing only the special task user ID w/o password
    - Special task user IDs are only defined in VSE Control File (e.g.DBDCCICS, CICSPROD)
    - They can not be used for Interactive Interface access (batch only)

(c) 1999 IBM Corporation

PDF created with FinePrint pdfFactory trial version http://www.fineprint.com

BSM User Profile Dialogs

- Maintain User Profiles dialog (fastpath 2 1 1)
- List screen - ADD, CHANGE, DELETE
- User attributes divided in segments
  - Base segment
    - Basic attributes (password, expiration date, ...)
  - Interactive Interface (II) segment
  - CICS segment
  - Resource Class segment
  - ICCF segment

(c) 1999 IBM Corporation

PDF created with FinePrint pdfFactory trial version http://www.fineprint.com

BSM User Profile Dialogs ...

```
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

    _     $SRV          01/01/97 *              2   IESERSUP  2
    _     ANNA                                  1   IESEADM   2
    _     CICSUSER      01/01/97 *              3   DFLESEL   2
    _     DBDCCICS                              1   DUMMY     1
    _     FORSEC                                1   IESEADM   2
    _     HUGO                                  2   IESEPROG  2
    _     HUGOB                                 2   IESEPROG  2
    _     HUGO2         03/17/99 *              2   IESEPROG  2
    _     JSCH                                  1   IESEADM   2
    _     JSC1          03/29/99 *              1   IESEADM   2
    _     OPER          01/01/97 *              2   IESEOPER  2
    _     POST                                  1   IESA$FST  1

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

Example of 'Maintain User Profile' screen

(c) 1999 IBM Corporation

PDF created with FinePrint pdfFactory trial version http://www.fineprint.com

BSM User Profile Dialogs ...

```
IESADMUPBA                ADD OR CHANGE USER PROFILE
Base     II       CICS     ResClass ICCF

To CHANGE, alter any of the entries except the userid.

  USERID.............. ANNA       4 - 8 characters (4 characters for ICCF users)

  INITIAL PASSWORD... _________   3 - 8 characters

  DAYS................ 000        0-365 Number of days before password expires
  REVOKE DATE........ _________   Date when Userid will be revoked (mm/dd/yy)

  USER TYPE.......... 1          1=Administrator, 2=Programmer, 3=General
  INITIAL NAME....... IESEADM    Initial function performed at signon
  NAME TYPE.......... 2          1=Application, 2=Selection Panel
  SYNONYM MODEL...... _________   Userid to be used as model for synonyms




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

Example of 'Add or Change User Profile' screen - Base segment

(c) 1999 IBM Corporation

PDF created with FinePrint pdfFactory trial version http://www.fineprint.com

BSM User Profile Dialogs ...

```
IESADMUPII                      USER AUTHORIZATION
Base     II        CICS     ResClass ICCF
Answer yes or no to the following questions for userid ANNA
Enter 1 for yes, 2 for no
  NEWS..................... 1   Should user receive news items?
  ESCAPE................... 1   Can user escape to CICS?
  CONFIRM DELETE........... 2   Does user want a confirmation message?
  VSE PRIMARY SUBLIBRARY..... 1   Does user want a PRIMARY sublibrary?
  SUBMIT TO BATCH.......... 1   Can user submit to Batch?
  VSAM FILES............... 1   Can user define VSAM files?
  VSAM CATALOGS............ 1   Can user manage VSAM catalogs?
  OLPD..................... 1   Can user delete OLPD incidents?
  CONSOLE COMMANDS......... 1   Can user enter all commands?
  CONSOLE OUTPUT........... 1   Can user see all messages?
  BATCH QUEUES............. 1   Can user manage all POWER jobs?
  APPLICATION PROFILES..... 1   Can user maintain application profiles?
  SELECTION PANELS......... 1   Can user maintain selection panels?
  USER PROFILES............ 1   Can user maintain user profiles?
  DEFAULT USER VSAM CATALOG.. IJSYSCT

PF1=HELP                    3=END                    5=UPDATE
PF7=BACKWARD   8=FORWARD
```

Example of 'User Authorization' screen - Interactive Interface segment

(c) 1999 IBM Corporation

PDF created with FinePrint pdfFactory trial version http://www.fineprint.com

BSM User Profile Dialogs ...

```
IESADMUPCI                ADD OR CHANGE CICS SEGMENT
Base     II       CICS     ResClass ICCF

   OPERATOR ID.............. SYA   Enter 3 character id for user ANNA
   OPERATOR PRIORITY....... 000   Operator priority between 0-255
   XRF SIGNOFF............. 2     Sign off after XRF takeover (1=yes,2=no)
   TIMEOUT................. 00    Minutes until sign off between 0-60

   PRIMARY LANGUAGE........       National language for CICS messages


     Place an 'X' next to the operator classes for this user

   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 _




PF1=HELP                     3=END                     5=UPDATE
PF7=BACKWARD   8=FORWARD
```

Example of 'Add or Change CICS Segment' screen

(c) 1999 IBM Corporation

PDF created with FinePrint pdfFactory trial version http://www.fineprint.com

BSM User Profile Dialogs ...

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

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

     Specify the access rights for 1-32 DTSECTAB access control classes
     ( _=No access, 1=Connect, 2=Read, 3=Update, 4=Alter )
   01 _   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 _

   READ DIRECTORY..... 1   User can read directory with Connect (1=yes, 2=no)
   B-TRANSIENTS....... 1   User can manipulate B-Transients     (1=yes, 2=no)

PF1=HELP                      3=END                        5=UPDATE
PF7=BACKWARD   8=FORWARD
```

Example of 'Add or Change Resource Access Rights' screen

(c) 1999 IBM Corporation

PDF created with FinePrint pdfFactory trial version http://www.fineprint.com

BSM Protecting Resources

(c) 1999 IBM Corporation

PDF created with FinePrint pdfFactory trial version http://www.fineprint.com

BSM Resource Profiles

- Protection rules
  - Files and libraries
    - No profile = no protection
  - Sublibraries and members
    - Protected only if library is protected
  - Transactions
    - No profile = no access allowed (by CICS)

(c) 1999 IBM Corporation

PDF created with FinePrint pdfFactory trial version http://www.fineprint.com

BSM Resource Profiles ...

- Profiles for **files, libraries, sublibraries, and members** are stored in DTSECTAB
  - 1-32 access classes
  - Skeleton DTRSECTRC (ICCF lib. 59)
- DTSECTAB loaded into SVA-24
- Activate DTSECTAB via
  - IPL with SYS SEC=YES specified
  - LNKEDT when cataloged to IJSYSRS.SYSLIB
    - Active when next user ID from a JCL is processed
    - Librarian internal information not replaced ==> IPL
- Logging and reporting via ACLR

(c) 1999 IBM Corporation

PDF created with FinePrint pdfFactory trial version http://www.fineprint.com

BSM Resource Profiles ...

- Profiles for **CICS transactions** are stored in DTSECTXN
- DTSECTXN activated and loaded into SVA-31 by CICS (via RACROUTE LIST request)
  - during CICS startup
  - via **CEMT PERFORM SECURITY REBUILD**
- LNKEDT when cataloged to IJSYSRS.SYSLIB
- Describes attributes of transaction
  - One access class per transaction (range 1-64)
  - UACC is not supported
  - Generic names are not allowed
- Logging and reporting via console messages

(c) 1999 IBM Corporation

PDF created with FinePrint pdfFactory trial version http://www.fineprint.com

BSM Resource Profiles ...

- New macro support for CICS transaction profiles

  DTSECTXN NAME={CICS-region}.transid
  ,TRANSEC=(class)
  ,SUBTYPE={INITIAL|FINAL}

  - **CICS-region** = user ID in CICS startup job
  - **transid** = up to 4 characters
    (.-_&, are not allowed)
  - **class** = {1|...|64}
    - TRANSEC=(1) for public transactions
    - TRANSEC=(61) for Interactive Interface transactions

(c) 1999 IBM Corporation

PDF created with FinePrint pdfFactory trial version http://www.fineprint.com

BSM Resource Dialogs

- Define Transaction Security (Fastpath 2 8)
  - Specify filter to list all defined transactions
    Filter can be
    - Prefix of the transaction name
    - The CICS region
  - MERGE (via PF6) other transaction entries into the security table DTRISEC.Z in IJSYSRS.SYSLIB
    - Entries with the same name will be replaced
    - Service entries are shipped in member DTRISEC.U
    - DTRISEC.Z is in IPF format

(c) 1999 IBM Corporation

PDF created with FinePrint pdfFactory trial version http://www.fineprint.com

BSM Resource Dialogs ...

```
 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.




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

Example of 'Specify Filter' screen

(c) 1999 IBM Corporation

PDF created with FinePrint pdfFactory trial version http://www.fineprint.com

BSM Resource Dialogs ...

```
 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................. ________    Enter the member name.

MEMBER TYPE................. ________    Enter the member type.

LIBRARY..................... ________    Enter the library name.

SUBLIBRARY.................. ________    Enter the sublibrary name.



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

Example of 'Merge Tables' screen

(c) 1999 IBM Corporation

PDF created with FinePrint pdfFactory trial version http://www.fineprint.com

BSM Resource Dialogs ...

- Define Transaction Security - ADD, ALTER, DELETE applicable on transaction list
  - PROCESS (via PF5 on the list of transactions)
    - Builds a table in DTSECTXN macro source format
    - Submits a job that assembles and catalogs the DTSECTXN phase in IJSYSRS.SYSLIB

(c) 1999 IBM Corporation

PDF created with FinePrint pdfFactory trial version http://www.fineprint.com

BSM Resource Dialogs ...

```
TAS$SEC1                  DEFINE TRANSACTION SECURITY

Enter the required data and press ENTER.

OPTIONS: 1 = ADD   2 = ALTER    5 = DELETE

 OPT       TRANSACTION NAME  CICS REGION   SECURITY CLASS

  _           AADD                          1
  _           ABRW                          1
  _           ACCT                          1
  _           ACEL                          1
  _           ACLG                          1
  _           AC01                          1
  _           AC02                          1
  _           AC03                          1
  _           AC05                          1
  _           AC06                          1

 LOCATE TRANSACTION NAME == >  _____
PF1=HELP       2=REDISPLAY  3=END                    5=PROCESS
               8=FORWARD
```

Example of 'Define Transaction Security' screen

(c) 1999 IBM Corporation

PDF created with FinePrint pdfFactory trial version http://www.fineprint.com

BSM Security Server

(c) 1999 IBM Corporation

PDF created with FinePrint pdfFactory trial version http://www.fineprint.com

BSM Security Server

- Used as
  - VSAM data base server to handle the access to the VSE Control File
  - Profile server for other resources (DTSECTXN)
- Runs in a static partition (default FB) to be active before jobs in other (i.e. POWER) partitions gets started
- It is started during BSM initialization.
- Will be stopped from the POWER procedure during PEND

(c) 1999 IBM Corporation

PDF created with FinePrint pdfFactory trial version http://www.fineprint.com

BSM Security Server ...

- BSM server phase BSTPSTS
  - Maintask handles incoming request or routes it to the related subtask
    - DB subtask processes access request to the VSE Control File
    - PS subtask loads profiles into storage (i.e. DTSECTXN) for RACROUTE LIST requests
- Request coming from
  - BSM via XPCC
  - Via operator command

(c) 1999 IBM Corporation

PDF created with FinePrint pdfFactory trial version http://www.fineprint.com

BSM Security Server ...

- Database caching
  - Fast retrieval of VSE Control File records
  - First access of a record loads this record also into a dataspace
  - Second request for the same record takes the information of this record from the dataspace
  - Saves XPCC and VSAM overhead for subsequent requests
  - Activated via DBSTARTCACHE command (default cache not active)

(c) 1999 IBM Corporation

PDF created with FinePrint pdfFactory trial version http://www.fineprint.com

BSM Security Server ...

- Database logging
  - Propagates VSE Control File updates
  - Keeps a list of keys to updated or added records in the VSE Control File
  - Used in a shared environment to make updates available to the database cache of each server

(c) 1999 IBM Corporation

PDF created with FinePrint pdfFactory trial version http://www.fineprint.com

BSM Security Server ...

- User interface
  - Command format **MSG xx,DATA=command**
  - Available commands
    - **HELP**, **?**, or **blank** provides a list of all commands
    - **STATUS** displays server internal status information
    - **DBSTARTCACHE** starts caching of VSE Control File records
    - **DBSTOPCACHE** stops caching
    - **LOGTIME=n** sets logtime interval (in minutes)
    - **RESET** resets server to its initial state
    - **STOP** stops the server
    - **OPENCNTL** opens the VSE Control File
    - **CLOSECNTL** closes the VSE Control File

(c) 1999 IBM Corporation

PDF created with FinePrint pdfFactory trial version http://www.fineprint.com

BSM Security Server ...

```
msg fb,data=help
AR 0015 1I40I  READY
FB 0011 BST221I POSSIBLE SECURITY SERVER COMMANDS ARE:
FB 0011   DBSTARTCACHE........: STARTS DATABASE CACHING
FB 0011   DBSTOPCACHE.........: STOPS DATABASE CACHING
FB 0011   STATUS[=ALL]........: SHOWS TOTAL SERVER STATUS
FB 0011   STATUS=[MAIN|PS|DB].: SHOWS SELECTED STATUS
FB 0011   LOGTIME=N...........: SETS LOGTIME TO N MINUTES (1..9)
FB 0011   RESET...............: CLEANUP EVERYTHING
FB 0011   STOP................: STOPS THE SERVER (USE WITH CAUTION!)
FB 0011   OPENCNTL............: OPENS THE II CONTROL FILE
FB 0011   CLOSECNTL...........: CLOSES THE II CONTROL FILE
```

Help command example

(c) 1999 IBM Corporation

PDF created with FinePrint pdfFactory trial version http://www.fineprint.com

BSM Security Server ...

```
msg fb,data=status
AR 0015 1I40I  READY
FB 0011 BST223I CURRENT STATUS OF THE SECURITY TRANSACTION SERVER:
FB 0011 SERVER GENERAL STATUS: (Build March 1999)
FB 0011   SERVER WAS STARTED AT ............... : 04/12/1999 18:09:09
FB 0011   TIME ELAPSED (DDDD::HH:MM:SS) ...... : 0000::18:04:44
FB 0011   NO. OF REQUESTS IN XPCC QUEUE ...... : 0
FB 0011   NO. OF REQ. IN INTERNAL REPLY QUEUE  : 0
FB 0011   NO. OF FREE (REUSABLE) REQ. BLOCKS . : 9
FB 0011   NO. OF CURRENTLY ALLOCATED BLOCKS .. : 10
FB 0011   SIZE OF ONE REQUEST BLOCK (BYTES) .. : 740
FB 0011   TOTAL NUMBER OF REQUESTS SO FAR .... : 17
FB 0011   HIGHEST NO. OF PARALLEL REQUESTS ... : 1
FB 0011   SERVER DEBUG LEVEL ................. : SMALL,CONSOFF
FB 0011   BSM DEBUG LEVEL .................... : CONSOFF
FB 0011   NUMBER OF SERVER RESETTINGS ........ : 0
FB 0011 PROFILE SERVICE SUBTASK STATUS:
FB 0011   PS SUBTASK STARTED .................. : YES
FB 0011   NO. OF ITEMS IN PS REQUEST QUEUE ... : 0
FB 0011 DATABASE SUBTASK STATUS:
FB 0011   DB SUBTASK STARTED .................. : YES
FB 0011   II CONTROL FILE OPEN ................ : YES
FB 0011   DATABASE CACHE INITIALIZED OK ...... : YES
FB 0011   DATABASE CACHING .................... : OFF
FB 0011   LOGTIME INTERVAL IN MINUTES ........ : 5
FB 0011   NO. OF ITEMS IN DB REQUEST QUEUE ... : 0
```

Server status example

(c) 1999 IBM Corporation

PDF created with FinePrint pdfFactory trial version http://www.fineprint.com

BSM Security Server ...

- Termination
  - Due to STOP or CANCEL request
    - Confirmation is requested
  - When a sever error occurred

- Restart
  - The SECSERV procedure has still control (message // PAUSE TO RESTART THE SECURITY SERVER ... is provided)
    - // EXEC PROC=RESTASEC
  - SECSERV procedure is not active
    - // EXEC PROC=$BJCL for SYS SEC=NO and security server partition is FB
    - Re-IPL for SYS SEC=YES

(c) 1999 IBM Corporation

PDF created with FinePrint pdfFactory trial version http://www.fineprint.com

BSM Security Server ...

- Changing the static partition for the security server
  - Default is FB
  - New partition should run a procedure with the same logic as SECSERV from $BJCL
  - The priority of the new partition should be adapted
  - Storage requirements like FB
  - Activation via SYS SERVPART=partition_id during IPL

(c) 1999 IBM Corporation

PDF created with FinePrint pdfFactory trial version http://www.fineprint.com

Hints and Tips

(c) 1999 IBM Corporation

PDF created with FinePrint pdfFactory trial version http://www.fineprint.com

BSM Migration

- User profiles
  - VSE/ESA 2.4 Control file records are not compatible with records of previous releases
  - Use utility IESBLDUP to migrate
- DTSECTAB
  - No change for resource entries
- Transaction profiles
  Two REXX procedures provided in library 59 to generate DTSECTXN definition
  - SKSECTXS uses the PCT as input
  - SKSECTX2 uses the output of the CICS Migration Utility (stage 1) as input (including online definitions)

(c) 1999 IBM Corporation

PDF created with FinePrint pdfFactory trial version http://www.fineprint.com

Recovery

- If an active security manager does not allow to recover from a problem use:

  IPL cuu LOADP ..P
  STOP=DPD
  0 SYS SEC=RECOVER
  0

  - No SAF will be loaded
  - BSSINIT will not start a security manager
  - Re-IPL required to start security manager again

(c) 1999 IBM Corporation

PDF created with FinePrint pdfFactory trial version http://www.fineprint.com

BSM Debugging Support

- Activate BSM trace
  DEBUG TRACE=BSM
  DEBUG ON
- Stop tracing for BSM only
  DEBUG TRACE=NOBSM
- Stop all tracing
  DEBUG OFF
- View trace information
  DEBUG SHOW=BSM
  DEBUG SHOW=BSM,ALL

(c) 1999 IBM Corporation

PDF created with FinePrint pdfFactory trial version http://www.fineprint.com

Status Information

```
sir
AR 0015 CPUID  VM = 5A46817596720000      VSE = FF11111196720000
AR 0015 VM-SYSTEM = VM/ESA          2.3.0       9807
AR 0015 PROCESSOR = 9672-5A         USERID    = VSETEST
AR 0015 PROC-MODE = ESA             IPL(150)    18:08:35      04/12/1999
AR 0015 SYSTEM    = VSE/ESA         2.4.0 LAR2                03/04/1999
AR 0015             VSE/AF          6.4.0       @DY45037      12/07/1998
AR 0015             VSE/POWER       6.4.0       DY-BASE
AR 0015 IPL-PROC  = $IPLESA         JCL-PROC  = $$JCL
AR 0015 SUPVR     = $$A$SUPX        TURBO-DISPATCHER (18) ACTIVE
AR 0015                             HARDWARE COMPRESSION ENABLED
AR 0015 SEC. MGR. = BASIC             SECURITY  = ONLINE and BATCH
AR 0015 VIRTCPU   = 0000:06:29.175      CP = 0000:00:37.741
AR 0015 CPU-ADDR. = 0000(IPL)   ACTIVE
AR 0015   ACTIVE  = 0000:05:23.334   WAIT = 0062:41:08.484
AR 0015   PARALLEL= 0000:01:25.157   SPIN = 0000:00:00.000
AR 0015 CPU timings MEASUREMENT INTERVAL    0062:49:58.274
AR 0015 TASKS ATT.= 00015           HIGH-MARK = 00015    MAX = 00200
AR 0015 DYN.PARTS = 00000           HIGH-MARK = 00000    MAX = 00012
AR 0015
AR 0015 COPY-BLKS = 00000           HIGH-MARK = 00028    MAX = 01500
AR 0015 CHANQ USED= 00003           HIGH-MARK = 00011    MAX = 00099
AR 0015 PGIN  TOT.= 0000000316      EXP.AVRGE.= 0000000000/SEC
AR 0015 PGOUT TOT.= 0000001093
AR 0015       UNC.= 0000000648      EXP.AVRGE.= 0000000000/SEC
AR 0015       PRE = 0000000445      EXP.AVRGE.= 0000000000/SEC
AR 0015 LOCKS EXT.= 0000001166      LOCKS INT.= 0000007613
AR 0015      FAIL = 0000000034           FAIL = 0000000127
AR 0015 LOCK I/O  = 0000000000      LOCK WRITE= 0000000000
AR 0015 1I40I  READY
```

SIR output example for security - BSM

(c) 1999 IBM Corporation

PDF created with FinePrint pdfFactory trial version http://www.fineprint.com

Status Information ...

```
sir
AR 0015 CPUID  VM = 5A46817596720000      VSE = FF11111196720000
AR 0015 VM-SYSTEM = VM/ESA          2.3.0       9807
AR 0015 PROCESSOR = 9672-5A         USERID    = VSETEST
AR 0015 PROC-MODE = ESA             IPL(150)    18:08:35      04/12/1999
AR 0015 SYSTEM    = VSE/ESA         2.4.0 LAR2                03/04/1999
AR 0015             VSE/AF          6.4.0       @DY45037      12/07/1998
AR 0015             VSE/POWER       6.4.0       DY-BASE
AR 0015 IPL-PROC  = $IPLESA         JCL-PROC  = $$JCL
AR 0015 SUPVR     = $$A$SUPX        TURBO-DISPATCHER (18) ACTIVE
AR 0015                             HARDWARE COMPRESSION ENABLED
AR 0015 SEC. MGR. = CAKSESM                SECURITY  = ACTIVE
AR 0015 VIRTCPU   = 0000:06:29.175        CP = 0000:00:37.741
AR 0015 CPU-ADDR. = 0000(IPL)   ACTIVE
AR 0015   ACTIVE  = 0000:05:23.334   WAIT = 0062:41:08.484
AR 0015   PARALLEL= 0000:01:25.157   SPIN = 0000:00:00.000
AR 0015 CPU timings MEASUREMENT INTERVAL    0062:49:58.274
AR 0015 TASKS ATT.= 00015           HIGH-MARK = 00015    MAX = 00200
AR 0015 DYN.PARTS = 00000           HIGH-MARK = 00000    MAX = 00012
AR 0015
AR 0015 COPY-BLKS = 00000           HIGH-MARK = 00028    MAX = 01500
AR 0015 CHANQ USED= 00003           HIGH-MARK = 00011    MAX = 00099
AR 0015 PGIN  TOT.= 0000000316      EXP.AVRGE.= 0000000000/SEC
AR 0015 PGOUT TOT.= 0000001093
AR 0015       UNC.= 0000000648      EXP.AVRGE.= 0000000000/SEC
AR 0015       PRE = 0000000445      EXP.AVRGE.= 0000000000/SEC
AR 0015 LOCKS EXT.= 0000001166      LOCKS INT.= 0000007613
AR 0015      FAIL = 0000000034           FAIL = 0000000127
AR 0015 LOCK I/O  = 0000000000      LOCK WRITE= 0000000000
AR 0015 1I40I  READY
```

SIR output example for security - ESM

(c) 1999 IBM Corporation

PDF created with FinePrint pdfFactory trial version http://www.fineprint.com

SAF Installation Exit

- SAF router exit ICHRTX00 is supported by VSE/ESA to:
  - Add own security checks
  - Modify security checking parameters
- Fore more information see VSE/ESA 2.4.0 Planning manual

(c) 1999 IBM Corporation

PDF created with FinePrint pdfFactory trial version http://www.fineprint.com

VSE/POWER Spool Access Support

- Improved access control for entries in RDR, LST, PUN, and XMT queues
  - Spool entries owned by, or target to, a specific user ID can only be accessed by:
    - A user who has performed a security logon
    - Security user ID must match with the origin or target user ID or must be an system administrator
  - Activation via SECAC=SYS in the SET statement of the VSE/POWER startup procedure when SYS SEC=YES was specified at IPL
  - Can be changed at entry level with the SECAC operand in JOB, LST, and PUN statements
  - Support is available with the BSM as well as with the ESM

(c) 1999 IBM Corporation

PDF created with FinePrint pdfFactory trial version http://www.fineprint.com

Documentation

- Online Message Explanation (OME)
- VSE/ESA Messages and Codes
  - Volume 1, SC33-6796
  - Volume 2, SC33-6798
  - Volume 3, SC33-6799
- VSE/ESA Planning, SC33-6703
- VSE/ESA Administration, SC33-6705
- VSE/POWER Administration and Operation, SC33-6733
- RACROUTE documentation on CDROM SK2T-0060

(c) 1999 IBM Corporation

PDF created with FinePrint pdfFactory trial version http://www.fineprint.com

Summary

(c) 1999 IBM Corporation

PDF created with FinePrint pdfFactory trial version http://www.fineprint.com

Summary

- New:
  - RACROUTE support
  - System Authorization Facility (SAF)
  - Security Manager (BSM/ESM)
  - Security server partition
  - Transaction Security Table (DTSECTXN)

(c) 1999 IBM Corporation

PDF created with FinePrint pdfFactory trial version http://www.fineprint.com

Summary ...

- Changes:
  - VSE Control File is the central repository for user profiles
  - User entries are extended to keep transaction class information
  - User IDs are removed from DTSECTAB
    Exception: FORSEC and DUMMY are needed for startup
  - VSE/POWER spool access control is improved

(c) 1999 IBM Corporation

PDF created with FinePrint pdfFactory trial version http://www.fineprint.com