IBM System z – WAVV 2009

Basic Security Manager from A to Z

Ingo Franzki

Trademarks

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

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

* Registered trademarks of IBM Corporation

The following are trademarks or registered trademarks of other companies.

LINUX is a registered trademark of Linus Torvalds

Tivoli is a trademark of Tivoli Systems Inc.

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

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

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

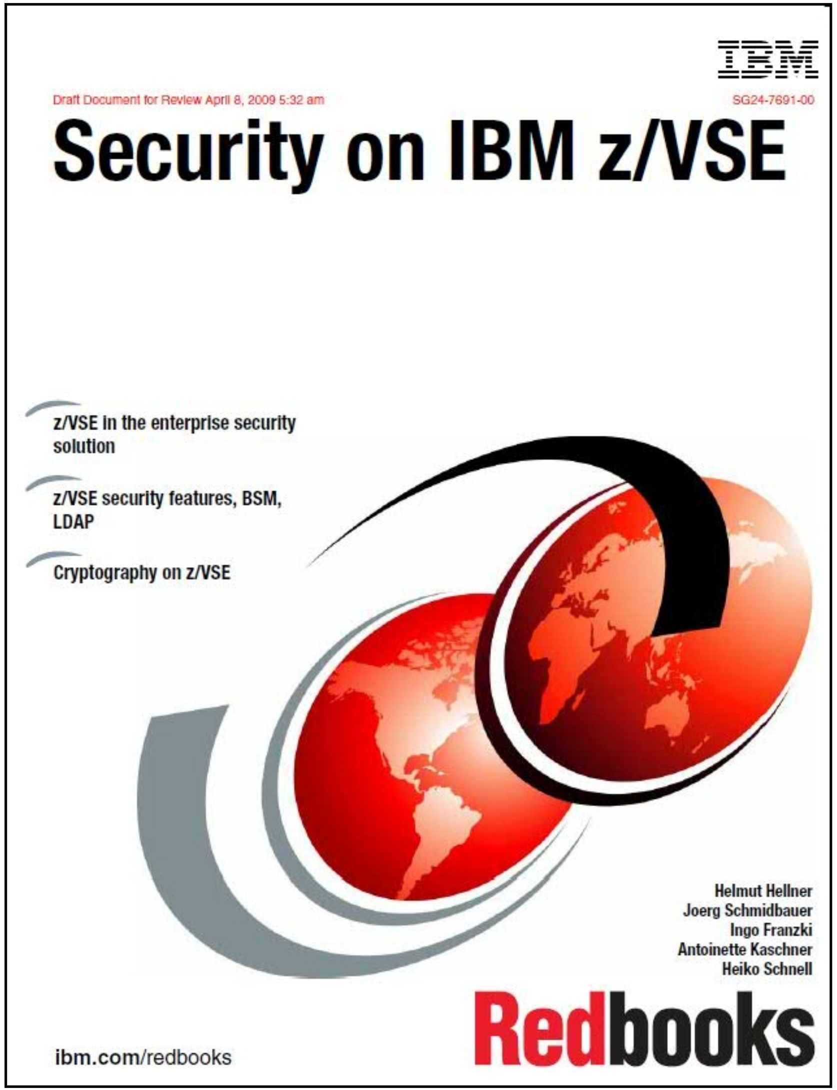
SET and Secure Electronic Transaction are trademarks owned by SET Secure Electronic Transaction LLC.

Intel is a registered trademark of Intel Corporation.

New Redbook: Security on IBM z/VSE - SG24-7691

- **Available as public draft since April**
- **http://www.redbooks.ibm.com/redpieces/abstracts/sg247691.html**
- **Explains security concepts as well as step by step setup**
- **It covers:**
  - Basic Security Manager
  - LDAP Authentication
  - Cryptography & SSL
  - TCP/IP Security
  - SecureFTP & Secure telnet
  - CICS Web Support Security
  - Connector Security
  - Security APIs

Open the Redbook



Draft Document for Review April 8, 2009 5:32 am

SG24-7691-00

Security on IBM z/VSE

z/VSE in the enterprise security solution

z/VSE security features, BSM, LDAP

Cryptography on z/VSE

Helmut Hellner
Joerg Schmidbauer
Ingo Franzki
Antoinette Kaschner
Heiko Schnell

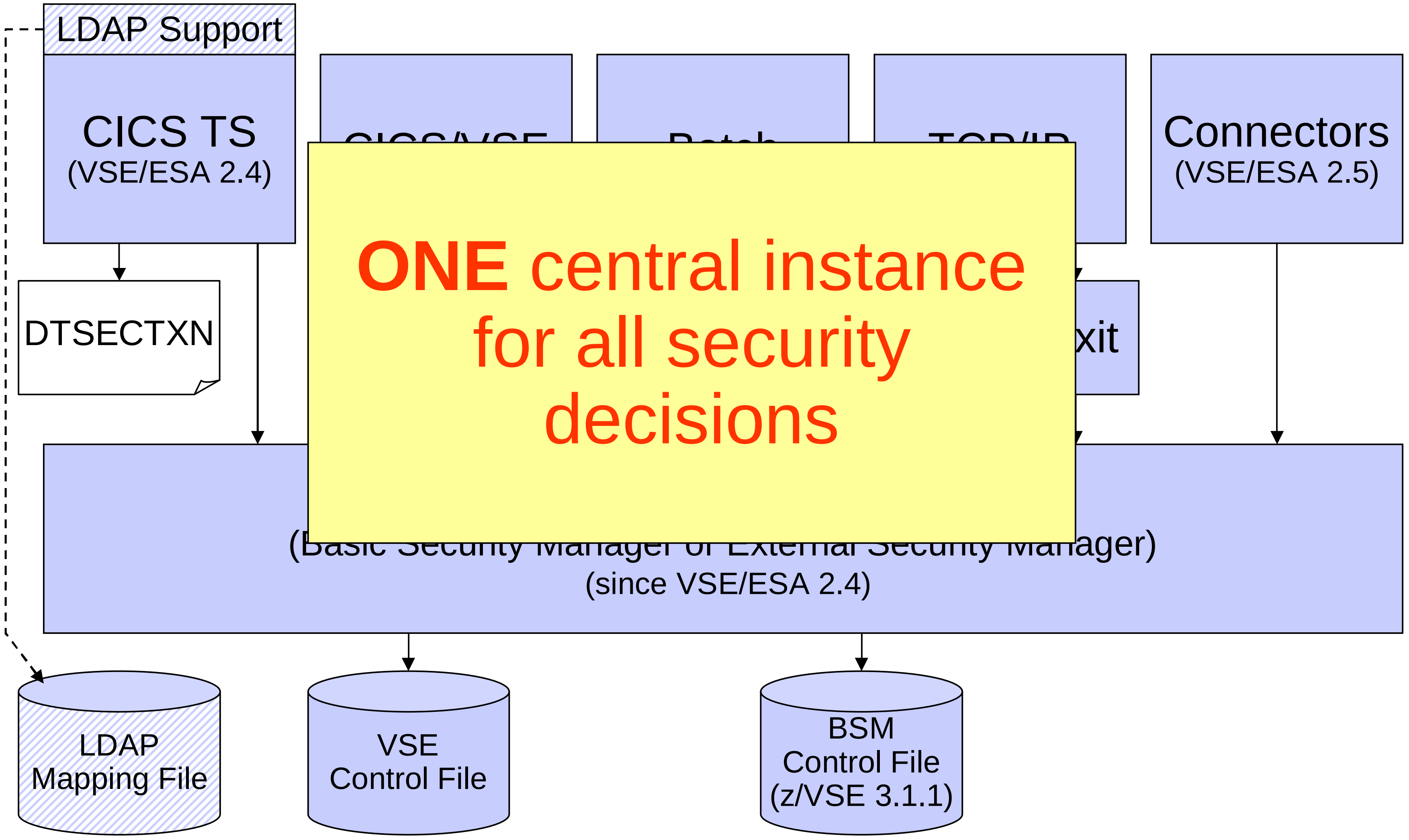
Redbooks

ibm.com/redbooks

Topics

- **Overview & basics**
- **Step by step**
  - Define a user-ID
  - Group maintanance
- **Hints & Tips**
  - Migration from older BSM versions
  - Security inheritance when submitting jobs
  - CICSUSER considerations
  - Critical transactions
- **Security Tools**
  - BSM Cross Reference Tool
  - RACROUTE Encapsulation Services

VSE Security Components



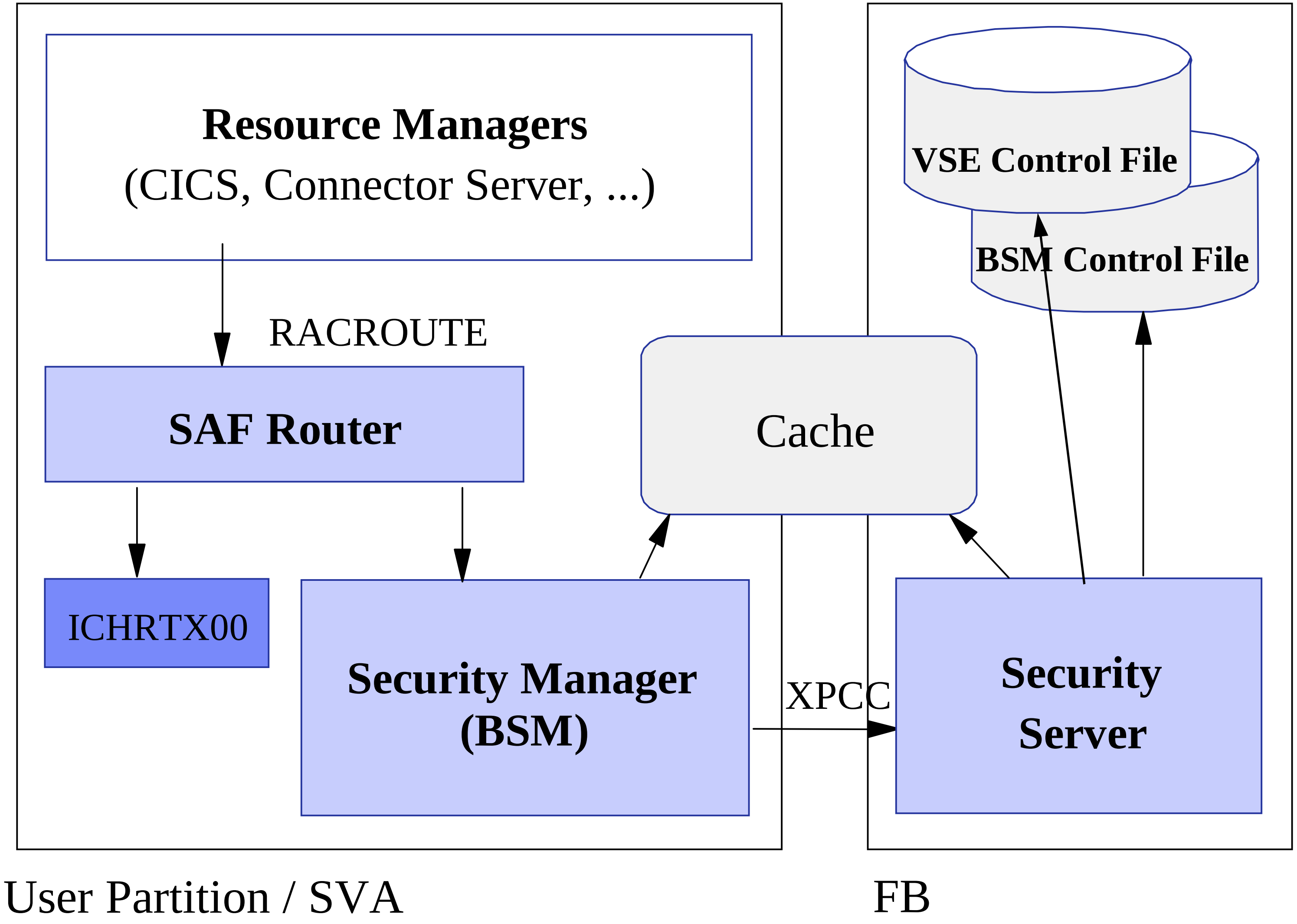
ONE central instance for all security decisions

Security Managers

- **Basic Security Manager (BSM)**
  - Part of VSE Central Functions
  - Sign on Security
  - Transaction Security
  - Resource Security

- **External Security Manager (ESM)**
  - CA-Top Secret
  - BIM Alert
  - Vendor

Security Authorization Facility (SAF) and Basic Security Manager



Defining a new user-ID

- **See Redbook chapter 2.3.2**
  - Define a new user-ID
    - Interactive Interface dialog **Maintain User Profiles** (211)
  - Connect the new user-ID to groups
    - Interactive Interface dialog **Maintain Security Profiles** (282)
    - Show **User List** (option 6) and add the user-ID to the group
    - Add the user-ID or groups to the access list of the desired resource profiles, if needed
    - You can also use BSTADMIN to do this in batch.
  - Perform a BSM Security Rebuild to activate the changes
  - If you are using LDAP Authentication, you also need to add the user-ID to the LDAP mapping file via IESLDUMA

Open the Redbook

Maintaining user-IDs

- **If you make changes to a user-ID, don‘t forget to update the groups and resources also**
  - When deleting a user-ID
    - Remove it from the groups it is belonging to
    - Remove it from the access lists of any resource profiles
  - When updating a user-ID
    - Adapt the groups it is belonging to, if required
    - Adapt the access lists of all resource profiles, if required
  - Use the BSM Cross Reference Tool to find out where the user-ID is referenced (see separate foil)
  - Perform a BSM Security Rebuild to activate the changes
  - If you are using LDAP Authentication, you also need to update the user-ID in the LDAP mapping file via IESLDUMA

Group maintanance

- **See Redbook chapter 2.3.3**
  - Per default there are GROUP01 to GROUP64
    - coresponding to the 64 CICS transaction security keys
  - Define a new group
    - Interactive Interface dialog **Maintain Security Profiles** (282)
    - Use option 1 (Add) to add a new group
  - Add user-IDs to the newly created group
    - Show **User List** (option 6) and add the User-ID to the group
  - Do NOT create groups that are named the same as user-IDs
  - You can also use BSTADMIN to do this in batch.
  - Perform a BSM Security Rebuild to activate the changes

Open the Redbook

Resource profiles

- **See Redbook chapter 2.3.4**
  - There are 2 repositories for resource profiles:
    - **DTSECTAB:** It contains the entries for z/VSE files, libraries, sublibraries, and members
      - Use skeleton DTSECTRC in ICCF library 59 to maintain the table
    - **BSM Control File:** It keeps the profiles for all the new resource classes supported by BSM
  - Access List specifies who (base on user-ID or group) has access (Read, Update, Alter) to the resource
  - If the access list contains both, a user-ID and a group that contains the user-ID
    - then the access rights specified with the User-ID is effective

Open the Redbook

Migrating from older BSM versions

- **Since z/VSE 3.1.1, BSM uses the BSM Control File instead of DTSECTXN**
  - You may need to migrate transaction security definitions from DTSECTXN to BSM Control file
- **The steps you can follow partly depends on:**
  - The VSE system level from which you installed z/VSE
  - Whether you performed an FSU (Fast Service Upgrade) or an initial installation.
  - Whether you wish to retain the use of your previous security definitions.
- **Please see Administration Manual Chapter 22 (page 325) for details**
  - See the table that describes the steps you need to perform before and after migration of VSE

Open Administration Manual

Security inheritance when submitting jobs

- **When you have batch security active (SYS SEC=YES), all your jobs need to specify a user-ID and password**
  - Either using the // ID statement within the job
  - or in the * $$ JOB card
- **When you submit jobs from the ICCF library**
  - The submitted job automatically inherits the user-ID and password from the submitting user
  - No need to specify a // ID statement or user-ID in the * $$ JOB card
- **Inheritance only works if batch security is active at the time you do the submit**
  - Jobs that have been submitted prior to activating batch security do not have any inherited security information
    - You may have to re-submit those jobs

CICSUSER considerations

- **Every transaction runs under the context of a user-id**
- **If no user is signed on, it runs under the default user**
  - DFHSIT: DFLTUSER=CICSUSER
- **CICSUSER is predefined after base install:**
  - Type 3 (ICCF is not allowed)
  - Is in GROUP01 , GROUP60-GROUP64
    - GROUP01 and GROUP60 is required by Interactive Interface
- **Actions to perform after installation**
  - Do not allow this user to use critical transactions lik CEDA, CEMT, ...
  - Adjust groups this user is belonging to

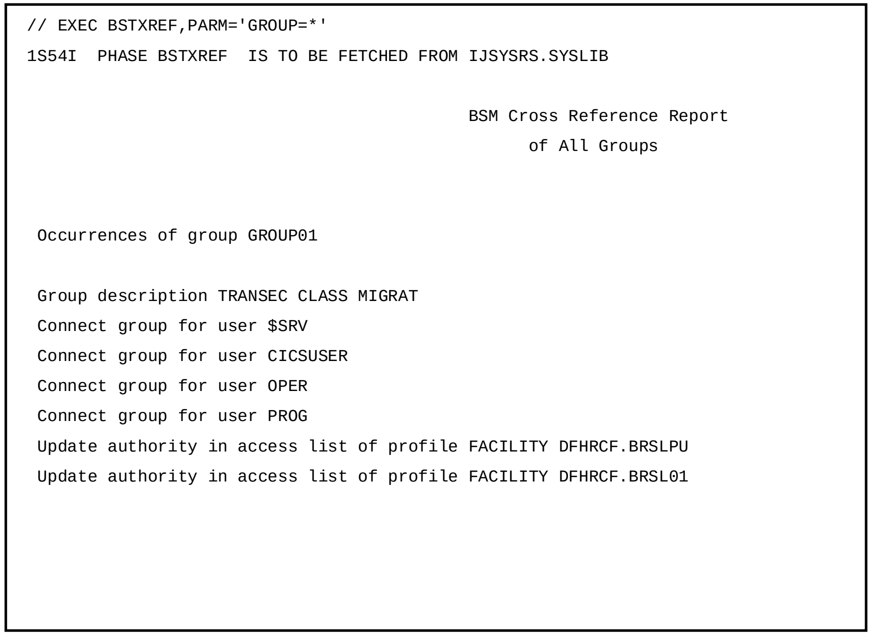
Critical transactions

Transaction	**Description**
USER	Display Activity Dialog, send Message to all users
CEMT	Master terminal
CEDA	Resource definition online
CEDB	Like CEDA, but no INSTALL possible
CEDC	Like CEDA, but read only
CECI	Command level interpreter
CEDF/CEDX	Execution diagnoistic facility
CETR	Trace control
CESN/CESF	Sign on/sign off
DITT	Online Ditto
others ?	

You need to protect these transactions to prevent system damage by users

BSM Cross Reference Tool

- **The z/VSE BSM Cross Reference Tool is intended to help administrators control the profile definitions in the BSM control file.**
- **Example:**
  - When you delete a user-ID, you can use it to ensure that you have removed the user-ID from all access lists and groups.
- **The following functions are provided:**
  - List all groups and resource profiles which contain a specified user-ID.
  - List all resource profiles where a specified group is on the access list.
  - List all user-IDs found in the BSM control file but is not defined in the VSE control file.
  - List all resource profiles that allow any user-ID to access a resource (UACC not NONE).

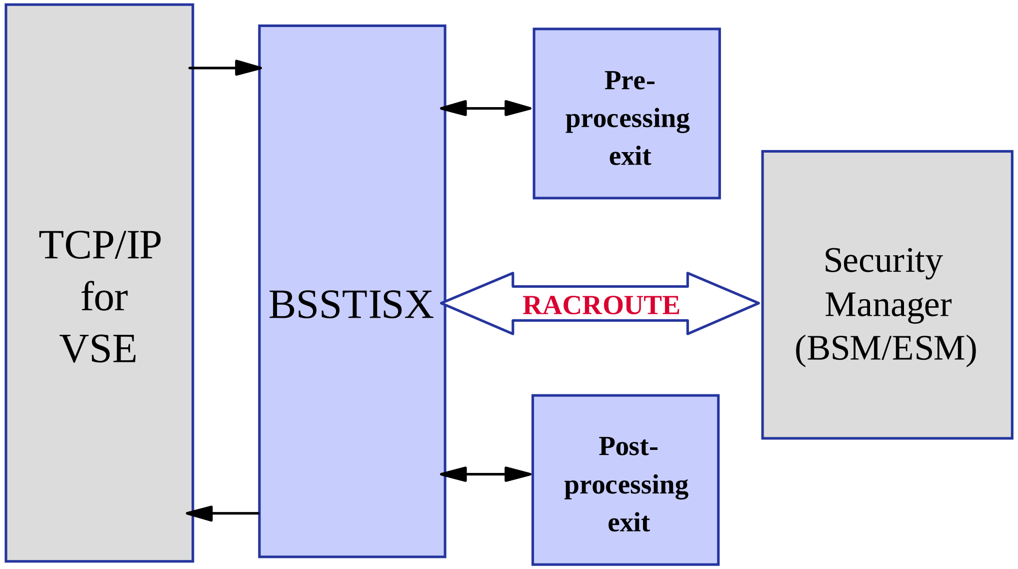


```
// EXEC BSTXREF,PARM='GROUP=*'
1S54I   PHASE BSTXREF  IS TO BE FETCHED FROM IJSYSRS.SYSLIB

                                            BSM Cross Reference Report
                                                  of All Groups



 Occurrences of group GROUP01


 Group description TRANSEC CLASS MIGRAT
 Connect group for user $SRV
 Connect group for user CICSUSER
 Connect group for user OPER
 Connect group for user PROG
 Update authority in access list of profile FACILITY DFHRCF.BRSLPU
 Update authority in access list of profile FACILITY DFHRCF.BRSL01
```

http://www.ibm.com/servers/eserver/zseries/zvse/downloads/tools.html#bsmxref

RACROUTE encapsulation services for TCP/IP

- **The IBM-provided TCP/IP security exit BSSTISX supports a pre- and post-processing interface**
  - These interfaces are solely intended to be used by customers to add self-written security checks
- **In particular when it is used to exploit the security definitions of the security manager, e.g. special profiles of the resource class FACILITY, normally one has to use the RACROUTE macro interface**
  - However, coding of RACROUTE requests can be very complex
- **Therefore these services were provided with BSSTXRRS to encapsulate the three basic RACROUTE requests:**
  - sign on
  - sign off
  - authorization checking for resource access.



http://www.ibm.com/servers/eserver/zseries/zvse/downloads/tools.html#racroute

Questions ?

?