VM/VSE Technical Conference

Orlando - May 2000 - Session E78

VSE/ESA 2.4 Basic Security Manager

Klaus-Dieter Wacker
VSE Development
kdwacker@de.ibm.com

RETURN TO INDEX

Security Requirements

- User identification and verification
- Authorization checking
- Logging and reporting
- Easy administration

Security Concept

General

- Security decisions delegated to Security Mgr
- Sign-on and Resource checking
- Architectured interface for security services (RACROUTE)
- Exchangeable Security Mgr component

Security Concepts

System Authorization Facility (SAF)

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

Security Concept

RACROUTE

- RACROUTE macro is the external security interface of the SAF
- To be used by resource managers, 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 mgr return code
  - Security mgr reason code

Security Concept

Security Managers

- Basic Security Manager (BSM)
  - Part of VSE Central Functions 6.4
  - Provides signon, transaction and DTSECTAB security
- External Security Manager (ESM)
  - Distributed by IBM
    - CA-Top Secret for VSE/ESA (VSE/ESA 2.4)
    - Needs IBM key (license) to fully activate it
  - Vendor supplied
    - CA-Top Secret for VSE (VSE/ESA 1.4 or higher)
    - BIM-Alert ??

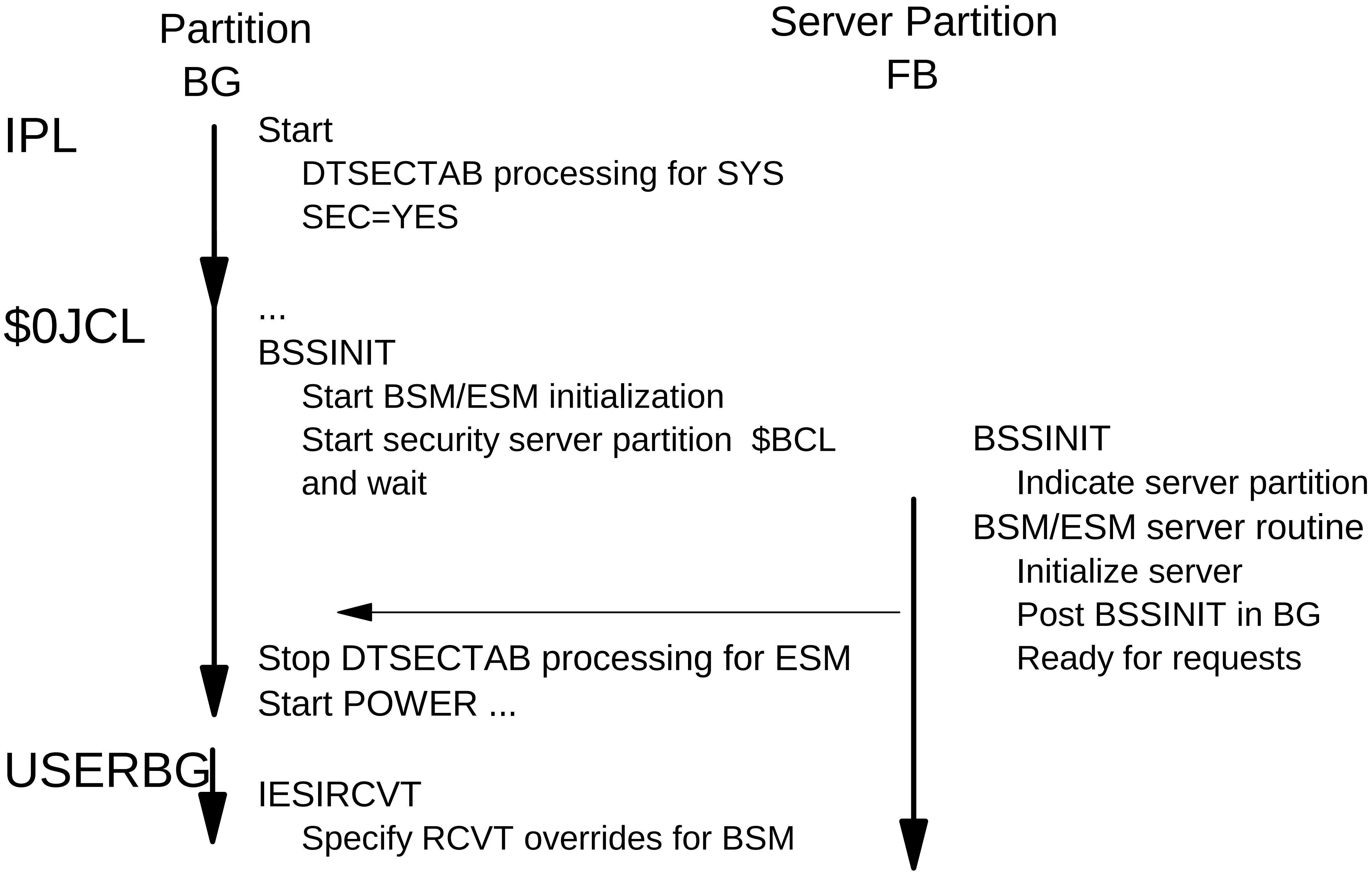
Security Concept

Common Security Startup

- The security manager has to be initialized before other partitions or POWER are active (Exception: OCCF partition at unattended node environment)
- BSSINIT will fail, if there are other partitions active
- Static partition required for security server
- To start ESM specify SYS ESM=phasename in the IPL procedure
- If no ESM is started, BSM is activated
- For SYS SEC=YES with ESM a DTSECTAB protection is active until ESM is initialized

Security Concept

Common Security Startup ...



Partition
BG

Server Partition
FB

IPL

Start
- DTSECTAB processing for SYS
- SEC=YES

$0JCL

...
BSSINIT
- Start BSM/ESM initialization
- Start security server partition $BCL and wait

BSSINIT
- Indicate server partition

BSM/ESM server routine
- Initialize server
- Post BSSINIT in BG
- Ready for requests

Stop DTSECTAB processing for ESM
Start POWER ...

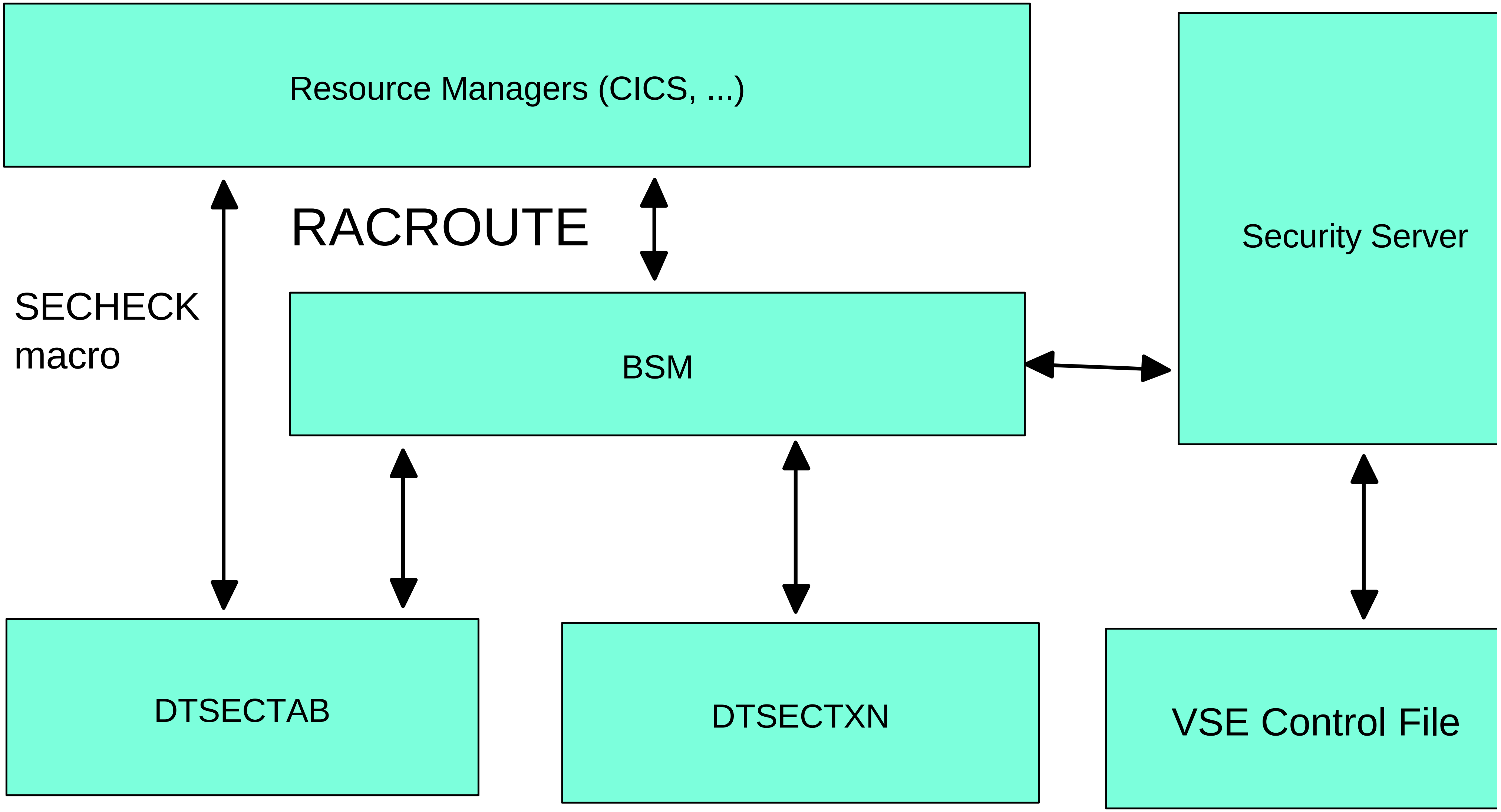
USERBG

IESIRCVT
- Specify RCVT overrides for BSM

Basic Security Mgr
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

Basic Security Mgr
Overview



Basic Security Mgr
Repositories

- VSE Control File
  - Central Repository for all user profiles
  - Used for CICS and Batch (SYS SEC=YES) signon
  - VSAM KSDS file
- DTSECTAB
  - Contains resources like files, libraries, sublibraries, and sublibrary members
  - Only 2 userids are still needed in DTSECTAB (FORSEC, DUMMY)
- DTSECTXN (new with VSE 2.4)
  - Transaction security profiles

Basic Security Mgr

Resource Protection

- "Access Class" is assigned to a resource. User needs a matching "Security Key" for access
- Profiles for files, libraries, sublibaries and members are stored in DTSECTAB as in the past
- Profiles for CICS Transactions are in DTSECTXN
  - ► New macro and dialog (2-8) support to define CICS transaction profiles
  - ► No profile means no access allowed!
- DTSECTXN activated and loaded into SVA-31
  - ► during CICS startup
  - ► via "CEMT PERFORM SEC REBUILD"
- Logging and reporting via console messages

Basic Security Mgr

Resource Prot. - CICS Prefixing

- CICS prefixing can be used to differentiate between two or more CICS Transaction Servers running on one VSE/ESA system.
- CICS prefix is identical with the userid of the CICS startup job (SECPRFX=YES in SIT)
  - For SYS SEC=YES the userid in $$JOB or ID statement is used
  - For SYS SEC=NO the userid in the ID statement is used
  - When no userid is given default value FORSEC is used

Basic Security Mgr

User Profiles

- VSE Control File (IESCNTL)
  - Central repository for userids
  - All CICS TS users must be defined here (SNT no longer supported!)
  - VSE/ESA 2.4 Control file records are not compatible with previous releases
  - Definition via User dialog (2-1-1) or batch utility IESUPDCF
- DTSECTAB
  - Activated via SYS SEC=YES
  - Contains 2 userids for ASI procedures
  - does not include CICS TS user settings

Basic Security Mgr

User identification and verification

- Passwords (user profiles in VSE control file)
  - 3 to 8 characters
  - Changeable by application users
  - expiration interval (0-365 days)
  - Password history
  - ID statement, $$JOB statement support 8 characters
- Rovoke date allows (timely) limited system access
- Number of invalid signon attempts exceed a certain limit (REVOKE COUNT in IESELOGO): userid is revoked

Basic Security Mgr

Security Server

- Handles the access to the VSE Control File (VSAM data base)
  - provides caching support
- Used also as a profile server for other resources (DTSECTXN)
- Server status can be changed via operator commands

Basic Security Mgr

CICS Coexistence

- CICS/VSE (in a VSE/ESA 2.4 system) uses SNT for user verification. Drawbacks:
  - Duplicate user definitions
  - SNT users cannot change password
- VSE 2.4 provides exit programs for CICS/VSE to do user verification against BSM user profiles
  - Programs DFHXSE and DFHXSSCO in PRD1.BASE (assembly requires RACROUTE macros from GENLIB)
  - Requires default user entry in SNT
  - Activate ESM in CICS/VSE (EXTSEC=YES in SIT)

Basic Security Mgr

Migration Topics

- Security related resources to be migrated
  - Interactive Interface user profiles from an old VSE control file
  - ICCF user records in DTSFILE
  - CICS user profiles from a CICS/VSE signon table (SNT)
  - Transaction definitions from CICS/VSE PCT
  - For Batch security users: DTSECTAB
- Use VSE migration utility IESBLDUP to migrate user profiles (see VSE/ESA System Utilities)

Security Mgr Independent Topics

Single User Definition

- Segment concept for user profiles
- Security Mgr holds settings for subsystems
  - CICS TS
    - operator ID, timeout, operator classes...
  - Interactive Interface (IES)
    - user type, initial panel, II access flags...
- Subsystem "extracts" user settings at signon
- No user definition to subsystem necessary
- Exception: ICCF user definition not in CA-TSS

Security Mgr independent topics

CICS TS signon

- Native CICS TS signon (CESN)
- VSE/Interactive Interface signon (IEGM)
- Private signon programs based on "CICS SIGNON"
- Signon characteristics
  - inherit user identification and password verification by security mgr
  - CICS TS and Interactive Interface extract subsystem specific user settings

Security Mgr independent Topics

RACROUTE exploiter

- CICS TS
- DITTO/ESA for VSE
- TCP/IP security exit
  - VSE/ESA 2.4 with new function in APAR DY45309
- Interactive Interface for signon

Appendix

DTSECTXN Macro

- Macro support for CICS transaction profiles
  DTSECTXN NAME={CICS-region.}transid
  ,TRANSEC=(class)
  ,SUBTYPE={INITIAL|FINAL}
  - CICS-region = userid in CICS startup job
  - transid = up to 4 characters (.-_&, are not allowed)
  - class = {1|...|64}
    - TRANSEC=(1) for public transactions
    - TRANSEC=(64) for Interactive Interface transactions

Appendix

BSM Security Server commands

- Command format "MSG xx,DATA=command"
- Command list

– HELP, ?	provides a list of all commands
– STATUS	displays server internal status info
– DBSTARTCACHE	starts caching of VSE user profiles
– DBSTOPCACHE	stops caching
– LOGTIME=n	sets logtime interval (in minutes)
– RESET	resets server to initial state
– STOP	stops the server
– OPENCTL	opens the VSE control file
– CLOSECTL	closes the VSE control file

Appendix

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
  - BSSINIT will not start a security manager
  - Re-IPL required to start security manager again