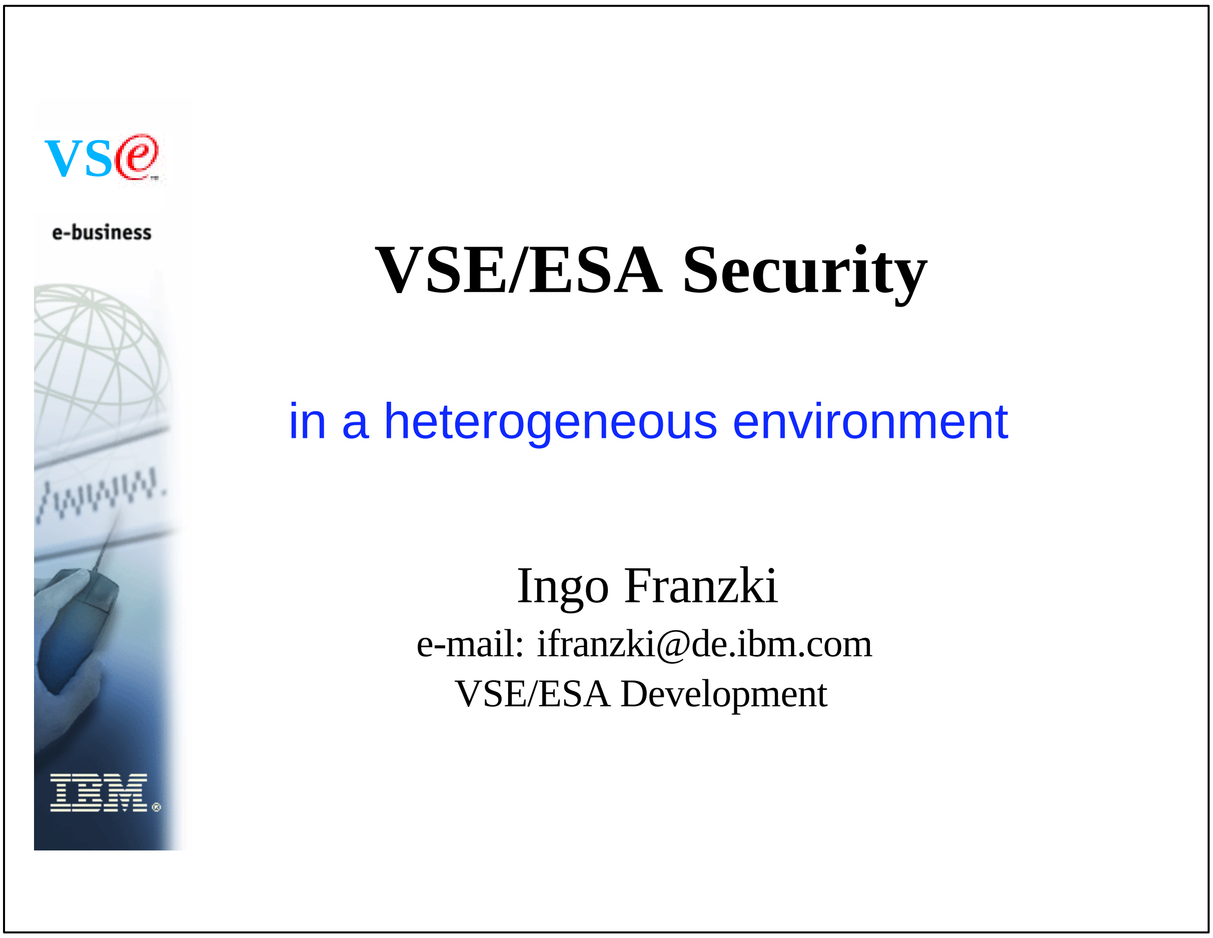
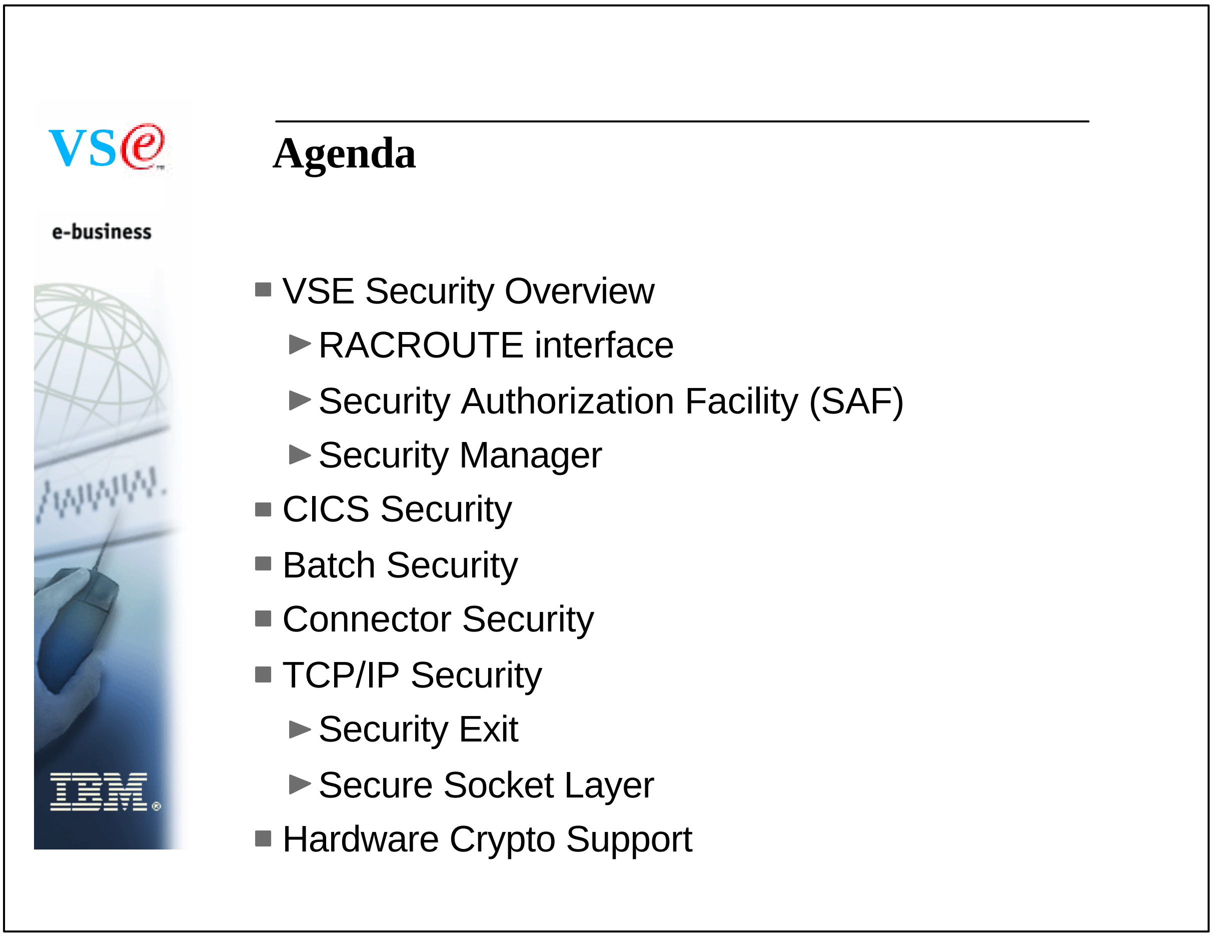


VSE/ESA Security

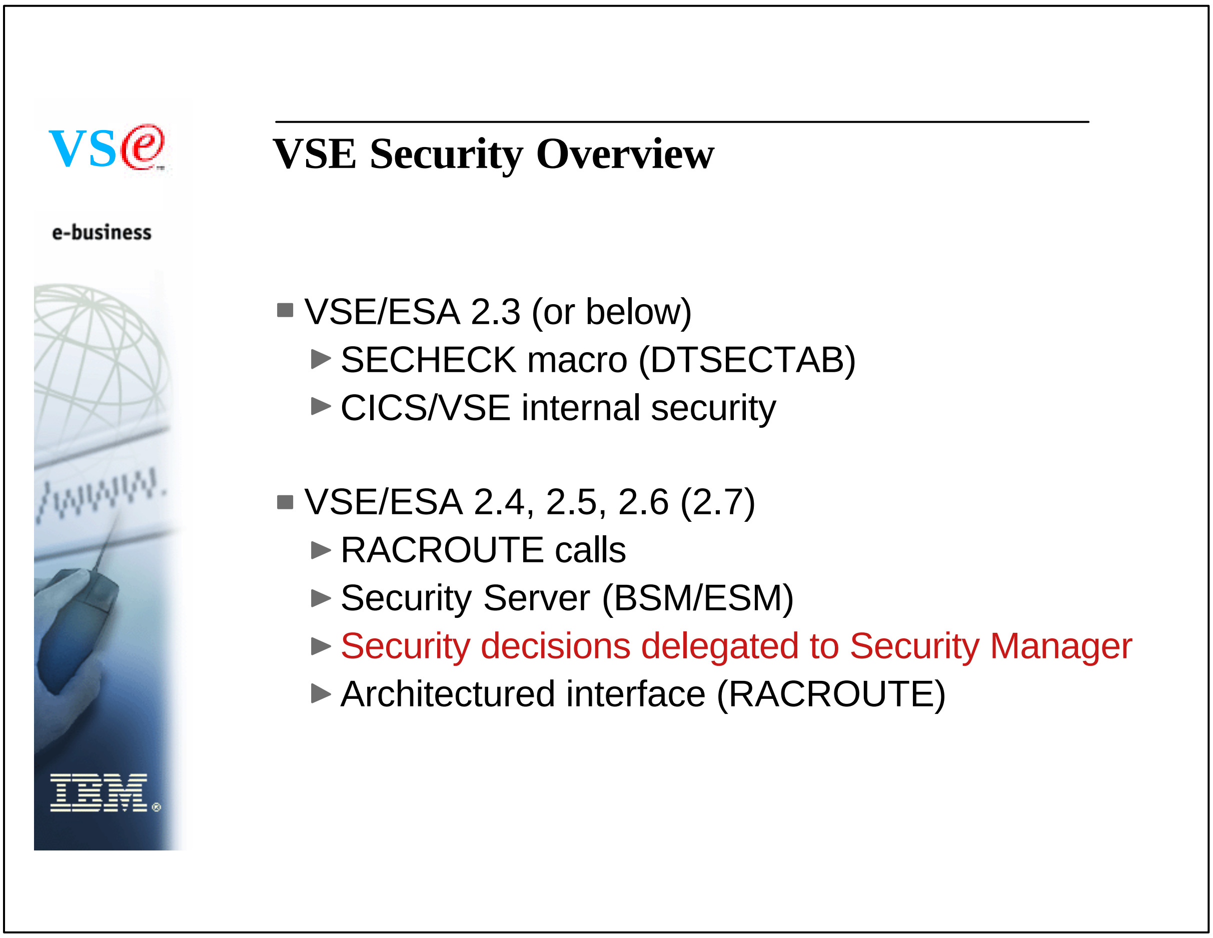
in a heterogeneous environment

Ingo Franzki
e-mail: ifranzki@de.ibm.com
VSE/ESA Development



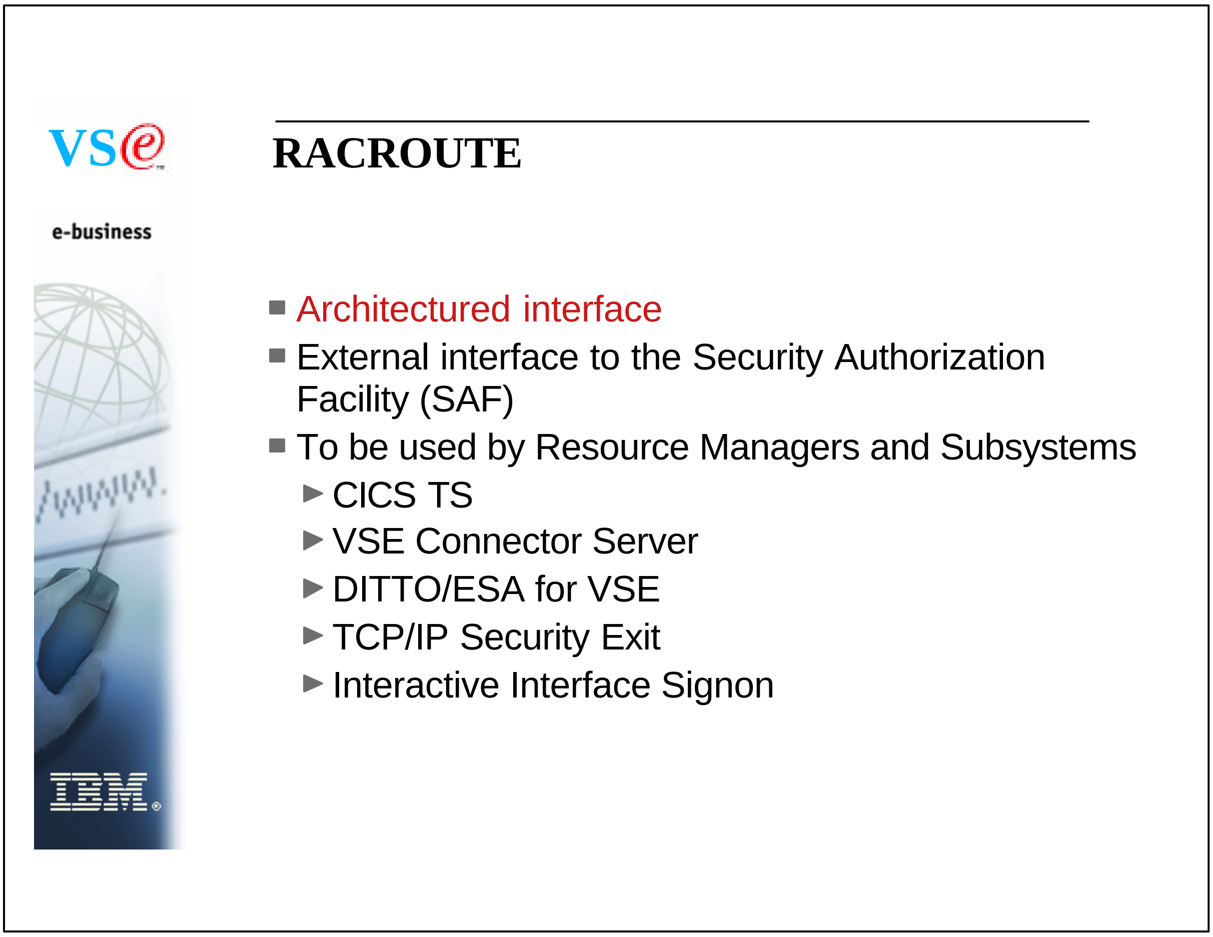
Agenda

- VSE Security Overview
  - RACROUTE interface
  - Security Authorization Facility (SAF)
  - Security Manager
- CICS Security
- Batch Security
- Connector Security
- TCP/IP Security
  - Security Exit
  - Secure Socket Layer
- Hardware Crypto Support



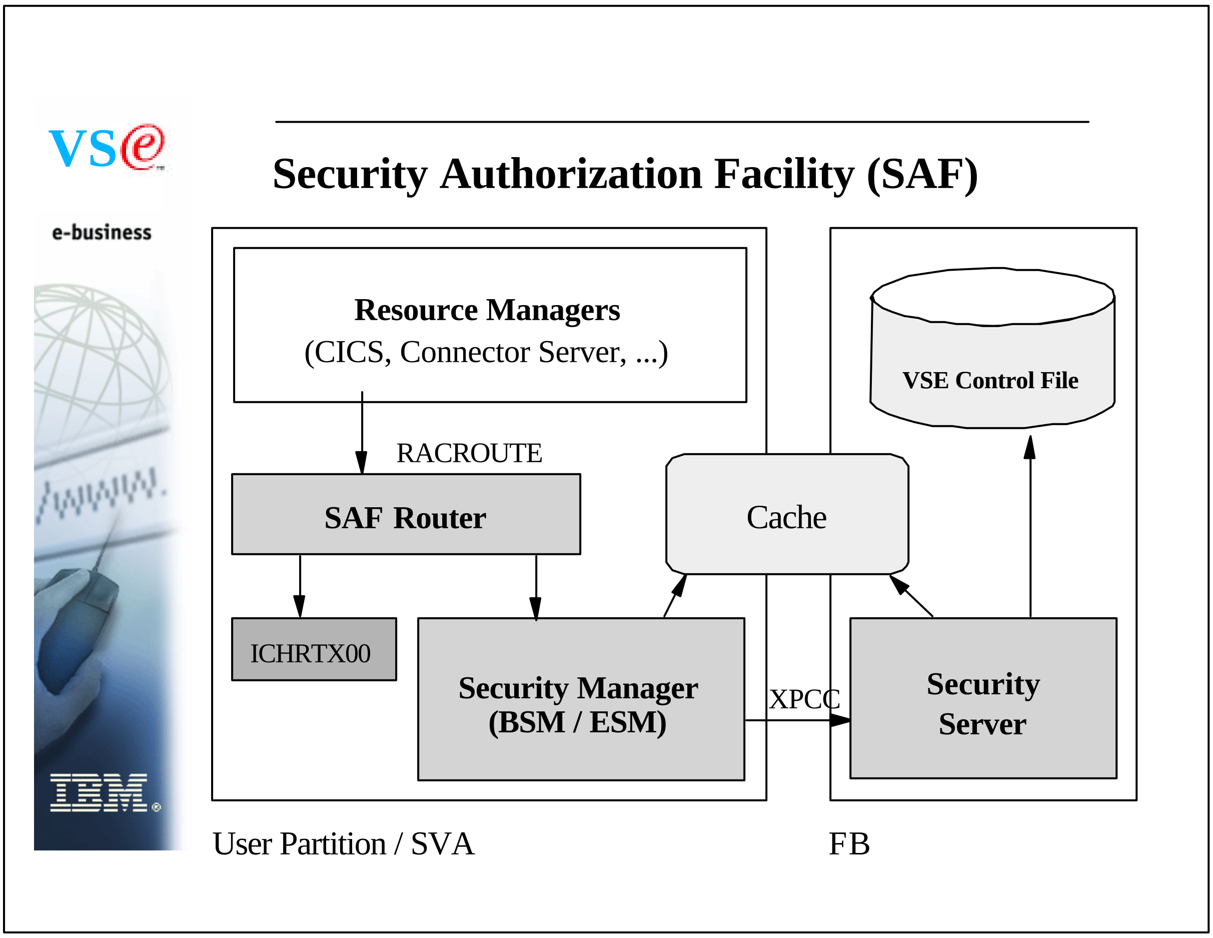
VSE Security Overview

- VSE/ESA 2.3 (or below)
  - SECHECK macro (DTSECTAB)
  - CICS/VSE internal security
- VSE/ESA 2.4, 2.5, 2.6 (2.7)
  - RACROUTE calls
  - Security Server (BSM/ESM)
  - Security decisions delegated to Security Manager
  - Architectured interface (RACROUTE)



RACROUTE

- Architectured interface
- External interface to the Security Authorization Facility (SAF)
- To be used by Resource Managers and Subsystems
  - CICS TS
  - VSE Connector Server
  - DITTO/ESA for VSE
  - TCP/IP Security Exit
  - Interactive Interface Signon



Security Authorization Facility (SAF)

Resource Managers
(CICS, Connector Server, ...)

RACROUTE

SAF Router

ICHRTX00

Security Manager
(BSM / ESM)

Cache

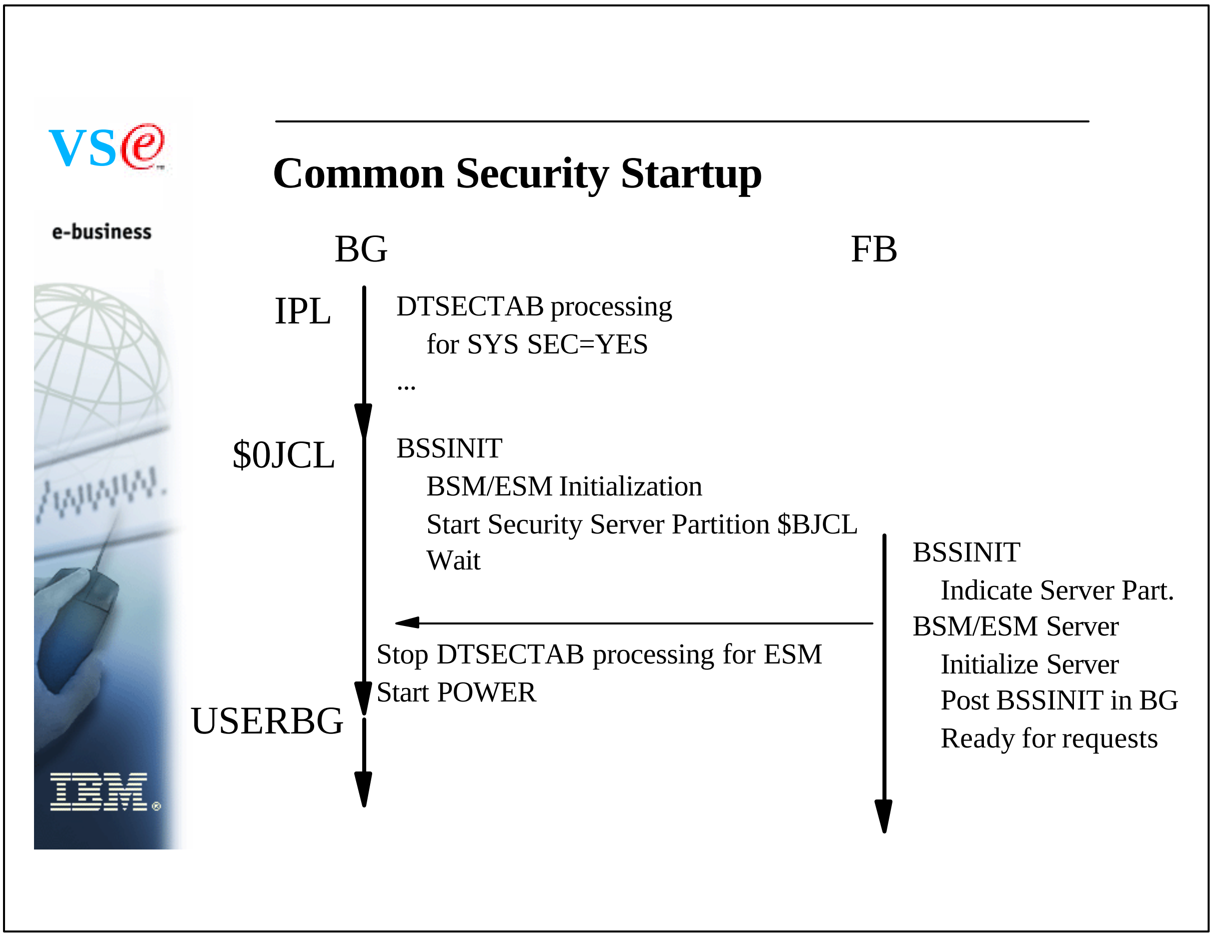
XPCC

VSE Control File

Security
Server

User Partition / SVA

FB



Common Security Startup

BG

FB

IPL

DTSECTAB processing
for SYS SEC=YES
...

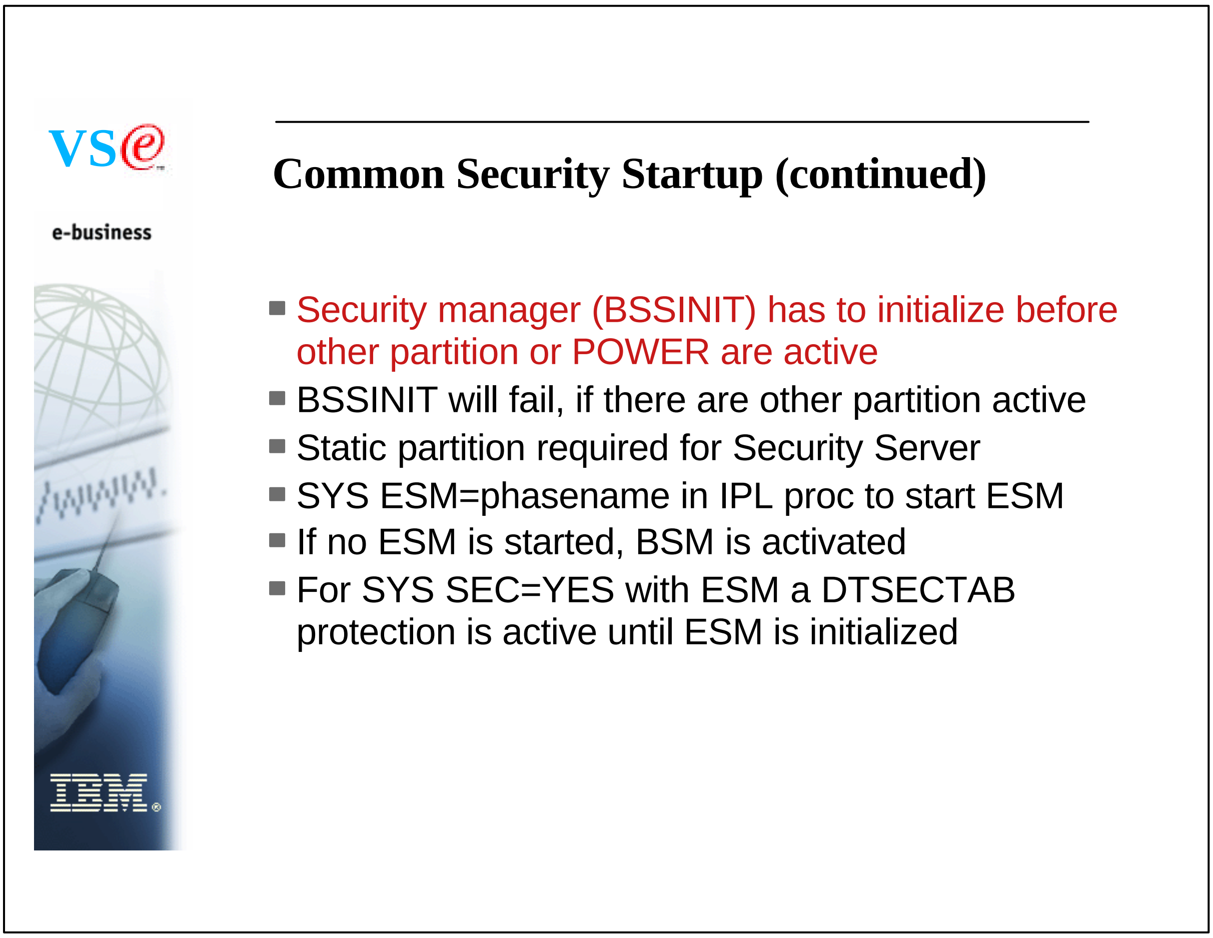
$0JCL

BSSINIT
BSM/ESM Initialization
Start Security Server Partition $BJCL
Wait

BSSINIT
Indicate Server Part.
BSM/ESM Server
Initialize Server
Post BSSINIT in BG
Ready for requests

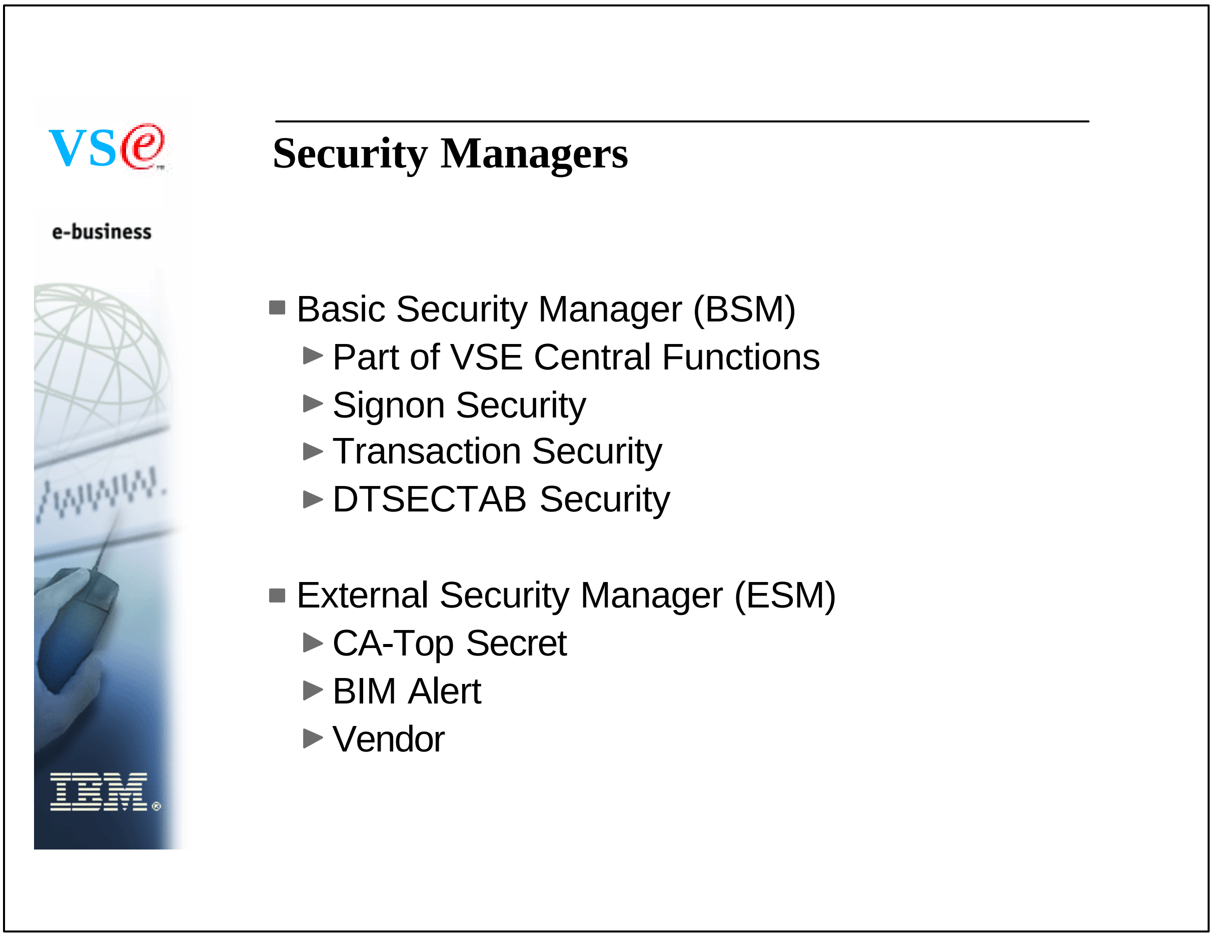
Stop DTSECTAB processing for ESM
Start POWER

USERBG



Common Security Startup (continued)

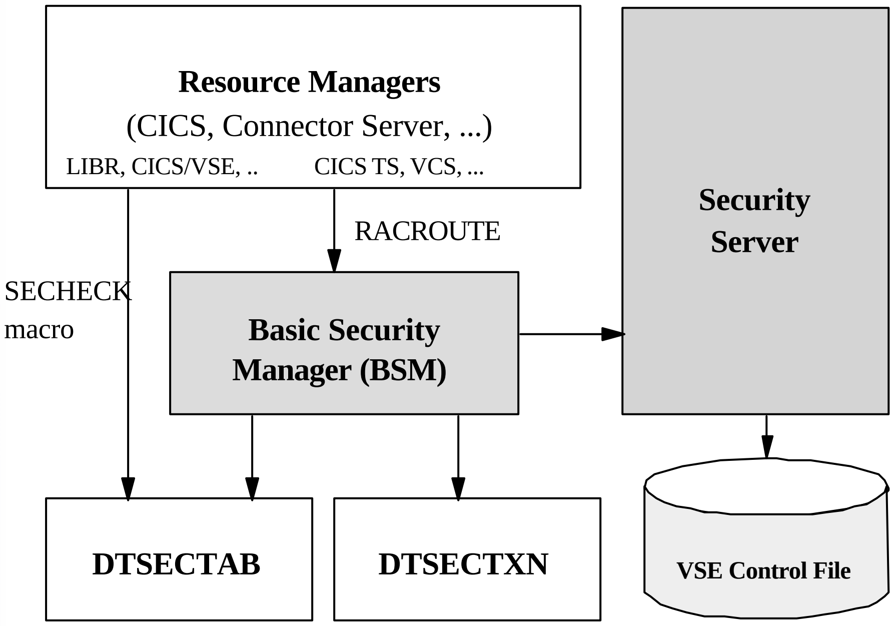
- Security manager (BSSINIT) has to initialize before other partition or POWER are active
- BSSINIT will fail, if there are other partition active
- Static partition required for Security Server
- SYS ESM=phasename in IPL proc to start ESM
- If no ESM is started, BSM is activated
- For SYS SEC=YES with ESM a DTSECTAB protection is active until ESM is initialized



Security Managers

- Basic Security Manager (BSM)
  - Part of VSE Central Functions
  - Signon Security
  - Transaction Security
  - DTSECTAB Security
- External Security Manager (ESM)
  - CA-Top Secret
  - BIM Alert
  - Vendor

Basic Security Manager



Resource Managers
(CICS, Connector Server, ...)
LIBR, CICS/VSE, ..
CICS TS, VCS, ...

RACROUTE

SECHECK macro

Basic Security Manager (BSM)

Security Server

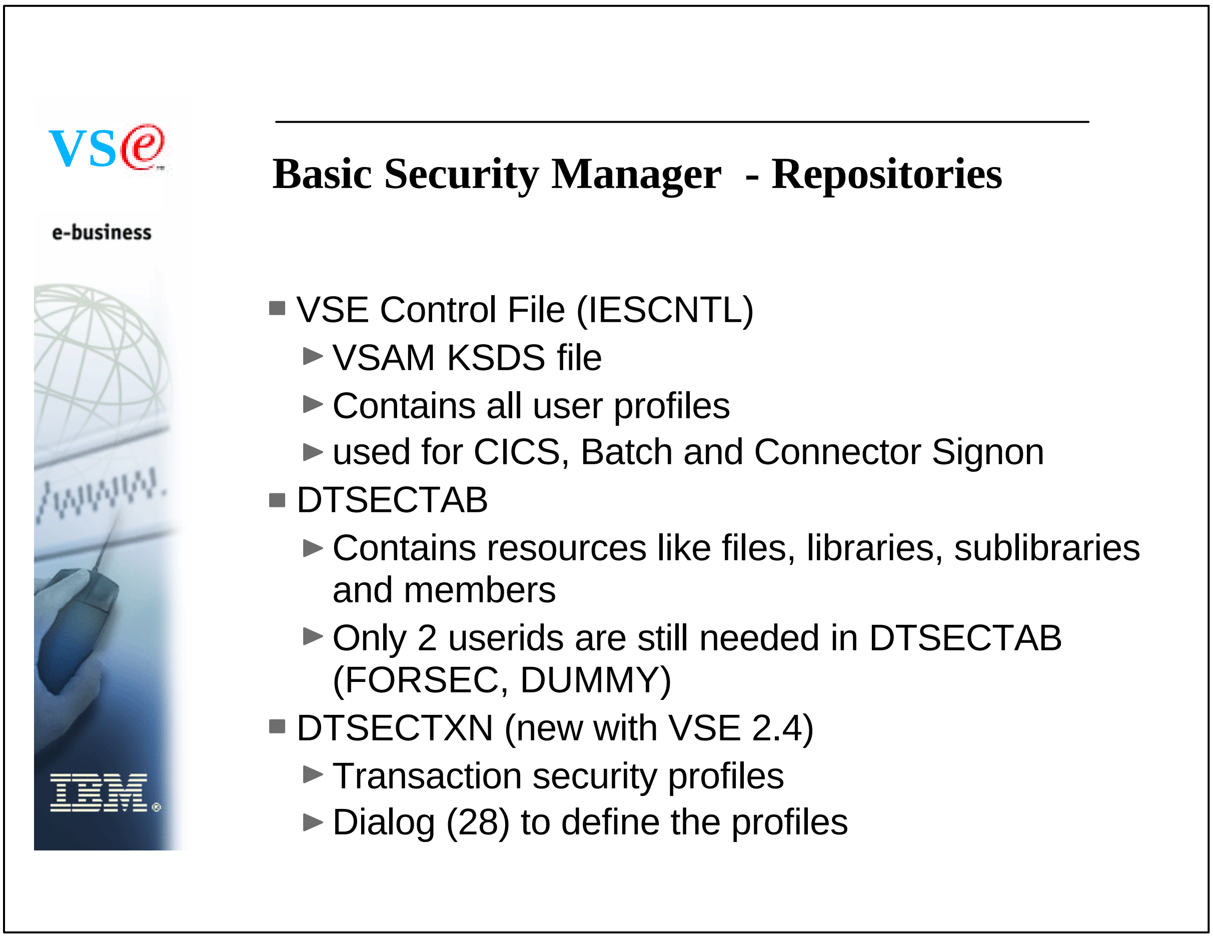
DTSECTAB

DTSECTXN

VSE Control File

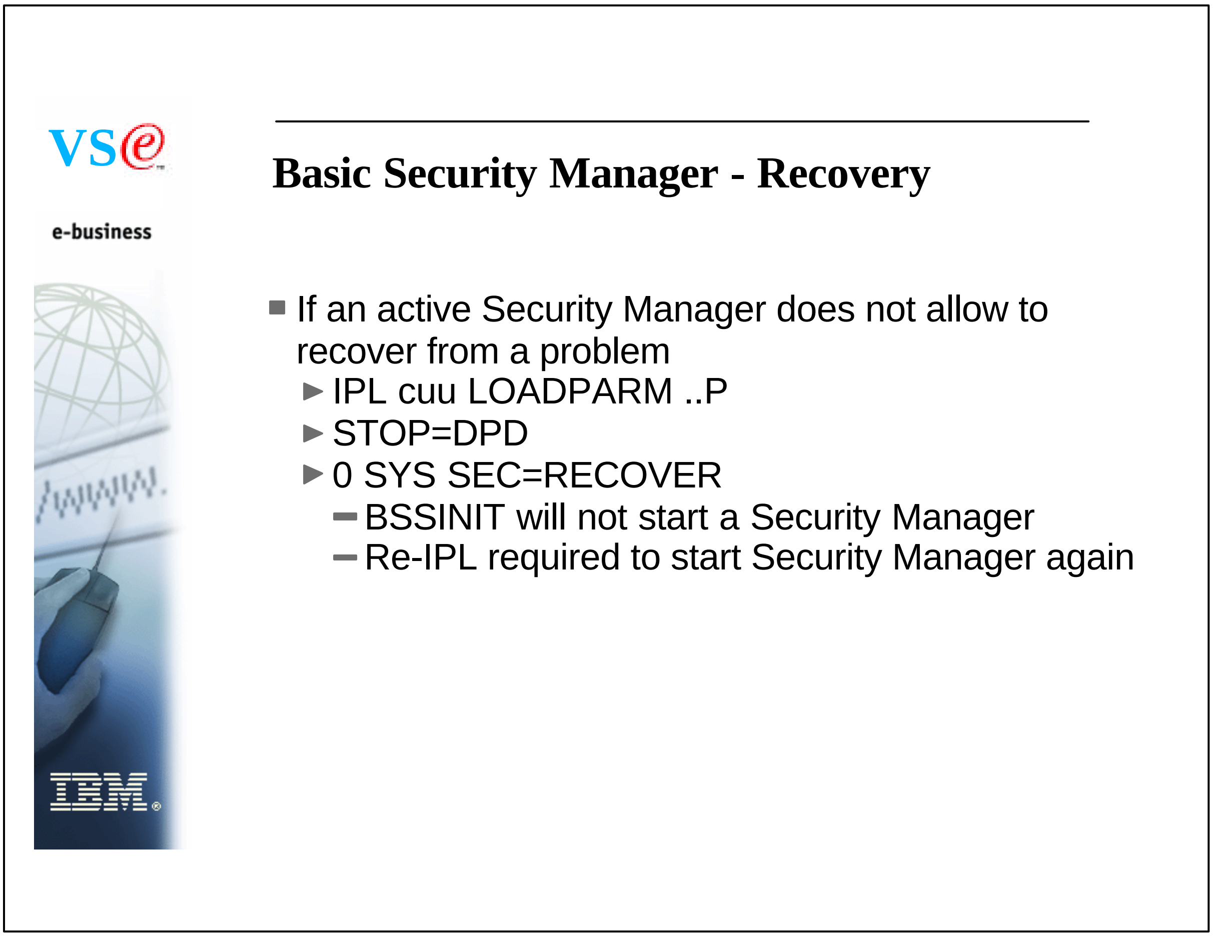
Basic Security Manager (continued)

- Provides RACROUTE support for
  - Signon (CICS and VSE Connector Server)
  - Batch signon (ID statement)
  - Transaction security
- Supports also the SVC-based security calls
  - SECHECK
- Resource classes
  - USER
  - DATASET
  - VSELIB, VSESLIB, VSEMEM
  - TCICSTRN



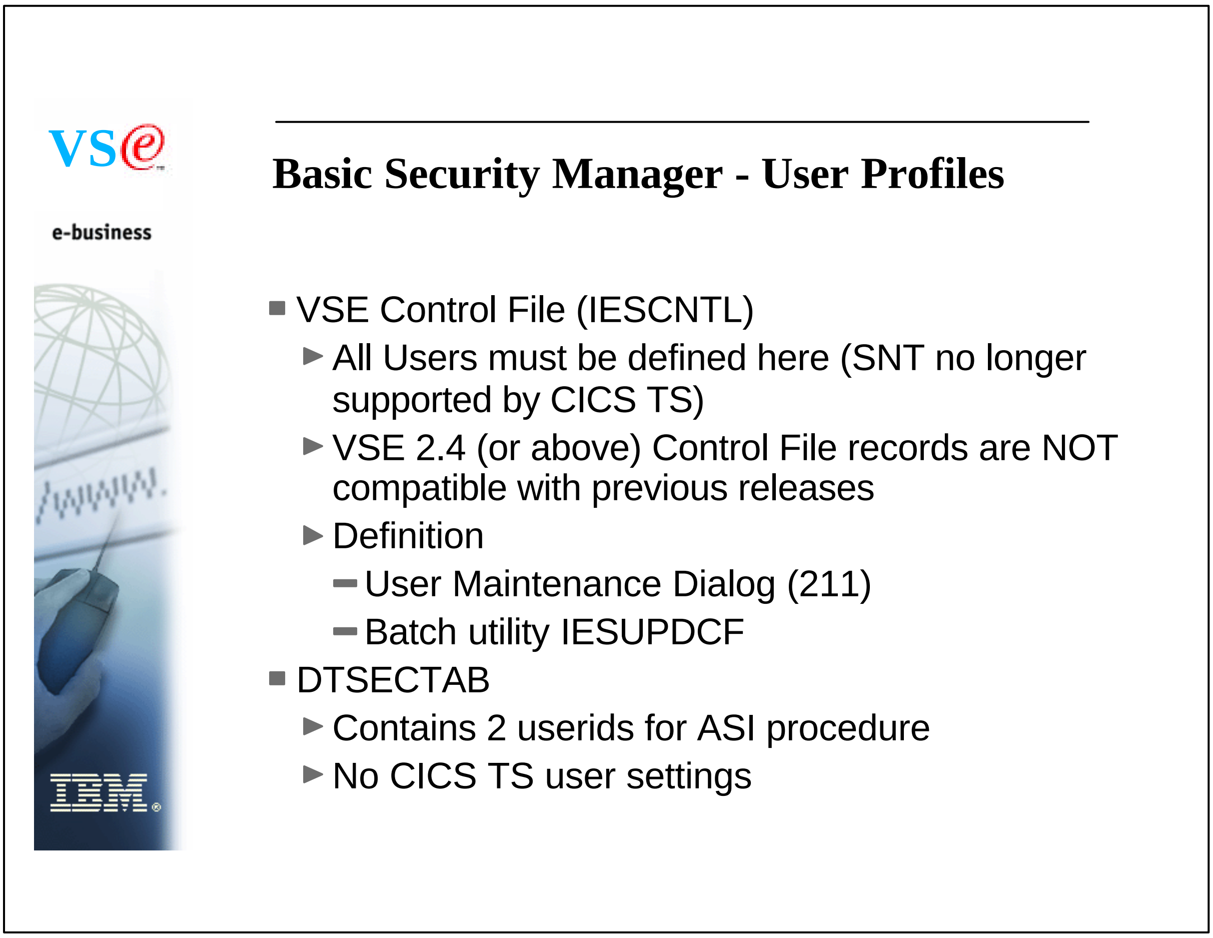
Basic Security Manager - Repositories

- VSE Control File (IESCNTL)
  - VSAM KSDS file
  - Contains all user profiles
  - used for CICS, Batch and Connector Signon
- DTSECTAB
  - Contains resources like files, libraries, sublibraries and members
  - Only 2 userids are still needed in DTSECTAB (FORSEC, DUMMY)
- DTSECTXN (new with VSE 2.4)
  - Transaction security profiles
  - Dialog (28) to define the profiles



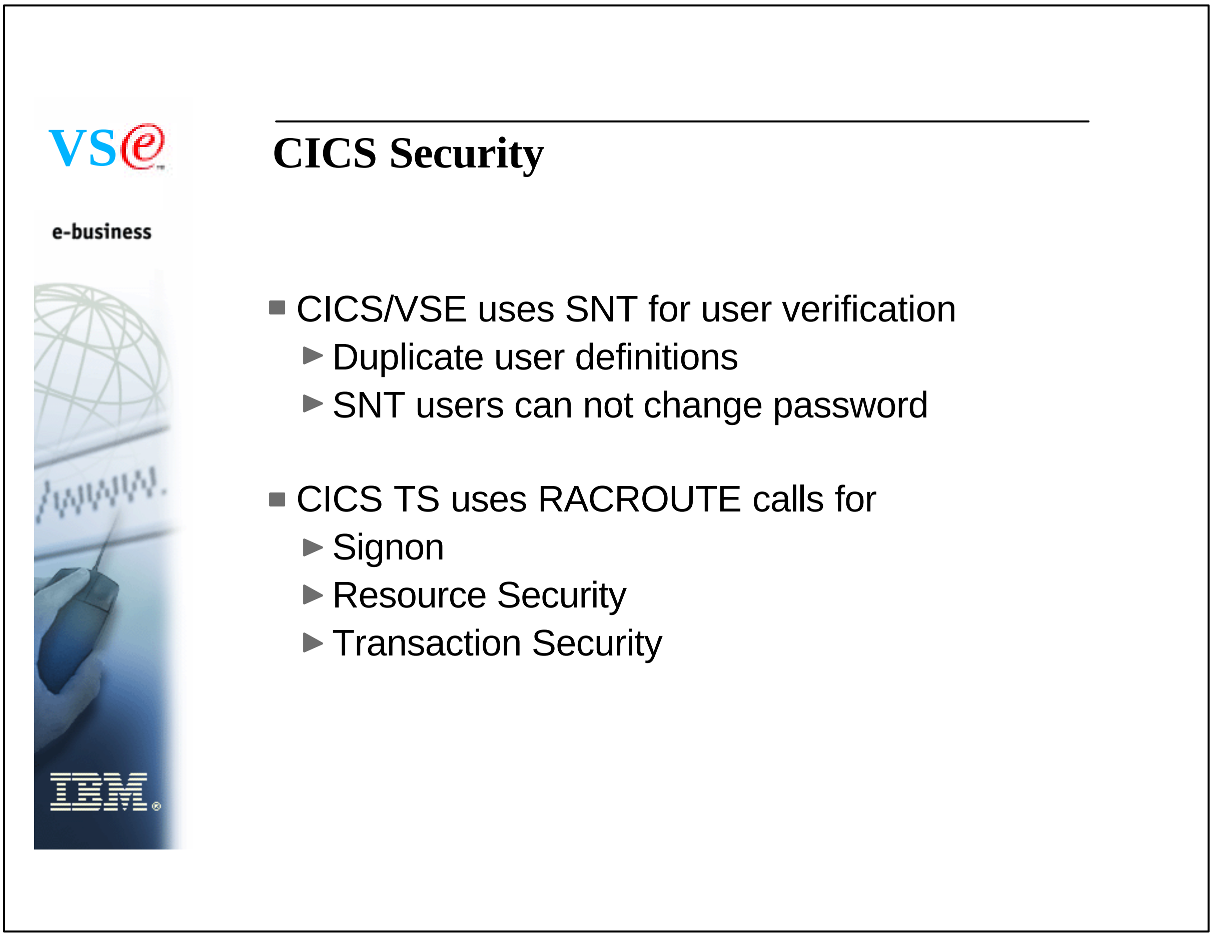
Basic Security Manager - Recovery

- If an active Security Manager does not allow to recover from a problem
  - IPL cuu LOADPARM ..P
  - STOP=DPD
  - 0 SYS SEC=RECOVER
    - BSSINIT will not start a Security Manager
    - Re-IPL required to start Security Manager again



Basic Security Manager - User Profiles

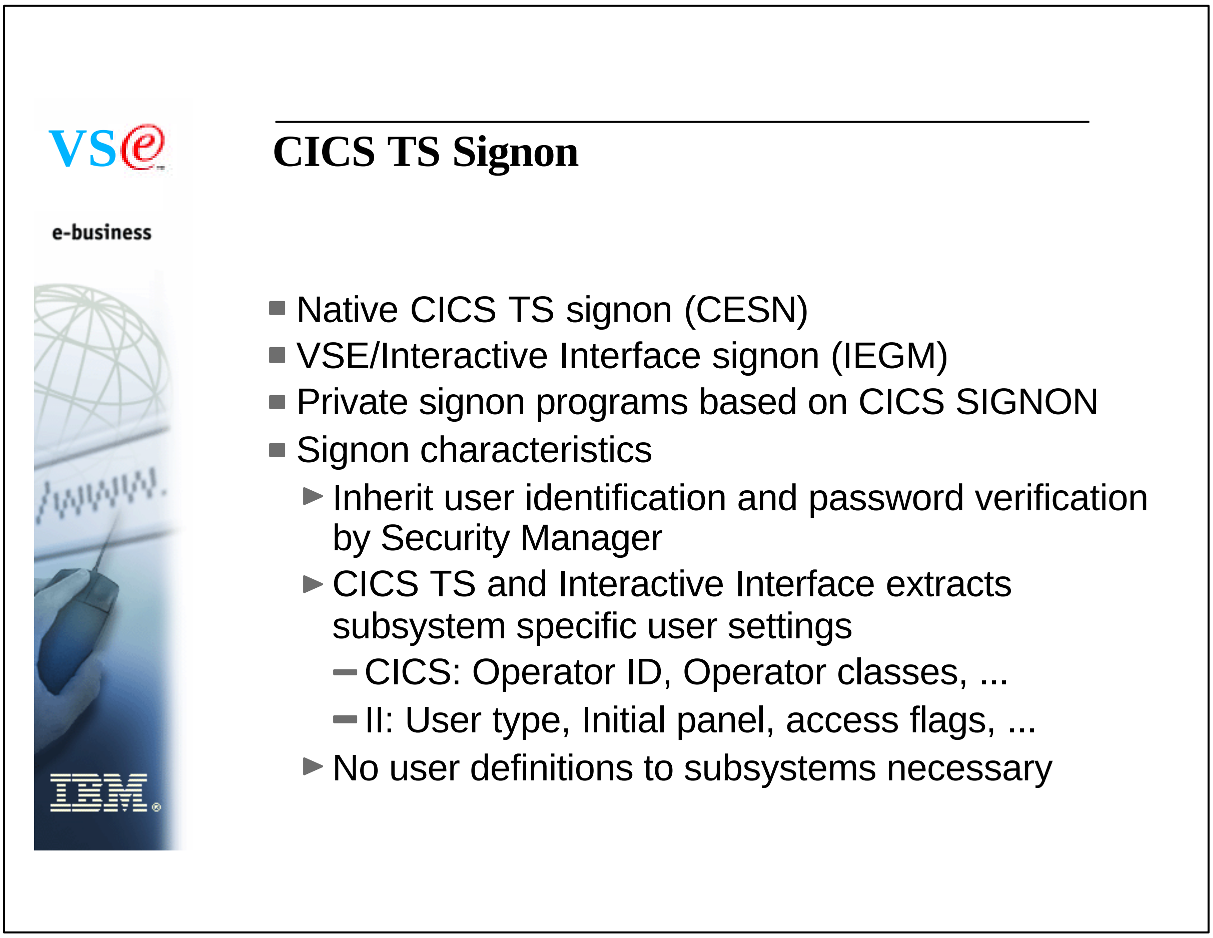
- VSE Control File (IESCNTL)
  - All Users must be defined here (SNT no longer supported by CICS TS)
  - VSE 2.4 (or above) Control File records are NOT compatible with previous releases
  - Definition
    - User Maintenance Dialog (211)
    - Batch utility IESUPDCF
- DTSECTAB
  - Contains 2 userids for ASI procedure
  - No CICS TS user settings



CICS Security

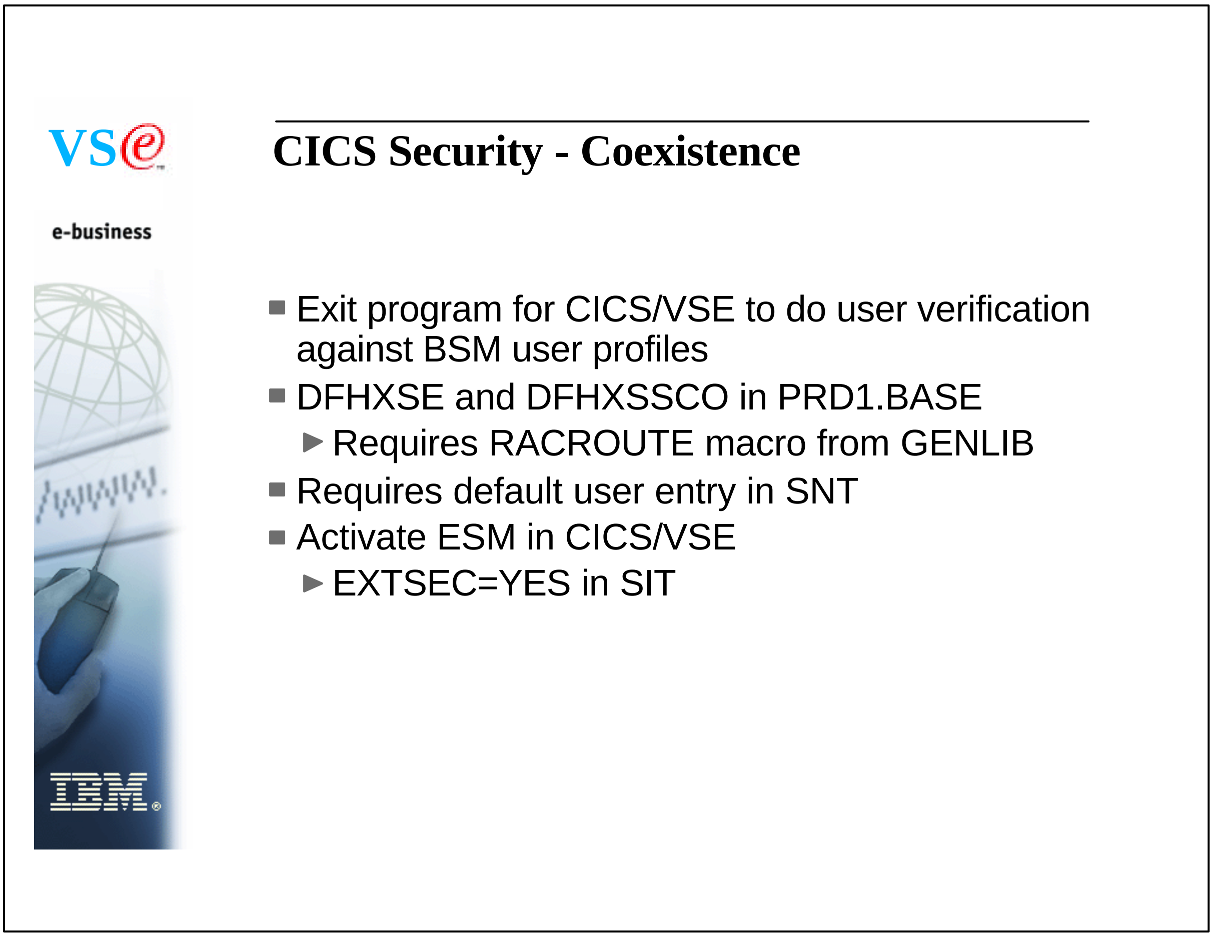
- CICS/VSE uses SNT for user verification
  - Duplicate user definitions
  - SNT users can not change password

- CICS TS uses RACROUTE calls for
  - Signon
  - Resource Security
  - Transaction Security



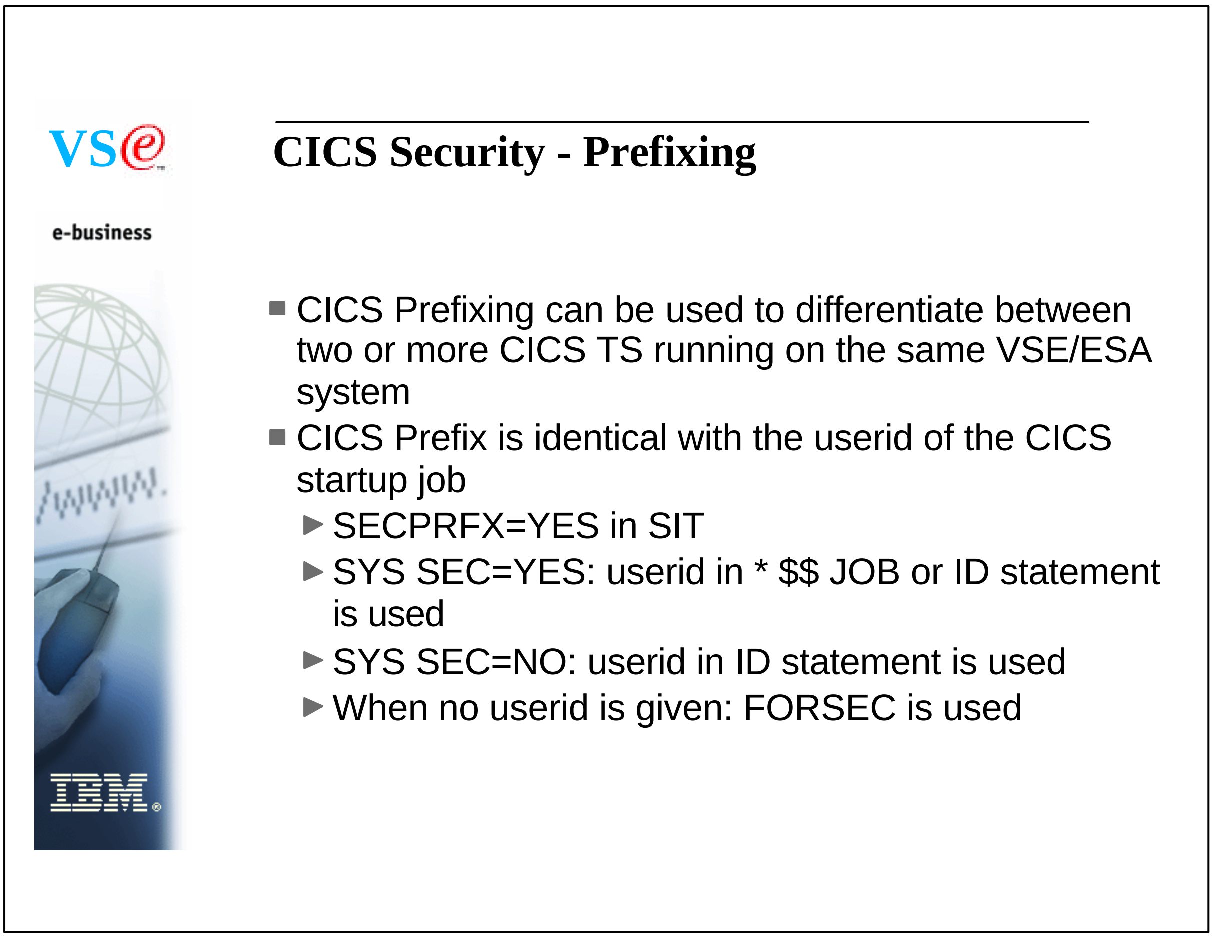
CICS TS Signon

- 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 Manager
  - CICS TS and Interactive Interface extracts subsystem specific user settings
    - CICS: Operator ID, Operator classes, ...
    - II: User type, Initial panel, access flags, ...
  - No user definitions to subsystems necessary



CICS Security - Coexistence

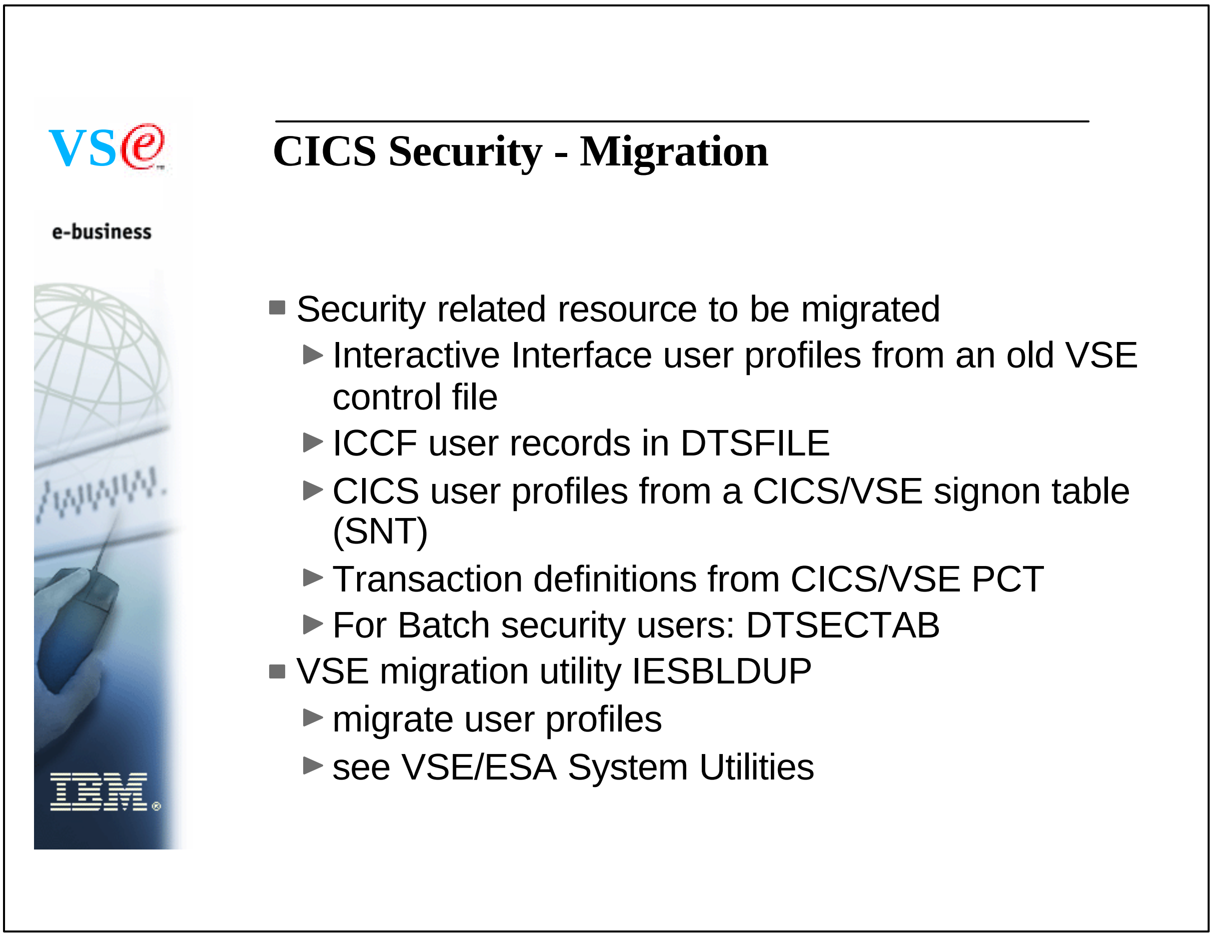
- Exit program for CICS/VSE to do user verification against BSM user profiles
- DFHXSE and DFHXSSCO in PRD1.BASE
  - Requires RACROUTE macro from GENLIB
- Requires default user entry in SNT
- Activate ESM in CICS/VSE
  - EXTSEC=YES in SIT



VS@
e-business
www.
IBM

CICS Security - Prefixing

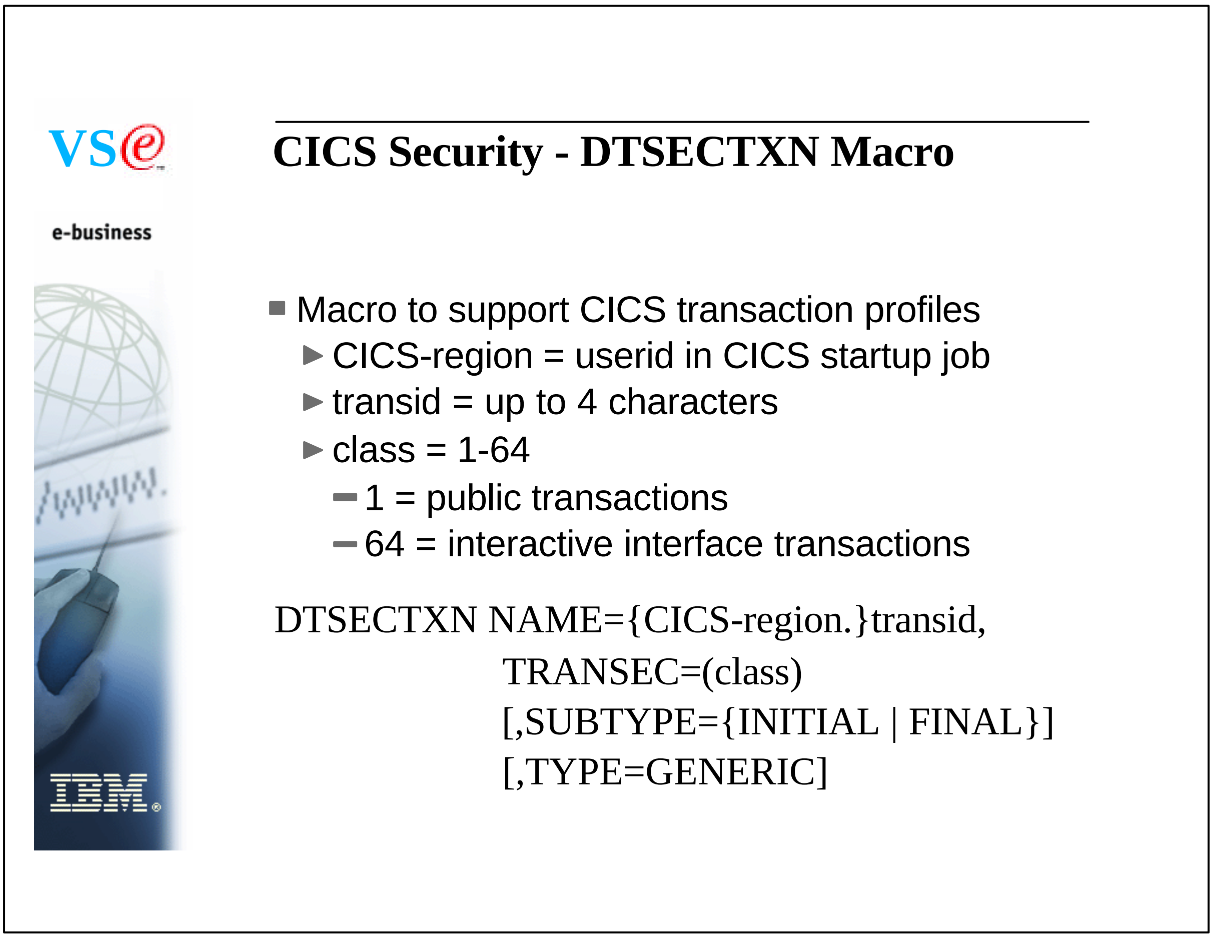
- CICS Prefixing can be used to differentiate between two or more CICS TS running on the same VSE/ESA system
- CICS Prefix is identical with the userid of the CICS startup job
  - ▶ SECPRFX=YES in SIT
  - ▶ SYS SEC=YES: userid in * $$ JOB or ID statement is used
  - ▶ SYS SEC=NO: userid in ID statement is used
  - ▶ When no userid is given: FORSEC is used



VS@
e-business
www.
IBM

CICS Security - Migration

- Security related resource 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
- VSE migration utility IESBLDUP
  - ▶ migrate user profiles
  - ▶ see VSE/ESA System Utilities



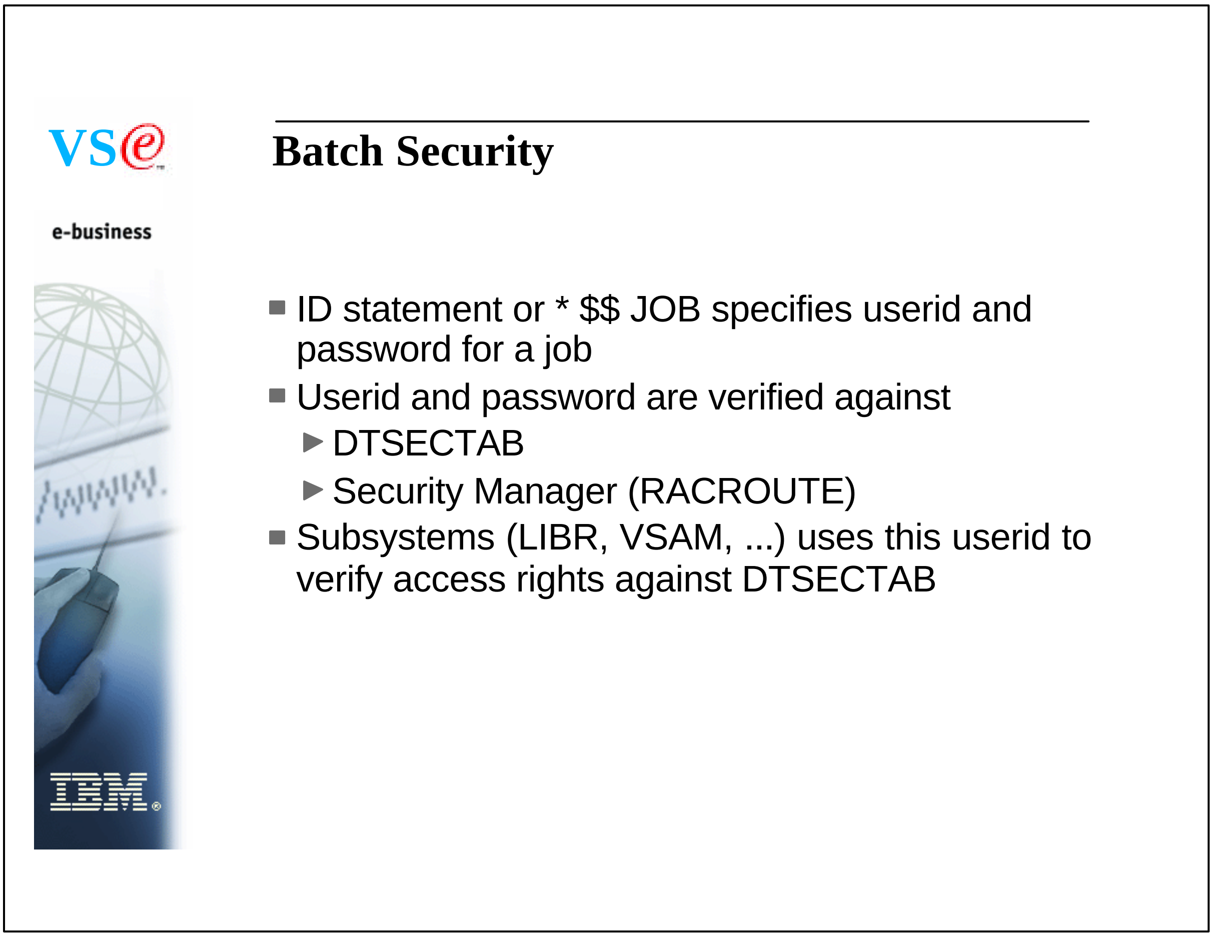
VS*e*

e-business

CICS Security - DTSECTXN Macro

- Macro to support CICS transaction profiles
  - CICS-region = userid in CICS startup job
  - transid = up to 4 characters
  - class = 1-64
    - 1 = public transactions
    - 64 = interactive interface transactions

```
DTSECTXN NAME={CICS-region.}transid,
         TRANSEC=(class)
         [,SUBTYPE={INITIAL | FINAL}]
         [,TYPE=GENERIC]
```



VS*e*

e-business

Batch Security

- ID statement or * $$ JOB specifies userid and password for a job
- Userid and password are verified against
  - DTSECTAB
  - Security Manager (RACROUTE)
- Subsystems (LIBR, VSAM, ...) uses this userid to verify access rights against DTSECTAB

Connector Security

- VSE Connector Server acts as a Resource Manager
  - Issues RACROUTE calls for
    - Userid and password verification
    - Resource security
- Connector userids are the same as for CICS TS and Batch
- No additional user profile setup required
- But:
  - Additional access restriction by userid and/or IP address possible

Connector Security - Logon

- VSE Connector Server requires a client to logon with valid userid and password
- Userid and password is checked via RACROUTE calls
- Additional information is extracted from ACEE and IUI or AF segment
  - User type, access flags, ...
- The user's ACEE is kept during the whole session
  - Used to do resource access checking
- Multiple logon attempts with same userid is possible

Connector Security - Resource Security

- When a client issues a resource access request
  - The server does RACROUTE calls to check if the user is allowed to access the resource
  - Access is done only if user is allowed to access the resource
- VSE Connector Server runs under a special userid (VCSRV)
  - specified in ID statement in startup job
  - should be allowed to access all resources

Connector Security - Internals

- Logon processing
  - RACROUTE VERIFY CREATE
  - RACROUTE EXTRACT (user type checking)
    - AF segment, if this fails (e.g. CA-TopSecret) IUI segment
  - Flags used in AF segment
    - AFADMIN   user is a administrator = type 1
    - AFMCONS   user is allowed to open a console
  - Flags used in IUI segment
    - IESISUTP   user type (1,2 or 3)
    - IESISFL1   user flag byte 1
    - IESISFL2   user flag byte 2

Connector Security - User types

- Type 1 (Administrator)
  - read and write access for all resources
- Type 2 (Programmer)
  - read only access for all resources
  - allowed to submit jobs
- Type 3 (Application User)
  - read only access for selected resources

Connector Security - Resource classes

- The following Resource class are used
  - VSELIB, VSESLIB, VSEMEM (LIBR)
  - DATASET (VSAM)
- Resource not protected by Security Manager
  - POWER queue entries
    - protected by user type and access flag
  - Console
    - protected by user type and access flag
    - If user is allowed to access the console, he can issue all console commands,
      even REIPL NOPROMPT (!)
  - ICCF Libraries and Members
  - VSAM Record Mappings

Connector Security - Additional Security

- Configuration member allows to restrict logon (connect) by
  - Userid
  - IP address
- See skeleton SKVCSUSR in ICCF library 59

```
* *******************************************************************
* USERS FROM THIS IP'S ARE ALLOWED TO LOGON
* *******************************************************************
IP   = *,            LOGON = ALLOWED
* IP = 9.164.123.456, LOGON = DENIED
* IP = 9.165.*      , LOGON = DENIED
* IP = 10.0.0.*     , LOGON = ALLOWED
* *******************************************************************
* THIS USERS ARE ALLOWED TO LOGON
* *******************************************************************
USER = *,            LOGON = ALLOWED
* USER = BOBY,       LOGON = ALLOWED
* USER = SYS*,       LOGON = DENIED
```

Deactivation of Connector Security

- Since PTF UQ66736 (VSE 2.6), UQ66733 (VSE 2.5) Connector Security can be deactivated
- New keyword SECURITY in main configuration member:
  - SECURITY = FULL (default, as before)
  - SECURITY = RESOURCE (no user type checking)
  - SECURITY = LOGON (no resource, only logon)
  - SECURITY = NO (no security at all)
- Access restriction (previous foil) is still active, even if SECURITY = NO

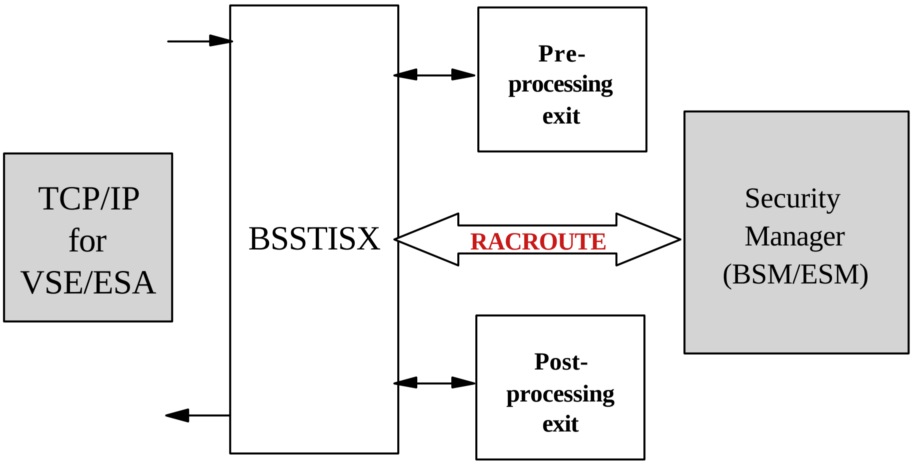
VS@ e-business

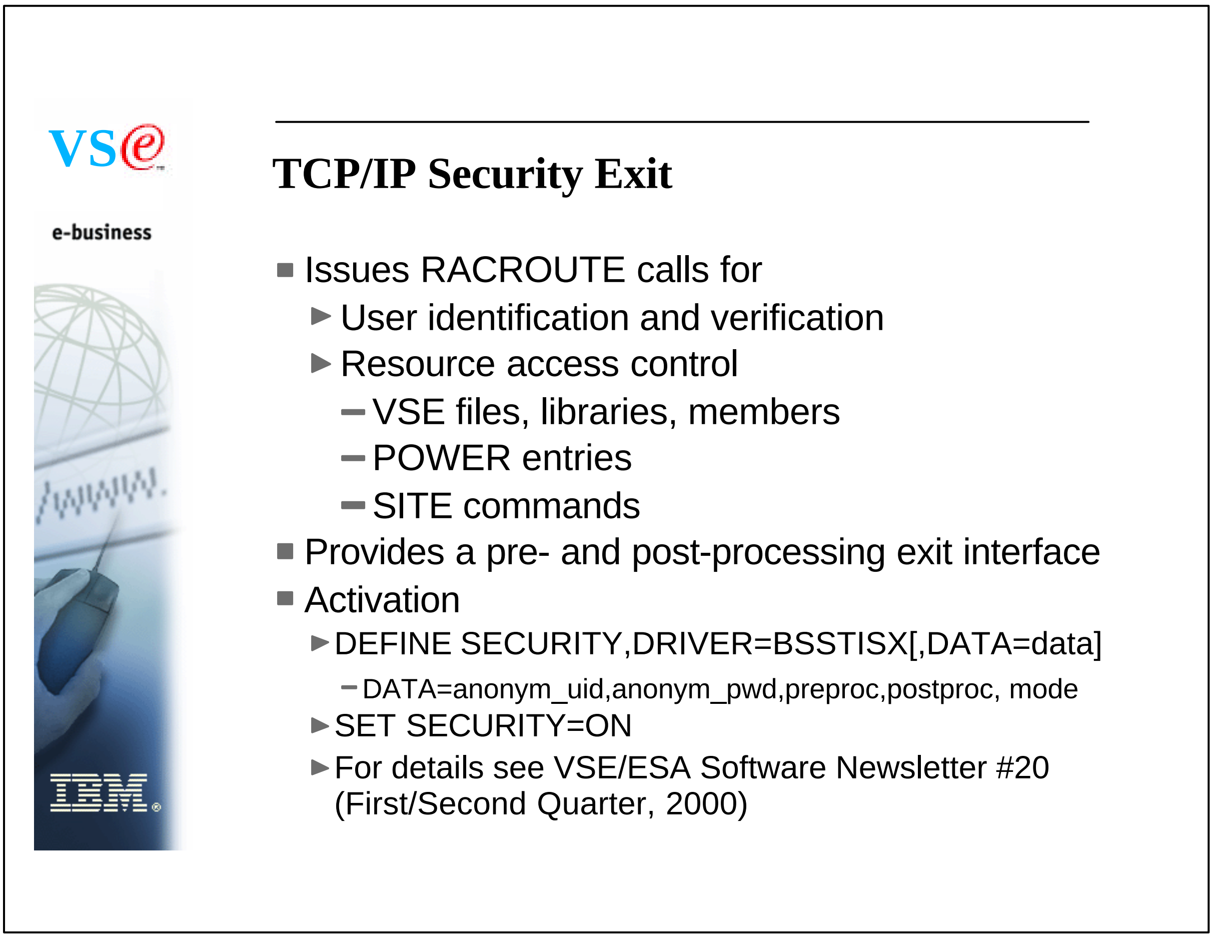
TCP/IP Security

- In general TCP/IP uses its own userid definitions
  - DEFINE USER,ID=user,PASSWORD=pwd
  - Readable in initialization member (IPINITxx.L)
  - Duplicate user definitions
  - Used for
    - FTP
- Security Exit available from IBM to check the userids and resource access via Security Manager
  - see next foil

VS@ e-business

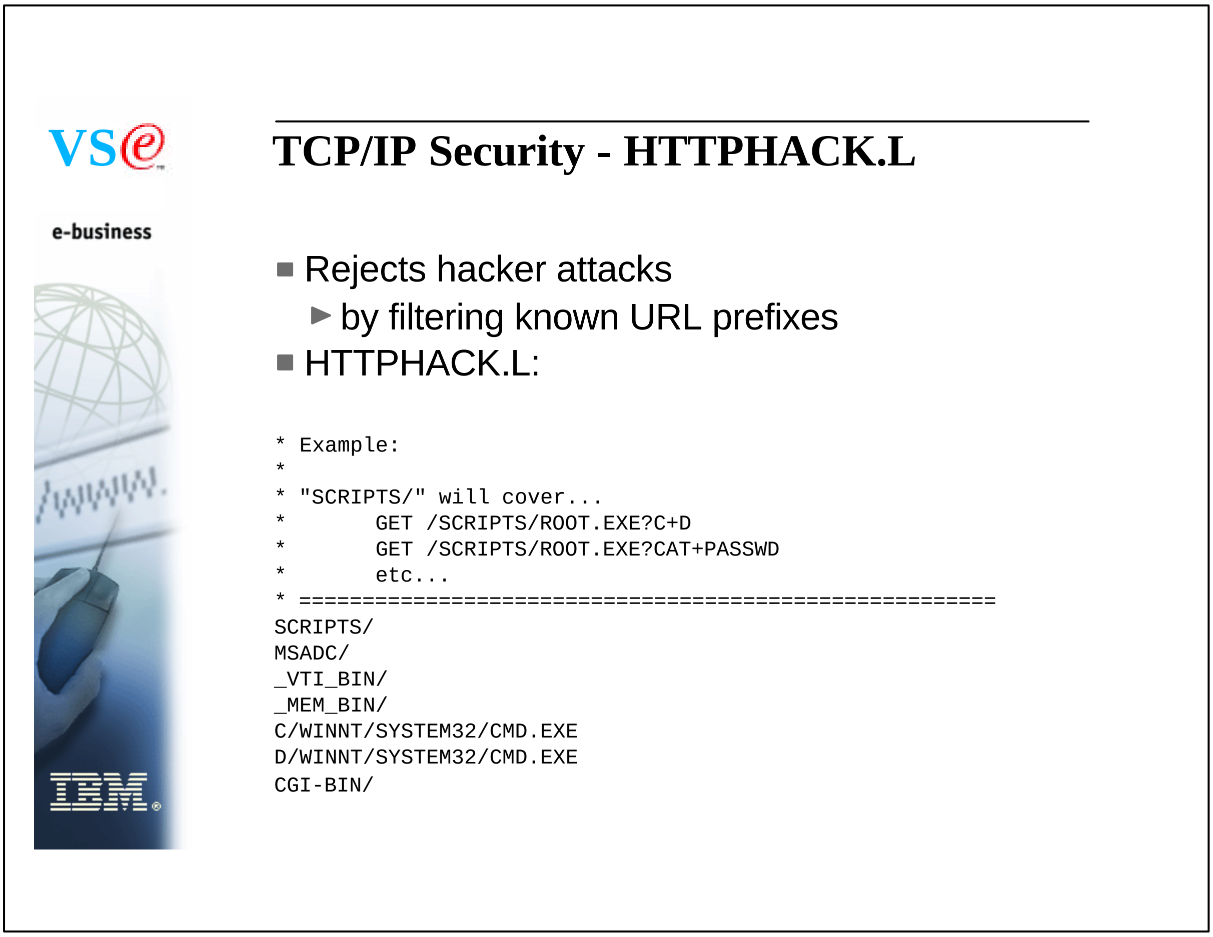
TCP/IP Security Exit





TCP/IP Security Exit

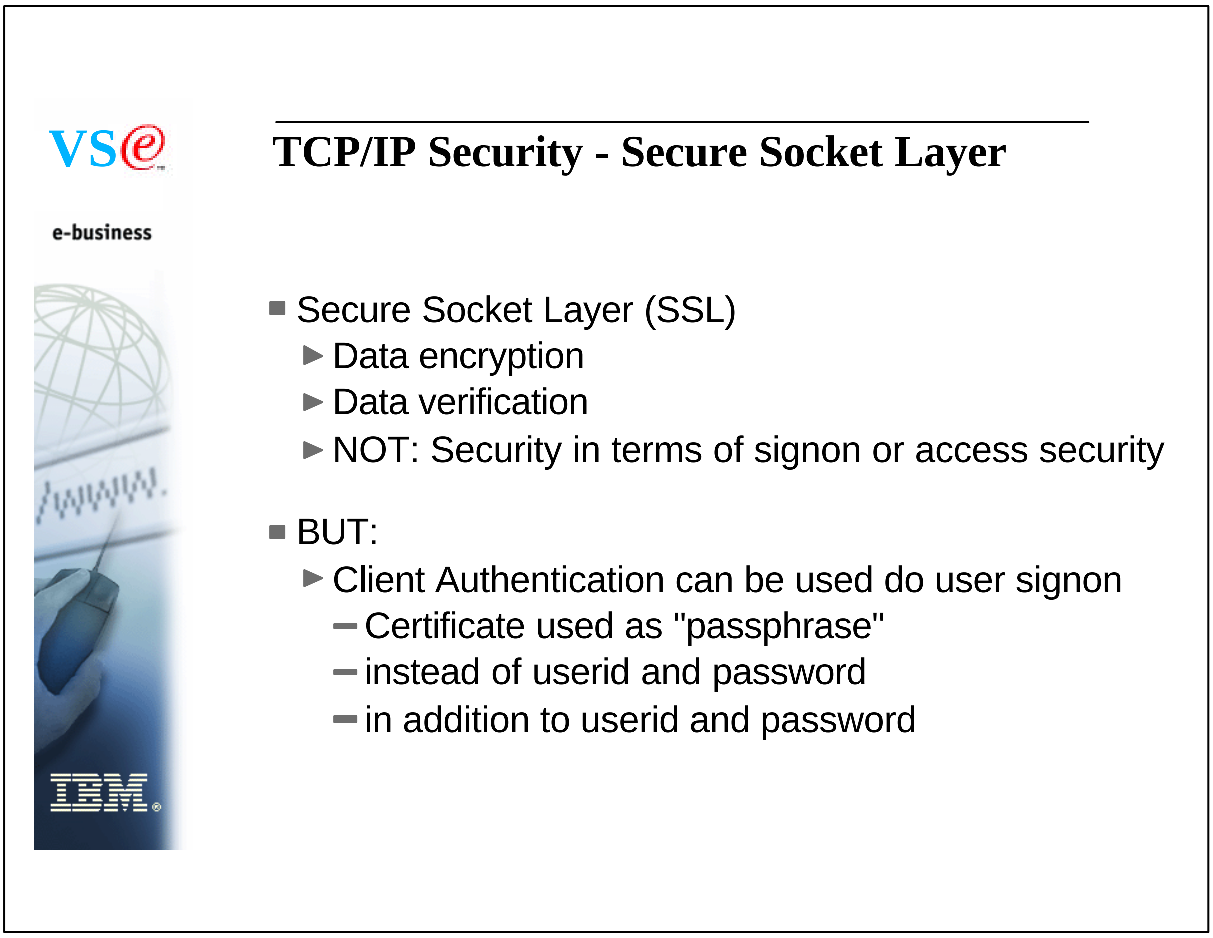
- Issues RACROUTE calls for
  - User identification and verification
  - Resource access control
    - VSE files, libraries, members
    - POWER entries
    - SITE commands
- Provides a pre- and post-processing exit interface
- Activation
  - DEFINE SECURITY,DRIVER=BSSTISX[,DATA=data]
    - DATA=anonym_uid,anonym_pwd,preproc,postproc, mode
  - SET SECURITY=ON
  - For details see VSE/ESA Software Newsletter #20 (First/Second Quarter, 2000)



TCP/IP Security - HTTPHACK.L

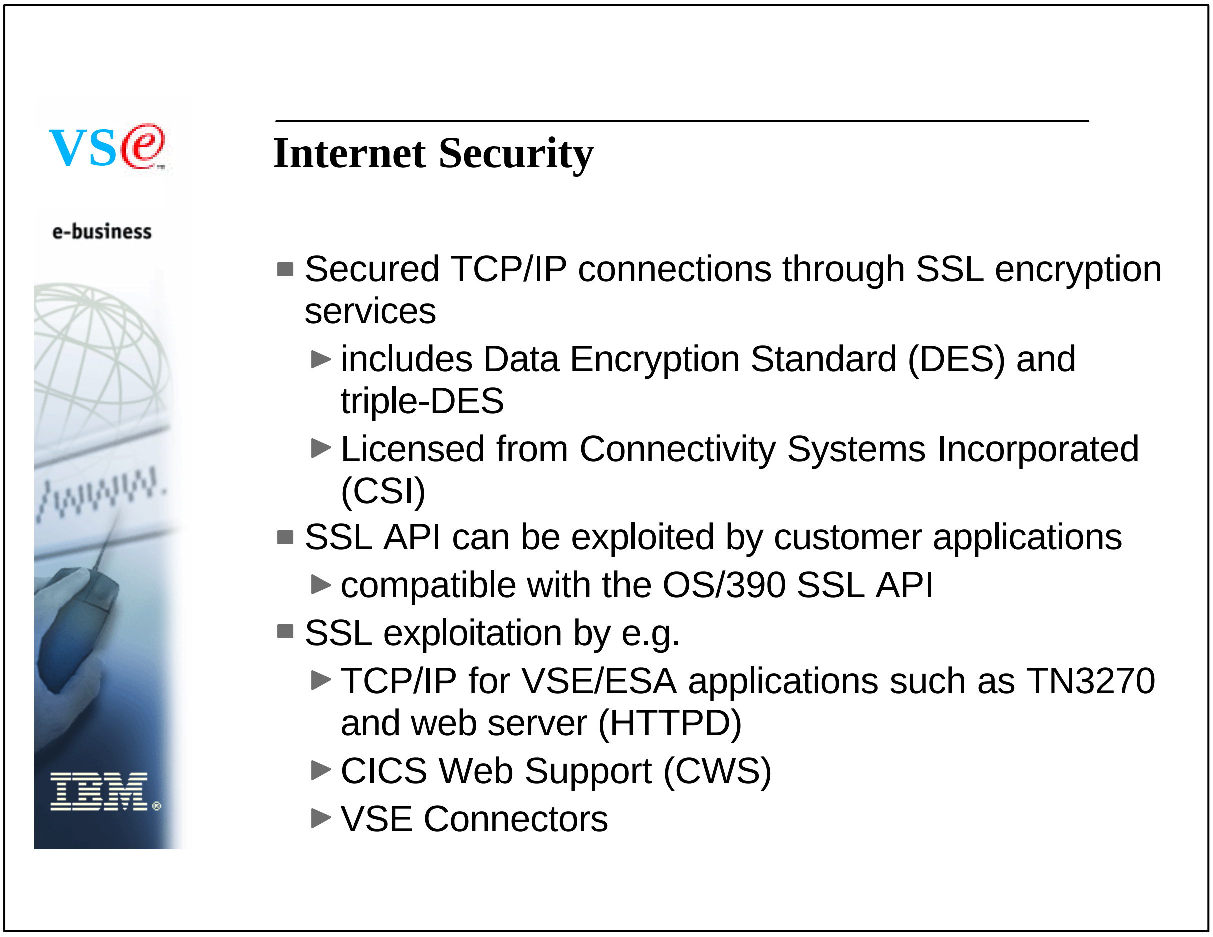
- Rejects hacker attacks
  - by filtering known URL prefixes
- HTTPHACK.L:

```
* Example:
*
* "SCRIPTS/" will cover...
*       GET /SCRIPTS/ROOT.EXE?C+D
*       GET /SCRIPTS/ROOT.EXE?CAT+PASSWD
*       etc...
* =======================================================
SCRIPTS/
MSADC/
_VTI_BIN/
_MEM_BIN/
C/WINNT/SYSTEM32/CMD.EXE
D/WINNT/SYSTEM32/CMD.EXE
CGI-BIN/
```



TCP/IP Security - Secure Socket Layer

- Secure Socket Layer (SSL)
  - Data encryption
  - Data verification
  - NOT: Security in terms of signon or access security
- BUT:
  - Client Authentication can be used do user signon
    - Certificate used as "passphrase"
    - instead of userid and password
    - in addition to userid and password



Internet Security

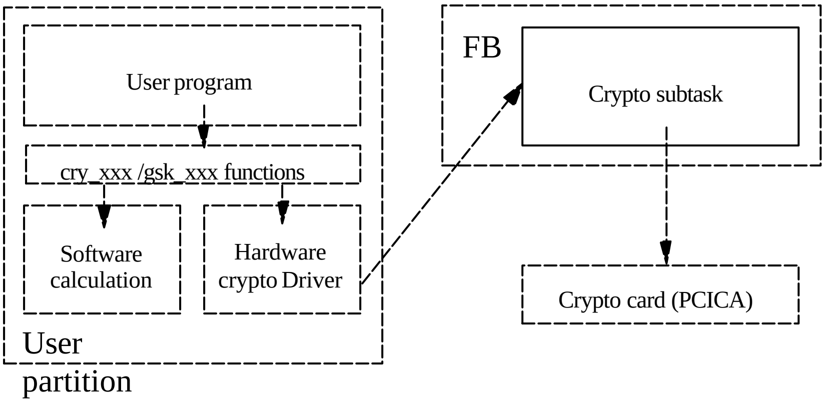
- Secured TCP/IP connections through SSL encryption services
  - includes Data Encryption Standard (DES) and triple-DES
  - Licensed from Connectivity Systems Incorporated (CSI)
- SSL API can be exploited by customer applications
  - compatible with the OS/390 SSL API
- SSL exploitation by e.g.
  - TCP/IP for VSE/ESA applications such as TN3270 and web server (HTTPD)
  - CICS Web Support (CWS)
  - VSE Connectors

Hardware Crypto Overview

- Requires VSE/ESA 2.7 and TCP/IP for VSE/ESA 1.5
- Supported crypto cards
  - PCI Cryptographic Accelerator (PCICA)
    - Feature code 0862
    - Available for zSeries (z800, z900)
- The crypty card is plugged into the Adjunct Processor
- Currently only RSA (asymmetric) is supported
  - Of benefit for Session initiation (SSL-Handshake)
- Also supported with
  - z/VM 4.2 + APAR VM62905
  - z/VM 4.3

Hardware Crypto Overview - continued

- New crypto subtask in Security Server (SECSERV) running in FB
  - Or as separate job if no SECSERV is running
  - Crypto card is polled by crypto task



VS@

e-business

Security Checklist

- SYS SEC=YES/NO
  - YES if batch security is required
- CICS SIT SEC=YES (!)
  - If NO, all users can logon without a password
- TCP/IP Security
  - SET SECURITY=ON
  - Use Security Exit
- Change passwords for predefined users
  - POST, PROG, OPER, SYSA, ...

VS@

e-business

Questions

?